1. Startpagina . . . 7
1.1 Algemeen . . . 9
1.1.1 Algemene introductie . . . 10
1.1.1.1 Afnemers . . . 11
1.1.1.1.1 Aansluiten als dienstverlener . . . 12
1.1.1.1.2 Meedoen als dienstafnemer . . . 13
1.1.1.1.3 Aansluiten als dienstbemiddelaar . . . 14
1.1.1.2 Deelnemers en diensten . . . 15
1.1.1.2.1 Verantwoordelijkheden Authenticatiedienst . . . 16
1.1.1.2.2 Verantwoordelijkheden Herkenningsmakelaar . . . 17
1.1.1.2.3 Verantwoordelijkheden Machtigingenregister . . . 18
1.1.1.2.4 Verantwoordelijkheden Middelenuitgever . . . 20
1.1.1.2.5 Verantwoordelijkheden eIDAS-berichtenservice . . . 21
1.1.1.3 Historie en status . . . 22
1.1.1.3.1 Versie 1.1 . . . 23
1.1.1.3.2 Versie 1.2 . . . 24
1.1.1.3.3 Versie 1.3 . . . 25
1.1.1.3.4 Versie 1.4 . . . 26
1.1.1.3.5 Versie 1.5 . . . 27
1.1.1.3.6 Versie 1.6 . . . 28
1.1.1.3.7 Versie 1.7 . . . 29
1.1.1.3.8 Versie 1.8 . . . 30
1.1.1.3.9 Versie 1.9 . . . 31
1.1.1.3.10 Versie 1.10 . . . 32
1.1.1.3.11 Versie 1.11 . . . 33
1.1.1.4 Marktwerking . . . 34
1.1.2 Begrippenlijst . . . 35
1.1.2.1 Afgeschermde kopie WID . . . 36
1.1.2.2 Afsprakenstelsel (AS) . . . 37
1.1.2.3 Akte . . . 38
1.1.2.4 Associatieverklaring . . . 39
1.1.2.5 Attribuutcatalogus (AC) . . . 40
1.1.2.6 Authenticatie (authenticeren) . . . 41
1.1.2.7 Authenticatiedienst (AD) . . . 42
1.1.2.8 Authenticatiemiddel . . . 43
1.1.2.9 Authenticatieverklaring . . . 44
1.1.2.10 Autorisatie . . . 45
1.1.2.11 Autorisatielijst BSN . . . 46
1.1.2.12 AVG . . . 47
1.1.2.13 Backend . . . 48
1.1.2.14 Bedrijf . . . 49
1.1.2.15 Beheerorganisatie (BO) . . . 50
1.1.2.16 Betrouwbaarheidsniveau . . . 51
1.1.2.17 Beveiligingsincident . . . 52
1.1.2.18 Bevoegdheid . . . 53
1.1.2.19 BSN . . . 54
1.1.2.20 BSN-domein . . . 55
1.1.2.21 BSNk . . . 56
1.1.2.22 BSN koppelregister . . . 57
1.1.2.23 Certificatie (certificeren) . . . 58
1.1.2.24 Commissie van Deskundigen (CvD) . . . 59
1.1.2.25 Controle van bevoegdheid . . . 60
1.1.2.26 Dataminimalisatie . . . 61
1.1.2.27 Deelnemer . . . 62
1.1.2.28 Dienst . . . 63
1.1.2.29 Dienstaanbieder (DA) . . . 64
1.1.2.30 Dienstafnemer . . . 65
1.1.2.31 Dienstbemiddelaar (DB) . . . 66
1.1.2.32 Dienstbemiddeling . . . 67
1.1.2.33 Dienstencatalogus (DC) . . . 68
1.1.2.34 Dienstverlener (DV) . . . 69
1.1.2.35 eIDAS-berichtenservice (EB) . . . 70
1.1.2.36 eIDAS-koppelpunt . . . 71
1.1.2.37 eIDAS-verordening . . . 72
1.1.2.38 Eigenaar . . . 73
1.1.2.39 Erkende aanbieder eHerkenning . . . 74
1.1.2.40 Europese Economische Ruimte (EER) . . . 75
1.1.2.41 Extern verkoopkanaal . . . 76
1.1.2.42 Gebruiker . . . 77
1.1.2.43 Geïnformeerde uitdrukkelijke toestemming . . . 78
1.1.2.44 Gemachtigde . . . 79
1.1.2.45 Gevalideerd attribuut . . . 80
1.1.2.46 Geverifieerd attribuut . . . 81
1.1.2.47 Handelsregister . . . 82
1.1.2.48 Hergebruik . . . 83
1.1.2.49 Herkenning . . . 84
1.1.2.50 Herkenningsdiensten . . . 85
1.1.2.51 Herkenningsmakelaar (HM) . . . 86
1.1.2.52 HSM . . . 87

1.1.2.53 Identificatie (identificeren) . . . 88
1.1.2.54 Identificerend kenmerk . . . 89
1.1.2.55 Identificerend nummer . . . 90
1.1.2.56 Identifier Set . . . 91
1.1.2.57 Identiteit . . . 92
1.1.2.58 Identity provider (IdP) . . . 93
1.1.2.59 Intermediaire partij . . . 94
1.1.2.60 Intern pseudoniem . . . 95
1.1.2.61 Inzageregister (IR) . . . 96
1.1.2.62 Inzetgebied . . . 97
1.1.2.63 Ketenmachtiging . . . 98
1.1.2.64 Ketenverklaring . . . 99
1.1.2.65 Koppelvlak . . . 100
1.1.2.66 Leveranciersoverleg (gremium) . . . 101
1.1.2.67 Machtiging (machtigen) . . . 102
1.1.2.68 Machtigingenbeheerder . . . 103
1.1.2.69 Machtigingenregister (MR) . . . 104
1.1.2.70 Machtiging-verklaring . . . 105
1.1.2.71 Middelenuitgever (MU) . . . 106
1.1.2.72 Native app . . . 107
1.1.2.73 Natuurlijk persoon . . . 108
1.1.2.74 Netwerk (voor Elektronische Toegangsdiensten) . . . 109
1.1.2.75 Niet natuurlijk persoon . . . 110
1.1.2.76 Onderneming . . . 111
1.1.2.77 Ontvangende Partij . . . 112
1.1.2.78 Optioneel te verstrekken attribuut . . . 113
1.1.2.79 Optionele functionaliteit . . . 114
1.1.2.80 Overeenkomst . . . 115
1.1.2.81 Overheidsdienstverlener . . . 116
1.1.2.82 Partij . . . 117
1.1.2.83 Persistent Pseudoniem . . . 118
1.1.2.84 Polymorfe Identiteit . . . 119
1.1.2.85 Polymorfe pseudonimisering . . . 120
1.1.2.86 Polymorf Pseudoniem . . . 121
1.1.2.87 Privépersoon . . . 122
1.1.2.88 Pseudoniem . . . 123
1.1.2.89 Public Key Infrastructure (PKI) . . . 124
1.1.2.90 Publieke domein . . . 125
1.1.2.91 Randomisatie . . . 126
1.1.2.92 Rechtspersoon . . . 127
1.1.2.93 Rol . . . 128
1.1.2.94 Secretariaat van de Commissie van Deskundigen . . . 129
1.1.2.95 Service provider (SP) . . . 130
1.1.2.96 Single Sign On (SSO) . . . 131
1.1.2.97 Sleutelmateriaal . . . 132
1.1.2.98 Sleutelverstrekkingslijst . . . 133
1.1.2.99 Specifiek pseudoniem . . . 134
1.1.2.100 Stamgegeven . . . 135
1.1.2.101 Status tbv InzageRegister . . . 136
1.1.2.102 Strategisch Beraad (gremium) . . . 137
1.1.2.103 Tactisch Beraad (gremium) . . . 138
1.1.2.104 Toegang verlenen . . . 139
1.1.2.105 Toezichthouder . . . 140
1.1.2.106 Transactiebericht . . . 141
1.1.2.107 User consent . . . 142
1.1.2.108 Verklarende Partij . . . 143
1.1.2.109 Verklaring . . . 144
1.1.2.110 Verplicht te verstrekken attribuut . . . 145
1.1.2.111 Versleutelde Identiteit . . . 146
1.1.2.112 Versleuteld Pseudoniem . . . 147
1.1.2.113 Vertegenwoordigde . . . 148
1.1.2.114 Vertegenwoordigde dienstafnemer . . . 149
1.1.2.115 Vertegenwoordiger . . . 150
1.1.2.116 Vertegenwoordiging (vertegenwoordigen) . . . 151
1.1.2.117 Vestiging . . . 152
1.1.2.118 Wettelijke vertegenwoordiging . . . 153
1.1.2.119 Wettelijk identificatie document (WID) . . . 154
1.1.2.120 Zelfstandige Zonder Personeel (ZZP) . . . 155
1.1.2.121 Zelfverklaard attribuut . . . 156
1.2 Juridica . . . 157
1.2.1 Juridisch kader . . . 158
1.2.1.1 Organen en taakverdeling . . . 159
1.2.1.1.1 Strategisch Beraad . . . 161
1.2.1.1.2 Tactisch Beraad . . . 162
1.2.1.1.3 Operationeel Beraad . . . 163
1.2.1.1.4 Leveranciersoverleg . . . 164
1.2.1.1.5 Bekostiging . . . 165
1.2.1.2 Inrichting toezicht . . . 166
1.2.1.2.1 Beëindiging van de Deelnemersovereenkomst . . . 168

1.2.1.2.2 Indirect toezicht op de Dienstverlener . . . 169
1.2.1.3 Toetredingseisen . . . 170
1.2.1.4 Juridische structuur . . . 171
1.2.1.5 Aanvullende verplichtingen . . . 172
1.2.1.6 Vertegenwoordiging, volmacht en machtiging . . . 173
1.2.1.6.1 Privaatrechtelijke vertegenwoordiging . . . 174
1.2.1.6.2 Publiekrechtelijke vertegenwoordiging . . . 175
1.2.1.6.3 Ketenmachtiging (recht op substitutie) . . . 176
1.2.1.7 Aansprakelijkheid . . . 177
1.2.1.8 Betrouwbaarheidsniveaus . . . 178
1.2.1.9 Samenwerking met externe verkoopkanalen . . . 179
1.2.2 Gebruiksvoorwaarden Elektronische Toegangsdiensten . . . 180
1.2.2.1 Artikel 1. Definities . . . 181
1.2.2.2 Artikel 2. Toepassingsgebied . . . 183
1.2.2.3 Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname . . . 184
1.2.2.4 Artikel 4. Beperking van aansprakelijkheid . . . 185
1.2.2.5 Artikel 5. Geheimhouding . . . 186
1.2.2.6 Artikel 6. Achterhalen netwerkfalen . . . 187
1.2.2.7 Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst . . . 188
1.2.2.8 Artikel 8. Toepasselijk recht . . . 189
1.2.2.9 Verplichtingen voor de Dienstafnemer . . . 190
1.2.2.9.1 Artikel 10. Dienstafnemer . . . 191
1.2.2.9.2 Artikel 11. Beveiligingsverplichting van de Dienstafnemer . . . 192
1.2.2.9.3 Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen . . . 193
1.2.2.9.4 Artikel 13. Vervulling rol(len) door de Dienstafnemer . . . 194
1.2.2.10 Verplichtingen van de Dienstverlener . . . 195
1.2.2.10.1 Artikel 14. Vaststellen openstellingsbesluit . . . 196
1.2.2.10.2 Artikel 15. Melding onregelmatigheden . . . 197
1.2.2.10.3 Artikel 16. Beveiliging dienstverlener . . . 198
1.2.2.10.4 Artikel 17. SSO . . . 199
1.2.2.11 Artikel 18. Beveiliging . . . 200
1.2.2.12 Artikel 19. Betrouwbaarheidsniveaus . . . 201
1.2.2.13 Artikel 20. Informatieverplichting . . . 202
1.2.2.14 Artikel 21. Privacy . . . 203
1.2.2.15 Artikel 22. Cookies . . . 204
1.2.2.16 Artikel 23. Toezicht . . . 205
1.3 Organisatie . . . 206
1.3.1 Operationeel handboek . . . 207
1.3.1.1 Helpdesk . . . 208
1.3.1.2 Proces aanvragen BSNk-sleutelmateriaal . . . 209
1.3.1.3 Proces attribuutcatalogus . . . 210
1.3.1.4 Proces beheren simulator . . . 212
1.3.1.5 Proces beheren testnetwerk . . . 213
1.3.1.6 Proces certificaatwissel . . . 214
1.3.1.7 Proces change en release . . . 216
1.3.1.7.1 Proces realisatie koppelvlak wijzigingen . . . 221
1.3.1.8 Proces contentmanagement . . . 224
1.3.1.9 Proces distributie en publicatie van documenten . . . 226
1.3.1.10 Proces doorvoeren nieuwe dienstencatalogus . . . 227
1.3.1.11 Proces implementatie koppelvlakrelease . . . 230
1.3.1.12 Proces incidentmanagement . . . 234
1.3.1.13 Proces informeren Toezichthouder . . . 239
1.3.1.14 Proces instandhouding en naleven . . . 243
1.3.1.15 Proces managementrapportage . . . 247
1.3.1.15.1 Rapportage Belastingdienstmiddelen . . . 252
1.3.1.15.2 Rapportage Ketenmachtigingen . . . 253
1.3.1.16 Proces meldingenbeheer . . . 254
1.3.1.17 Proces migratie sleutelmateriaal voor polymorfe pseudonimisering . . . 256
1.3.1.18 Proces netwerkmetadata . . . 258
1.3.1.19 Proces onderhoud cookieserver . . . 262
1.3.1.20 Proces toetreden . . . 263
1.3.1.21 Proces uittreden . . . 270
1.3.1.21.1 Handreiking exitplan . . . 277
1.3.1.22 Proces uitvoeren centrale penetratietest . . . 279
1.3.1.23 Proces wijziging rechtspersoon . . . 283
1.3.2 Businessmodel . . . 284
1.3.3 Service level . . . 285
1.3.3.1 Beschikbaarheid . . . 286
1.3.3.1.1 Beschikbaarheidsvenster . . . 287
1.3.3.1.2 Onderhoudsvenster . . . 288
1.3.3.1.3 Servicevenster . . . 292
1.3.3.1.4 Openstellingsvenster . . . 293
1.3.3.1.5 Rekenmethode . . . 294
1.3.3.2 Performance . . . 297
1.3.3.3 Contentmanagement . . . 298
1.3.3.4 Incidenten . . . 299
1.3.3.5 Managementrapportage . . . 300
1.3.3.6 Monitoring . . . 301
1.3.3.7 Ondersteuning . . . 302

1.3.3.8 Responsetijden . . . 303
1.3.4 Communicatie . . . 304
1.3.4.1 Eisen communicatie bij samenwerking met externe verkoopkanalen . . . 305
1.3.4.2 Richtlijnen naam- en merkgebruik eHerkenning . . . 306
1.3.4.3 Richtlijnen communicatie eHerkenning . . . 307
1.3.4.4 Huisstijlhandboek eHerkenning . . . 308
1.3.4.5 Huisstijlhandboek eIDAS . . . 309
1.3.4.6 Richtlijnen communicatie eIDAS . . . 310
1.4 Techniek en functionaliteit . . . 311
1.4.1 Use cases . . . 312
1.4.1.1 Use cases voor Gebruik . . . 313
1.4.1.1.1 GUC1 Gebruiken eToegang als dienstafnemer . . . 315
1.4.1.1.2 GUC2 Gebruiken eToegang als vertegenwoordiger . . . 317
1.4.1.1.3 GUC3 Aantonen identiteit . . . 319
1.4.1.1.4 GUC4 Aantonen bevoegdheid . . . 324
1.4.1.1.5 Use case overschrijdende alternatieve scenario's . . . 335
1.4.1.1.6 Use cases Single Sign-On . . . 342
1.4.1.2 Use cases voor Administratie . . . 345
1.4.1.2.1 AUC1 Aansluiten dienst . . . 346
1.4.1.2.2 AUC2 Verkrijgen authenticatiemiddel . . . 347
1.4.1.2.3 AUC3 Registreren bevoegdheid . . . 348
1.4.1.2.4 AUC4 Registreren attribuut . . . 351
1.4.1.2.5 AUC6 Activeren BSN . . . 352
1.4.1.2.6 AUC7 Proces verlenen toestemming dienstbemiddeling . . . 354
1.4.1.2.7 AUC8 Verkrijgen lijst Authenticatiediensten . . . 355
1.4.1.2.8 AUC9 Verstrekken sleutelmateriaal Dienstverleners . . . 356
1.4.1.2.9 AUC10 Transformeren . . . 357
1.4.1.2.10 AUC11 . . . 360
1.4.2 Gebruikersinterface . . . 361
1.4.2.1 Dialoogbeschrijving . . . 362
1.4.2.1.1 Dialoogbeschrijving Authenticatiedienst . . . 363
1.4.2.1.2 Dialoogbeschrijving Herkenningsmakelaars . . . 364
1.4.2.2 Toegankelijkheid . . . 365
1.4.3 Interface specifications . . . 366
1.4.3.1 Interface specifications web . . . 367
1.4.3.1.1 Interface specifications HM-EB . . . 369
1.4.3.1.2 Interface specifications HM-MR . . . 371
1.4.3.1.3 Interface specifications HM-AD . . . 379
1.4.3.1.4 Interface specifications DB-DA . . . 393
1.4.3.1.5 Interface specifications DV-HM . . . 397
1.4.3.2 Interface specifications DV-HM RequestADlist . . . 414
1.4.3.3 Interface specifications AD-BSNk . . . 416
1.4.3.4 Interface specifications MR-BSNk . . . 417
1.4.3.5 Information security requirements . . . 418
1.4.3.5.1 Digital signature . . . 419
1.4.3.5.2 DNSSEC . . . 420
1.4.3.5.3 Encryption . . . 421
1.4.3.5.4 End-to-end encryption . . . 425
1.4.3.5.5 PKIoverheid . . . 428
1.4.3.5.6 Secure connection . . . 429
1.4.3.5.7 Secure cookies . . . 430
1.4.3.5.8 Synchronize system clocks . . . 431
1.4.3.6 Interface Specifications Auxillary Systems . . . 432
1.4.3.6.1 Interface specifications aux HM-BSNk - ProvideDVkeys . . . 433
1.4.3.6.2 Interface Specifications aux MR - BSNk . . . 435
1.4.3.7 Alternative interfaces . . . 456
1.4.3.8 Attribute elements . . . 457
1.4.3.8.1 Generic attribute elements . . . 458
1.4.3.8.2 SAML attribute elements . . . 471
1.4.3.8.3 XACML attribute elements . . . 481
1.4.3.9 Bindings . . . 495
1.4.3.10 Error handling . . . 497
1.4.3.11 Single sign-on and user sessions . . . 499
1.4.3.12 SubjectConfirmation . . . 500
1.4.3.13 Web services . . . 501
1.4.3.14 Linking of Assertions . . . 502
1.4.3.15 Polymorphic Pseudonymization Notation . . . 504
1.4.3.16 Interface specifications and the interpretation of LOAs . . . 510
1.4.3.17 Interface specifications HM-MR chain authorization . . . 511
1.4.3.18 Discovery Interface MR-MR chain authorisations . . . 515
1.4.3.18.1 MR-MR webservice Security . . . 521
1.4.4 Attribuutverstrekking . . . 523
1.4.4.1 Identificerende kenmerken . . . 524
1.4.4.1.1 EntityConcernedID:eIDASLegalIdentifier . . . 525
1.4.4.1.2 EntityConcernedID:KvKnr . . . 526
1.4.4.1.3 EntityConcernedID:PROBASnr . . . 527
1.4.4.1.4 EntityConcernedID:Pseudo . . . 528
1.4.4.1.5 EntityConcernedID:RSIN . . . 529
1.4.4.1.6 ServiceRestriction:SubdossierNr . . . 530

1.4.4.1.7 ServiceRestriction:Vestigingsnr . . . 531
1.4.4.1.8 urn:etoegang:1.12:EntityConcernedID:BSN . . . 532
1.4.4.1.9 urn:etoegang:1.12:EntityConcernedID:PseudoID . . . 533
1.4.4.1.10 urn:etoegang:1.13:EntityConcernedID:Pseudo . . . 534
1.4.4.2 Attribuutcatalogus . . . 535
1.4.4.2.1 Attribuutcatalogus generiek . . . 538
1.4.4.2.2 Attribuutcatalogus natuurlijke personen . . . 540
1.4.4.2.3 Attributencatalogus niet-natuurlijke personen . . . 541
1.4.4.3 Handreiking Polymorphic Pseudonimization Notation . . . 542
1.4.5 SAML metadata . . . 548
1.4.5.1 DV metadata for HM . . . 549
1.4.5.2 HM metadata for DV . . . 552
1.4.5.3 Metadata for participants . . . 554
1.4.5.4 Network metadata . . . 561
1.4.5.5 Authorization List BSN format . . . 562
1.4.5.6 Key provisioning list format . . . 563
1.4.6 Service catalog . . . 564
1.4.7 Testing . . . 578
1.4.7.1 Requirements for testing . . . 579
1.4.7.1.1 Acquire test means . . . 580
1.4.7.1.2 Announce chain test . . . 581
1.4.7.1.3 Exchange metadata . . . 582
1.4.7.1.4 Process service catalog . . . 583
1.4.7.2 Network monitoring . . . 584
1.5 Informatiebeveiliging en privacy . . . 585
1.5.1 Beleid voor informatiebeveiliging . . . 586
1.5.1.1 Organisatie van verantwoordelijkheid voor informatiebeveiliging . . . 587
1.5.1.2 Generieke beleidsuitgangspunten voor informatiebeveiliging . . . 588
1.5.1.2.1 Afweging van beveiligingsrisico's van het Stelsel . . . 589
1.5.1.2.2 Stelselnormenkader voor informatiebeveiliging . . . 590
1.5.1.2.3 Naleving en Toezicht . . . 591
1.5.1.3 Specifieke beleidsuitgangspunten voor informatiebeveiliging . . . 592
1.5.1.3.1 Afspraken Stelselrisicoanalyse en Gemeenschappelijk Normenkader . . . 593
1.5.1.3.2 Afspraken implementatie Gemeenschappelijk normenkader informatiebeveiliging, certificatie en assurance . . . 594
1.5.1.3.3 Afspraken Gemeenschappelijke Classificatie van Stelselinformatie . . . 595
1.5.1.3.4 Afspraken archivering, logging en opvraging . . . 597
1.5.1.3.5 Afspraken voor de integriteit van medewerkers . . . 598
1.5.1.3.6 Beleid voor penetratietesten . . . 599
1.5.2 Privacybeleid . . . 600
1.5.2.1 Beleidsuitgangspunten voor de naleving van de AVG . . . 601
1.5.2.2 Verantwoordelijkheden partijen afsprakenstelsel elektronische toegangsdiensten . . . 602
1.5.2.3 Invulling voorwaarden voor rechtmatige verwerking . . . 603
1.5.2.3.1 Afbakening set van persoonsgegevens en doel van de verwerking . . . 604
1.5.2.3.2 Transparantie . . . 611
1.5.2.3.3 Zorgvuldigheid . . . 612
1.5.2.3.4 Doelbinding . . . 613
1.5.2.4 Controle op de naleving en privacy managementcyclus . . . 614
1.5.3 Gemeenschappelijk normenkader informatiebeveiliging . . . 615
1.5.4 Normenkader betrouwbaarheidsniveaus . . . 629
1.5.4.1 Technische specificaties en procedures voor uitgifte van authenticatiemiddelen . . . 630
1.5.4.1.1 Eisen Identificatie op Afstand . . . 662
1.5.4.2 Specificaties voor het beheer van bevoegdheden . . . 683
1.5.4.3 Eisen voor geldigheid van verklaringen voor Dienstverleners . . . 688
1.5.5 Attributenbeleid . . . 691
1.6 Templates en formulieren . . . 692
1.6.1 Template deelnemersovereenkomst . . . 693
1.6.2 Template verzoek tot (uitbreiding) toetreding . . . 696
1.6.3 Template wijziging rechtspersoon deelnemer . . . 698
1.6.4 Template zelfverklaring Dienstverlener . . . 700
2. snippets . . . 702
2.1 Afsprakenstelsel Elektronische Toegangsdiensten . . . 703
2.2 Elektronische Toegangsdiensten . . . 704
2.3 footer . . . 705
2.4 header . . . 707
2.5 Herkenningsmakelaar . . . 708
2.6 Netwerk . . . 709
2.7 snippet.ad.mr.participants . . . 710
2.8 snippet.antwoord . . . 711
2.9 snippet.beperking.dienstbemiddeling . . . 712
2.10 snippet.betrouwbaarheidsniveaus . . . 713
2.11 snippet.bewaartermijnen . . . 714
2.12 snippet.branding . . . 715
2.13 snippet.bsnk_specs . . . 716
2.14 snippet.bzk . . . 717
2.15 snippet.calamiteit . . . 718
2.16 snippet.checklist . . . 719
2.17 snippet.checklist.ad . . . 720
2.18 snippet.checklist.hm . . . 721
2.19 snippet.checklist.mr . . . 722

2.20 snippet.colofon . . . 724
2.21 snippet.colofon.gebruikersvoorwaarden . . . 725
2.22 snippet.determine.appropriate.identifiers . . . 726
2.23 snippet.diensten . . . 727
2.24 snippet.doelomschrijving . . . 728
2.25 snippet.duur.publicatie . . . 729
2.26 snippet.ecta . . . 730
2.27 snippet.email.bo . . . 731
2.28 snippet.gebruikservaring.attributen . . . 732
2.29 snippet.handreikingloa . . . 733
2.30 snippet.hm.participants . . . 734
2.31 snippet.implementatietermijn.RFC2040.1 . . . 735
2.32 snippet.implementatietermijn.RFC2040.2 . . . 736
2.33 snippet.instellingsbesluit . . . 737
2.34 snippet.Interface specification HM-MR response . . . 738
2.35 snippet.Interface specifications DV-HM response . . . 742
2.36 snippet.interface specifications HM-AD . . . 754
2.37 snippet.issues . . . 766
2.38 snippet.loa-rule.ad . . . 767
2.39 snippet.loa-rule.hm . . . 768
2.40 snippet.loa-rule.mr . . . 769
2.41 snippet.ondergetekende . . . 770
2.42 snippet.ondertekening . . . 771
2.43 snippet.optionele.functionaliteit . . . 772
2.44 snippet.primaire.componenten . . . 773
2.45 snippet.saas . . . 774
2.46 snippet.samlbindingspdf . . . 775
2.47 snippet.secundaire.componenten . . . 776
2.48 snippet.servicerestriction . . . 777
2.49 snippet.startingpoint.happy . . . 778
2.50 snippet.testen.betrouwbaarheidniveaus . . . 779
2.51 snippet.tls . . . 780
2.52 snippet.uitfaseren.eh1 . . . 781
2.53 snippet.url.ac . . . 782
2.54 snippet.url.ac.prod . . . 783
2.55 snippet.url.ac.test . . . 784
2.56 snippet.url.dc.prod . . . 785
2.57 snippet.url.dc.test . . . 786
2.58 snippet.url.managementrapportage . . . 787
2.59 snippet.url.metadata.prod . . . 788
2.60 snippet.url.metadata.test . . . 789
2.61 snippet.url.simulator . . . 790
2.62 snippet.url.sso . . . 791
2.63 snippet.url.website . . . 792
2.64 snippet.urnprefix . . . 793
2.65 snippet.wachtwoord . . . 794
2.66 snippet.wiki . . . 795

Startpagina

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Omwille van de leesbaarheid van de tekst is overal ‘hij’ geschreven waar ‘hij of zij’ bedoeld wordt.

De woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten (“MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergeven. De betekenis van deze woorden is:

- MOET: een absolute vereiste
- MAG NIET: een absoluut verbod
- ZOU MOETEN: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- ZOU NIET MOETEN: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAG: een vrije keuze, een optie

Op deze pagina vindt u de meest actuele versie van het Afsprakenstelsel Elektronische Toegangsdiensten. Het afsprakenstelsel is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan eHerkenning wordt geleverd. De afspraken hebben als doel om samenwerking en zekerheid in het Netwerk te garanderen. Tegelijkertijd bieden de afspraken ook voldoende vrijheid aan de deelnemers om competitieve proposities te leveren aan hun klanten. Het afsprakenstelsel wordt inhoudelijk compleet beschreven in onderstaande documenten:

Algemeen

Hier vindt u de algemene introductie op het Afsprakenstelsel Elektronische Toegangsdiensten. Dit document beschrijft de werking van Elektronische Toegangsdiensten en geeft tevens een overzicht van de andere onderdelen van het afsprakenstelsel.

- Algemene introductie — In dit hoofdstuk vindt u de algemene introductie op het Afsprakenstelsel Elektronische Toegangsdiensten. Dit deel geeft een overzicht van het afsprakenstelsel, de diensten, rollen en gebruikers. De teksten gelden voor eHerkenning en Idensys. Waar nodig wordt voor één merk een verbijzondering gemaakt.
- Begrippenlijst — Binnen Elektronische Toegangsdiensten wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden.

Juridica

Hier vindt u de juridische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: het juridisch kader en de gebruiksvoorwaarden. Deze documenten bevatten informatie over de besturing van Elektronische Toegangsdiensten, de naleving van het afsprakenstelsel, de overeenkomst tussen de beheerorganisatie en de aanbieders en de minimale gebruiksvoorwaarden waaronder de dienstverleners en ondernemers Elektronische Toegangsdiensten mogen gebruiken.

- Juridisch kader — Beschrijft het juridisch kader, het besturingsmodel en de controle op en monitoring van de naleving van het afsprakenstelsel.
- Gebruiksvoorwaarden Elektronische Toegangsdiensten — Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van Elektronische Toegangsdiensten.

Organisatie

Hier vindt u de organisatorische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: het operationele handboek, de service level, het businessmodel en het handboek huisstijl. Deze documenten bevatten informatie over de stelselbrede beheerprocessen, de algemene service level die Elektronische Toegangsdiensten hanteert en het gebruik van het beeldmerk van eHerkenning bij externe communicatie.

- Operationeel handboek — Dit document beschrijft de operationele beheerprocessen voor het Netwerk. Deze processen hebben als doel om het merk Elektronische Toegangsdiensten te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.
- Businessmodel — Dit document beschrijft het businessmodel voor Elektronische Toegangsdiensten. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het Netwerk (voor Elektronische Toegangsdiensten) invullen. Het is bedoeld voor deelnemers en dienstverleners.
- Service level — Dit document beschrijft de Service Level afspraken die gelden voor deelnemers en de beheerorganisatie van Elektronische Toegangsdiensten. Het betreft een beschrijving van het minimale Service Level dat de deelnemers moeten leveren aan elkaar en hun dienstafnemers en het minimale Service Level dat de beheerorganisatie levert aan de deelnemers.
- Communicatie — Dit document beschrijft de richtlijnen voor naam en merkgebruik, huisstijl afspraken en communicatierichtlijnen voor de merken eHerkenning en eIDAS. Het is bedoeld voor alle betrokken partijen: deelnemers en dienstverleners. De beheerorganisatie levert richtlijnen, standaard tekst- en beeldmateriaal en andere tools die de deelnemers en dienstverleners dienen te gebruiken.

Techniek en functionaliteit

Hier vindt u de technische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: de koppelvlakspecificaties, de use cases en testen voor deelnemers. Deze documenten bevatten informatie over welke standaarden worden gehanteerd, de functionaliteit, de berichten en koppelvlakken die Elektronische Toegangsdiensten ondersteunt en de testen die worden uitgevoerd.

- Use cases — Beschrijft de functionaliteit van Elektronische Toegangsdiensten in detail.
- Gebruikersinterface — Dit hoofdstuk beschrijft eisen die worden gesteld aan de gebruikersinterface met de gebruiker.
- Interface specifications
- Attribuutverstrekking — Een AD, MR of EB kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in de Attribuutcatalogus beschreven worden.
- SAML metadata — This chapter describes the metadata the participants must supply, how the Beheerorganisatie publishes the aggregated metadata, and how it is to be interpreted by the participants.
- Service catalog — This chapter describes the format and publication of the Dienstencatalogus (DC) (service catalog).
- Testing — This document describes the tests that (aspiring) participants should perform.

Informatiebeveiliging en privacy

Dit hoofdstuk bevat de normenkaders en het beleid aangaande borging van veiligheid, privacy en continuïteit van Elektronische Toegangsdiensten.

- Beleid voor informatiebeveiliging — Dit document bevat het beleid voor informatiebeveiliging dat onderdeel is van het Afsprakenstelsel Elektronische Toegangsdiensten.
- Privacybeleid — Om Herkenningsdiensten te kunnen leveren worden persoonsgegevens verwerkt. De verwerking van persoonsgegevens is alleen rechtmatig als wordt voldaan aan de voorwaarden die de Algemene verordening gegevensbescherming (AVG) of andere toepasselijke specifieke privacy wet- en regelgeving hieraan stelt.
- Gemeenschappelijk normenkader informatiebeveiliging — ISO 27001:2013 beheersdoelstellingen en beheersmaatregelen binnen de scope van eToegangsdiensten, - activiteiten, -objecten en -informatie
- Normenkader betrouwbaarheidsniveaus — Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast.
- Attributenbeleid

Templates en formulieren

- Template deelnemersovereenkomst — De overeenkomst tussen deelnemers en beheerorganisatie op basis waarvan deelnemers gehouden zijn het afsprakenstelsel toe te passen. Deze deelnemersovereenkomst verwijst naar het afsprakenstelsel maar is er (strikt genomen) zelf geen onderdeel van.
- Template verzoek tot (uitbreiding) toetreding
- Template wijziging rechtspersoon deelnemer
- Template zelfverklaring Dienstverlener

Algemeen

Hier vindt u de algemene introductie op het Afsprakenstelsel Elektronische Toegangsdiensten. Dit document beschrijft de werking van Elektronische Toegangsdiensten en geeft tevens een overzicht van de andere onderdelen van het afsprakenstelsel.Deze categorie bevat de volgende onderdelen:

- Algemene introductie — In dit hoofdstuk vindt u de algemene introductie op het Afsprakenstelsel Elektronische Toegangsdiensten. Dit deel geeft een overzicht van het afsprakenstelsel, de diensten, rollen en gebruikers. De teksten gelden voor eHerkenning en Idensys. Waar nodig wordt voor één merk een verbijzondering gemaakt.
- Begrippenlijst — Binnen Elektronische Toegangsdiensten wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden.

Toegankelijkheid

Loopt u tegen een toegankelijkheidsprobleem aan? Of heeft u een vraag of opmerking over toegankelijkheid? Neem dan contact op via info@eherkenning.nl.

Wat kunt u van ons verwachten?

- Binnen 5 werkdagen krijgt u een ontvangstbevestiging.
- We informeren u over de voortgang en de uitkomst.
- Binnen 3 weken is uw verzoek afgehandeld.

Handhavingsprocedure

Bent u niet tevreden met de manier waarop uw klacht is behandeld? Of hebben we niet op tijd gereageerd?
Dan kunt u contact opnemen via https://www.nationaleombudsman.nl/klacht-indienen/uw-klacht.

Algemene introductie

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Nederland digitaliseert. Mensen en organisaties kunnen via het internet steeds meer zaken digitaal regelen, bijvoorbeeld online aankopen doen, een bouwvergunning aanvragen of een belastingaangifte indienen. Bij de ontwikkeling van digitale dienstverlening moet iedere organisatie een aantal vraagstukken op het gebied van geautoriseerde toegang oplossen. Het Afsprakenstelsel Elektronische Toegangsdiensten biedt een uniforme set van standaarden, afspraken en voorzieningen voor de geautoriseerde toegang tot digitale diensten. Hiermee kunnen persoonsgebonden, vertrouwelijke gegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld worden. De afspraken gelden tussen de partijen die een erkende rol spelen bij het verlenen en gebruik van toegangsdiensten, beheer en doorontwikkeling, sturing en toezicht.

eHerkenning

Het Afsprakenstelsel Elektronische Toegangsdiensten regelt de afspraken en voorzieningen voor eHerkenning.

Deelnemers vormen een netwerk dat diensten levert

De kern van het afsprakenstelsel is het netwerk dat partijen – de zogenaamde deelnemers – samen vormen om toegangdiensten te leveren. In dat netwerk nemen partijen deel die authenticatiemiddelen uitgeven en bijbehorende diensten verlenen. Bestaande en toekomstige authenticatiemiddelen – zoals gebruikersnaam/wachtwoorden, card readers, VPN tokens, maar ook apps kunnen zo worden gebruikt. Ook nemen bij eHerkenning partijen deel die machtigingen van bedrijven en organisaties registreren en hierover informatie verstrekken. Bijvoorbeeld het feit dat firma F haar werkneemster mevrouw Pietersen machtigt om namens firma F belastingaangifte te doen. Via het netwerk worden partijen met hun authenticatiemiddelen en machtigingen gekoppeld aan dienstverleners die hun diensten elektronisch willen ontsluiten en bedrijven en andere organisaties die diensten van deze dienstverleners willen afnemen.

Het Afsprakenstelsel Elektronische Toegangsdiensten is de Nederlandse oplossing om te voldoen aan de eIDAS-verordening. Daarmee worden de diensten van de aangesloten (publieke) Dienstverleners via het stelsel ontsloten voor gebruikers uit andere eIDAS-lidstaten.

De basis van het netwerk ligt vast in afspraken

Om een dergelijk netwerk tot stand te brengen, te laten functioneren en evolueren, is een set van afspraken nodig: het Afsprakenstelsel Elektronische Toegangsdiensten. Deze afsprakenset is minimaal van opzet, genoeg om samenwerking en zekerheid in het netwerk te garanderen, en tegelijk zo ruim dat het voldoende vrijheid biedt om competitieve proposities van de deelnemers mogelijk te maken. Daartoe bevat het afsprakenstelsel bepalingen over de volgende onderwerpen:

- de rollen in het netwerk, de relaties tussen die rollen en de te leveren dienstverlening;
- de precieze werking van het netwerk: technische relaties, ondersteunde functionaliteit, kwaliteit van gegevens en dienstverlening;
- de onderliggende infrastructuur: welke standaarden worden gehanteerd, en welke berichten en koppelvlakken worden ondersteund;
- beheer en beveiliging, inclusief de organisatie daarvan. Dit deel omvat tevens afspraken over de handhaving van de gemaakte afspraken, wat van essentieel belang is om de werking van het netwerk en het vertrouwen in het netwerk conform het afsprakenstelsel te waarborgen.

Doel en doelgroep van dit hoofdstuk

Binnen de totale documentatieset van het afsprakenstelsel geeft dit hoofdstuk op hoofdlijnen inhoudelijk inzicht in gedrag en werking van het afsprakenstelsel.

De doelgroepen voor dit document zijn:

- beslisser: degene die beslist over aansluiting op eHerkenning als deelnemer (leverancier van toegangsdiensten in het netwerk) of in de rol van dienstverlener (organisatie die diensten levert aan gebruikers, mensen en organisaties;
- adviseur: degene die de beslisser inhoudelijk adviseert;
- implementator: degene die aansluiting op (een deel van) het afsprakenstelsel in de breedste zin wil implementeren (juridisch, technisch, organisatorisch, procesmatig, etc.) en/of dit wil managen, in de rol van deelnemer of dienstverlener.
- toezichthouder: degene die toeziet op de betrouwbare en veilige werking van het Afsprakenstelsel Elektronische Toegangsdiensten.

Voor beslisser en adviseur zou de inhoud toereikend moeten zijn. Voor de implementator bevat het al die zaken die voor een implementatie van belang zijn; voor vragen die specifiek zijn voor bijvoorbeeld technische aansluiting zijn ook andere delen van de documentatieset noodzakelijk. Voor een eerste oriëntatie voor bedrijven die eHerkenning willen gebruiken zijn communicatiemiddelen (https://www.eherkenning.nl/aansluiten-op-eherkenning/communicatie/) van eHerkenning te gebruiken.

Afnemers

De deelnemers aan het Afsprakenstelsel Elektronische Toegangsdiensten leveren eToegangsdiensten aan gebruikers. Deze diensten zorgen voor vertrouwen (op een bepaald betrouwbaarheidsniveau) aangaande identiteiten en bevoegdheden. Er bestaan twee soorten afnemers binnen het Afsprakenstelsel Elektronische Toegangsdiensten:

- Dienstverlener (DV): een partij die digitale diensten *aanbiedt*. Bijvoorbeeld een online webshop of een overheidsorganisatie als de Belastingdienst. Dienstverleners kunnen via het afsprakenstelsel gebruikers veilig toegang geven tot de digitale diensten die zij aanbieden. Als twee dienstverleners samenwerken om een dienst te leveren, spreken we van Dienstbemiddeling. De dienstverleners kennen we dan als een Dienstaanbieder (DA) die de inhoudelijke afhandeling van een dienst verzorgt en de Dienstbemiddelaar (DB) die de gebruikersinteractie verzorgt en daarmee de dienstafnemer ondersteunt.
- Dienstafnemer een bedrijf, rechtspersoon, privépersoon of een afnemende overheidsorganisatie die digitale diensten afneemt. Bijvoorbeeld: een gebruiker die een aankoop doet in een webshop of zijn belastingaangifte online indient. Gebruikers loggen in met inlogmiddelen die voldoen aan het afsprakenstelsel. Een gebruiker kan zo zijn identiteit aantonen en aanvullende informatie over bijvoorbeeld zijn bevoegdheden geven.

Het authenticatie- en autorisatieproces op hoofdlijnen

- De dienstafnemer (voor de leesbaarheid hierna te noemen: gebruiker) wil een digitale dienst afnemen en bezoekt de website van de dienstverlener;
- Op de website van de dienstverlener logt de gebruiker in met een authenticatiemiddel met het gevraagde betrouwbaarheidsniveau;
- De deelnemers binnen het afsprakenstelsel vormen een netwerk dat de gebruiker authenticeert en de bevoegdheden controleert;
- Als de controle op authenticatie en bevoegdheden goed verloopt, verklaart het netwerk hierover aan de dienstverlener door middel van een set aan verklaringen;
- Op basis van deze informatie weet de dienstverlener wie de gebruiker is en wat hij mag doen;
- De dienstverlener besluit op basis van de set verklaringen of hij de dienst verleent waar de gebruiker om vraagt;
- Om dit proces mogelijk te maken sluit de dienstverlener aan op het afsprakenstelsel via een makelaar en koopt de gebruiker (één of meerdere) inlogmiddel(en) die voldoen aan het afsprakenstelsel.

Aansluiten als dienstverlener

Waarom zou ik aansluiten?

Dienstverleners gebruiken eHerkenning om een veilige toegang en gebruik van hun elektronische diensten door dienstafnemers (gebruikers) mogelijk te maken.

Wat betekent aansluiten?

De dienstverlener neemt het gestandaardiseerde koppelvlak van eHerkenning op in de toegang tot deze diensten. De dienstverlener heeft primair met één rol van het netwerk te maken, de zogeheten herkenningsmakelaar. De dienstverlener selecteert een partij die deze dienst levert en sluit daarmee een contract. De dienstverlener kan vervolgens aansluiten op het netwerk zodra zij haar systemen gereed heeft en er een positieve test op de werking van de I nterface specifications DV-HM is uitgevoerd. De herkenningsmakelaar zorgt er vervolgens voor dat iedere keer dat de dienst wordt aangeroepen eerst via het netwerk de vereiste verklaringen worden geleverd. Omdat in het bedrijvendomein het voor alle herkenningsmakelaars verplicht is alle achterliggende authenticatiediensten en machtigingenregisters te ontsluiten, kan de dienstverlener een herkenningsmakelaar selecteren ongeacht de toepassing of klantgroep.

Diensten inschalen op betrouwbaarheidsniveau en definitie

Voorafgaand aan het aansluiten moet de dienstverlener bepalen welk Betrouwbaarheidsniveau van eHerkenning toegang geeft tot de digitale diensten, of vereist is voor het zetten van de elektronische handtekening. Het door de dienstverlener vereiste betrouwbaarheidsniveau wordt vastgelegd in een dienstencatalogus. In deze catalogus neemt de dienstverlener op of zij beogen een dienst met SSO toegankelijk te maken, hoe de dienst gedefinieerd wordt, of de dienst bemiddeld kan worden door een dienstbemiddelaar en welk soort dienstafnemers toegang kan krijgen. Ten aanzien van de definitie is het van belang dat de dienstverlener de dienst een omschrijving geeft die bij een eindgebruiker en/of machtigingenbeheerder herkenbaar en betekenisvol is. De eindgebruiker of diegene die machtigen beheert moet kunnen herleiden wat "de dienst" is. Als onderdeel van de aansluiting dient tevens bepaald te worden hoe de diensten die aangeboden worden gedefinieerd zijn, zodat machtigingenregisters bevoegdheden voor specifieke diensten kunnen vastleggen.

Verantwoordelijkheden van de dienstverlener bij transacties door dienstafnemers:

- moet zich houden aan de technische beveiligingseisen van het toegepaste koppelvlak en aan de beveiligingsrichtlijnen van het NCSC;
- is zelf verantwoordelijk voor het controleren van de herkomst van ontvangen berichten;
- moet vanaf het moment dat een gebruiker toegang heeft een logoutknop bieden.
- Is verantwoordelijk voor het definiëren van de Dienst (het benoemen en beschrijven van de dienst) en voor de keuze betrouwbaarheidsniveau (LoA);
- Moet besluiten of hij een dienst openstelt voor Dienstbemiddeling; indien hij hiertoe besluit moet hij dit doorgeven aan de Herkenningsmakelaar die dit opneemt in de dienstencatalogus;
- Indien Dienstbemiddeling wordt toegestaan: Draagt de inhoudelijk verantwoordelijkheid van de dienst zelf.
    - Moet een eenduidige technische interface voor Dienstbemiddeling opstellen en beschikbaar stellen aan Dienstbemiddelaars;
    - Moet toestemming tot Dienstbemiddeling verstrekken aan een Dienstbemiddelaar.
        - De door de dienstverlener ingeschakelde Herkenningsmakelaar zal de Gebruiksvoorwaarden van het AS hierbij in het contract /algemene voorwaarden met de Dienstbemiddelaar van toepassing verklaren
- Mag Attributen ontvangen.
- Moeten akkoord gaan met aansluitvoorwaarden BSNk wanneer zij Versleutelde Pseudoniemen of Versleutelde Identiteiten wensen te ontvangen.

Verdere informatie

Er zijn Service level definities in het afsprakenstelsel opgenomen waarin de minimale service level afspraken zijn opgenomen die van toepassing zijn op de dienstverlening van de herkenningsmakelaar en de dienstverlener. Tussen de herkenningsmakelaar en de dienstverlener wordt een overeenkomst afgesloten die betrekking heeft op dienst(en) die door de herkenningsmakelaar worden geleverd en waarop tevens de Gebruiksvoorwaarden Elektronische Toegangsdiensten van toepassing zijn. Hier kunnen ook (additionele) service level afspraken in worden opgenomen. In Interface specifications DV-HM is het koppelvlak tussen dienstverlener en Herkenningsmakelaar technisch beschreven en de specificatie van de dienstencatalogus uitgewerkt.

Sluit u als (SaaS-)leverancier aan namens een Dienstverlener (DV)? Er is sprake van Dienstbemiddeling in de volgende gevallen:

1. U wilt gebruikmaken van uw eigen SSL-certificaat;
2. U kunt geen gebruikmaken van het SSL-certificaat van de dienstverlener;
3. Hetzelfde portaal/dezelfde aansluiting wordt namens meer dan één dienstverlener aangeboden.

Meedoen als dienstafnemer

Hoe doe ik mee als dienstafnemer?

Dienstafnemers kunnen meedoen met eHerkenning door de aanschaf van een authenticatiemiddel waarmee ze kunnen inloggen bij een dienstverlener die aangesloten is op eHerkenning. Met dit middel kunnen ze inloggen en een dienst afnemen of een elektronische handtekening zetten. Bij eHerkenning kan ook een vertegenwoordiger van de dienstafnemer gemachtigd worden voor het doen van transacties. Deze vertegenwoordigingsbevoegdheid moet in een machtigingenregister zijn vastgelegd.

Met wie doe ik zaken als dienstafnemer?

Een dienstafnemer bepaalt zelf welk middel hij aanschaft, zolang het maar aan het gevraagde betrouwbaarheidsniveau voldoet. Deze keuzevrijheid geldt ook voor het registreren van machtigingen. Het Afsprakenstelsel is zo opgezet dat veel verschillende soorten authenticatiemiddelen gebruikt kunnen worden, bijvoorbeeld gebruikersnaam/wachtwoorden, card / card readercombinaties, VPN tokens, maar ook mobiele telefoons met TANs. De beheerorganisatie maakt een steeds actueel overzicht van de toegetreden aanbieders van authenticatiemiddelen openbaar, zie https://eherkenning.nl/leveranciers. Een dienstafnemer mag middelen bij meer dan één middelenuitgever aanschaffen en bevoegdheden in meerdere machtigingenregisters laten vastleggen. Omdat de registratieprocedures voor het verkrijgen van authenticatiemiddelen en het vastleggen van bevoegdheden gedeeltelijk dezelfde gegevens betreffen kan het voorkomen dat middelenuitgever en machtigingenregister samenwerken door de benodigde registraties in één proces aan bedrijven aan te bieden.

Gebruiksvoorwaarden

De Deelnemers zijn verplicht om een overeenkomst af te sluiten op basis waarvan de Herkenningsdiensten worden verleend en waarop de Deelnemer verplicht is de Gebruiksvoorwaarden Elektronische Toegangsdiensten van toepassing te verklaren. Wanneer een dienstafnemer het gebruik van eHerkenning wil beëindigen kan zij bevoegdheden en eventueel authenticatiemiddelen laten intrekken.

Betrouwbaarheidsniveaus

Binnen het afsprakenstelsel zijn middelen op verschillende betrouwbaarheidsniveaus beschikbaar. De dienstverlener geeft aan met welk betrouwbaarheidsniveau de dienstafnemer moet inloggen of ondertekenen. De dienstafnemer bepaalt op welk betrouwbaarheidsniveau hij een inlogmiddel wil aanschaffen, zolang hij met dit middel maar aan het betrouwbaarheidsniveau voldoet wat voor de afname van een dienst vereist is. Conform de eisen van dit betrouwbaarheidsniveau wordt zijn identiteit vastgesteld en wordt het middel daadwerkelijk verstrekt. De procedure daarvoor varieert per betrouwbaarheidsniveau. De verschillen in de registratieprocedures per betrouwbaarheidsniveau zijn te vinden in Normenkader betrouwbaarheidsniveaus.

Aansluiten als dienstbemiddelaar

Binnen het stelsel wordt bij het begrip Dienstverlener onderscheid gemaakt in dienstbemiddelaar en dienstaanbieder. Dit onderscheid is vooral van belang bij Dienstbemiddeling. De Dienstbemiddelaar is een Dienstverlener (DV) die de Dienstafnemer ondersteunt in het afnemen van een digitale Dienst ten behoeve van de Dienstaanbieder (DA) door middel van Dienstbemiddeling.

Waarom zou ik aansluiten als Dienstbemiddelaar?

Sluit u als (SaaS-)leverancier aan namens een Dienstverlener (DV)? Er is sprake van Dienstbemiddeling in de volgende gevallen:

1. U wilt gebruikmaken van uw eigen SSL-certificaat;
2. U kunt geen gebruikmaken van het SSL-certificaat van de dienstverlener;
3. Hetzelfde portaal/dezelfde aansluiting wordt namens meer dan één dienstverlener aangeboden.

Als er geen sprake is van dienstbemiddeling zal de dienstaanbieder zelf het 'zichtbare' gedeelte van een dienst tonen. Dit is de plaats waar de authenticatie, machtigingen en alle andere gegevens van de gebruiker die nodig zijn voor het afnemen van een dienst worden opgevraagd. Het komt echter ook voor dat een *andere* partij dan de dienstaanbieder de dienstafnemer ondersteunt in het afnemen van een digitale dienst. Deze dienstverlenende partij biedt dan het 'zichtbare' deel van de dienst aan, en wordt dan de 'dienstbemiddelaar' genoemd.

Het voordeel voor de dienstbemiddelaar is dat het mogelijk is aan te sluiten op een gestandaardiseerde werkwijze voor het verkrijgen van autorisaties om namens de dienstafnemer de diensten te kunnen afnemen. De dienstafnemers worden daarbij ontzorgd door de dienstbemiddelaar en zijn er op grond van onweerlegbare bewijzen van verzekerd dat de dienstbemiddelaar alleen met hun instemming de diensten via dienstbemiddeling voor hen kan afnemen.

Wat betekent aansluiten?

Een dienstbemiddelaar heeft een verantwoordelijkheid richting gebruiker om diens beoogde gebruikerswens correct te vertalen en aan te bieden richting dienstverlener. Hiertoe dient de dienstbemiddelaar ook alle verklaringen omtrent identiteit, machtigingen en gegevens die door de gebruiker benodigd zijn om geautoriseerd te worden voor de dienst te verzamelen. Met het onlosmakelijk verbinden van deze verklaringen aan het 'transactiebericht' verklaart de dienstbemiddelaar zelf over dit proces (zie Associatieverklaring).

Door het aangaan van de overeenkomst met de herkenningsmakelaar aanvaardt de dienstbemiddelaar de aansprakelijkheid voor zijn eigen handelen en /of nalaten bij het leveren van diensten op basis van het afsprakenstelsel.

De dienstbemiddelaar voldoet aan de koppelvlakspecificaties van Elektronische Toegangsdiensten om de verklaringen te verkrijgen.

Verder dient de dienstbemiddelaar zich te houden aan de technische beveiligingseisen van het toegepaste koppelvlak en aan de beveiligingsrichtlijnen van het NCSC en verantwoordelijkheid te nemen voor het controleren van de herkomst van ontvangen verklaringen.

Verantwoordelijkheden/rechten van een dienstbemiddelaar zijn in ieder geval:

- Verkrijgen van toestemming van de dienstaanbieder om dienstbemiddeling voor een dienst te realiseren.
- Juist transformeren van invoer en bedoeling van de gebruiker naar transactieberichten voor de dienst en de informatie van een dienst juist transformeren voor de gebruiker.
- Verkrijgen van instemming van de gebruiker in het afnemen van de dienst.
- De Verklaringen van Herkenning verzamelen en op juiste wijze verbinden met het transactiebericht en aan dienstaanbieder aanleveren met transactiebericht.
- Informeren van de gebruiker als het transactiebericht niet bij de dienstaanbieder afgeleverd kan worden.
- De dienstbemiddelaar ontvangt alleen identificerende kenmerken; attributen worden van het stelsel niet aan de dienstbemiddelaar geleverd.
- Moet vanaf het moment dat een handelend natuurlijk persoon toegang heeft, al dan niet op basis van een vraag waarvoor SSO is toegestaan, een logoutknop bieden.
- Moet zich houden aan de technische beveiligingseisen van het toegepaste koppelvlak en aan de beveiligingsrichtlijnen van het NCSC.
- Is zelf verantwoordelijk voor het controleren van de herkomst van ontvangen berichten.

Verdere informatie
Er zijn Service level definities in het afsprakenstelsel opgenomen waarin de minimale service level afspraken zijn opgenomen die van toepassing zijn op de dienstverlening van de herkenningsmakelaar en de dienstbemiddelaar. Tussen de herkenningsmakelaar en de dienstbemiddelaar wordt een overeenkomst afgesloten die betrekking heeft op dienst(en) die door de herkenningsmakelaar worden geleverd en waarop tevens de Gebruiksvoorwaarden Elektronische Toegangsdiensten van toepassing zijn. Hier kunnen ook (additionele) service level afspraken in worden opgenomen. In Interface specifications DV-HM is het koppelvlak tussen dienstbemiddelaar en herkenningsmakelaar technisch beschreven en de specificatie van de dienstencatalogus uitgewerkt.

Deelnemers en diensten

De doelstelling van het Afsprakenstelsel Elektronische Toegangsdiensten is om het eenvoudig mogelijk te maken voor burgers, bedrijven en overheden om veilig online in te loggen en transacties te kunnen doen bij bedrijven en overheden.

Hiervoor worden de volgende diensten geleverd door de deelnemers aan het afsprakenstelsel:

- Identificatie en authenticatie op een bepaald betrouwbaarheidsniveau: is de gebruiker wie hij zegt te zijn? En kan hij dit aantonen met de gewenste zekerheid?
- Verstrekken van aanvullende, gevalideerde persoonsgegevens (attributen) op verzoek van de gebruiker zoals geslachtsnaam, voornaam, initialen, geboortedatum/plaats en voldoen aan leeftijdsgrens;
- Machtigingen: de bevoegdheid aantonen om (rechtsgeldig) te kunnen handelen namens iemand die jou gemachtigd heeft;

Om deze diensten te kunnen leveren werken de volgende rollen samen in het Netwerk:

- Authenticatiedienst (AD): authenticeert gebruikers;
- Herkenningsmakelaar (HM): vormt de linking pin tussen het netwerk voor eHerkenning en de dienstverleners, en heeft een routeer- en navigatiefunctie in het netwerk; dit reduceert het aantal relaties tussen dienstverleners enerzijds en authenticatiediensten, machtigingenregisters en het BSNk anderzijds;
- Machtigingenregister (MR): registreert, onderhoudt en controleert bevoegdheden;
- Middelenuitgever (MU): geeft authenticatiemiddelen uit voor het identificeren en bij uitgifte authenticeren van natuurlijke personen;
- BSNk: zorgt voor de koppeling van authenticatiemiddelen aan BSN's voor de authenticatie van personen;
- eIDAS-berichtenservice (EB): onderdeel van het eIDAS-koppelpunt ; zorgt voor ontsluiting van het Afsprakenstelsel Elektronische Toegangsdiensten voor eIDAS-gebruikers en -diensten volgens de eIDAS-verordening.

Om rollen te vervullen in het netwerk dient de deelnemer daartoe toegetreden te zijn. De toetredingseisen zijn te vinden op de pagina Toetredingseisen. De tails over de functionaliteit kan de lezer vinden in de Use cases. De specificaties van de gebruikte koppelvlakken tussen de verschillende rollen staan beschreven in Interface specifications.

Van iedere rol wordt op hoofdlijnen de verantwoordelijkheid aangegeven, voor zover deze verplicht zijn voor alle deelnemers.

Verantwoordelijkheden Authenticatiedienst

Een Authenticatiedienst (AD) authenticeert dienstafnemers of hun vertegenwoordigers.

Verantwoordelijkheden

- De authenticatiedienst is verantwoordelijk voor het authenticeren van personen op basis van hun authenticatiemiddel.
- De authenticatiedienst biedt daartoe aan een gebruiker een online interface om zich te (laten) authenticeren.
- De authenticatiedienst verwerkt een authenticatievraag conform de gesloten overeenkomst en overeengekomen service levels tussen de deelnemers en hun klanten.
- De authenticatiedienst ziet erop toe dat authenticatievragen alleen worden verwerkt indien zij kunnen worden verwerkt aan de hand van toegelaten authenticatiemiddelen van toegelaten middelenuitgevers.
- De authenticatiedienst verwerkt bijbehorende logoutberichten en toont de gebruiker een scherm met een bevestiging van de logout nadat deze succesvol heeft plaatsgevonden (indien de authenticatiedienst geen SSO ondersteunt of heeft uitgevoerd dan wordt een in die situatie passende boodschap getoond).
- De authenticatiedienst draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.

Indien de AD attribuutverstrekking ondersteunt

Zie Attributenbeleid

Eisen

- De authenticatiedienst MOET bewaken dat zowel de identificatie (i.c. het gebruikte authenticatiemiddel) als het proces van de authenticatie van minimaal het door de dienstverlener gewenste betrouwbaarheidsniveau is.
- De authenticatiedienst MOET op elke getoonde web pagina de naam van dienstverlener tonen zoals die in de dienstencatalogus is opgenomen.
- De authenticatiedienst MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de Eigenaar.
- De authenticatiedienst MOET alle processen inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Normenkader betrouwbaarheidsniveaus.
- De authenticatiedienst MOET toegang hebben tot de relevante door de middelenuitgever vastgelegde informatie om tot een authenticatie van het betreffende betrouwbaarheidsniveau te komen.
- De authenticatiedienst MOET zich houden aan de Richtlijnen naam- en merkgebruik eHerkenning.

Indien de authenticatiedienst single sign-on ondersteunt

- De authenticatiedienst MOET single sign-on zodanig uitvoeren dat er geen risico's op hergebruik of afluisteren van het authenticatiemechanisme bestaan.
- De authenticatiedienst MOET zodra een vraag van een dienstverlener ontvangen wordt waarin geen verplichte authenticatie door de gebruiker gespecificeerd is, de optie aanbieden om ingelogd te blijven. De authenticatiedienst MAG deze optie ook bieden indien wel een verplichte authenticatie gespecificeerd is. Het is toegestaan instellingen van de gebruiker aangaande het al dan niet aangemeld blijven na eerste authenticatie op een andere manier vast te leggen en toe te passen. Deze specificatie door de gebruiker blijft alleen relevant indien het een vraag betreft waarbij de dienstverlener single sign-on toestaat.
- Als een gebruiker persoon kiest om niet ingelogd te blijven, MOET deze keuze door de authenticatiedienst onthouden worden.
- De authenticatiedienst MOET de gebruiker middels teksten op het scherm of anderszins duidelijk maken in welke situatie de gebruiker zich bevindt (time-out van een SSO sessie, gedwongen authenticatie tijdens een bestaande SSO sessie, logout, etc.)
- De authenticatiedienst MOET vanaf de eerste authenticatie met SSO het maximum AD-tijdsverloop bewaken. Een volgende authenticatie op basis van SSO ZOU MOETEN worden gegeven indien deze binnen dit maximum AD-tijdsverloop valt tenzij een logoutbericht is ontvangen of er sprake is van afgedwongen authenticatie.
- Na het ontvangen van een logoutbericht MAG de gebruiker NIET geauthenticeerd worden op basis van SSO.

> **Toelichting**
>
> De authenticatiediensten gaan initieel het BSN ondersteunen voor de eIDAS implementatie van eHerkenning. Dit houdt in dat vooralsnog de EB het BSN van de authenticatiedienst mag ontvangen.

Aangezien de authenticatiedienst het BSN-domein ondersteunt

- De authenticatiedienst MOET het koppelvlak voor online (de)registreren van het BSNk implementeren.
- De authenticatiedienst MOET alle processen beschrijven en inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Normenkader betrouwbaarheidsniveaus. De beschrijvingen MOETEN via de website van de middelenuitgever/authenticatiedienst worden gepubliceerd.
- Het betrouwbaarheidsniveau voor het identificatie- en registratieproces MOET minstens voldoen aan de criteria voor niveau EH3.
- De authenticatiedienst MOET een overeenkomst met de gebruiker sluiten. Zie ook Juridisch kader.
- De authenticatiedienst MOET voor de gebruiker het BSN registreren bij het BSNk, via het daarvoor aangewezen koppelvlak.
- De authenticatiedienst MOET de registratie afmelden indien het middel en/of het pseudoniem niet (meer) toegeschreven kunnen worden aan de gebruiker.
- De authenticatiedienst is verantwoordelijk om te voldoen aan de aansluitvoorwaarden van BSNk.

Verantwoordelijkheden Herkenningsmakelaar

De Herkenningsmakelaar (HM) vormt de linking pin tussen het Netwerk (voor Elektronische Toegangsdiensten) en de dienstverleners, en heeft een routeer- en navigatiefunctie in het netwerk. Dit reduceert het aantal relaties tussen dienstverleners enerzijds en authenticatiediensten, machtigingenregisters en het BSNk anderzijds.

Verantwoordelijkheden

- De Herkenningsmakelaar routeert binnen het netwerk ten behoeve van een dienstverlener conform de afgesloten overeenkomst en overeengekomen service levels.
- De Herkenningsmakelaar sluit een duidelijke Service Level Agreement met de dienstverlener af. Deze Service Level Agreement kan onderdeel uitmaken van de overeenkomst.
- De Herkenningsmakelaar sluit alleen toegelaten authenticatiediensten en machtigingenregisters aan en houdt deze aangesloten, een en ander conform hetgeen hiertoe is vastgelegd in het Afsprakenstelsel.
- Om aan te tonen dat de Dienstverlener/Dienstbemiddelaar/Dienstaanbieder voldoet aan de voor hem geldende verplichtingen aan het afsprakenstelsel overlegt deze de ingevulde Template zelfverklaring Dienstverlener aan de Herkenningsmakelaar.
- De Herkenningsmakelaar is verantwoordelijk voor het testen van de dienstverlener opdat de dienstverlener, alvorens hij wordt aangesloten op het netwerk, aan alle in het afsprakenstelsel opgenomen specificaties voldoet.
- De Herkenningsmakelaar is het centrale aanspreekpunt voor de dienstverlener en de beheerorganisatie, onder andere in het geval van calamiteiten of een beveiligingsincident bij een dienstverlener. De Herkenningsmakelaar verstrekt als centraal aanspreekpunt de dienstverlener en de beheerorganisatie alle benodigde informatie.
- De Herkenningsmakelaar MOET borgen dat de naam van de Dienstverlener/Dienstbemiddelaar/Dienstaanbieder in de Dienstencatalogus overeenkomt met de naam in het gebruikte PKI-certificaat. Indien een PKIo-certificaat wordt gebruikt, dient het OIN daarin ook overeen te komen met het OIN in diens EntityID.
- De Herkenningsmakelaar draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.
- Indien de Herkenningsmakelaar twijfelt of van mening is dat de Dienstverlener niet langer aan zijn verplichtingen voldoet, geeft hij dit terstond door aan de Toezichthouder.
- Een Herkenningsmakelaar die een koppelvlak aanbiedt met de eIDAS-berichtenservice (EB) sluit een overeenkomst met de staatssecretaris van Binnenlandse Zaken als verantwoordelijke voor de eIDAS-berichtenservice (EB) om de interoperabiliteit tussen het Afsprakenstelsel Elektronische Toegangsdiensten en de eIDAS-oplossingen van andere lidstaten te realiseren ten behoeve van grensoverschrijdend inloggen met door de Europese Commissie op grond van artikel 9 van de eIDAS-verordening erkende authenticatiemiddelen.

Eisen

Een Herkenningsmakelaar MOET:

- Aan Dienstverleners een gestandaardiseerd koppelvlak leveren waarover toegangsdiensten kunnen worden geïnitieerd en gevraagde verklaringen kunnen worden geleverd.
- Voor Authenticatiediensten en Machtigingenregisters tenminste de twee meest recente gestandaardiseerde koppelvlakken ondersteunen zolang dit voor migratie en/of het gekozen Inzetgebied noodzakelijk is.
- Aan Gebruikers een online interface leveren om de gebruiker in staat te stellen indien nodig een Authenticatiedienst of een Machtigingenregister te selecteren.
- Bij de selectie van de Authenticatiedienst MOET de Herkenningsmakelaar alle instanties van de eIDAS-berichtenservice als Authenticatiedienst tonen als de dienstinstantie (ServiceInstance) is geclassificeerd als 'eIDAS-inbound'. Anders MOET de Herkenningsmakelaar deze NIET tonen.
- Indien het Inzetgebied bedrijven/consumenten wordt bediend
    - zowel het koppelvlak voor online bevragen van machtigingenregisters als het koppelvlak voor verificatie van de volgende schakel aan een Machtigingenregister ondersteunen.
    - in staat zijn om op basis van een authenticatieverklaring en een of meer machtigingsverklaringen ontvangen van Machtigingsregisters een verklaring aan de Dienstverlener over authenticatie en ketenmachtiging samen te stellen. Voorafgaand aan verstrekking moet de Herkenningsmakelaar de consistentie van alle verklaringen en gespecificeerde informatie controleren.
- Gebruikers bij de selectie van de Authenticatiedienst de optie bieden om deze instelling te bewaren. Iedere Herkenningsmakelaar moet zorgen dat een gebruiker waarvoor de selectie van de Authenticatiedienst bewaard is, deze vraag niet opnieuw voorgelegd krijgt.
- SSO ondersteunen en daartoe vragen met SSO doorgeven aan een Authenticatiedienst en logoutberichten verwerken en doorsturen naar de Authenticatiedienst.
- Registreren welke attributen een Dienstverlener wil uitvragen bij iedere authenticatie.
- Attributen doorgeven precies zoals ze ontvangen zijn van Authenticatiediensten of Machtigingenregisters.
- Na ontvangst van een verklaring van een Machtigingenregister controleren of het een incomplete keten betreft die alleen geldig is indien aanvullende schakels ook geverifieerd kunnen worden.
- Zich houden aan de richtlijnen naam- en merkgebruik eHerkenning.
- De Dienstverlener ontzorgen bij het verkrijgen van sleutelmateriaal voor het ontsleutelen van Versleutelde Pseudoniemen en/of Versleutelde Identiteiten.

Verantwoordelijkheden Machtigingenregister

Dienstafnemers kunnen iemand vragen om namens hen te handelen. Dit regelen ze via een machtiging. Binnen het netwerk wordt deze machtiging op raadpleegbare wijze vastgelegd in een Machtigingenregister (MR). In het machtigingenregister wordt de koppeling gelegd tussen het authenticatiemiddel van gemachtigde en de bevoegdheid. Op basis van die gegevens samen kan het netwerk met een bepaald betrouwbaarheidsniveau verklaren dat iemand met een bepaald authenticatiemiddel namens een bepaald bedrijf mag handelen voor de afname van een bepaalde dienst.

De procedure voor het vastleggen van bevoegdheden varieert naar gelang het betrouwbaarheidsniveau. Hoe hoger het niveau, des te meer bewijzen dienen overlegd te worden. De registraties hiervoor worden uitgevoerd onder verantwoordelijkheid van de dienstafnemer conform Meedoen als dienstafnemer. Een vertegenwoordigde dienstafnemer kan een beheerder laten vastleggen die zijn bevoegdheden beheert. Uiteraard dient de vastlegging van deze beheerder tenminste op hetzelfde betrouwbaarheidsniveau te gebeuren.

Verantwoordelijkheden

- **Het Machtigingenregister levert de volgende functionaliteiten aan Machtigingenregisters:**

    1.Ondersteunen van Discovery Interface MR-MR chain authorisations

    2. de registratie van identificerende kenmerken van gebruikers die door de dienstafnemer zijn of worden gemachtigd om namens de dienstafnemer elektronische verklaringen af te leggen en/of in ontvangst te nemen;

    3. het toekennen van pseudoniemen aan gebruikers waarbij de eisen van dataminimalisatie aantoonbaar worden gevolgd;

    4. het registreren van machtigingen die door de dienstafnemer zijn afgegeven, waarbij de koppeling met identificerende kenmerken en/of pseudoniemen aantoonbaar is terug te voeren op de in de registratiefase door de dienstafnemer, of namens deze de machtigingenbeheerder, verschafte gegevens;

    5. een proces, in welke vorm dan ook, voor het opvoeren, onderhouden en intrekken van registraties van machtigingen, dat voldoet aan de in het afsprakenstelsel gedefinieerde betrouwbaarheidsniveaus.

    6. MOET BSN gegevens polymorf versleutelen (zie Polymorfe pseudonimisering) indien deze geregistreerd staan bij een eenmanszaak.

    7. MOET het BSNk bevragen voor het verkrijgen van polymorfe pseudoniemen en polymorfe Identiteiten (PI).

    8. MOET zelf de administratie van interne pseudoniemen bijhouden.

- Het machtigingenregister zorgt voor vastlegging van duidelijke afspraken over de validatie van de vertegenwoordigingsbevoegdheid van de gebruiker van de dienstafnemer voor zover het een publiekrechtelijke rechtspersoon betreft.
- Het machtigingenregister voorkomt dat een ingetrokken of geblokkeerde registratie van een machtiging als geldige registratie wordt verwerkt.
- Het machtigingenregister zorgt voor een verwerking van registraties van machtigingen conform de afgesloten overeenkomst en overeengekomen service levels.
- Het machtigingenregister draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.
- Het Machtigingenregister levert de volgende functionaliteiten aan Machtigingenregisters:
    1. Ondersteunen van Discovery Interface MR-MR chain authorisations

Eisen

- Het machtigingenregister MOET bewaken dat het registratieproces waarmee de bevoegdheidsverklaring is vastgelegd minimaal van het door de dienstverlener vereiste betrouwbaarheidsniveau is.
- Het machtigingenregister MOET de naam van dienstverlener tonen zoals die in de dienstencatalogus is opgenomen.
- Het machtigingenregister MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- Het machtigingenregister MOET alle processen inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Nor menkader betrouwbaarheidsniveaus.
- Het machtigingenregister MOET het hoogst mogelijke betrouwbaarheidsniveau hanteren in het antwoord. Dat wil zeggen dat als er bijv. een algemene bevoegdheid is geregistreerd op een laag niveau, maar voor de betreffende dienst ook een specifieke bevoegdheid is vastgelegd op een hoger niveau dat het machtigingenregister dan het hogere niveau MOET hanteren.
- Het machtigingenregister MOET zich houden aan de richtlijnen naam- en merkgebruik eHerkenning.

Zie ook Attributenbeleid.

Eisen richting het InzageRegister:

- Een MachtigingsRegister MOET de statusgegevens van elke 'verzameling van machtigingen' registeren en actueel houden bij het BSNk-InzageRegister .

Voor Ketenmachtigingen geldt:

- Registratie van de identificerende kenmerken van partijen die geen natuurlijk persoon zijn en die bevoegd zijn om namens een vertegenwoordigde dienstafnemer bepaalde elektronische diensten af te nemen bij dienstverleners;
- Vastleggen in welk volgend machtigingenregister een volgend deel van een keten zich bevindt;
- Vastleggen van beperkingen van de strekking van machtigingen die specifiek zijn voor ketenmachtigingen (Bij uitbreiding naar meer schakels moeten de controles aangaande kennisgeving bij substitutie hier worden toegevoegd.). In het bijzonder dat een dienst "voor derden" mag worden uitgevoerd door betreffende gemachtigde en de mogelijkheid om de vertegenwoordigde dienstafnemer waarvoor de ketenmachtiging benut mag worden te specificeren;

- Ondersteunen van het koppelvlak voor verificatie van de volgende schakel in geval van ketenmachtiging en de uitbreidingen voor het doorgeven van informatie over de intermediaire partij (Vervallen_Interface specifications HM-MR chain authorization).

Het machtigingenregister MOET in volgende prioriteitsvolgorde de informatie aangaande de compleetheid van de keten benutten:

1. Hetgeen gespecificeerd is bij een gevonden geldige machtiging
2. Hetgeen in de vraag als specificatie is meegegeven
3. Hetgeen bij ontbreken van bovenstaande aan de gebruiker gevraagd is.



Het is mogelijk om deze bevoegdheid te beperken tot één vestiging van de vertegenwoordigde dienstafnemer. Dit leidt tot een machtigingsketen op grond waarvan een gebruiker (gebruiker) de betreffende vestiging van de vertegenwoordigde dienstafnemer mag vertegenwoordigen.

Indien het Machtigingenregister het BSN-domein ondersteunt

- De MR is verantwoordelijk om te voldoen aan de aansluitvoorwaarden van BSNk.

Verantwoordelijkheden Middelenuitgever

De middelenuitgever geeft authenticatiemiddelen uit voor het identificeren en authenticeren van gebruikers.

Verantwoordelijkheden en eisen:

- De middelenuitgever regelt voor dienstafnemers en/of natuurlijke personen conform de afgesloten overeenkomst en overeengekomen service levels:
    1. de uitgifte, beheer en intrekking van authenticatiemiddelen en het zorgvuldig vastleggen van alle daarvoor conform de betrouwbaarheidsniveaus geregistreerde gegevens in een administratie;
    2. het ten behoeve van de uitgifte identificeren en authenticeren van handelende natuurlijke personen;
    3. het ondersteunen van één of meer betrouwbaarheidsniveaus;
    4. het doorgeven van benodigde informatie aan één of meer authenticatiediensten conform het afsprakenstelsel.
    5. optioneel: het ten behoeve van uitgifte identificeren en authenticeren van natuurlijke personen in hun rol als **consument** of **burger**.
- De middelenuitgever draagt zorg voor correcte uitvoering van alle aan haar in het Afsprakenstelsel voorgeschreven verplichtingen, waaronder auditverplichtingen.
- De middelenuitgever MOET zich houden aan de richtlijnen naam- en merkgebruik eHerkenning.
- Een middelenuitgever moet (als Dienstverlener) zelf ook gebruik (gaan) maken van het Afsprakenstelsel Elektronische Toegangsdiensten voor haar overige dienstverlening, indien en voor zover deze met hetzelfde middel wordt ontsloten en de use case wordt ondersteund door het Afsprakenstelsel.

    - Een middelenleverancier moet aangeven op welke wijze en welke termijn ze hieraan gaat voldoen. Het Tactisch Beraad beoordeelt of dit acceptabel is. Binnen het Tactisch Beraad zal het gesprek over redelijkheid gevoerd worden.
    - Deze voorwaarde is dus niet gekoppeld aan de formele toetredingsprocedure, omdat de toetredingsprocedure en besluitvorming buiten de governance is geplaatst.

Verantwoordelijkheden eIDAS-berichtenservice

Verantwoordelijkheden

Aan de eIDAS-berichtenservice (EB) worden bij authenticatie van een persoon met een buitenlands authenticatiemiddel de volgende eisen gesteld:

De eIDAS-berichtenservice

- achterhaalt**,** zodra daar wettelijke basis voor bestaat, in de Dienstencatalogus (DC) of de Nederlandse dienstverlener een BSN vereist.
- achterhaalt in de dienstencatalogus welke attributen de Nederlandse dienstverlener nodig heeft. De eIDAS Berichtenservice staat het toe dat de dienstverlener een subset van de in de catalogus bij de dienst gemarkeerde attributen vraagt. De eIDAS-berichtenservice (EB) mag het niet toestaan dat de dienstverlener meer attributen vraagt dan in de dienstencatalogus aangegeven.
- neemt de bij dienstverlener of makelaar gemaakte landenkeuze voor authenticatie over.
- biedt de handelende persoon een landenkeuze voor authenticatie als die keuze nog niet bij de dienstverlener of makelaar gemaakt is.
- vormt de eIDAS attributen om naar eTD attributen.
- vormt (zodra daar wettelijke basis voor bestaat en indien het een BSN dienst betreft) de eIDAS attributen om naar BRP attributen.
- honoreert de verwerkingsregels die vanuit het stelsel eTD zijn afgesproken in relatie tot het verwerken van antwoord- en resultaatberichten voor zover de verordening dit toelaat.

Historie en status

- Versie 1.1
- Versie 1.2
- Versie 1.3
- Versie 1.4
- Versie 1.5
- Versie 1.6
- Versie 1.7
- Versie 1.8
- Versie 1.9
- Versie 1.10
- Versie 1.11

Versie 1.1

In opdracht van het Ministerie van EZ heeft het programma eHerkenning het proces georganiseerd om met geïnteresseerde marktpartijen te komen tot versie 1.1 van het afsprakenstelsel eHerkenning. Dit is gebeurd met een iteratief werkgroepproces, waarbij zowel marktpartijen als dienstverleners hun inbreng leverden. De behoeften van dienstverleners werden hierbij vertegenwoordigd door de Gebruikersraad. (Voorafgaand aan oprichting van de Gebruikersraad vervulde het Launching Customer overleg deze functie. Gedurende 2010 bestond dit "Launching Customer" overleg uit Agentschap NL, Kamer van Koophandel, LNV. Immigratie- en Naturalisatiedienst (IND), Belastingdienst. Inspectie Verkeer en Waterstaat, Dimpact, IPO (Inter Provinciaal Overleg), OLO (Omgevingsloket Online) en Antwoord voor bedrijven.)

Het aldus gezamenlijk gerealiseerde afsprakenstelsel is vervolgens tijdelijk in beheer genomen door Stichting ICTU (zie voor de verdere uitwerking van de inrichting van het het beheer Organen en taakverdeling. In 2012 is het beheer overgedragen aan Logius). De verantwoordelijkheid voor het beheer van het afsprakenstelsel eHerkenning omvat ook het verder regisseren van de doorontwikkeling van dat afsprakenstelsel.

Immers, de toepassing van afsprakenstelsel eHerkenning versie 1.1 levert nu al bewezen unieke en waardetoevoegende oplossingen, onder andere in de proefimplementatie bij Agentschap NL. Zo verschaft het zekerheid of de persoon met wie de dienstverlener zaken doet wel is voor wie hij of zij zich uitgeeft. Ook maakt het duidelijk of deze persoon wel bevoegd is om voor het handelende Nederlandse bedrijf deze (overheids)diensten af te nemen.

Tegelijk liggen er breed gedragen wensen voor uitbreidingen van eHerkenning na versie 1.0. Zo dienen – alleen al vanwege EU-richtlijnen – ook buitenlandse bedrijven eHerkenning te kunnen gaan gebruiken, niet alleen Nederlandse. Verder ligt er het voornemen voor uitbreiding van eHerkenningsfunctionaliteit met bijvoorbeeld ondertekendiensten, waarbij de afnemer van de dienst zijn wilsuiting – bijvoorbeeld een belastingaangifte of vergunningsaanvraag – elektronisch kan bekrachtigen. Ook is het ondersteunen van een keten van machtigingen gewenst – niet alleen firma F die haar eigen werkneemster Pietersen kan machtigen, maar ook firma F die accountantsfirma A machtigt, die op haar beurt haar werkneemster Elimami machtigt om namens firma F belastingaangifte te doen. Tenslotte ligt er de behoefte om eHerkenning voor machine-to-machine communicatie geschikt te maken. Evenzovele zaken die om regie vragen door de beheerorganisatie van het afsprakenstelsel.

Versie 1.2

Gedurende 2011 is het aantal bedrijven dat eHerkenning gebruikt en het aantal dienstverleners dat aangesloten is sterk gegroeid. In deze versie 1.2 is de functionaliteit uitgebreid met attribuutverstrekking, wordt vastgelegd hoe optionele functionaliteit beschreven wordt en worden diverse RfCs uit het reguliere beheerproces verwerkt. Vanaf deze versie mogen meerdere versies van koppelvlakken binnen het netwerk toegepast worden voor zover deze in het afsprakenstelsel beschreven zijn.

Concreet betekent dat dat versie 1.1 van de koppelvlakken gedurende deze versie mag bestaan naast versie 1.2. Tevens zijn tekstuele verbeteringen doorgevoerd en enkele inconsistenties tussen documenten opgelost. Deze laatste zaken betreffen geen inhoudelijke wijzigingen.

Versie 1.3

Deze versie omvat een aantal RfCs met functionele wijzigingen die voortbouwen op versie 1.2, waaronder ten aanzien van attribuutverstrekking en foutafhandeling. Daarnaast bevat deze versie een grote hoeveelheid tekstuele verbeteringen op basis van het reviewcommentaar van de vier banken die intentieverklaring eHerkenning hebben onderschreven, alsook diverse verbeteringen rond beheer en het implementatieproces voor nieuwe versies. Tevens zijn de teksten ten aanzien van governance aangepast aan hetgeen per eind 2011 afgesproken is aangaande het beleggen van de beheerorganisatie bij Logius.

Versie 1.4

Deze versie omvat een aantal RfCs met functionele wijzigingen die voortbouwen op versie 1.3 voor o.a. toepassing van nieuwe KvK vestigingsnummer betere aansluiting op de voor overheid verplichte webrichtlijnen, voor het faciliteren van G2G gebruik. De term "bedrijf" die afkomstig was uit de beginfase is daarbij door het algemenere "dienstafnemer" vervangen, wel is in voorbeelden onveranderd uitgegaan van de belangrijkste doelgroep, namelijk bedrijven. Nieuwe versies van de deelnemersovereenkomst en gebruiksvoorwaarden en verder uitgewerkte procesbeschrijvingen van enkele cruciale beheerprocessen. In deze versie is tevens de nieuwe governance van het afsprakenstelsel verwerkt.

Versie 1.5

Deze versie omvat een aantal RfCs die de Betrouwbaarheidsniveaus van eHerkenning meer in lijn brengen met de internationale STORK norm. Daarnaast bevat deze versie RFCs die pilotbare functionaliteit bevatten voor B2C dienstverlening en attributen voor beroepsbeoefenaren. Verder bevat deze versie een vernieuwd Juridisch Kader inclusief nalevingsbeleid en gebruiksvoorwaarden. Beheerprocessen rond change- en releasemanagement, metadata, dienstencatalogus en penetratietesten zijn in meer detail beschreven.

Versie 1.6

Deze versie is een tussenversie waarin veel onderdelen van het afsprakenstelsel zijn opgeschoond maar die geen nieuwe functionaliteit bevat. Het is tevens de eerste nieuwe versie die is vastgesteld onder beheer van Logius. Alle pilotbare functionaliteit is uit het afsprakenstelsel verwijderd, evenals de verwijzigingen naar non-standaard koppelvlakken. De koppelvlakdocumenten zijn ontdubbeld. Procesbeschrijvingen zijn aangevuld en aangescherpt en de informatiebeveiligingsdocumenten zijn geactualiseerd. De eisen aan verwerken van (kopie) WID documenten zijn verduidelijkt . Tenslotte is de deelnemersovereenkomst geactualiseerd.

Versie 1.7

Deze versie bevat verschillende nieuwe functionaliteiten, te weten Single Sign On (SSO), uitgebreide attribuutverstrekking, ketenmachtigingen, ondersteuning van B2C authenticatiediensten en authenticatie van beroepsbeoefenaren. Voor deelnemers en dienstverleners is dit optionele functionaliteit waarvoor zij separaat kunnen toetreden. Ook is in deze versie het koppelvlak DV-HM verder gestandaardiseerd zodat dienstverleners gebruik kunnen maken van standaard SAML pakketten om aan te sluiten op eHerkenning. Daarnaast is de compensatieregeling voor migraties verder uitgewerkt en het Juridisch Kader verder aangescherpt.

Versie 1.8

Versie 1.8 bevat een aanscherping van enkele processen in het Operationeel handboek, alsmede wijzigingen in het Juridisch kader. In technische zin bevat deze versie een verscherping van de afspraken over het automatisch verspreiden van de netwerkmetadata en de dienstencatalogus. De koppelvlakspecificaties blijven gelijk aan die van 1.7.

Versie 1.9

Release 1.9 is de eerste release die plaatsvindt onder het Instellingsbesluit Elektronische Toegangsdiensten. Onder dit Instellingsbesluit vallen de twee merken eHerkenning en Idensys. Release 1.9 bevat een aantal wijzigingen en extra functionaliteiten die nodig zijn voor de realisatie van het Introductieplat eau van Idensys. Op basis van het Introductieplateau van Idensys worden pilots uitgevoerd met Idensys. Daarnaast bevat release 1.9 een aantal verbeteringen relevant voor eHerkenning.

Pilots met Idensys

Met Idensys wordt een belangrijke stap gezet naar standaardisatie en integratie van toegangsdiensten voor overheid en bedrijfsleven. Het wordt mogelijk om met private inlogmiddelen in het BSN-domein in te loggen. Daarmee wordt ook voor het BSN-domein authenticatie op het hoogste betrouwbaarheidsniveau geregeld.

De pilots met Idensys vinden plaats in het BSN-domein (op betrouwbaarheidsniveau 3 en 4) en in het consumentendomein (op betrouwbaarheidsniveaus 2, 2+, 3 en 4). De pilots duren tot medio/eind 2016 waarna geëvalueerd wordt en besluitvorming over verdere invoering/opschaling plaatsvindt.

Tijdens de pilots worden de volgende functionaliteiten ondersteund:

- Inloggen: Identificatie en authenticatie
  - Op betrouwbaarheidsniveau 2, 2+, 3 en 4 bij bedrijven
  - Op betrouwbaarheidsniveaus 3 en 4 bij bedrijven en de overheid
- Attribuutverstrekking: het leveren van aanvullende, gevalideerde persoonsgegevens op basis van User consent. Deze informatie wordt door de authenticatiedienst verstrekt en is gevalideerd op basis van een WID. Het gaat om de volgende aanvullende gegevens:
  - Geslachtsnaam, voornaam, initialen, geboortedatum-/plaats
  - Leeftijdsverificatie

Functionaliteiten zoals machtigingen en ontsluiten van andere attribuutregisters zijn nog geen onderdeel van Idensys in de pilotfase.

eHerkenning

De toevoeging van de ServiceUUID aan de Dienstencatalogus maakt het mogelijk om diensten over te dragen naar een andere Dienstverlener (ofwel dezelfde dienst te delen met meerdere Dienstverleners) met behoud van geregistreerde machtigingen.

De portaalfunctie (GUC4.3 Portaalfunctie) is uitgebreid; de gebruiker kan nu voor meerdere diensten tegelijk inloggen.

Algemeen

Door het toevoegen van het BSN-domein zijn een aantal privacy-verhogende maatregelen getroffen, waaronder:

- De Artifact-binding wordt gebruikt voor alle koppelvlakken, dit zorgt ook voor een betere user-experience
- End-to-end encryptie: alle attributen en identificerende kenmerken worden zodanig versleuteld dat deze alleen gelezen kan worden door de beoogde ontvanger, niet meer door tussenliggende partijen

Versie 1.10

Deze versie introduceert de mogelijkheid tot Dienstbemiddeling en voegt nadere specificaties toe voor de rol Ondertekendienst (OD), waardoor het mogelijk is voor deze rol toe te treden.

Versie 1.11

Deze koppelvlakrelease bevat de specificaties om authenticatie met middelen uit andere eIDAS-lidstaten te kunnen gebruiken bij Nederlandse publieke Dienstverleners. Nederland dient uiterlijk in 2018 het mogelijk te maken dat met genotificeerde middelen uit andere eIDAS-lidstaten diensten afgenomen kunnen worden bij Nederlandse publieke instellingen en overheden. Hiertoe is het ETD-stelsel ook de Nederlandse oplossing om te voldoen aan de eIDAS-verordening. Dienstverleners die aansluiten op een makelaar van eHerkenning of Idensys zijn daarmee "Europaproof" en voldoen hiermee aan de verordening (EU) nr. 910/2014.

Release 1.11 introduceert daarnaast een nieuw koppelvlak voor het ondersteunen van native apps. In toenemende mate maken Dienstverleners (DV's) gebruik van applicaties op mobiele en andere platformen (gekenmerkt door hun besturingssysteem) om hun diensten voor gebruikers te ontsluiten. Dit nieuwe koppelvlak is gericht op het ondersteunen van zogenaamde native apps, ofwel platformafhankelijke applicaties, anders dan webapplicaties. Dit verwijst naar verschillende platformen, waaronder mobiele platformen als smartphones en tablets, maar ook andersoortige kanalen, zoals mainframes, client-server applicaties, PC's, laptops, smart devices (zoals een smartwatch), of set-top-boxen.

Marktwerking

Marktwerking is een belangrijk uitgangspunt voor het Afsprakenstelsel Elektronische Toegangsdiensten. Met marktwerking streeft het Afsprakenstelsel Elektronische Toegangsdiensten de volgende doelstellingen na:

Keuzevrijheid

Gebruikers hebben te allen tijde keuzevrijheid om zelf te bepalen welke Middelenuitgever door haar wordt gebruikt. Dienstverleners mogen het gebruik van een specifieke Middelenuitgever niet verplichten noch verbieden. Toegang tot een dienst mag alleen worden geweigerd indien authenticatie met het middel niet tegemoet komt aan de eisen van de Dienstverlener met betrekking tot vanuit het stelsel ondersteunde functionaliteit (bijvoorbeeld een te laag betrouwbaarheidsniveau, of door het ontbreken van een geassocieerd verplicht attribuut of machtiging).

Diversiteit

Het stelsel maakt diversiteit mogelijk en zal actief toezien op beschikbaarheid van middelen voor met name individuen buiten de primaire doelgroep ((lichamelijke) beperkingen, ouderen, digibeten, kinderen, etc.).

Continuïteit

Het stelsel is niet afhankelijk van één Deelnemer. Als er één of meerdere Deelnemers zouden uitvallen, dan komt de continuïteit van de Nederlandse identiteitsinfrastructuur niet in gevaar. Andere partijen kunnen deze dienstverlening eenvoudig overnemen.

Innovatie

Het stelsel blijft ruimte bieden voor innovatie. Het stelsel blijft dankzij marktwerking aantrekkelijk voor nieuwe, innoverende proposities op het gebied van online identificatie. Hiermee wordt voorkomen dat de ontwikkeling stil blijft staan. Deelnemers kunnen binnen de eigen dienstverlening innoveren, maar worden ook de mogelijkheid geboden om innovaties en functionele eisen in het stelsel te brengen.

Betaalbaarheid

Dankzij concurrentie tussen partijen wordt de markt gedwongen om continu naar optimalisatie van hun processen te zoeken. Hiermee wordt voorkomen dat er een onnodig hoge prijs wordt betaald voor online identificatie.

Veiligheid

Het toezicht op het stelsel kan daadkrachtig worden ingezet omdat het zwaarste dwangmiddel - uitsluiting van het stelsel - kan worden toegepast. Dit in tegenstelling tot een éénpartijstelsel, waarbij uitsluiting geen optie is.

Begrippenlijst

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Binnen Elektronische Toegangsdiensten wordt één begrippenlijst gehanteerd. In deze lijst zijn enkelvoudsvormen van zelfstandige naamwoorden en werkwoorden opgenomen. Waar in dit document de werkwoordsvorm van deze zelfstandige naamwoorden wordt gehanteerd, heeft deze dezelfde betekenis als de gedefinieerde zelfstandige naamwoorden.

Afgeschermde kopie WID

Kopie Wettelijk identificatie document (WID) waarbij de bijzondere persoonsgegevens, te weten pasfoto, BSN en nationaliteit, zijn afgeschermd.

Herkomst

Eigen definitie conform Richtsnoeren AP

Afsprakenstelsel (AS)

Het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. procedures en regels aangaande het Netwerk (voor Elektronische Toegangsdiensten) in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd netwerk voor eHerkenning.

Herkomst

Eigen definitie naar analogie van definitie van PKI

Akte

Een getekend geschrift dat een bewijsbestemming heeft. Een akte heeft als bijzondere eigenschap dat deze in een juridische procedure dwingende bewijskracht heeft. Een elektronische vorm hiervan kan een document zijn, getekend met een elektronische handtekening volgens de wet op de elektronische handtekeningen.

(Naar wetboek van burgerlijke rechtsvordering art. 156 lid 1.)

Associatieverklaring

Een elektronisch vastgelegd bericht dat verklaringen verbindt met een Transactiebericht en deze samenstelling niet meer wijzigbaar maakt.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Attribuutcatalogus (AC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle via het netwerk verkrijgbare optionele attributen bevat inclusief de aanduiding waarmee zij opgevraagd kunnen worden.

Zie ook Attribuutcatalogus.

Herkomst

Eigen definitie analoog aan dienstencatalogus

Authenticatie (authenticeren)

De controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau.

Herkomst

Analoog aan KPMG[1], Modinis[2], opdrachtformulering Vraagstuk eHerkenning bedrijven en instellingen d.d. 10-1-2008, NTP Authorization Policy (AP) v1.1. Definitie is tevens analoog aan PKIoverheid[3] alwaar opgemerkt wordt: *In de Wet EH wordt de term "Authentificatie" gebruikt. Het oorspronkelijke Engelstalige woord is "Authentication". In alle technische vakliteratuur wordt dit echter vertaald met "Authenticatie". In dit document wordt dit laatste dan ook gehanteerd.*

Voetnoten:

1. Forum Standaardisatie, Verkenning Authenticatie, KPMG R.2007.ISC.18 (2007)
2. Modinis, Common Terminological Framework for Interoperable Electronic Identity Management (2005)
3. PKIoverheid, Programma van Eisen deel 4: Definities en Afkortingen, versie 2.1, 11 januari 2010

Authenticatiedienst (AD)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte Authenticatiemiddel.

T.o.v. de definitie in Vraagstuk eHerkenning bedrijven en instellingen is hier onderscheid gemaakt in middelenuitgever enerzijds en authenticatiedienst anderzijds.

Authenticatiemiddel

Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.

Herkomst

Analoog aan KPMG

Authenticatieverklaring

Een Verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een Authenticatie (authenticeren) die heeft plaatsgevonden in de context van een bepaalde handeling of dienst.

Herkomst

Eigen definitie

Autorisatie

Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren.

Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie.

Nota bene

Autorisatie is geen synoniem voor machtiging

Herkomst

Analoog aan Modinis / PKI overheid begrippenlijst (2005) waarbij autorisatie overeenkomt met betekenis 1 en toegang verlenen met betekenis 2 / Van Dale Groot woordenboek van de Nederlandse taal 14, maar specifiek gemaakt voor de context van Elektronische Toegangsdiensten. Te vens analoog aan Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os). PKIoverheid hanteert een algemenere definitie die niet in strijd is met bovenstaande.

Autorisatielijst BSN

De Autorisatielijst BSN is de lijst met Dienstverlener (DV)s die geautoriseerd zijn voor ontvangst van het BSN, beschikbaar gesteld en ondertekend door de Beheerorganisatie BSNk. Deze Dienstverlener moet daarvoor minimaal één Dienst hebben waarvoor hij een wettelijke taak uitvoert waarbij een BSN nodig is.

AVG

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

Backend

Een server die via een frontend communiceert. Gebruikers benaderen een backend server niet rechtstreeks. Voorbeelden van backend systemen in ETD zijn:

- De server van een dienstverlener waarmee de gebruiker via een app communiceert.
- De server van een authenticatiedienst waarmee de gebruiker via zijn browser en de authenticatiedienst web-server communiceert.

Wanneer een Deelnemer, Dienstverlener of andere rol een backend implementeert, wordt deze in het Afsprakenstelsel aangeduid met de afkorting van de rol en de toevoeging "-backend", bijvoorbeeld "DV-backend" in het geval van een backend server behorende bij een koppelvlak van een Dienstverlener.

Bedrijf

Een partij die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

- natuurlijk persoon die een onderneming drijft (een eenmanszaak), of
- een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of
- een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener, of
- een natuurlijk persoon die als burger een dienst afneemt van een dienstverlener die gerechtigd is het BSN te gebruiken

Een dienstafnemer is de Gebruiker of wordt vertegenwoordigd door een gebruiker.

Nota bene: In proposities aan bedrijven is het toegestaan de abstracte term “dienstafnemer” concreet te maken en te vervangen door “bedrijf”.

Herkomst

Herkomst: o.a. gebaseerd op Hrw 2007 en BW deel 3, artikel 15d en BAO artikel 47 lid 1.

Beheerorganisatie (BO)

De Beheerorganisatie van het Afsprakenstelsel (AS) die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en het monitoren van de naleving van het Afsprakenstelsel door de Dienstaanbieders (DA) en de Deelnemers in opdracht van de Eigenaar.

Herkomst

Eigen definitie

Betrouwbaarheidsniveau

Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).

Herkomst

Vertaald uit engels van STORK “assurance level” en aangepast aan terminologie afsprakenstelsel.

Er bestaat nog verschil van mening in de werkgroepen over de vertaling van assurance in zekerheid dan wel betrouwbaarheid. Er is gekozen voor betrouwbaarheidsniveaus omdat deze term ook door PKIoverheid gehanteerd wordt, echter zonder daar expliciet te zijn gedefinieerd.

Beveiligingsincident

Een gebeurtenis die een bedreiging vormt of kan vormen voor de betrouwbaarheid, vertrouwelijkheid of beschikbaarheid van een elektronische toegangsdienst en/of een inbreuk op beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Bevoegdheid

Het recht van een persoon om een handeling te verrichten.

Herkomst

Eigen definitie

BSN

Burgerservicenummer: Persoonlijke identificatie van de Nederlandse overheid voor natuurlijke personen.

Herkomst

Gebaseerd op Artikel 1 sub b Wabb: het aan een natuurlijk persoon toegekende nummer. Zie https://wetten.overheid.nl/BWBR0022428/2018-07-28

BSN-domein

Het onderdeel binnen het Publieke domein waarin het BSN bij de interactie gebruikt wordt.

BSNk

Een publieke voorziening, onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, die ten behoeve van Polymorfe pseudonimisering pseudoniemen en Sleutelmateriaal verstrekt.

Bron

Eigen definitie specifiek voor de context van het afsprakenstelsel

BSN koppelregister

Oude benaming voor BSNk.

Certificatie (certificeren)

Een brede (zowel technisch als niet-technisch) evaluatie van de beveiligingseigenschappen van een informatiesysteem of, zoals in het kader van de PKI voor de overheid, een managementsysteem uitgevoerd door een onafhankelijke derde. Certificatie wordt uitgevoerd als een onderdeel van een proces, waarbij wordt nagegaan in welke mate een managementsysteem overeenkomt met een vastgestelde verzameling van eisen (ETSI TS 101 456).

Herkomst

PKIoverheid (en ETSI TS 101 456).

Nota bene: in sommige Europese richtlijnen, waaronder de richtlijn elektronisch handtekening wordt dit als accreditatie aangeduid.

Commissie van Deskundigen (CvD)

Een door de Ministerraad benoemde commissie die de minister van Binnenlandse Zaken adviseert over betreffende toetreding, handhaving en **incidenten**. De Commissie van Deskundigen wordt ondersteund door het Secretariaat van de Commissie van Deskundigen.

Voluit: Commissie van Deskundigen voor het Toezicht op het ETD-stelsel.

Zie **https://zoek.officielebekendmakingen.nl/stcrt-2016-20595.html**

Controle van bevoegdheid

Controle van bevoegdheid zoals deze blijkt uit een in een machtigingenregister geregistreerde vertegenwoordigingsrelatie. Reden van het onderscheid tussen machtiging sec en controle van bevoegdheid is dat de machtiging ook kan bestaan los van het machtigingenregister.

Herkomst

Eigen definitie

Dataminimalisatie

Het zodanig inrichten van een gegevensverwerking dat er zo weinig mogelijk identificerende gegevens bekend hoeven te zijn bij zo weinig mogelijk partijen.

Herkomst

Eigen definitie

Deelnemer

Een partij die conform hetgeen daarover in het Afsprakenstelsel (AS) is vastgelegd één of meer rollen vervult binnen het Netwerk (voor Elektronische Toegangsdiensten). Deelnemers kunnen rollen voor eigen gebruik en/of voor gebruik door derden vervullen.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel

Dienst

Een Dienst is een samenstel van elektronisch aanbod waarvoor Herkenning voorwaardelijk is, onder meer gericht op:

- het tot stand komen van een rechtsbetrekking (het nemen van een besluit of sluiten van een overeenkomst);
- het leveren van een product of besluit;
- het beantwoorden van een informatievraag.

De Dienst wordt aangeboden door een Dienstverlener en opgenomen in de Dienstencatalogus. Een Dienst kan door de Dienstafnemer rechtstreeks bij de Dienstaanbieder worden afgenomen of via een Dienstbemiddelaar. In beide gevallen is sprake van afname van de Dienst.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Dienstaanbieder (DA)

De Dienstaanbieder is een Dienstverlener welke bij Dienstbemiddeling de afgenomen Dienst aanbiedt. De Dienstaanbieder verzorgt de inhoudelijk afhandeling van de Dienst in het achterliggende systeem.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Dienstafnemer

Een partij die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

- natuurlijk persoon die een onderneming drijft (een eenmanszaak), of
- een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of
- een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener, of
- een natuurlijk persoon die als burger een dienst afneemt van een dienstverlener die gerechtigd is het BSN te gebruiken

Een dienstafnemer is de Gebruiker of wordt vertegenwoordigd door een gebruiker.

Nota bene: In proposities aan bedrijven is het toegestaan de abstracte term “dienstafnemer” concreet te maken en te vervangen door “bedrijf”.

Herkomst

Herkomst: o.a. gebaseerd op Hrw 2007 en BW deel 3, artikel 15d en BAO artikel 47 lid 1.

Dienstbemiddelaar (DB)

De Dienstbemiddelaar is een Dienstverlener (DV) die de Dienstafnemer ondersteunt in het afnemen van een digitale Dienst ten behoeve van de Dienstaan bieder (DA) door middel van Dienstbemiddeling. De Dienstbemiddelaar verzorgt bij Dienstbemiddeling de gebruikersinteractie welke het afnemen van de dienst mogelijk maakt.

Sluit u als (SaaS-)leverancier aan namens een Dienstverlener (DV)? Er is sprake van Dienstbemiddeling in de volgende gevallen:

1. U wilt gebruikmaken van uw eigen SSL-certificaat;
2. U kunt geen gebruikmaken van het SSL-certificaat van de dienstverlener;
3. Hetzelfde portaal/dezelfde aansluiting wordt namens meer dan één dienstverlener aangeboden.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Dienstbemiddeling

Dienstbemiddeling is het geautomatiseerd ondersteunen van een Dienstafnemer bij het afnemen van een Dienst. Bij Dienstbemiddeling is er sprake van een technische opdeling in een Dienstbemiddelaar (DB), de gebruikersinterface, en een Dienstaanbieder (DA), het achterliggend systeem. De gebruikersinterface verzorgt de gebruikersinteractie en daarmee de ondersteuning van de Dienstafnemer, het achterliggende systeem de inhoudelijke afhandeling van de Dienst.

Bij Dienstbemiddeling wordt de Dienst afgenomen door de Dienstafnemer.

Sluit u als (SaaS-)leverancier aan namens een Dienstverlener (DV)? Er is sprake van Dienstbemiddeling in de volgende gevallen:

1. U wilt gebruikmaken van uw eigen SSL-certificaat;
2. U kunt geen gebruikmaken van het SSL-certificaat van de dienstverlener;
3. Hetzelfde portaal/dezelfde aansluiting wordt namens meer dan één dienstverlener aangeboden.

Andere voorbeelden van Dienstbemiddeling zijn:

- het helpen indienen van een informatievraag, waarbij de gebruiker van extra uitleg of informatie wordt voorzien.
- geautomatiseerde belastingaangifte vanuit een administratiesysteem.
- het aggregeren van meerdere diensten.
- het ontsluiten van een dienst in een andere gelijkwaardige presentatievorm.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Dienstencatalogus (DC)

Een elektronisch bevraagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat, welke voor het vastleggen van bijzondere machtigingen, dat wil zeggen machtigingen die zich beperken tot bepaalde diensten, minimaal noodzakelijk is.

Zie ook Service catalog.

Herkomst

Eigen definitie

Dienstverlener (DV)

Een Partij die elektronische Diensten aanbiedt aan Gebruikers waarvoor Herkenningsdiensten voorwaardelijk zijn. Dit kan een Dienstaanbieder (DA) of Dienstbemiddelaar (DB) zijn. De Dienstverlener kan binnen Elektronische Toegangsdiensten een Overheidsdienstverlener zijn of een private Partij die diensten aanbiedt.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

eIDAS-berichtenservice (EB)

De eIDAS-berichtenservice (EB) is een component/rol binnen het Netwerk (voor Elektronische Toegangsdiensten) welke Elektronische Toegangsdiensten verbindt met de andere eIDAS-lidstaten en vice versa. Via de eIDAS-berichtenservice worden diensten in Elektronische Toegangsdiensten ontsloten voor gebruikers met een authenticatiemiddel uitgegeven in een andere eIDAS-lidstaat. De eIDAS-berichtenservice ondersteunt alleen web-diensten, geen Native apps.

Voor inkomend eIDAS berichtenverkeer heeft de EB de eTD-rol van Authenticatie Dienst (en mogelijk in de toekomst Machtigings Register).

- Voor uitgaand eIDAS berichtenverkeer acteert de EB als Dienst Verlener, en zelfs als Dienst Bemiddelaar t.o.v. het BRP. In feite fungeert hij als proxy voor de buitenlandse dienstverlener. Hij sluit in deze rol dus aan op een eTD-Herkennings Makelaar.



Waar in het Afsprakenstelsel de term eIDAS Berichtenservice (EB) wordt gebruikt, gaat dit over "inkomend eIDAS Berichtenverkeer" (eIDAS Inbound), indien dit niet verder wordt gespecificeerd.
Waar de rol van de eIDAS Berichtenservice voor eIDAS Outbound wordt bedoeld, wordt dit ook expliciet zo benoemd.

eIDAS-koppelpunt

Het eIDAS-koppelpunt is een actor en publieke voorziening, welke communicatie tussen andere eIDAS-lidstaten en Nederland faciliteert. Het eIDAS-koppelpunt bestaat uit een aantal componenten waarvan alleen de eIDAS-berichtenservice (EB) onderdeel is van het Netwerk (voor Elektronische Toegangsdiensten).

eIDAS-verordening

EU verordening nr. 910/2014 van het Europees Parlement en de Raad (23 juli 2014) en de Uitvoeringsverordening EU 2015/1501 en 2015/1502 (8 september 2015), betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Niet alleen EU-lidstaten implementeren de eIDAS-verordening, daarom wordt er aan implementerende landen gerefereerd met "eIDAS-lidstaten".



De eIDAS-verordening is integraal te lezen op http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&from=EN

Eigenaar

De staatssecretaris van Binnenlandse Zaken die politiek verantwoordelijk is voor de veilige en betrouwbare werking van het Afsprakenstelsel (AS) en als merkeigenaar verantwoordelijk voor de bescherming van het woord- en beeldmerk dat voor het Afsprakenstelsel wordt gebruikt.

Erkende aanbieder eHerkenning

Als een deelnemer is toegetreden tot het Afsprakenstelsel MAG hij de term erkende aanbieder eHerkenning gebruiken.

Europese Economische Ruimte (EER)

De Europese Economische Ruimte (EER) is het product van een akkoord uit 1992 tussen Europese landen uit de Europese Gemeenschap (later Europese Unie) en de Europese Vrijhandelsassociatie. De EER bewerkstelligt vrij verkeer van personen, goederen, diensten en kapitaal in de interne markt van de Europese Unie. De Nederlandse uitvoeringswet ging van kracht op 11 november 1993.



Zie de EER-uitvoeringswet op http://wetten.overheid.nl/BWBR0006249/1996-01-01

Extern verkoopkanaal

Een partij buiten het afsprakenstelsel die namens één of meerdere erkende Leveranciers inlogmiddelen van deze Leverancier(s) verkoopt. Deze partij MAG geen rol hebben en/of activiteiten uitvoeren in het (deel)proces van de rollen waarmee de Deelnemer is toegetreden.

Gebruiker

Een Natuurlijk persoon die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener.

Zie ook Dienstafnemer.

Herkomst

Eigen definitie specifiek voor de context van het Afspraken-stelsel

Geïnformeerde uitdrukkelijke toestemming

De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.

Herkomst

AVG (EU) 2016/679 overweging 32

Gemachtigde

De partij die (op grond van wet of machtiging c.q volmacht) bevoegd is om in naam van de vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde.

Voorzover gemachtigde een natuurlijk persoon is, geldt geen beperking ten aanzien van het voorkomen van niet ingezetenen als gemachtigde. Zo kan ook een buitenlandse natuurlijke persoon gemachtigde zijn.

Herkomst

Artikel 3:60 lid 1 BW; Artikel 2:1 lid 1 AWB.

Gevalideerd attribuut

Een attribuut waarvan de gegevens zijn gecontroleerd aan de hand van gegevens uit een officiële, neutrale en betrouwbare bron.

Herkomst

Eigen definitie.

Geverifieerd attribuut

Een attribuut waarvan de gegevens zijn gecontroleerd aan de hand van gegevens uit een officiële, neutrale en betrouwbare bron.

Herkomst

Eigen definitie.

Handelsregister

Voor in Nederland gevestigde bedrijven is dit de Nederlandse basisregistratie van ondernemingen en rechtspersonen die inschrijfplichtig zijn in Nederland, voor andere EU lidstaten is dat het vergelijkbare openbare register van het betreffende land.

Een overzicht van deze openbare registers is gegeven in BAO bijlage 5.

Herkomst

Eigen definitie o.b.v. Handelsregisterwet 2007

Hergebruik

Hergebruik van authenticatiemiddelen: Het toepassen van eerder voor andere doeleinden en onder eigen voorwaarden uitgegeven authenticatiemiddelen binnen Elektronische Toegangsdiensten op basis van aanmelding van het authenticatiemiddel door de houder ervan.

Herkomst

Eigen definitie

Herkenning

In deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het Netwerk (voor Elektronische Toegangsdiensten) gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken gebruikers.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel. Generalisatie van de begrippen authenticatie, bevoegdheid en wilsuiting.

Herkenningsdiensten

Diensten voor Herkenning, te weten: Authenticatie (authenticeren), controle van Bevoegdheid, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

Herkenningsmakelaar (HM)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners Herkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatie diensten, machtigingenregisters.

Herkomst

Eigen definitie

HSM

Een Hardware Security Module (HSM) is een fysiek apparaat dat bescherming biedt voor de opslag, management en gebruik van cryptografisch materiaal.

Identificatie (identificeren)

Het noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden. In de context van Elektronische Toegangsdiensten gaat het over identificatie van partijen.

Herkomst

Analoog aan KPMG, NTP Authorization Policy (AP) v1.1. Nota bene: definitie van PKIoverheid spreekt van “vaststellen” van de identiteit. De hier gebruikte definitie is preciezer en heeft niet het risico dat vaststellen geassocieerd wordt met authenticeren.

Identificerend kenmerk

Een reeks karakters waarmee iets of iemand (een partij) in een bepaalde context uniek wordt aangeduid. Indien het kenmerk enkel uit cijfers bestaat wordt ook van Identificerend nummer gesproken.

Herkomst

Eigen definitie

Identificerend nummer

Een Identificerend kenmerk dat bestaat uit cijfers

Herkomst

Eigen definitie

Identifier Set

Een Identifier Set is een verzameling identificerende kenmerken die een dienstverlener specificeert per dienst in de Dienstencatalogus (DC). Hierdoor is het mogelijk voor een dienstverlener om meerdere identificerende kenmerken op te vragen.

Identiteit

De volledige maar dynamische set van alle attributen behorende bij een bepaalde entiteit die het mogelijk maakt betreffende entiteit van andere te onderscheiden. Elke entiteit heeft maar één identiteit. De identiteit behoort toe aan de entiteit.

Herkomst

Analoog aan KPMG en Modinis

Identity provider (IdP)

Een vorm van een service provider die identiteitsgegevens aanmaakt, onderhoud en beheert ten behoeve van partijen en hen authenticeert ten behoeve van andere service providers in de context van een federatie.

Herkomst

Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os)

Intermediaire partij

Een partij die bevoegd is te handelen op grond van een aan hem verleende machtiging.

Herkomst

Eigen definitie

Intern pseudoniem

Een Intern Pseudoniem wordt gemaakt door de AD en kan gebruikt worden door de MR om een Specifiek Pseudoniem te maken.

Herkomst

Eigen definitie

Inzageregister (IR)

Het BSNk Inzageregister is een dienst van de Basis Voorziening van het BSNk, met als doel een persoon inzage in de elektronische authenticatiemiddelen en machtigingen die op zijn identiteit zijn uitgegeven

Inzetgebied

Een in het Afsprakenstelsel (AS) erkende groep gebruikers, waarvan het deelnemers vrij staat deze al dan niet te bedienen, welke echter in dat geval conform de in het afsprakenstelsel opgenomen eisen moet worden aangeboden.

Een inzetgebied wordt in technische zin gekenmerkt door één of meer Identificerende kenmerken. Voorbeelden zijn: bedrijven (EntityConcernedID:KvKnr en EntityConcernedID:RSIN), beroepsbeoefenaren of consumenten (EntityConcernedID:Pseudo) .

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel

Ketenmachtiging

Bij een ketenmachtiging geeft een organisatie een Machtiging (machtigen) af aan een Intermediaire partij. Deze intermediair kan vervolgens de machtiging (door)geven aan een medewerker om namens de organisatie te handelen.

Bij een ketenmachtiging verricht de 'laatste schakel' (gebruiker) op basis van de vastgelegde machtigingen een transactie.

Ketenverklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een keten van bevoegdheden die aantoont dat een bepaalde gebruiker een bepaalde vertegenwoordigde dienstafnemer vertegenwoordigt ten behoeve van een bepaalde handeling of dienst op grond van controle van de gehele keten in machtigingenregisters

Herkomst

Eigen definitie

Koppelvlak

Een koppelvlak is de verbinding tussen twee systemen. Om een koppelvlak te realiseren zijn nodig (a) specificaties en (b) implementaties in mensen en middelen. Het Afsprakenstelsel (AS) levert de specificaties (a), het netwerk verzorgt de implementaties (b).

Synoniem met Engelse term 'interface'.

Herkomst

Eigen definitie

Leveranciersoverleg (gremium)

Het leveranciersoverleg is een "voorportaal" van het Tactisch Beraad. Het leveranciersoverleg bestaat uit een afvaardiging van alle deelnemers die in dit overleg gezamenlijke de koers bepalen ten aanzien van:

- de doorontwikkeling van het stelsel
- de beleidsontwikkelingen op het stelsel te bespreken
- voorbereidingen te treffen voor de wettelijke fase.

Merk op dat het leveranciersoverleg geen onderdeel uitmaakt van de formele governance van het eTD stelsel zoals die in het instellingsbesluit is vastgelegd.

Machtiging (machtigen)

Een herroepbare bevoegdheid die een vertegenwoordigde verleent aan een andere partij (de gemachtigde) om in naam van eerstgenoemde rechtshandelingen te verrichten.

Een machtiging kan algemeen of bijzonder zijn. Een bijzondere machtiging is beperkt tot bepaalde rechtshandelingen of een bepaalde relevante omvang ten aanzien van rechtshandelingen.
Machtiging kan worden gezien als synoniem aan volmacht zij het dat de term machtiging voornamelijk in bestuursrechtelijke context wordt gebruikt.

Herkomst

Eigen definitie gebaseerd op Modinis

Machtigingenbeheerder

Een Gebruiker met de bevoegdheid om namens een Dienstafnemer machtigingen te registreren, te schorsen, in te trekken en anderszins bijbehorende registratieprocessen uit te voeren.

Machtigingenregister (MR)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de Gebruiker verstrekken van machtigingsverklaringen).

Herkomst

Eigen definitie

Machtiging-verklaring

Een elektronisch vastgelegde verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een in een geregistreerde machtiging zoals deze gecontroleerd is in een Machtigingen-registerten behoeve van een bepaalde handeling of dienst.

Herkomst

Eigen definitie

Middelenuitgever (MU)

Een vereiste rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het uitgeven van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.

Herkomst

Eigen definitie

Native app

Een native applicatie (Native App) is software die specifiek ontwikkeld en geïmplementeerd is voor een gegeven (mobiel) apparaat of zijn besturingssysteem. Omdat Native Apps zijn geschreven voor een specifiek platform, kunnen ze profiteren van de functies van het besturingssysteem en van andere software die mogelijk op dat platform is geïnstalleerd. Omdat een Native App is gebouwd voor een bepaald apparaat en besturingssysteem, heeft het de mogelijkheid om apparaat-specifieke hardware en software te gebruiken. Dit betekent dat Native Apps kunnen profiteren van de nieuwste technologie die op (mobiele) apparaten beschikbaar komt.

Voorwaardelijk voor native apps voor Elektronische Toegangsdiensten is dat het device over een gebruikersinterface (user interface) beschikt.

Wanneer een Deelnemer, Dienstverlener of andere rol functionaliteit aanbiedt middels een native app, dan wordt de native app aangeduid met de afkorting van de rol gevolgd door de "-app", bijvoorbeeld "DV-app" in het geval van een native app van een Dienstverlener.

Natuurlijk persoon

Een individueel menselijk wezen en subject van rechten en drager van plichten.

Iedere natuurlijk persoon is een persoon in de zin van de hier gegeven definitie van persoon.

Herkomst

Eigen definitie overeenkomstig Catalogus Nieuw Handelsregister

Netwerk (voor Elektronische Toegangsdiensten)

De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel (AS) en gezamenlijk Herkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen Herkenningsmakelaar (HM), Middelenuitgever (MU), Authenticatiedienst (AD), Machtigingenregister (MR) en BSNk, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met dienstverleners en de processen voor uitgifte van middelen, registratie van bevoegdheden en aanmelding voor hergebruik vanuit bedrijven, inclusief de benodigde voorzieningen voor beheer conform het Afsprakenstelsel.

Herkomst

Eigen definitie

Niet natuurlijk persoon

Hetzij een rechtspersoon, hetzij een samenwerkingsverband van natuurlijke personen en/of niet-natuurlijke personen.

Niet iedere niet natuurlijke persoon is een persoon in de zin van de hier gegeven definitie van persoon, samenwerkingsverbanden zijn namelijk verbanden van personen maar zelf geen persoon.

Herkomst

Eigen definitie, overeenkomstig Catalogi Basisregistraties (www.stelselcatalogus.nl)

Onderneming

Een onderneming in de zin van de Handelsregisterwet 2007 of een onderneming conform de voorschriften van een andere EU lidstaat welke ingeschreven is in het handelsregister van betreffende lidstaat.

Herkomst

Handelsregisterwet 2007

Ontvangende Partij

Een Ontvangende Partij (OP) is de beoogde ontvanger van een Bevoegdheidsverklaring met een (specifiek voor deze OP) Versleutelde Identiteit / Versleuteld Pseudoniem (VI@OP of VP@OP) van de Gebruiker.

NB

De Ontvangende Partij ontvangt een specifiek voor hem versleutelde Bevoegdheidsverklaring. De Ontvangende Partij kan onder andere zijn de Dienstverlener, andere Deelnemers, en de eIDAS Berichtenservice.

Engels: relying party

Optioneel te verstrekken attribuut

Een attribuut dat een Deelnemer MAG verstrekken.

Herkomst

Eigen definitie.

Optionele functionaliteit

Een in het Afsprakenstelsel (AS) beschreven dienst of aanvulling op andere dienst waarvan het deelnemers vrij staat deze al dan niet aan te bieden, welke echter indien aangeboden conform de in het afsprakenstelsel opgenomen eisen moet worden aangeboden.

> **Herkomst**
>
> Eigen definitie specifiek voor de context van het afsprakenstelsel

Het betreft de volgende functionaliteiten:

	Herkennings makelaar	Middelen uitgever	Authenticatie dienst	Machtigingen register
eHerkenning				
Bedrijven (G2B, B2B)	O			
Consumenten (B2C)		O	O	
Aanvullende features				
Gevalideerde attributen		O	O	O
Single sign-on			O	

Overeenkomst

De overeenkomst tussen de Dienstafnemer en de Deelnemer, of de overeenkomst tussen de Dienstverlener (DV) en de Deelnemer, op grond waarvan de Deelnemer Herkenningsdiensten verleent en waarop de Gebruiksvoorwaarden van toepassing zijn.

Overheidsdienstverlener

Een Dienstverlener (DV) die onderdeel van de Nederlandse overheid is. Voor zover zaken zowel overheidsdienstverleners als private dienstverleners kunnen betreffen wordt gesproken van “dienstverleners”.

Herkomst

Eigen definitie

Partij

Een persoon of samenwerkingsverband die in de context van Herkenning voorkomt of zou kunnen voorkomen en die zonodig uniek geïdentificeerd en geauthenticeerd kan worden. Voorbeelden van partijen zijn: Deelnemers, dienstverleners, bedrijven, vertegenwoordigden, gemachtigden, …

De term wordt gehanteerd als generalisatie.

Herkomst

Gebaseerd op Identified Entity Party (STORK Glossary and Acronyms v6.0), Principal en System Entity (SAML glossary) en Identifiable Entity (Modinis) en vervolgens specifiek gemaakt voor Afsprakenstelsel Elektronische Toegangsdiensten.

Persistent Pseudoniem

Een persistent Pseudoniem (P) is een pseudoniem op basis van Polymorfe pseudonimisering. Het persistent Pseudoniem kan door een daartoe gerechtigde Ontvangende Partij worden ontsleuteld uit een Versleuteld Pseudoniem door middel van Sleutelmateriaal. Het persistent Pseudoniem is uniek voor die ontvangende partij en kan niet door andere partijen worden gerelateerd aan de oorspronkelijke identiteit op basis van kenmerken van het persistent Pseudoniem alleen.

Het persistent Pseudoniem zoals bedoeld in polymorfe pseudonimisering moet niet worden verward met een pseudoniem in algemene zin.

De in het Afsprakenstelsel gebruikte Engelse vertaling van Pseudoniem is "persistent Pseudonym".

Bron

Eigen definitie specifiek voor de context van het afsprakenstelsel

Polymorfe Identiteit

Een Polymorfe Identiteit (PI) is een specifiek cryptografisch element dat op aanvraag van een Middelenuitgever door het BSNk afgeleid kan worden van een identiteit van de Gebruiker (BSN in geval van het Publiek Domein). Het PI is specifiek voor de aanvragende Middelenuitgever en wordt daarom genoteerd als PI@MU.

Het PI@MU kan gebruikt worden door een Authenticatiedienst om een Gebruiker te authenticeren. Dit kan als de Authenticatiedienst dezelfde partij is als de Middelenuitgever of als een Authenticatiedienst hiervoor speciaal geautoriseerd is door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). In dat geval kan de Authenticatiedienst de PI@MU transformeren naar een Ontvangende Partij specifieke Versleutelde Identiteit (VI@OP).

Een Polymorfe Identiteit verschilt van een Polymorf Pseudoniem in dat een Polymorfe Identiteit kan worden getransformeerd naar een Versleutelde Identiteit waaruit (wanneer hiertoe gerechtigd) wél een BSN kan worden afgeleid; waar een Polymorf Pseudoniemkan worden getransformeerd naar een Versleuteld Pseudoniem waaruit géén BSN kan worden afgeleid, maar een Persistent Pseudoniem.

De in het Afsprakenstelsel gehanteerde Engelse vertaling van Polymorfe Identiteit is "Polymorphic Identity".

Polymorfe pseudonimisering

Een vorm van versleuteling, waarbij specifieke pseudoniemen voor een gebruiker worden gevormd per Ontvangende Partij, zonder dat de vormende partij het specifiek pseudoniem kan herleiden of de identiteit van de gebruiker bij gebruik hoeft te kennen.

Polymorfe pseudonimisering is gebaseerd op cryptografie, waardoor het onder andere de bovengenoemde eigenschappen kan bieden.

Bron

Eigen definitie specifiek voor de context van het afsprakenstelsel

Polymorf Pseudoniem

Een Polymorfe Pseudoniem (PP) is een specifiek cryptografisch element dat op aanvraag van een Middelenuitgever door het BSNk afgeleid wordt van een identiteit van de Gebruiker (BSN in geval van het Publiek Domein). Het PP is specifiek voor de aanvragende Middelenuitgever en wordt daarom genoteerd als PP@MU.

Deze PP@MU wordt gebruikt door een Authenticatiedienst om een Gebruiker te authenticeren. Dit is mogelijk als de Authenticatiedienst dezelfde partij is als de Middelenuitgever of als een Authenticatiedienst hiervoor speciaal geautoriseerd is door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). In dat geval zal de Authenticatiedienst de PP@MU transformeren naar een Ontvangende Partij specifiek Versleuteld Pseudoniem (VP@OP).

Een polymorf pseudoniem verschilt van een Polymorfe Identiteit in dat een polymorf pseudoniem wordt getransformeerd naar een Versleuteld Pseudoniem waaruit géén BSN kan worden afgeleid, maar een Persistent Pseudoniem; waar een polymorfe identiteit kan worden getransformeerd naar een Versleutelde Identiteit waaruit (wanneer hiertoe gerechtigd) wél een BSN kan worden afgeleid.



De in het Afsprakenstelsel gehanteerde Engelse vertaling van Polymorf Pseudoniem is "Polymorphic Pseudonym".

Privépersoon

Een Natuurlijk persoon, echter uitsluitend voor situaties en dienstafnames bij niet-overheidsdienstverleners c.q. in B2C diensten.

Herkomst

Eigen definitie

Pseudoniem

Een arbitrair Identificerend kenmerk dat op basis van een bewerking van een ander identificerend kenmerk wordt geproduceerd op een wijze die steeds hetzelfde pseudoniem oplevert bij hetzelfde kenmerk zonder dat deze laatste herleid kan worden uit het pseudoniem. Er kunnen meerdere pseudoniemen bestaan bij één Identificerend kenmerk, ieder met een eigen werkingsdomein. In dat geval zijn twee pseudoniemen van hetzelfde kenmerk in verschillende domeinen niet aan elkaar te relateren.

Herkomst

Gebaseerd op Modinis

Public Key Infrastructure (PKI)

Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op ‘public key cryptografie’. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Herkomst

PKIoverheid

Publieke domein

Het domein waarbij interacties plaatsvinden tussen natuurlijke personen / niet-natuurlijke personen enerzijds en de Dienstverleners met een publieke taak anderzijds.

Een Dienstverlener is 'publiek' wanneer het een bestuursorgaan in de zin van afdeling 1.1 van de Algemene wet bestuursrecht betreft, maar ook wanneer het andere overheidsorganen alsmede natuurlijke en rechtspersonen, niet zijnde overheidsorganen betreft, die vanwege het uitoefenen van een publieke taak gerechtigd zijn het burgerservicenummer (BSN) te gebruiken

Randomisatie

Het maken van een kopie van een polymorfe vorm (Polymorfe identiteit/pseudoniem, Versleutelde Identiteit/Pseudoniem) dat cryptografisch niet te herleiden is naar het origineel.

Een polymorfe vorm is technisch gezien een ElGamal versleuteld bericht en met randomisatie maakt men een nieuw versleuteld bericht met dezelfde inhoud, maar dat er 'aan de buitenkant' anders uitziet. Voor randomisatie is geen geheime sleutel benodigd.

Omdat randomisaties ook buiten de HSM kunnen worden uitgevoerd, wordt dit in detail gespecificeerd. Een PI, PP, VI en VP bestaan elk uit drie punten op een elliptische curve, (P, Q, S). Bij randomisatie wordt een willekeurig (‘random’) getal r gekozen met 0 < r < q waar q de grootte van de elliptische groep is. De gerandomiseerde vorm is (P + r*S, Q + r*S, S).

Rechtspersoon

Een juridische eenheid en subject van rechten en drager van plichten. Iets is een rechtspersoon op grond van de wet of omdat het conform wettelijke vereisten is ontstaan, een rechtspersoon heeft een bepaalde rechtsvorm.

Scope: Rechtspersonen welke niet in een handelsregister of vergelijkbaar openbaar register van enige EU lidstaat zijn ingeschreven conform de voorschriften van betreffend land vallen buiten de scope van Elektronische Toegangsdiensten.

Herkomst

Definitie conform Catalogus Basisregistraties

Rol

Eén van de verantwoordelijkheden die binnen het Netwerk (voor Elektronische Toegangsdiensten) voorkomt die gezamenlijk met de andere rollen Herkenningsdiensten levert.

Indien rol voorkomt zonder de toevoeging "Netwerk (voor Elektronische Toegangsdiensten)" dan is de term rol algemener bedoeld dan hier gedefinieerd.

Herkomst

Eigen definitie specifiek voor het afsprakenstelsel

Secretariaat van de Commissie van Deskundigen

De Commissie van Deskundigen (CvD) heeft een eigen ambtelijke ondersteuning in de vorm van een secretariaat. Dit secretariaat bereidt dossiers voor en ondersteunt de CvD bij zijn toezichthoudende taken (informeren, toetsen, onderhouden, behandelen, sanctioneren). Het secretariaat is het aanspreekpunt voor de CvD.

Service provider (SP)

Een rol die vervuld wordt door een afgebakend en actief onderdeel van een systeem dat diensten aanbiedt aan partijen of aan andere onderdelen van dat systeem.

Herkomst

Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0 (saml-glossary-2.0-os)

Single Sign On (SSO)

Een functie die wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel (AS), waardoor een authenticatie van een gebruiker wordt hergebruikt, waardoor deze gebruiker niet opnieuw hoeft in te loggen.

Herkomst

Deze definitie komt overeen met de definitie bij DigiD.

Sleutelmateriaal

Er bestaan verschillende soorten cryptografische sleutels, ook wel sleutelmateriaal genoemd. Het Stelsel hanteert sleutels voor beveiliging van communicatie (PKI Overheid certificaten) en sleutels waarmee de polymorfe structuren worden gevormd en ontsleuteld.

Er zijn drie soorten polymorfe sleutels:

- Allereerst zijn er sleutels bij BSNk ten behoeve van activatie, i.e. waarmee Polymorfe Identiteiten en Pseudoniemen worden gevormd.
- Ten tweede zijn er sleutels aanwezig bij Authenticatiedienst**en** of BSNk waarmee transformaties naar Versleutelde Identiteiten en Pseudoniemen kunnen worden uitgevoerd. Voor het merendeel omvat dit gedeelde sleutels.
- Tot slot zijn er sleutels bij Dienstverlener**s**. Hiermee kunnen zij Versleutelde Identiteiten en Pseudoniemen ontsleutelen alsmede de authenticiteit daarvan vaststellen.

De eerste twee categorieën polymorfe sleutels hebben een lange levensduur en worden (daarom) in HSM**s** beheerd. De laatste categorie polymorfe sleutels kunnen relatief eenvoudig worden vervangen en hoeven daarom niet in HSMs te worden beheerd.

Sleutelverstrekkingslijst

Een publiekelijk toegankelijke lijst waarin de Beheerorganisatie BSNk de Dienstverleners publiceert die sleutelmateriaal verkregen hebben van het BSNk Sleutelbeheer

Kan {opnemen} niet aanmaken De pagina die meegerekend moet worden kon niet worden gevonden.

Specifiek pseudoniem

Pseudoniem dat gedurende een langere periode toegepast wordt in een specifiek werkingsdomein. Een dienstverlenerspecifiek pseudoniem is steeds hetzelfde voor dezelfde Dienstverlener (DV) in wiens context het gebruikt wordt, een dienstafnemerspecifiek pseudoniem is steeds hetzelfde voor de context van één dienstafnemer etc.

Herkomst

Eigen definitie

Stamgegeven

Een Identificerend kenmerk (BSN), dat in Polymorfe pseudonimisering wordt gebruikt om een Polymorf Pseudoniem te genereren middels een cryptografische bewerking. Op basis van een stamgegeven kan het BSNk een Polymorf Pseudoniem en Polymorfe Identiteit genereren. Het Stamgegeven kan uit een Polymorfe Identiteit worden afgeleid, uitsluitend door gerechtigde Ontvangende partijen die over het daartoe vereiste Sleutelmateriaal beschikken.

Bron

Eigen definitie specifiek voor de context van het afsprakenstelsel

Status tbv InzageRegister

Een MachtigingsRegister moet de status van elke *'Verzameling van Machtigingen'* (zie AUC3.2 Registreren status machtigingen eenmanszaken) voor een Eenmanszaak in het BSN-domein registeren en daarna actueel houden bij het Inzageregister (IR). Bij de status van de Verzameling van Machtigingen hoort een beschrijving die zinvol is voor de eigenaar van de eenmanszaak.De status van de 'Verzameling van Machtigingen' wordt bij het Inzageregister geregistreerd. De volgende statussen zijn zichtbaar voor de Gebruiker:

- **Activated** zolang er één active machtiging (in de Verzameling van Machtingen) bruikbaar is voor het BSN Domein.
- **Suspended** als de laatste active machtiging (in de Verzameling van Machtingen) niet (meer) actief is in het Publieke domein, bijvoorbeeld omdat de Gebruiker kiest om deze machtiging te de-activeren of omdat het MachtigingsRegister een indicatie heeft dat de machtiging misbruikt wordt.
- **Revoked** als de laatste active machtiging (in de Verzameling van Machtingen) ingetrokken is, bijvoorbeeld omdat de Gebruiker het middel niet meer onder zijn controle heeft (kwijt, gestolen) of als de relatie tussen Gebruiker en het MachtigingsRegister is beëindigd.
- **Expired** als de uiterste gebruiksdatum van de laatste active machtiging (in de Verzameling van Machtingen) verstreken is.

Strategisch Beraad (gremium)

Het strategische overleg inzake de publiek- private samenwerking ten behoeve van Elektronische Toegangsdiensten, waarvoor de beheerorganisatie het secretariaat voert en waarvoor de Eigenaar een onafhankelijke voorzitter benoemt en het Instellingsbesluit besturing Elektronische Toegangsdiensten vaststelt.

Zie ook Strategisch Beraad.

Herkomst

Eigen definitie

Tactisch Beraad (gremium)

Het tactische overleg aangaande beheer van het Afsprakenstelsel, dat wordt georganiseerd door de beheerorganisatie en binnen de grenzen van jaarplan, opdracht van ministerie van Binnenlandse Zaken en in Operationeel handboek vastgelegde procedures de beheerorganisatie tactisch bestuurt.

Zie Tactisch Beraad

Herkomst

Eigen definitie

Toegang verlenen

Een proces onder verantwoordelijkheid van de dienstverlener waarin op grond van door Elektronische Toegangsdiensten verstrekte verklaringen en mogelijke controles van andere relevante toegangsrechten die door de dienstverlener zelf zijn vastgelegd bepaald wordt of een gebruiker toegang krijgt tot een bepaalde dienst of gerechtigd is een bepaalde actie uit te voeren.

Herkomst

Eigen definitie

Toezichthouder

De staatssecretaris van Binnenlandse Zaken.

Als Eigenaar van het afsprakenstelsel voor elektronische toegangsdiensten, is de staatssecretaris van BZK tevens Toezichthouder. Om de rollen van Eigenaar en Toezichthouder zo veel als mogelijk te scheiden, is een Commissie van Deskundigen ingesteld door de Ministerraad.

Transactiebericht

Een set van gegevens in elektronische vorm die betrekking heeft op het gebruik van een Dienst.

Herkomst

Eigen definitie specifiek voor de context van het afsprakenstelsel.

User consent

De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.

Herkomst

AVG (EU) 2016/679 overweging 32

Verklarende Partij

Partij die een Verklaring verstrekt. Wordt in het stelsel ook wel "Attesting party" genoemd

Herkomst

Eigen definitie

Verklaring

Een elektronisch vastgelegd bericht dat gevraagde identiteitsinformatie en attributen bevat conform de koppelvlakspecificaties en waarvoor een bepaalde Deelnemer aantoonbaar instaat.

Afhankelijk van de betreffende identiteitsinformatie wordt gesproken van een authenticatieverklaring, een machtigingsverklaring of een Ketenverklaring. Een verklaring kan andere verklaringen omvatten en voor de aantoonbaarheid vereisen, dan wordt gesproken over een verklaring over x en y waarbij de wijze waarop de verklaringen in elkaar grijpen in detail in de Interface specifications is beschreven.

Herkomst

Eigen definitie

Verplicht te verstrekken attribuut

Een attribuut dat een Deelnemer MOET verstrekken.

Herkomst

Eigen definitie.

Versleutelde Identiteit

De Versleutelde Identiteit (VI) is een specifiek cryptografisch element die door een Authenticatiedienst gemaakt wordt door een Polymorfe Identiteit van een Gebruiker te transformeren voor een specifieke Ontvangende Partij. Omdat de VI specifiek is voor deze beoogde Ontvangende Partij wordt ze genoteerd als (voorbeeld Belastingdienst): VI@Belastingdienst.
Een Authenticatiedienst kan slechts een Middelenuitgever specifiek Polymorfe identiteit (PI@MU) transformeren als hij dezelfde partij is als de Middelenuitgever. In alle andere gevallen moet een Authenticatiedienst speciaal geautoriseerd worden door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). Pas dan kan de Authenticatiedienst de PI@MU transformeren naar een Ontvangende partij specifieke Versleutelde Identiteit (VI@OP). De betreffende Ontvangende Partij kan op zijn beurt deze VI@OP gebruiken om daaruit (met het juiste Sleutelmateriaal) de Gebruiker te identificeren met een originele identiteit (BSN in geval van het Publiek Domein).



De in het Afsprakenstelsel gehanteerde Engelse vertaling van Versleutelde Identiteit is "Encrypted Identity".

Versleuteld Pseudoniem

Een Versleuteld Pseudoniem (VP) is een specifiek cryptografisch element die door een Authenticatiedienst gemaakt wordt door een Polymorf Pseudoniem van een Gebruiker te transformeren voor een specifieke Ontvangende Partij. Omdat de VP specifiek is voor deze beoogde Ontvangende Partij wordt ze genoteerd als (voorbeeld Belastingdienst): VP@Belastingdienst.

Een Authenticatiedienst kan slechts een Middelenuitgever-specifiek Polymorfe Pseudoniem (PP@MU) transformeren als hij dezelfde partij is als de Middelenuitgever. In alle andere gevallen moet een Authenticatiedienst speciaal geautoriseerd worden door de betreffende Middelenuitgever (via "MU - AD affiliation" in de Metadata). Pas dan kan de Authenticatiedienst de PP@MU transformeren naar een Ontvangende partij specifieke Versleuteld Pseudoniem (VP@OP). De betreffende Ontvangende Partij kan op zijn beurt deze VP@OP gebruiken om daaruit (met het juiste Sleutelmateriaal) de Gebruiker te identificeren met een Persistent Pseudoniem.



De in het Afsprakenstelsel gehanteerde Engelse vertaling van Versleutelde Identiteit is "Encrypted Pseudonym".

Vertegenwoordigde

De partij die de vertegenwoordiger de bevoegdheid heeft verleend om in naam van eerstgenoemde te handelen.

Herkomst

Artikel 3:60 lid 1 BW; Analoog aan AP1.1. Zie definitie vertegenwoordiging

Vertegenwoordigde dienstafnemer

Dienstafnemer die niet zelf handelt maar zich laat vertegenwoordigen. De vertegenwoordigde dienstafnemer is de eerste partij in een keten van machtigingen.

Herkomst

Eigen definitie

Vertegenwoordiger

De Partij die bevoegd is om een andere partij (de vertegenwoordigde) te vertegenwoordigen in het verrichten van handelingen met derden.

Herkomst

Zie definitie vertegenwoordiging

Vertegenwoordiging (vertegenwoordigen)

De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde Partij (de Vertegenwoordiger of Gemachtigde) in naam van een andere partij (de Vertegenwoordigde dienstafnemer) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De Bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen.

In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.

Herkomst

Conform juridische toets prof. A. Mohr

Vestiging

Een vestiging is een onderdeel van een Dienstafnemer met een afbakening die in een Handelsregister is opgenomen.

Herkomst

Eigen definitie

Wettelijke vertegenwoordiging

Een Vertegenwoordiging (vertegenwoordigen) die voortvloeit uit de wet zonder dat er sprake is van het toekennen van een volmacht of machtiging door de Vertegenwoordigde.

Voorbeelden zijn: de bestuurder(s) van een Rechtspersoon, de curator, de ouders van een minderjarige.

Herkomst

Eigen definitie

Wettelijk identificatie document (WID)

Een geldig document als bedoeld in Wet ter voorkoming van witwassen en financieren van terrorisme artikel 11, lid 1 en nader gespecificeerd in de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme artikel 4 lid 1.

Dat wil zeggen onder andere een Nederlands of buitenlands paspoort, een Nederlandse identiteitskaart of rijbewijs, een rijbewijs uitgegeven door een andere EU lidstaat en vreemdelingendocumenten, allen mits geldig.

Herkomst

Eigen definitie

Zelfstandige Zonder Personeel (ZZP)

Een ZZP-er is een ondernemer die geen personeel in dienst heeft en zijn Onderneming niet drijft in een samenwerkingsverband of in een rechtspersoon waarin andere personen participeren.

Herkomst

Eigen definitie

Zelfverklaard attribuut

Een attribuut waarvan de gegevens NIET zijn gecontroleerd aan de hand van gegevens uit een officiële, neutrale en betrouwbare bron.

Herkomst

Eigen definitie.

Juridica

Hier vindt u de juridische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: het juridisch kader en de gebruiksvoorwaarden. Deze documenten bevatten informatie over de besturing van Elektronische Toegangsdiensten, de naleving van het afsprakenstelsel, de overeenkomst tussen de beheerorganisatie en de aanbieders en de minimale gebruiksvoorwaarden waaronder de dienstverleners en ondernemers Elektronische Toegangsdiensten mogen gebruiken.Deze categorie bevat de volgende onderdelen:

- Juridisch kader — Beschrijft het juridisch kader, het besturingsmodel en de controle op en monitoring van de naleving van het afsprakenstelsel.
- Gebruiksvoorwaarden Elektronische Toegangsdiensten — Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van Elektronische Toegangsdiensten.

Juridisch kader

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Elektronische Toegangsdiensten is gericht op het leveren van "vertrouwen". Duidelijke juridische kaders dragen daar aan bij evenals een goed georganiseerde besturing gebaseerd op duidelijke rollen en verantwoordelijkheden zoals uitgewerkt in Organen en taakverdeling.

Bovendien zijn de wettelijke eisen aangaande betrouwbaarheid van e-diensten, aangaande identificatie en ondertekening van belang voor het begrip en de uitwerking van de door het Netwerk te leveren Herkenningsdiensten.

Wet- en regelgeving

Het afsprakenstelsel baseert zich op bestaande Europese en Nederlandse wet- en regelgeving. De instelling van de besturing van het afsprakenstelsel elektronische toegangsdiensten is vastgelegd in het Instellingsbesluit Besturing Elektronische Toegangsdiensten.

Het juridisch kader inzake het Afsprakenstelsel Elektronische Toegangsdiensten is, behalve in toepasselijke wet- en regelgeving, verder uitgewerkt in het afsprakenstelsel zelf en de bijbehorende deelnemersovereenkomsten (Template deelnemersovereenkomst) en Gebruiksvoorwaarden Elektronische Toegangsdiensten.

Leeswijzer

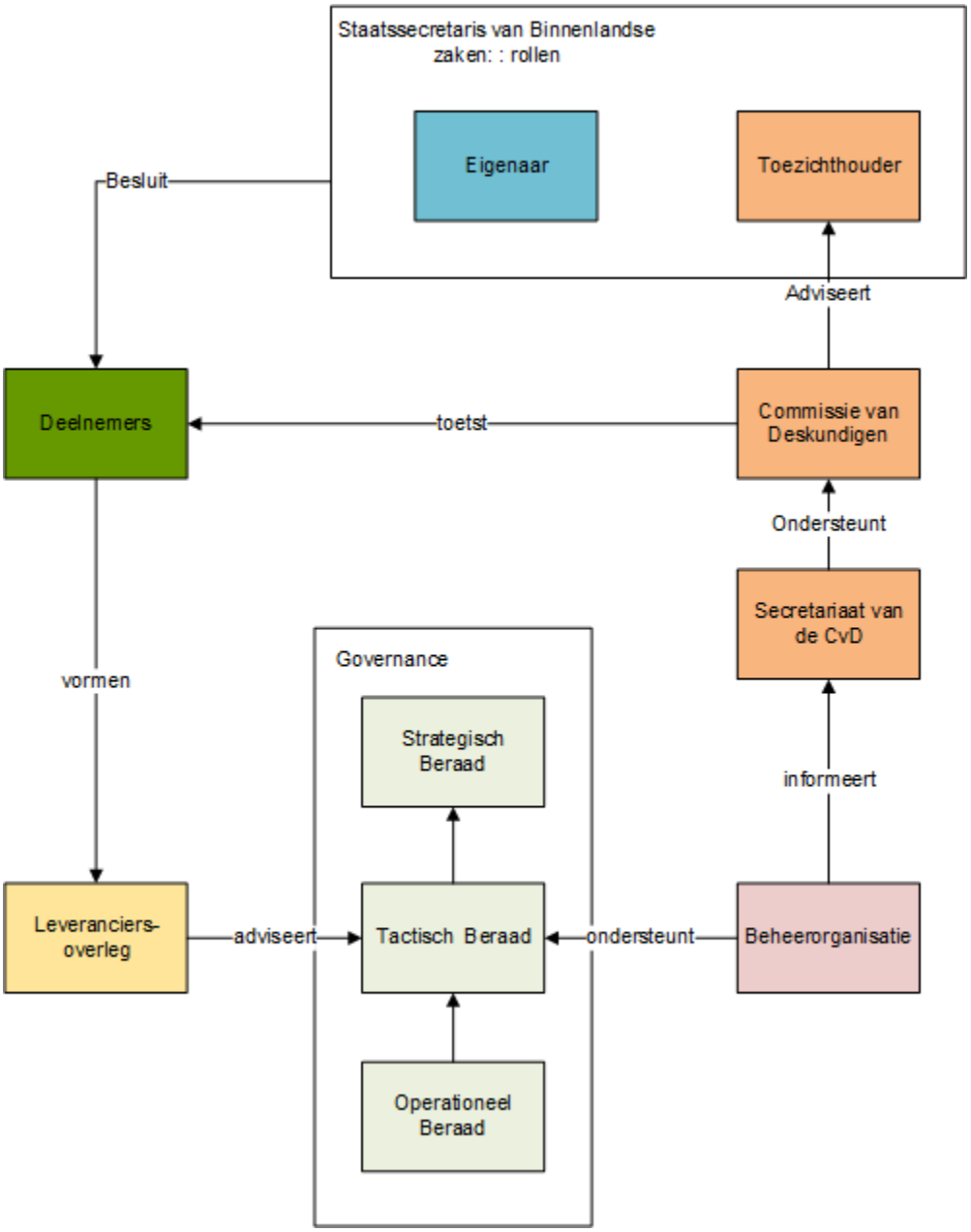
- Aansprakelijkheid — Binnen het afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten binnen de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers mogen en kunnen niet afwijken van deze algemene regels. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval.
- Aanvullende verplichtingen — In aanvulling op de juridisch bindende verplichtingen uit de genoemde documenten (Afsprakenstelsel Elektronische Toegangsdiensten, Template deelnemersovereenkomst en Gebruiksvoorwaarden Elektronische Toegangsdiensten) gelden specifiek nog de onderstaande verplichtingen voor de deelnemers en de dienstverleners
- Betrouwbaarheidsniveaus — Het vaststellen van het voor een bepaalde dienst vereiste Betrouwbaarheidsniveau wordt bepaald door de dienstaanbieder.
- Inrichting toezicht — Een goede naleving van het Afsprakenstelsel is onontbeerlijk voor het vertrouwen in het Netwerk (voor Elektronische Toegangsdiensten). Het toezicht op en het handhaven van de naleving is belegd bij de staatssecretaris van Binnenlandse Zaken die naast de rol van Eigenaar ook de rol van Toezichthouder vervult. De Toezichthouder houdt toezicht op de naleving van stelselafspraken door de Eigenaar, Beheerorganisatie, Deelnemers en BSNk.
- Juridische structuur — Het afsprakenstelsel geldt voor alle partijen die deelnemen aan of gebruik maken van Elektronische Toegangsdiensten. Het afsprakenstelsel is vastgelegd in een aantal documenten. Zie Startpagina voor een opsomming van deze documenten. In al deze documenten kunnen voor een of meer partijen juridisch bindende verplichtingen zijn neergelegd. Vanzelfsprekend moeten alle juridisch bindende verplichtingen door de betreffende partij worden nageleefd.
- Organen en taakverdeling — In de besturing van Elektronische Toegangsdiensten worden drie lagen onderscheiden:
- Samenwerking met externe verkoopkanalen
- Toetredingseisen — Alle deelnemers aan het afsprakenstelsel dienen te voldoen aan de algemene toetredingseisen. De toetredingseisen worden gesteld om een aantal redenen. De belangrijkste daarvan is de wetenschap dat het netwerk alleen goed zal kunnen functioneren als afnemers van diensten voldoende vertrouwen hebben in het afsprakenstelsel. Vertrouwen in het afsprakenstelsel en in de snippet.diensten die in kader van het afsprakenstelsel geleverd worden vereist vertrouwen in de individuele deelnemers. Het afsprake
- Vertegenwoordiging, volmacht en machtiging — Vertegenwoordiging is binnen het afsprakenstelsel zowel op grond van het burgerlijk recht als op grond van het bestuursrecht van belang. De privaatrechtelijke kant doet zich voor bij vertegenwoordiging van rechtspersonen en natuurlijke personen. De publiekrechtelijke kant is van belang bij vertegenwoordiging van bestuursorganen.

Organen en taakverdeling

In de besturing van Elektronische Toegangsdiensten worden drie lagen onderscheiden:

1. Strategisch beheer. Dit omvat o.a. de continuïteit van het afsprakenstelsel, Elektronische Toegangsdiensten als voorziening voor e-diensten van de overheid, het bredere gebruik van Elektronische Toegangsdiensten, het stellen van kaders wat betreft belangrijke wijzigingen en lange termijn doorontwikkeling van het afsprakenstelsel .
2. Tactisch beheer. Dit omvat o.a. het managen van het wijzigingenbeheer van het afsprakenstelsel, indien nodig het managen van incidenten en , de algemene communicatie over Elektronische Toegangsdiensten.
3. Operationeel beheer. Dit omvat het voorbereiden van wijzigingen op het afsprakenstelsel, het in stand houden van de technische voorzieningen van de beheerorganisatie voor dagelijks gebruik van het netwerk en voor testen en conformiteitstoetsen.

Daarnaast is er een Toezichthouder op het afsprakenstelsel. De Toezichthouder beslist over Toetredingen tot het Stelsel en bewaakt het publieke belang van het Stelsel. Om de rollen van eigenaar en toezichthouder zo veel als mogelijk te scheiden, is een Commissie van Deskundigen ingesteld door de Ministerraad. De Commissie van Deskundigen adviseert over te nemen stappen in het kader van toezicht. Hiermee krijgt de minister een onafhankelijk advies over toetredingen en te ondernemen acties in het kader van handhaving en optreden bij incidenten.



Op basis van bovenstaande ordening zijn voor de besturing van Elektronische Toegangsdiensten de in de onderliggende pagina's beschreven organen met bijbehorende verantwoordelijkheden ingericht.

Afvaardiging

De afgevaardigden van de deelnemers, dienstverleners en gebruikers die zitting hebben in het Strategisch Beraad, het Tactisch Beraad of het Operationeel Beraad zijn verantwoordelijk voor een inbreng in de gremia die door hun achterban wordt gedragen. De afgevaardigden leggen de wijze waarop de achterban hun zienswijze naar voren kunnen brengen en vertegenwoordigd willen zien vast in een procedure die voor de achterban duidelijk en toegankelijk is.

Strategisch Beraad

Het Strategisch Beraad is het strategische orgaan. Het Strategisch Beraad is een overleggremium dat tot taak heeft onderwerpen aan de orde te stellen overeenkomstig het door haar opgestelde strategisch meerjarenplan. Ook kunnen onderwerpen worden ingebracht van strategische aard, zoals financiering, doorontwikkeling, vraagstukken van transparantie, toezicht, veiligheid en van internationale aard.

In het Strategisch Beraad zijn Deelnemers, Dienstverleners en Dienstafnemers afgevaardigd.

> In deze afvaardiging wordt aangenomen dat overheidsorganisaties die Elektronische Toegangsdiensten voor G2G gebruiken afgevaardigd zijn via de lijn van de overheidsdienstverleners en dat marktpartijen die Elektronische Toegangsdiensten B2B gebruiken afgevaardigd zijn via de lijn van de dienstafnemers.

> Hiermee wordt het advies van prof. T. Ottervanger opgevolgd die in zijn notitie van 8 april 2011 "Mededingingsrechtelijke beoordeling Afsprakenstelsel v 0.8 eHerkenning" adviseerde dat "De samenstelling van het bestuur (of een ander nog in te richten orgaan dat formeel de leiding heeft in het Afsprakenstelsel)", in casu de opvolger van het kernteam, gewijzigd dient te worden, bijvoorbeeld door onafhankelijke personen of een goede afspiegeling van alle rollen. Dezelfde afspiegeling wordt gehanteerd voor de opvolger van het bestuur van de tijdelijke beheerorganisatie.

In deze afvaardiging wordt aangenomen dat overheidsorganisaties die Elektronische Toegangsdiensten voor G2G gebruiken afgevaardigd zijn via de lijn van de overheidsdienstverleners en dat marktpartijen die Elektronische Toegangsdiensten B2B gebruiken afgevaardigd zijn via de lijn van de dienstafnemers. Hiermee wordt het advies van prof. T. Ottervanger opgevolgd die in zijn notitie van 8 april 2011 "Mededingingsrechtelijke beoordeling Afsprakenstelsel v 0.8 eHerkenning" adviseerde dat "De samenstelling van het bestuur (of een ander nog in te richten orgaan dat formeel de leiding heeft in het Afsprakenstelsel)", in casu de opvolger van het kernteam, gewijzigd dient te worden, bijvoorbeeld door onafhankelijke personen of een goede afspiegeling van alle rollen. Dezelfde afspiegeling wordt gehanteerd voor de opvolger van het bestuur van de tijdelijke beheerorganisatie.

Het Strategisch Beraad kent een onafhankelijke voorzitter. Het Instellingsbesluit Elektronische Toegangsdiensten beschrijft de wijze van afvaardiging, de stemverhoudingen, de positie van de minister en de relatie met de beheerorganisatie. De Eigenaar van benoemt de onafhankelijke voorzitter en stelt het Instellingsbesluit Elektronische Toegangsdiensten vast; daarmee staat zij borg voor de continuïteit van Elektronische Toegangsdiensten. De beheerorganisatie voert het secretariaat van het Strategisch Beraad. Agenda's en vergaderstukken van het Strategisch Beraad worden tijdig bekendgemaakt aan al de in de raad afgevaardigde partijen.

Het Strategisch Beraad is een samenwerkingsverband zonder rechtspersoonlijkheid en is geen bestuursorgaan in de zin van de Awb.

De vergaderstukken van het beraad worden (krachtens art. 9 van het Instellingsbesluit) gepubliceerd op de website van eHerkenning (www.eherkenning.nl) gedurende een periode van 1 jaar. De stukken zijn daarna op te vragen bij de secretaris van het betreffende beraad. De leden worden hierover geïnformeerd.

Tactisch Beraad

Het Tactisch Beraad is een afvaardiging van alle deelnemers, dienstverleners en dienstafnemers en heeft tot taak tactische onderwerpen aan de orde te stellen overeenkomstig het vastgestelde jaarplan.

Daarnaast kunnen ook overige tactische of operationele onderwerpen worden ingebracht zoals veiligheidsincidenten, het beheer van de website en vraagstukken ten aanzien van het wijzigingsproces. Ook ervaringen van eindgebruikers kunnen aan de orde komen. Zonodig kan het Tactisch Beraad (werk)groepen instellen om operationele kwesties uit te werken. De beheerorganisatie voert het secretariaat van het Tactisch Beraad.

De vergaderstukken van het beraad worden (krachtens art. 9 van het Instellingsbesluit) gepubliceerd op de website van eHerkenning (www.eherkenning.nl) gedurende een periode van 1 jaar. De stukken zijn daarna op te vragen bij de secretaris van het betreffende beraad. De leden worden hierover geïnformeerd.

Operationeel Beraad

Het Operationeel Beraad bereidt onder meer wijzigingen van het afsprakenstelsel voor, zogeheten Requests For Change (RFC's). Het Operationeel Beraad brengt advies uit aan het Tactisch Beraad over (de impact van) nieuwe wijzigingen en de (samenstelling van) releases op het netwerk.

De beheerorganisatie voert het secretariaat van het Operationeel Beraad.

De vergaderstukken van het beraad worden (krachtens art. 9 van het Instellingsbesluit) gepubliceerd op de website van eHerkenning (www.eherkenning.nl) gedurende een periode van 1 jaar. De stukken zijn daarna op te vragen bij de secretaris van het betreffende beraad. De leden worden hierover geïnformeerd.

Leveranciersoverleg

Het Leveranciersoverleg heeft tot taak onderwerpen te behandelen rond eHerkenning die een gezamenlijke inspanning of standpunt behoeven vanuit de deelnemers. Hierbij kan gedacht worden aan onderwerpen als het prioriteren van werkzaamheden, het vormen van een gezamenlijk standpunt, het opstellen van een advies richting het Tactisch Beraad en Eigenaar. Het leveranciersoverleg moet gezien worden als een "voorportaal" van het Tactisch Beraad. Doel is om in dit overleg gezamenlijke koers te bepalen ten aanzien van de doorontwikkeling van het stelsel (denk aan de invulling van releases). Ook zal dit overleg het platform zijn om de impact van beleidsontwikkelingen op het stelsel te bespreken en voorbereidingen te treffen voor de wettelijke fase.

Bemensing. Het overleg staat open voor alle deelnemers van het afsprakenstelsel eTD. Deelnemers worden verzocht een gemandateerd persoon uit hun organisatie af te vaardigen;

Frequentie. Het leveranciersoverleg komt maandelijks bijeen.

Mandaat. Het leveranciersoverleg heeft mandaat om onderling besluiten te nemen over onderwerpen die buiten de scope van de governance vallen. In die zin maakt het geen deel uit van de governance zoals die in het instellingsbesluit is vastgelegd. In de andere gevallen kan het leveranciersoverleg het Tactisch Beraad adviseren via de eigen leden.

Voorzitterschap. Leveranciers regelen zelf het voorzitterschap voor dit overleg;

Secretariaat. Logius levert een secretaris voor dit overleg. De secretaris zal geen agendavormende rol spelen zoals bij het Tactisch en Strategisch Beraad het geval is, maar uitsluitend faciliterende werkzaamheden verrichten (organiseren, notuleren);

Vergaderstukken. Het secretariaat stuur de agenda en vergaderstukken uiterlijk 8 werkdagen van tevoren. De vergaderstukken en het verslag van het leveranciersoverleg zijn niet openbaar (en worden niet gepubliceerd op eHerkenning.nl).

Link met Tactisch Beraad. De vertegenwoordigers van de leveranciers in het Tactisch Beraad vormen de linking-pin met dit overleg. Zij koppelen maandelijks terug over hetgeen besproken is.

Rol beheerorganisatie. Een vertegenwoordiger van de beheerorganisatie Logius zal de eerste 3 bijeenkomsten aanwezig zijn om het overleg op gang te helpen. Na deze 3 keer zal gezamenlijk met leveranciers worden geëvalueerd of een verdere rol van Logius in dit overleg gewenst is.

Bekostiging

De bekostiging van de beheerorganisatie inclusief het secretariaat van de besturingsstructuur van Elektronische Toegangsdiensten is onderdeel van de beheeropdracht van de Eigenaar aan Logius.

Inrichting toezicht

Een goede naleving van het Afsprakenstelsel is onontbeerlijk voor het vertrouwen in het Netwerk (voor Elektronische Toegangsdiensten). Het toezicht op en het handhaven van de naleving is belegd bij de staatssecretaris van Binnenlandse Zaken die naast de rol van Eigenaar ook de rol van Toezichthouder vervult. De Toezichthouder houdt toezicht op de naleving van stelselafspraken door de Eigenaar, Beheerorganisatie, Deelnemers en BSNk.

Om de rollen van Eigenaar en Toezichthouder zo veel als mogelijk te scheiden, is een Commissie van Deskundigen (CvD) ingesteld die adviseert over te nemen stappen in het kader van toezicht. Hiermee krijgt de minister een onafhankelijk advies over toetredingen en te ondernemen acties in het kader van handhaving en optreden bij incidenten. De Commissie van Deskundigen wordt bij de uitvoering van haar taken ondersteund door het Secretariaat van de Commissie van Deskundigen.

Toezicht, instandhouding en naleving

Deze paragraaf beschrijft de manier waarop het toezicht op het Afsprakenstelsel is georganiseerd, waarbij de “Commissie van Deskundigen voor het toezicht op het ETD-stelsel (hierna Commissie van Deskundigen genoemd) de Toezichthouder adviseert.

Het Secretariaat van de Commissie van Deskundigen ondersteunt de Commissie van deskundigen in al haar werkzaamheden en is binnen het Afsprakenstelsel het eerste aanspreekpunt voor communicatie met de Toezichthouder.

In het Proces informeren Toezichthouder is een beschrijving opgenomen hoe de informatiestroom richting de Toezichthouder georganiseerd is. Het Proces instandhouding en naleven beschrijft op welke wijze de werking en het vertrouwen in het gehele Afsprakenstelsel is geborgd.

De Toezichthouder

Een goede naleving van het Afsprakenstelsel is onontbeerlijk voor het vertrouwen in het Netwerk (voor Elektronische Toegangsdiensten). Het toezicht op en het handhaven van de naleving is belegd bij de staatssecretaris van Binnenlandse Zaken die naast de rol van Toezichthouder op het Afsprakenstelsel als Eigenaar van het merknaam eHerkenning verantwoordelijk is voor de bescherming van het woord- en beeldmerk dat voor het Afsprakenstelsel wordt gebruikt en als Eigenaar politiek verantwoordelijk is voor de veilige en betrouwbare werking van het Afsprakenstelsel.

De Toezichthouder houdt daarbij toezicht op de naleving van stelselafspraken door de Beheerorganisatie, Deelnemers en het BSNk die betrekking hebben op de veilige en betrouwbare werking van het Afsprakenstelsel.

> Alle partijen binnen het Afsprakenstelsel zijn gehouden aan de AVG en staan derhalve ook onder toezicht van de Autoriteit Persoonsgegevens.

Bevoegdheden van de Toezichthouder

De Toezichthouder heeft de volgende bevoegdheden:

- Het doen van onderzoek en waarheidsvinding ter toetsing van conformiteit met het Afsprakenstelsel;
- het nemen een besluit, in de rol van eigenaar, omtrent toetreding of uittreding van Deelnemers aan het Afsprakenstelsel;
- op basis van een transparant en proportioneel interventiebeleid, interveniëren bij non-conformiteit met het Afsprakenstelsel.

Daarbij bestaan de volgende interventiemogelijkheden:

- Verzoek of aanwijzing om een tekortkoming op te heffen;
- opdracht geven aan een Deelnemer om de dienstverlening of delen daarvan, tijdelijk te schorsen;
- de deelnemersovereenkomst met een Deelnemer te beëindigen;
- een formele waarschuwing geven;
- uitsluiting van pilots en andere nieuwe ontwikkelingen;
- een verbod uitvaardigen om nieuwe gebruikers aan te nemen;
- een verbod uitvaardigen om nieuwe dienstverleners te bedienen;
- opdracht geven aan Deelnemers om:
    a. een uitgegeven authenticatiemiddel in te trekken;
    b. een dienstverlener te schorsen;
    c. een gebruiker te schorsen als gebruiker van een authenticatiemiddel en/of machtiging.

Inzake de uitoefening van deze bevoegdheden wordt de toezichthouder geadviseerd door de Commissie van Deskundigen.

Het Secretariaat van de Commissie van Deskundigen

De Commissie van Deskundigen wordt bij de uitvoering van al haar taken ondersteund door het Secretariaat van de Commissie van Deskundigen.

De werkzaamheden van het Secretariaat van de Commissie van Deskundigen bestaan onder andere uit het op verzoek van de Commissie van Deskundigen:

- verzamelen van informatie met als doel onderzoek en waarheidsvinding betreffende de conformiteit met het Afsprakenstelsel te controleren;
- uitvoeren van aangekondigde en onaangekondigde inspecties met als doel onderzoek en waarheidsvinding betreffende de conformiteit met het Afsprakenstelsel te controleren;
- rapporteren van bevindingen aan de Commissie van Deskundigen;
- geven van (on)gevraagd advies aan de Commissie van Deskundigen;
- overleggen met (externe) auditors en experts;

- samenwerken en afspraken maken voor de Commissie van Deskundigen met toezichthouders zoals bijvoorbeeld de Autoriteit Persoonsgegevens, de Autoriteit Consument en Markt en de Nederlandsche Bank over de uitvoering van het toezicht op de aandachtsgebieden die elkaar raken of overlappen.

Toetsingsmethoden die worden toegepast bij inspecties: dossier reviews, deelwaarnemingen (steekproeven) en interviews.
Toetsingskader: naast vigerende wet- en regelgeving worden de normen en toetsingskaders van het Afsprakenstelsel gehanteerd

Meer lezen?

- Beëindiging van de Deelnemersovereenkomst — Als uiterste sanctie in geval van het niet naleven van het afsprakenstelsel, kan de Eigenaar besluiten om de Deelnemersovereenkomst met de deelnemer te beëindigen, zoals is voorzien in artikel 5.2 van de deelnemersovereenkomst. Het is evident dat deze uiterste sanctie slechts in zeer bijzondere omstandigheden wordt gehanteerd, indien de deelnemer naar het oordeel van de toezichthouder het afsprakenstelsel niet kan of wil naleven.
- Indirect toezicht op de Dienstverlener

Beëindiging van de Deelnemersovereenkomst

Als uiterste sanctie in geval van het niet naleven van het afsprakenstelsel, kan de Eigenaar besluiten om de Deelnemersovereenkomst met de deelnemer te beëindigen, zoals is voorzien in artikel 5.2 van de deelnemersovereenkomst. Het is evident dat deze uiterste sanctie slechts in zeer bijzondere omstandigheden wordt gehanteerd, indien de deelnemer naar het oordeel van de toezichthouder het afsprakenstelsel niet kan of wil naleven.

Hiervan is bijvoorbeeld sprake bij een ernstige schending van het afsprakenstelsel en de Deelnemersovereenkomst, een ernstige schending van de beschikbaarheid, betrouwbaarheid, integriteit en vertrouwelijkheid van Elektronische Toegangsdiensten, een ernstige aantasting van de reputatie en het imago van Elektronische Toegangsdiensten, het niet binnen de gestelde redelijke termijn alsnog in overeenstemming met het afsprakenstelsel handelen of het weigeren een niet-naleving van het afsprakenstelsel ongedaan te maken.



Voorafgaand aan deze sanctie tot beëindiging van de Deelnemersovereenkomst zal de deelnemer/dienstverlener worden geschorst, teneinde een onderzoek door de toezichthouder te laten uitvoeren.

Beëindiging van de Deelnemersovereenkomst heeft tot gevolg dat het de voormalig deelnemer niet meer is toegestaan gebruik te maken van het merk eHerkenning, en het technisch onmogelijk wordt gemaakt om deel te nemen aan het Netwerk.

Indirect toezicht op de Dienstverlener

Een zelfverklaring geeft invulling aan het indirecte toezicht op de Dienstverlener (DV). Deze zelfverklaring wordt door de Dienstverlener aan de Herkenning smakelaar (HM) overlegd bij het aangaan van de Overeenkomst. De Toezichthouder ziet toe op de naleving van de verplichting van de Herkenningsmakelaar in zijn relatie met de Dienstverlener. De Herkenningsmakelaar dient over de volgende bewijsstukken te beschikken:

- positieve testresultaten voor aansluiting DV-HM, en

- de Dienstverleningsovereenkomst HM-DV inclusief Gebruiksvoorwaarden Elektronische Toegangsdiensten, en
- een rechtsgeldig ondertekende zelfverklaring van de Dienstverlener.

Het uitgangspunt is dat de zelfverklaring éénmalig door de Dienstverlener wordt ondertekend, tenzij er sprake is van:

- een wijziging in de juridische entiteit van de Dienstverlener (bijvoorbeeld overname of splitsing) en/of;
- een grote technische wijziging die impact heeft op het Koppelvlak DV-HM en/of;
- nieuwe online diensten van de Dienstverlener en/of;
- een substantiële wijzing aan reeds aangesloten diensten (bijvoorbeeld vernieuwing of herinrichting, gevolgen voor het betrouwbaarheidsniveau) en/of;
- een substantieel wijziging aan infrastructuur die onderliggend is aan de online dienst (uitbesteding aan een andere partij, grootschalige vervangingen van apparatuur).

In bovengenoemde gevallen dient de Dienstverlener opnieuw de zelfverklaring te ondertekenen.

Toetredingseisen

Alle deelnemers aan het afsprakenstelsel dienen te voldoen aan de algemene toetredingseisen. De toetredingseisen worden gesteld om een aantal redenen. De belangrijkste daarvan is de wetenschap dat het netwerk alleen goed zal kunnen functioneren als afnemers van diensten voldoende vertrouwen hebben in het afsprakenstelsel. Vertrouwen in het afsprakenstelsel en in de Herkenningsdiensten die in kader van het afsprakenstelsel geleverd worden vereist vertrouwen in de individuele deelnemers. Het afsprakenstelsel moet dus voorzien in duidelijke inhoudelijke eisen op basis waarvan deelnemers mogen toetreden (en uittreden).

Algemene toetredingseisen

Het is van belang dat de deelnemer identificeerbaar is en kan voldoen aan zijn verplichtingen. Daarvoor is het volgende nodig:

- De deelnemer drijft een onderneming en is ingeschreven in het Nederlandse Handelsregister
- De deelnemer hanteert binnen Elektronische Toegangsdiensten uitsluitend een geregistreerde handelsnaam.
- De deelnemer verkeert niet in staat van faillissement, aan hem is geen surséance van betaling verleend en voor hem geldt geen schuldsaneringsregeling. Ook is ten aanzien van de deelnemer geen faillissement aangevraagd en heeft de deelnemer niet opgehouden zijn schulden te betalen.

Als combinaties van deelnemers willen toetreden dan is dat mogelijk. In dat geval dienen alle deelnemers te voldoen aan de toetredingseisen.

Als een Deelnemer gebruik maakt van derden (denk aan een onderaannemer) bij het vervullen van de rol (MU, AD, MR, HM) dan is de Deelnemer verantwoordelijk dat deze gehele keten voldoet aan de afspraken en verplichtingen genoemd in het stelsel. Indien een Deelnemer gebruik wil maken/ gebruik maakt van derden dan wordt dit gezien als een proceswijziging waarvoor het toetredingsproces voor moet worden doorlopen. De Deelnemer biedt deze diensten (HM, MU, AD, MR) aan op eigen naam en/of label

Let op: Het leveren van diensten als derde bij verkoopactiviteiten van de Deelnemer wordt niet gezien als het ondersteunen van het vervullen van de rol (MU, AD, MR, HM). Voor het gebruik maken van derden bij verkoopactiviteiten gelden de beschreven afspraken onder Samenwerking met externe verkoopkanalen en Eisen communicatie bij samenwerking met externe verkoopkanalen. Het is niet toegestaan dat deze derden een rol vervullen of activiteiten uitvoeren in het (deel)proces van de rollen waarmee de Deelnemer is toegetreden. Als ze dat wel doen dan wordt dat gezien als het ondersteunen als derde (als onderaannemer) in het vervullen van de rol waarvoor het toetredingsproces moet worden doorlopen.

De Deelnemer dient met deze derden (te weten onderaannemers) in een onderlinge overeenkomst afspraken te maken over:

- Exit(plan)
- Eigendom van klant- en loggegevens
- Aansprakelijkheid

Bij wijzigingen/overdracht van derden (te weten onderaannemers) dient de continuïteit van de dienstverlening van de deelnemer te zijn gewaarborgd.

Indien de combinatie onder een gemeenschappelijke naam Herkenningsdiensten wil verrichten, dienen de leden van de combinatie vanaf de start van deelname zodanig samen te werken dat ieder van de combinanten hoofdelijk aansprakelijk is voor de volledige en correcte nakoming van alle verbintenissen jegens de Eigenaar. Alle combinanten dienen te voldoen aan de toetredingseisen. Bij wijziging in de samenstelling van de combinatie moet de toetredingsprocedure voor nieuwe combinanten opnieuw worden doorlopen.

Ter bevordering van de kwaliteit van de dienstverlening, dient bij het leveren van Herkenningsdiensten betrokken personeel voldoende bekwaam te zijn. Daarvoor is het volgende nodig:

De deelnemer heeft op basis van CV's van personeel aangetoond over voldoende opleiding en ervaring te beschikken om aan het afsprakenstelsel te kunnen voldoen, met name op de volgende gebieden: juridisch, techniek, standaarden en het aanbieden van online diensten. Het betreffende personeel hoeft niet in een arbeidsrelatie tot de deelnemer te staan, het gaat erom dat de deelnemer kan aantonen dat het personeel dat bij het leveren van Herkenningsdiensten betrokken is, voldoende opgeleid en ervaren is. Een deelnemer kan op andere wijze invulling geven aan het aantonen van kwalificaties van de mensen waarvan zij gebruik maken die relevant zijn in kader van Elektronische Toegangsdiensten.

Wat betreft de toetredingsprocedure geldt dat:

- De deelnemer de toetredingsprocedure als beschreven in het afsprakenstelsel dient te accepteren en met goed gevolg dient te doorlopen. Het voorafgaand aan de toetreding succesvol doorlopen van de testen van de conformiteit van technische voorzieningen is hier onderdeel van.
- De deelnemer alle processen en procedures die noodzakelijk zijn voor het leveren van Herkenningsdiensten op het gespecificeerde betrouwbaarheidsniveau volledig dient te hebben gedocumenteerd en op te leveren. Wanneer een deelnemer relevante wijzigingen aanbrengt kan het zijn dat onderdelen van de toetredingsprocedure herhaald moeten worden.
- De deelnemer beschikt over de certificaties die expliciet voor het afsprakenstelsel noodzakelijk zijn of die uit toepasselijke wet- en regelgeving volgen.
- De deelnemer de deelnemersovereenkomst dient te ondertekenen en deze volledig dient te accepteren.

Juridische structuur

Het vertrouwen dat partijen in elkaar stellen bij gebruik van het Netwerk (voor Elektronische Toegangsdiensten) is gebaseerd op overeenkomsten die worden gesloten tussen:

1. De Minister van Binnenlandse Zaken en de Deelnemers;
2. De deelnemers en degenen aan wie diensten worden verleend

De samenwerking van partijen is daarbij gebaseerd op de volgende documenten:

1. Afsprakenstelsel Elektronische Toegangsdiensten samen met
2. de Template deelnemersovereenkomst, en
3. de Gebruiksvoorwaarden Elektronische Toegangsdiensten

Het afsprakenstelsel geldt voor alle partijen die deelnemen aan of gebruik maken van Elektronische Toegangsdiensten. Het afsprakenstelsel is vastgelegd in een aantal documenten. Zie Startpagina voor een opsomming van deze documenten. In al deze documenten kunnen voor een of meer partijen juridisch bindende verplichtingen zijn neergelegd. Vanzelfsprekend moeten alle juridisch bindende verplichtingen door de betreffende partij worden nageleefd.De deelnemersovereenkomst bevat de basisafspraken tussen de beheerorganisatie en de deelnemers. Deze overeenkomst is voor alle deelnemers gelijk. Deze overeenkomst zorgt ervoor dat de deelnemers gebonden zijn om de op hen rustende verantwoordelijkheden en verplichtingen zorgvuldig uit te voeren en binden de deelnemers ook aan de besturings- en nalevingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen. Deelnemers mogen alleen Herkenningsdiensten verrichten indien zij deze deelnemersovereenkomst hebben gesloten met de beheerorganisatie.

De gebruiksvoorwaarden zijn van toepassing op alle overeenkomsten die een deelnemer (Middelenuitgever (MU), Authenticatiedienst (AD) of Machtigingen register (MR) sluit met een Dienstafnemer, en op alle overeenkomsten die een deelnemer (Herkenningsmakelaar (HM) sluit met een Dienstverlener (DV). De deelnemers zijn, binnen de kaders van het afsprakenstelsel, vrij om zelf met de dienstafnemers of dienstverleners in een overeenkomst nadere afspraken te maken over de inhoud en de omvang van hun dienstverlening. Een deelnemer dient echter wel altijd de gebruiksvoorwaarden van toepassing te verklaren tussen hem en de dienstafnemer of tussen hem en de dienstverlener, maar in de verdere inrichting van zijn overeenkomst is hij vrij.

Alle bovenstaande relaties zijn privaatrechtelijk van aard.

Rollen en verantwoordelijkheden in relatie tot de Wet bescherming persoonsgegevens

Voor het kunnen verrichten van elektronische toegangsdiensten worden persoonsgegevens verwerkt. Iedere deelnemer is 'verantwoordelijke' in de zin van de Wet bescherming persoonsgegevens voor de verwerking van de persoonsgegevens voor de rol waarvoor hij tot het afsprakenstelsel is toegetreden. Dit houdt in dat de deelnemers ook zelf verantwoordelijk zijn voor de implementatie en de naleving van de voorwaarden die de AVG aan een rechtmatige verwerking van persoonsgegevens stelt. Om ervoor te zorgen dat persoonsgegevens door de partijen binnen het afsprakenstelsel op een eenduidige wijze worden verwerkt en om vragen over rechtmatigheid van deze verwerkingen te voorkomen, zal een Privacybeleid en bijbehorende handreikingen (waaronder verdere duiding van de Meldplicht datalekken) vanuit het stelsel worden opgesteld. Op basis van deze documenten kunnen partijen ook aantonen en wordt ook controleerbaar gemaakt dat partijen persoonsgegevens overeenkomstig het bepaalde in de privacy wet- en regelgeving verwerken.

Naast de rol van 'verantwoordelijke' in de zin van de AVG, zijn de authenticatiedienst en het machtigingsregister ook 'verwerkers' in de zin van de AVG voor de verwerking van het BSN nummer. De authenticatiedienst en het machtigingsregister verwerken het BSN nummer op basis van een vewerkersovereenkomst met de minister van BZK. De Minister van BZK is de verantwoordelijke in de zin van de AVG voor deze verwerking van het BSN nummer door het BSNk. De wettelijke basis voor verwerking van het BSN door het BSNk is belegd in de wet Elektronisch berichtenverkeer Belastingdienst en de daarbij behorende AMvB 1. "De authenticatiedienst en het machtigingsregister zijn verplicht de verwerkingen van persoonsgegevens in hun hoedanigheid als 'verantwoordelijke' en 'verwerker' in de zin van de AVG strikt gescheiden te houden en hun organisaties zijn hier op ingericht.

Toezicht

Het toezicht op het afsprakenstelsel is belegd bij de staatssecretaris van Binnenlandse Zaken.

De reikwijdte van het toezicht omvat:

- de deelnemers;
- de beheerorganisatie;
- de eigenaar;
- de centrale voorzieningen die noodzakelijk zijn om het netwerk van het stelsel van elektronische toegangsdiensten te laten functioneren, waaronder het BSNk;
- de handhavingsverzoeken, meldingen en klachten van Deelnemers, Dienstverleners en Dienstafnemers.

Het toezicht op de gebruikers van het afsprakenstelsel (dienstafnemers en dienstverleners) bestaat uit het indirect toezicht. Dit indirecte toezicht houdt in dat:

- de herkenningsmakelaar de naleving van de stelselafspraken door de dienstverlener controleert;
- de middelenuitgever, de authenticatiedienst, het machtigingenregister en de stelselafspraken met hun dienstafnemers controleren;
- de toezichthouder er op toeziet dat de Deelnemers op afdoende wijze zijn gebruikers controleert op naleving van de stelselafspraken.

Aanvullende verplichtingen

In aanvulling op de juridisch bindende verplichtingen uit de genoemde documenten (Afsprakenstelsel Elektronische Toegangsdiensten, Template deelnemersovereenkomst en Gebruiksvoorwaarden Elektronische Toegangsdiensten) gelden specifiek nog de onderstaande verplichtingen voor de deelnemers en de dienstverleners:

- Informatie - en medewerkingsplicht deelnemer: verstrekking van alle noodzakelijke informatie aan de beheerorganisatie met betrekking tot deelname aan het Netwerk (voor Elektronische Toegangsdiensten) en op eerste verzoek van de toezichthouder het verstrekken van de gevraagde informatie, alsmede desgevraagd zijn medewerking te verlenen aan een onderzoek van de toezichthouder.
- Beveiliging- en auditverplichtingen: De deelnemers en dienstverleners zijn verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en systemen en voldoen aan de auditverplichtingen, conform wet- en regelgeving en zoals vastgelegd in het afsprakenstelsel.
- Intellectuele eigendom: Alle Intellectuele Eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de beheerorganisatie, komen toe aan de beheerorganisatie behoudens hetgeen hierover is bepaald in het document Interface specifications. De deelnemers en dienstverleners dienen zich te onthouden van inbreuken op de Intellectuele Eigendomsrechten van zaken die door, voor of namens de beheerorganisatie zijn ontwikkeld.
- Geheimhouding: Partijen dienen strikte geheimhouding in acht nemen ten aanzien van vertrouwelijke informatie en informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt. Naleving van deze verplichting zal geen vrijwaring van strafrechtelijke vervolging met zich meebrengen.
- Wijziging Gebruiksvoorwaarden Elektronische Toegangsdiensten: De beheerorganisatie is gerechtigd de Gebruiksvoorwaarden te wijzigen nadat deze zijn vastgesteld overeenkomstig de change en release cyclus van Elektronische Toegangsdiensten. Deelnemers communiceren de gewijzigde Gebruiksvoorwaarden Elektronische Toegangsdiensten richting hun klanten.
- Overdraagbaarheid rechten en verplichtingen afsprakenstelsel: Partijen zijn niet bevoegd hun rechten en verplichtingen uit het afsprakenstelsel over te dragen aan een derde, behalve na schriftelijke toestemming van diens wederpartij en voor zover de afspraken neergelegd in het afsprakenstelsel zich niet tegen deze overdracht verzetten. In het geval deelnemer zijn rechten en plichten wil overdragen, dient de overnemende Partij eveneens toegetreden te zijn tot het Netwerk als deelnemer in dezelfde rol en op hetzelfde betrouwbaarheidsniveau.
- Merkenrecht: de staatssecretaris van Binnenlandse Zaken is, om zijn verantwoordelijkheden voor Elektronische Toegangsdiensten waar te kunnen maken, eigenaar van het merkenrecht betreffende het Netwerk. De Staat der Nederlanden is dus eigenaar van het merk eHerkenning. Het merkenrecht is gekoppeld aan toe- en uittreding en daarmee een belangrijk sturingsinstrument voor BZK. In het afsprakenstelsel is een transparante procedure vastgelegd die potentiële deelnemers gelijke kansen biedt rond toetreding. In het afsprakenstelsel is eveneens een procedure voor vrijwillige en onvrijwillige uittreding opgenomen. Bij onvrijwillige uittreding wordt het publieke belang van het stelsel op objectieve en onderbouwde gronden gewogen tegen de belangen van de deelnemer en diens gebruikers. In de praktijk zal BZK deze bevoegdheden niet veelvuldig gebruiken. De governance van het afsprakenstelsel voorziet in procedures die onder meer de normale gang van zaken omtrent toe- en uittreding en uitvoering van het nalevingsbeleid op zich nemen.
- De informatietaak van de beheerorganisatie: publicatie wat conform het afsprakenstelsel verstrekt dient te worden en bescherming van concurrentiegevoelige informatie.
- De informatieplicht van de beheerorganisatie: informatieverstrekking aan de toezichthouder van alle bij de beheerorganisatie aanwezige informatie die de beheerorganisatie in het kader van de uitoefening van haar taken, verantwoordelijkheden en bevoegdheden als beheerorganisatie van het Afsprakenstelsel tot haar beschikking heeft.
- Koppeling met eigen registraties: Wanneer een DV het mogelijk maakt meer dan één Herkenningsmiddel te koppelen aan één account uit de eigen registratie (meervoudige koppeling van middelen), moet voldoende zeker zijn dat elk gekoppeld Herkenningsmiddel dezelfde dienstafnemer betreft. Bijvoorbeeld door tijdens het koppelen van een tweede middel een additionele controle uit te voeren. In het bedrijvendomein kan de DV controleren of tenminste het KvK-nummer overeenkomt met dat uit een eerdere koppeling. In het consumentendomein kan een DV meegeleverde attributen controleren om zekerheid te hebben dat het dezelfde persoon betreft, maar zijn andere controles met vergelijkbare zekerheid ook mogelijk.
    - Is een dergelijke controle niet mogelijk, dan moet bij het koppelen van het tweede middel de eerste koppeling ongedaan worden gemaakt.
    - De DV moet zijn makelaar informeren over eventuele meervoudige koppeling van middelen met een beschrijving van het proces dat zekerheid moet bieden dat het dezelfde dienstafnemer betreft.
- De dienstaanbieder neemt in de dienstencatalogus op dat een of meer van zijn diensten beschikbaar is voor Dienstbemiddeling. Daarbij geeft de dienstaanbieder aan of de betreffende dienst vrij bemiddelbaar is of dat een dienstbemiddelaar alleen wordt toegelaten na voorafgaand akkoord van de dienstaanbieder.
- De dienstaanbieder geeft in de dienstencatalogus aan welk betrouwbaarheidsniveau minimaal vereist is voor de betreffende dienstbemiddelaar.
- De dienstaanbieder staat alleen een dienstbemiddelaar toe om Bemiddelingsdiensten te verrichten indien de dienstbemiddelaar heeft aanvaard dat hij alle verplichtingen moet nakomen die op grond van het afsprakenstelsel op hem rusten en dat hij aansprakelijk is voor zijn eigen handelen en nalaten.
- De herkenningsmakelaar ziet er op toe dat de dienstbemiddelaar alle op hem rustende verplichtingen van het afsprakenstelsel naleeft. Dit betreft onder meer de beveiliging van de verbinding en haar systemen, de website en de koppeling met de dienstaanbieder.

Vertegenwoordiging, volmacht en machtiging

Het Netwerk moet het mogelijk maken om de vertegenwoordigingsbevoegdheid van de Gebruiker te controleren. Vertegenwoordiging (vertegenwoordigen) is de overkoepelende term voor de situatie waarin de ene Natuurlijk persoon (de Vertegenwoordiger) de Bevoegdheid heeft om in naam van een andere persoon (de Vertegenwoordigde) een rechtshandeling te verrichten met het gevolg dat die ander is gebonden door de rechtshandeling.

Vertegenwoordiging is binnen het afsprakenstelsel zowel op grond van het burgerlijk recht als op grond van het bestuursrecht van belang. De privaatrechtelijke kant doet zich voor bij vertegenwoordiging van rechtspersonen en natuurlijke personen. De publiekrechtelijke kant is van belang bij vertegenwoordiging van bestuursorganen.

Voor de wijze waarop een vertegenwoordigingsbevoegde kenbaar maakt namens een ander te handelen bestaan geen vaste vormen. Het Burgerlijk Wetboek legt wel vast dat degene die gevraagd wordt bevoegdheid te vertrouwen (hier: de dienstverlener) een schriftelijke onderbouwing kan vragen of een bevestiging van de vertegenwoordigde. Voor overheidsdienstverleners volgt dit eveneens uit art. 2.1 Algemene Wet Bestuursrecht.

Elektronisch gebruik van vertegenwoordigingsbevoegdheden vereist vastlegging in elektronische vorm. De partij die verantwoordelijk is voor deze registratie is het Machtigingenregister (MR). Deze moet bewijs vastleggen dat de elektronische bevoegdheid is terug te voeren op de wil van de vertegenwoordigde dienstafnemer om zich op die wijze te laten vertegenwoordigen of op wettelijke vertegenwoordiging.

Bij de vastlegging in elektronische vorm wordt de strekking van de vertegenwoordigingsbevoegdheid uitgedrukt in termen van de elektronische diensten die de bevoegde namens de vertegenwoordigde mag uitvoeren. Deze vastlegging is de verantwoordelijkheid van de vertegenwoordigde dienstafnemer. Deze moet de strekking correct opgeven aan het machtigingenregister. Het machtigingenregister controleert dat de strekking niet breder is dan uit het meegeleverde bewijs blijkt. (Naast deze beperking kunnen er nog andere beperkingen aan de strekking bestaan).

Een vertegenwoordigingsbevoegdheid eindigt door herroeping door de vertegenwoordigde of doordat hetzij de vertegenwoordigingsbevoegde, hetzij de vertegenwoordigde overlijdt, opgeheven wordt, onder curatele komt, failliet wordt verklaard of in schuldsanering komt. Dit moet tevens leiden tot beëindiging van iedere elektronische registratie van betreffende vertegenwoordigingsbevoegdheid.

In een machtigingenregister vastgelegde bevoegdheden worden beschouwd als informatie die alleen gedeeld mag worden met de betrokkenen: de vertegenwoordigde, degene die laat registreren en de bevoegde. Verklaringen worden alleen verstrekt voor dienstverleners die de in een bevoegdheid opgenomen dienst aanbieden en in de dienstencatalogus hebben laten registreren.

Privaatrechtelijke vertegenwoordiging

Vertegenwoordigingsbevoegdheid kan ontstaan op grond van de wet of op grond van volmacht. Voorbeelden van vertegenwoordiging op grond van de wet zijn:

- vertegenwoordiging van minderjarigen door ouders of voogd;
- vertegenwoordiging van onder curatele gestelden door een curator;
- vertegenwoordiging van rechtspersonen zoals verenigingen, stichtingen, NV's en BV's, door hun bestuurders;
- vertegenwoordiging door een zaakwaarnemer die andermans belangen waarneemt.

Volmacht is de bevoegdheid die een volmachtgever verleent aan een ander, de gevolmachtigde, om in zijn naam rechtshandelingen te verrichten. Hieronder wordt ook verstaan het in ontvangst nemen van een verklaring. Het gaat erom dat voor de derde duidelijk is dat de gevolmachtigde als vertegenwoordiger voor een ander, namelijk de volmachtgever, optreedt. Met het geven van een volmacht blijft de bevoegdheid van de volmachtgever om zelf te handelen te allen tijde bestaan.

Een volmacht kan uitdrukkelijk of stilzwijgend worden verleend. De wet maakt een onderscheid tussen de algemene volmacht en de bijzondere volmacht. Een rechtshandeling verricht door de gevolmachtigde, binnen de grenzen van zijn volmacht en in naam van de volmachtgever, bindt de volmachtgever. De gevolmachtigde "valt er tussenuit". Juridisch zijn de volmachtgever en de derde aan elkaar gebonden. Indien de gevolmachtigde buiten zijn volmacht handelt, is de volmachtgever toch gebonden indien hij de betreffende rechtshandeling bekrachtigt, of indien er sprake is van de schijn van volmachtverlening, dan wel de schijn van vertegenwoordigingsbevoegdheid. De schijn van volmachtverlening doet zich voor indien een pseudo-gevolmachtigde zonder een toereikende volmacht handelt en de derde op grond van een verklaring of gedraging van de pseudo-volmachtgever heeft aangenomen en onder de gegeven omstandigheden redelijkerwijs mocht aannemen dat er wel een toereikende volmacht was verleend.

Publiekrechtelijke vertegenwoordiging

De Machtiging (machtigen) heeft de volgende juridische achtergrond. In bestuursrechtelijke verhoudingen kan een ieder zich ter behartiging van zijn belangen in het verkeer met bestuursorganen:

- laten bijstaan; of
- door een gemachtigde laten vertegenwoordigen.

Door te spreken van machtiging in plaats van volmacht wenst de wetgever aan te geven dat de regeling van volmacht niet rechtstreeks van toepassing is maar alleen "voor zover de aard van de rechtshandeling of de rechtsbetrekking zich daartegen niet verzet". In de documentatie van Elektronische Toegangsdiensten wordt de term machtiging ook in meer algemene zin gebruikt wanneer vertegenwoordigingsbevoegdheid bedoeld is.

Ketenmachtiging (recht op substitutie)

Bij ketenmachtigingen gaat het om het doorgeven van een volmacht. Dit wordt ook het recht op substitutie genoemd. Het uitgangspunt van het recht op substitutie is dat dit recht expliciet door de volmachtgever aan de gemachtigde moet worden verleend. Vervolgens kan de gemachtigde, op grond van dit recht op substitutie, de volmacht doorgeven. De substituut volmacht kan zowel aan een natuurlijk persoon als aan een onderneming of rechtspersoon worden verleend. De volmachtgever dient in de volmacht aan de gevolmachtigde op te nemen of de gevolmachtigde al dan niet met toestemming van de volmachtgever de volmacht aan een ander (substituut volmacht) mag verlenen.

Een ander uitgangspunt bij het recht op substitutie is dat de volmachtgever tenminste op de hoogte moet worden gesteld in het geval substitutie plaatsvindt zodat hij kan bepalen of hij de vertegenwoordigingsbevoegd van de substituut gevolmachtigde wil handhaven.

Dit uitgangspunt geldt o.m. niet voor de bevoegde die zijn werknemer inzet om de aan hem verleende bevoegdheden te gebruiken. Verder kan in een overeenkomst door een vertegenwoordigde "anders bepaald" worden.

Een vertegenwoordigde weet dus wie namens hem zou kunnen handelen, met uitzondering mogelijk van de laatste schakel, indien dit een werknemer is van de één na laatste bevoegde. Andersom wordt er van uitgegaan dat degene die als bevoegde optreedt dit met een helder doel voor ogen doet, namelijk het realiseren van een rechtshandeling voor de vertegenwoordigde, derhalve kan er van uitgegaan worden dat deze de hele keten naar zich toe kent.

In een keten van vertegenwoordiging kent eenieder de keten "boven" hem. Ieder kent ook degene aan wie hij zelf een bevoegdheid heeft verleend op grond van substitutie. De vertegenwoordigde tenslotte kent de hele keten, met uitzondering van de laatste schakel indien dit een werknemer van de bevoegde betreft en voorzover niet anders bepaald bij overeenkomst.

De vertegenwoordigde moet een bevoegdheid en een verleend recht van substitutie te allen tijde kunnen intrekken. Eveneens moet een bevoegde die substitutie heeft verleend deze kunnen intrekken. Derhalve moet een geregistreerde bevoegdheid te allen tijde kunnen worden ingetrokken door degene die daartoe gerechtigd is.

Evenals bij een volmacht blijft bij een substituut volmacht, de volmachtgever bevoegd de rechtshandelingen waarvoor volmacht is verleend te verrichten, De bevoegdheid om zelf te handelen blijft ook voor de gemachtigde bestaan. Dit is slechts anders als tussen partijen is overeengekomen, bijvoorbeeld in een overeenkomst tot lastgeving, dat de volmachtgever voor de duur van die overeenkomst zelf niet meer bevoegd is de betreffende rechtshandelingen te verrichten.

Het is mogelijk het recht van substitutie ook van toepassing te verklaren op vormen van vertegenwoordiging die niet voortvloeien uit volmacht, zoals machtigingen voor publiekrechtelijke taken of mandatering binnen een overheidsorganisatie. Door voor het publiekrechtelijke domein te spreken van machtiging in plaats van volmacht, wenst de wetgever aan te geven dat de regeling van volmacht niet rechtstreeks van toepassing is maar alleen "voor zover de aard van de rechtshandeling of de rechtsbetrekking zich daartegen niet verzet". Zie ook artikel 3:79 BW. Een dergelijke beperking kan bijvoorbeeld zijn gelegen in specifieke wet en regelgeving voor een overheidsdienstverleners.

Aansprakelijkheid

Binnen het afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten binnen de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers mogen en kunnen niet afwijken van deze algemene regels. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval.
De deelnemer kan zijn aansprakelijkheid beperken in de overeenkomst die hij sluit met een dienstafnemer of met een dienstverlener. Daarbij blijft hij gebonden aan de algemene regels van het Nederlandse recht inzake aansprakelijkheid en schadevergoeding.

Weliswaar is BSNkgeen deelnemer van het afsprakenstelsel, BSNk speelt wel een essentiële rol binnen het netwerk van het afsprakenstelsel in het BSN domein. Ook voor BSNk geldt dat zij aansprakelijk is voor haar eigen handelen en/of nalaten binnen de rol die zij vervult. Ook de dienstbemiddelaar is aansprakelijk voor zijn eigen handelen en/of nalaten.

Weliswaar is de eIDAS-berichtenservice (EB) geen Deelnemer van het afsprakenstelsel, de eIDAS-berichtenservice speelt wel een essentiële rol binnen het netwerk van het afsprakenstelsel. De eIDAS-berichtenservice valt onder de ministeriële verantwoordelijkheid van de staatssecretaris van Binnenlandse Zaken. Dit houdt in dat de staatssecretaris van Binnenlandse Zaken ook aansprakelijk is voor handelen en/of nalaten van de rol van de eIDAS-berichtenservice.

Betrouwbaarheidsniveaus

Het vaststellen van het voor een bepaalde dienst vereiste Betrouwbaarheidsniveau wordt bepaald door de dienstaanbieder.

Indien de dienstaanbieder voor (een van) zijn diensten het BSN specificeert (=urn:etoegang:1.12:EntityConcernedID:BSN), dan geldt de regel dat deze dienst minimaal het betrouwbaarheidsniveau substantieel moet uitvragen.

Dit om te voorkomen dat een grote onderneming minder drempels heeft om in te loggen in vergelijking met een zelfstandige onderneming.

Dit geldt zowel voor een publiek- als een privaatrechtelijke dienstaanbieder. De overheidsdienstaanbieder moet ter naleving van de Awb invulling geven aan de norm van een betrouwbare en vertrouwelijke communicatie.

De dienstaanbieder zal dus steeds bij het aanbieden van een dienst een risicoanalyse moeten uitvoeren en na moeten gaan welke maatregelen moeten worden genomen om de elektronische communicatie voldoende betrouwbaar en vertrouwelijk te laten plaatsvinden. Onderdeel hiervan is een keuze voor het vereiste betrouwbaarheidsniveau voor een bepaalde dienst waarvoor Herkenningsdiensten worden gebruikt. Naast het vaststellen van het door de dien staanbieder gekozen betrouwbaarheidsniveau zal de overheidsdienstaanbieder nog andere maatregelen moeten nemen om een dienst conform de vereisten van de Awb betrouwbaar elektronisch aan te bieden. De extra te treffen maatregelen zijn afhankelijk van het betrouwbaarheidsniveau.

Waar Elektronische Toegangsdiensten wordt toegepast voor e-diensten buiten de overheid (B2B en B2C) gelden de specifieke Awb eisen uiteraard niet. In geval van B2B en B2C diensten geldt dat middelenuitgevers, machtigingenregisters en ook de betreffende dienstverleners een "dienst van de informatiemaatschappij" en/of een zogenaamde 'dienst op afstand' (als gedefinieerd in het Burgerlijk Wetboek) aanbieden. Deze partijen zijn zelf verantwoordelijk om aan de daarbij behorende informatieplichten en plichten ten aanzien van de totstandkoming van een rechtsgeldige overeenkomst, zoals opgenomen in het Burgerlijk Wetboek, te voldoen.

Samenwerking met externe verkoopkanalen

De Deelnemer MAG samenwerken met externe, niet-toegetreden, partijen voor de verkoop van zijn eHerkenningsmiddelen. Het gaat hierbij om niet-toegetreden partijen die (een deel van) het verkoopproces voor de Deelnemer uitvoeren en daarbij geen rol hebben en/of activiteiten uitvoeren in het (deel) proces van de rollen waarmee de Deelnemer is toegetreden

De Deelnemer MOET zich daarbij houden aan de volgende afspraken:

- De Deelnemer blijft eindverantwoordelijk voor de uitgifte van de middelen, of andere taken die zijn voorbehouden aan de Deelnemer (juridisch, technisch, procedureel e.d.);
- De Deelnemer blijft verantwoordelijk voor het voldoen aan de eisen in het Afsprakenstelsel, o.a. t.a.v. incidenten, privacy, beveiliging, vraag- en klachtafhandeling;
- De Deelnemer MOET erop toezien dat het externe verkoopkanaal waarmee zij samenwerkt de eisen t.a.v. samenwerking met externe verkoopkanalen naleeft;
- De Deelnemer ziet er op toe dat het verkoopkanaal waarmee samengewerkt wordt, het vertrouwen in en de goede naam van eHerkenning niet beschadigd;
- De Deelnemer MOET afspraken over de samenwerking vastleggen in een overeenkomst met het externe verkoopkanaal;
- De Deelnemer MOET in de overeenkomst met deze partij in ieder geval afspraken maken over:
    - Eigendom van klant- en loggegevens;
    - Naleving Afsprakenstelsel;
    - Wijze van communiceren;
    - Beëindiging van de overeenkomst (incl. opzegtermijn en recht op schade) indien de externe verkoper zich niet houdt aan de afspraken.

Meldplicht

De Deelnemer MOET de intentie om samen te gaan werken met een extern verkoopkanaal voor de Nederlandse markt melden bij het Secretariaat van de Commissie van Deskundigen en de volgend informatie aanleveren:

- De statutaire naam en kvk-nummer van de externe partij waarmee de partij is ingeschreven in het Nederlands handelsregister;
- De domeinnaam/-namen en handelsnaam/ -namen die de externe verkoper beoogd te gebruiken in het verkoopproces;
- Een zelfverklaring waarmee de Deelnemer verklaart dat de samenwerking met de externe verkoper voldoet aan de eisen uit het Afsprakenstelsel en aan de eisen ten aanzien van communicatie bij samenwerking met externe verkoopkanalen.
- het samenwerkingscontract

Nadat het Secretariaat van de Commissie van Deskundigen de wijze van samenwerking heeft beoordeeld meldt de Deelnemer de samenwerking met specifieke externe verkoopkanalen bij de Beheerorganisatie.

Gebruiksvoorwaarden Elektronische Toegangsdiensten

Gebruikersvoorwaarden				
Versie	G1.7		Geldig vanaf versie van het AS	1.13p

Deze Gebruiksvoorwaarden zijn van toepassing op het verlenen van diensten door Deelnemers aan Dienstverleners en Dienstafnemers in het kader van Elektronische Toegangsdiensten.

- Artikel 1. Definities
- Artikel 2. Toepassingsgebied
- Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname
- Artikel 4. Beperking van aansprakelijkheid
- Artikel 5. Geheimhouding
- Artikel 6. Achterhalen netwerkfalen
- Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst
- Artikel 8. Toepasselijk recht
- Verplichtingen voor de Dienstafnemer
    - Artikel 10. Dienstafnemer
    - Artikel 11. Beveiligingsverplichting van de Dienstafnemer
    - Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen
    - Artikel 13. Vervulling rol(len) door de Dienstafnemer
- Verplichtingen van de Dienstverlener
    - Artikel 14. Vaststellen openstellingsbesluit
    - Artikel 15. Melding onregelmatigheden
    - Artikel 16. Beveiliging dienstverlener
    - Artikel 17. SSO
- Artikel 18. Beveiliging
- Artikel 19. Betrouwbaarheidsniveaus
- Artikel 20. Informatieverplichting
- Artikel 21. Privacy
- Artikel 22. Cookies
- Artikel 23. Toezicht

Artikel 1. Definities

Alle in deze Gebruiksvoorwaarden met een hoofdletter geschreven begrippen hebben de volgende betekenis.

Afsprakenstelsel (AS)

Het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. procedures en regels aangaande het Netwerk (voor Elektronische Toegangsdiensten) in een bepaalde vastgestelde versie. Het doel is betrouwbare authenticatie en verstrekking van identiteitsinformatie op basis van de eHerkenningsdiensten van een goed gereguleerd netwerk voor eHerkenning.

Authenticatiedienst (AD)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het authenticeren van natuurlijke personen op basis van het door de natuurlijk persoon gebruikte Authenticatiemiddel.

Authenticatiemiddel

Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.

Beheerorganisatie (BO)

De Beheerorganisatie van het Afsprakenstelsel (AS) die verantwoordelijk is voor het faciliteren van het beheer en de doorontwikkeling van het Afsprakenstelsel, alsmede de controle op en het monitoren van de naleving van het Afsprakenstelsel door de Dienstaanbieders (DA) en de Deelnemers in opdracht van de Eigenaar.

Betrouwbaarheidsniveau

Een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie / identiteitsclaim, bevoegdheid, controle van bevoegdheid of wilsuiting dat wordt gevormd door een samenhangend geheel van factoren, waar van toepassing bestaande uit: de sterkte van de voorafgaande registratie, identificatie, authenticatie en uitgifte; de sterkte van het middel zelf en het gebruik van het middel (het authenticatiemechanisme).

Beveiligingsincident

Een gebeurtenis die een bedreiging vormt of kan vormen voor de betrouwbaarheid, vertrouwelijkheid of beschikbaarheid van een elektronische toegangsdienst en/of een inbreuk op beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Deelnemer

Een partij die conform hetgeen daarover in het Afsprakenstelsel (AS) is vastgelegd één of meer rollen vervult binnen het Netwerk (voor Elektronische Toegangsdiensten). Deelnemers kunnen rollen voor eigen gebruik en/of voor gebruik door derden vervullen.

Herkenning

In deze context wordt onder (electronische) herkenning verstaan: ieder van de functies van het Netwerk (voor Elektronische Toegangsdiensten) gericht op het handhaven en controleren van vertrouwen aangaande identiteiten, machtigingen, wilsuitingen en bevoegdheden in relaties of transacties tussen dienstverleners en bedrijven en de daarin betrokken gebruikers.

Herkenningsdiensten

Diensten voor Herkenning, te weten: Authenticatie (authenticeren), controle van Bevoegdheid, vastlegging van een wilsuiting en de daarbij benodigde identificaties en garanties voor onweerlegbaarheid evenals de daartoe benodigde registratieprocessen.

Herkenningsmakelaar (HM)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die het single point of contact vormt waarlangs dienstverleners Herkenningsdiensten afnemen, die de verantwoordelijkheid heeft om het berichtenverkeer van en naar de dienstverleners te ontkoppelen van de interne berichten binnen het netwerk en die optreedt als routeerder naar alle deelnemende authenticatiediensten, machtigingenregisters.

Machtigingenbeheerder

Een Gebruiker met de bevoegdheid om namens een Dienstafnemer machtigingen te registreren, te schorsen, in te trekken en anderszins bijbehorende registratieprocessen uit te voeren.

Machtigingenregister (MR)

Een vereiste Rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het registreren, beheren, controleren van machtigingen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden (c.q. het op verzoek van de Gebruiker verstrekken van machtigingsverklaringen).

Middelenuitgever (MU)

Een vereiste rol binnen het Netwerk (voor Elektronische Toegangsdiensten) die door een Deelnemer aan het Afsprakenstelsel (AS) wordt ingevuld en die de verantwoordelijkheid heeft voor het uitgeven van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.

Dienstafnemer

Een partij die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener. De dienstafnemer is een partij van de vorm

- natuurlijk persoon die een onderneming drijft (een eenmanszaak), of
- een niet natuurlijk persoon conform de identificatie waarmee het is ingeschreven in het Nederlandse handelsregister of in een vergelijkbaar buitenlands openbaar register conform de voorschriften van het betreffende land, of
- een natuurlijk persoon die als privépersoon een dienst afneemt van een dienstverlener, of
- een natuurlijk persoon die als burger een dienst afneemt van een dienstverlener die gerechtigd is het BSN te gebruiken

Een dienstafnemer is de Gebruiker of wordt vertegenwoordigd door een gebruiker.

Nota bene: In proposities aan bedrijven is het toegestaan de abstracte term “dienstafnemer” concreet te maken en te vervangen door “bedrijf”.

Eigenaar

De staatssecretaris van Binnenlandse Zaken die politiek verantwoordelijk is voor de veilige en betrouwbare werking van het Afsprakenstelsel (AS) en als merkeigenaar verantwoordelijk voor de bescherming van het woord- en beeldmerk dat voor het Afsprakenstelsel wordt gebruikt.

Gebruiker

Een Natuurlijk persoon die Elektronische Toegangsdiensten gebruikt om een dienst af te nemen bij een dienstverlener.
Zie ook Dienstafnemer.

Gebruiksvoorwaarden

Deze gebruiksvoorwaarden

Gemachtigde

De partij die (op grond van wet of machtiging c.q volmacht) bevoegd is om in naam van de vertegenwoordigde bepaalde handelingen te verrichten waarvan de rechtsgevolgen worden toegerekend aan de vertegenwoordigde.
Voorzover gemachtigde een natuurlijk persoon is, geldt geen beperking ten aanzien van het voorkomen van niet ingezetenen als gemachtigde. Zo kan ook een buitenlandse natuurlijke persoon gemachtigde zijn.

Netwerk (voor Elektronische Toegangsdiensten)

De verzameling onderling verbonden componenten die gereguleerd worden door het Afsprakenstelsel (AS) en gezamenlijk Herkenningsdiensten leveren en daartoe bestaan uit tenminste één invulling door een Deelnemer van de rollen Herkenningsmakelaar (HM), Middelenuitgever (MU), Authenticatiedienst (AD), Machtigingenregister (MR) en BSNk, hun onderlinge verbindingen, de verbindingen tot en met het koppelvlak met dienstverleners en de processen voor uitgifte van middelen, registratie van bevoegdheden en aanmelding voor hergebruik vanuit bedrijven, inclusief de benodigde voorzieningen voor beheer conform het Afsprakenstelsel.

Overeenkomst

De overeenkomst tussen de Dienstafnemer en de Deelnemer, of de overeenkomst tussen de Dienstverlener (DV) en de Deelnemer, op grond waarvan de Deelnemer Herkenningsdiensten verleent en waarop de Gebruiksvoorwaarden van toepassing zijn.

Partij

Een persoon of samenwerkingsverband die in de context van Herkenning voorkomt of zou kunnen voorkomen en die zonodig uniek geïdentificeerd en geauthenticeerd kan worden. Voorbeelden van partijen zijn: Deelnemers, dienstverleners, bedrijven, vertegenwoordigden, gemachtigden, …

De term wordt gehanteerd als generalisatie.

Single Sign On (SSO)

Een functie die wordt gefaciliteerd zoals omschreven in het Afsprakenstelsel (AS), waardoor een authenticatie van een gebruiker wordt hergebruikt, waardoor deze gebruiker niet opnieuw hoeft in te loggen.

Toezichthouder

De staatssecretaris van Binnenlandse Zaken.
Als Eigenaar van het afsprakenstelsel voor elektronische toegangsdiensten, is de staatssecretaris van BZK tevens Toezichthouder. Om de rollen van Eigenaar en Toezichthouder zo veel als mogelijk te scheiden, is een Commissie van Deskundigen ingesteld door de Ministerraad.

Artikel 2. Toepassingsgebied

De Deelnemer dient deze Gebruiksvoorwaarden van toepassing te verklaren op de Overeenkomst die de Dienstafnemer en de Dienstverlener in het kader van het Netwerk voor Elektronische Toegangsdiensten sluiten met een Deelnemer.

Een Deelnemer kan één of meer van de volgende rollen vervullen.

- De Middelenuitgever geeft authenticatiemiddelen uit en identificeert natuurlijke personen.
- De Authenticatiedienst authenticeert personen.
- Het Machtigingenregister faciliteert het registreren, onderhouden en controleren van machtigingen.
- De Herkenningsmakelaar vervult een routeer- en navigeerfunctie en vormt het koppelpunt tussen het Netwerk voor Elektronische Toegangsdiensten en de Dienstverleners.

Artikel 3. Tussentijdse beëindiging van de Overeenkomst door beëindiging deelname

De Overeenkomst eindigt van rechtswege indien en zodra de deelname van de Deelnemer aan het Afsprakenstelsel Elektronische Toegangsdiensten eindigt. De Deelnemer stelt de Dienstafnemer en/of de Dienstverlener met wie de Deelnemer een Overeenkomst is aangegaan, door middel van een aangetekende brief direct op de hoogte van deze beëindiging.

Indien de in dit artikel bedoelde tussentijdse beëindiging zich voordoet, is de Deelnemer verplicht alle medewerking te verlenen om de continuïteit van de verlening van Elektronische Toegangsdiensten door andere Deelnemers zeker te stellen.

Artikel 4. Beperking van aansprakelijkheid

De aansprakelijkheid van een Partij jegens de andere Partij is beperkt tot het eigen handelen en/of nalaten in het kader van (de rol binnen) het Afsprakenstelsel.

In het kader van de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

Artikel 5. Geheimhouding

5.1 Partijen zullen strikte geheimhouding in acht nemen ten aanzien van vertrouwelijke informatie en informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, die in het kader van de uitvoering van de Overeenkomst wordt uitgewisseld, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

Artikel 6. Achterhalen netwerkfalen

6.1 Onder een netwerkfalen wordt verstaan het niet naar behoren verlopen van een transactie tussen de Dienstafnemer en de Dienstverlener of tussen een Dienstaanbieder en een Dienstbemiddelaar, bijvoorbeeld als gevolg van een Beveiligingsincident dan wel naar aanleiding van de onjuiste verwerking en/of doorgeleiding van:

- de authenticatie van een gebruiker en/of de Dienstafnemer;
- de registratie van een machtiging;
- een wilsuiting.

6.2 In geval van een vermoeden van een netwerkfalen, ondernemen de Partijen stappen om oorzaak van het netwerkfalen te achterhalen. De Dienstafnemer en Dienstverlener dienen hun medewerking hieraan te verlenen en te begrijpen dat de Beheerorganisatie en/of de Toezichthouder op enig moment ingeschakeld kunnen worden.

Artikel 7. Overdraagbaarheid rechten en verplichtingen Overeenkomst

7.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij. In het geval een Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn aan het Netwerk voor Elektronische Toegangsdiensten als Deelnemer in dezelfde rol.

Artikel 8. Toepasselijk recht

8.1 Op deze Gebruiksvoorwaarden is Nederlands recht van toepassing.

Verplichtingen voor de Dienstafnemer

Artikel 10. Dienstafnemer

10.1 De Dienstafnemer voldoet aan alle op hem rustende verplichtingen op grond van het Afsprakenstelsel.

10.2 De Dienstafnemer dient aan de Deelnemer tijdig juiste en volledige informatie aan te leveren, indien de Deelnemer daarom verzoekt.

10.3 Indien de Dienstafnemer niet tijdig, dan wel onjuiste en/of onvolledige informatie verstrekt, dan kan dit niet aan de Deelnemer worden toegerekend, tenzij de Deelnemer wist of behoorde te weten dat er sprake is van onjuiste en/of onvolledige informatie en de Deelnemer deze informatie niettemin heeft verwerkt.

10.4 De Dienstafnemer geeft direct alle relevante mutaties door aan de Deelnemer, en trekt direct daaraan gerelateerde Authenticatiemiddelen en machtigingen in of blokkeert deze.

10.5 Indien ten aanzien van een Authenticatiemiddel en/of een machtiging sprake is van onbevoegd of anderszins onjuist gebruik, of indien dit wordt vermoed, doet de Dienstafnemer direct na kennisname melding van aan de betreffende Middelenuitgever, dan wel trekt de Dienstafnemer de registratie van de betreffende machtiging in.

10.6 Indien een Dienstaanbieder voor het gebruik van een dienst de functionaliteit SSO toestaat, is het de keuze van de Dienstafnemer om al dan niet van deze functionaliteit gebruik te maken.

Artikel 11. Beveiligingsverplichting van de Dienstafnemer

11.1 De Dienstafnemer draagt zorg voor de voldoende beveiliging van de netwerkverbindingen en de systemen die onder diens verantwoordelijkheid vallen en door de Dienstafnemer worden gebruikt in het kader van Elektronische Toegangsdiensten.

11.2 De Dienstafnemer meldt het aan de Deelnemer indien er een vermoeden is van een Beveiligingsincident. De Deelnemer meldt dit vermoeden van een Beveiligingsincident aan de Beheerorganisatie. De Beheerorganisatie meldt dit vermoeden aan de Toezichthouder.

Artikel 12. Toezicht van de Dienstafnemer op gedragingen van personen

12.1 De Dienstafnemer is zich ervan bewust dat een middel persoonsgebonden en niet overdraagbaar is. De informatie die de Dienstafnemer met gebruik van persoonsgebonden Authenticatiemiddelen kan raadplegen, aanvragen en bewerken (wijzigen) is vaak van privacygevoelige aard, vertrouwelijk en persoonlijk. De Dienstafnemer wordt er in dit verband met klem op gewezen dat strikte geheimhouding van zijn Authenticatiemiddel geboden is.

12.2 De Dienstafnemer ziet toe op en is verantwoordelijk voor de gebruiker die optreedt namens de Dienstafnemer. De Dienstafnemer laat geen werkwijze toe die leidt tot onzorgvuldig handelen van zijn vertegenwoordigers, zoals het gebruik van persoonsgebonden Authenticatiemiddelen door meerdere personen, het onbevoegd gebruik van persoonsgebonden Authenticatiemiddelen, het gebruik van Authenticatiemiddelen voor een ander doel dan het doel waarvoor zij zijn afgegeven, etc.

12.3 De Dienstafnemer is verplicht misbruik of een vermoeden van misbruik van Authenticatiemiddelen te melden bij de Deelnemer. Gelijktijdig met deze melding wordt door de Dienstafnemer een verzoek tot het intrekken of schorsing van het desbetreffende Authenticatiemiddel bij de Deelnemer ingediend.

12.4 De Dienstafnemer ziet er op toe dat degene die het als Machtigingenbeheerder heeft aangewezen zorgvuldig handelt bij de verstrekking en het beheren van die machtigingen alsmede dat deze machtigingen zorgvuldig worden gebruikt.

Artikel 13. Vervulling rol(len) door de Dienstafnemer

13.1 Indien de Dienstafnemer zelf één of meer rollen binnen het Netwerk voor Elektronische Toegangsdiensten vervult, gelden voor hem alle verplichtingen die aan de desbetreffende rol zijn verbonden.

Verplichtingen van de Dienstverlener

Artikel 14. Vaststellen openstellingsbesluit

14.1 De Dienstverlener voldoet aan alle op hem rustende verplichtingen op grond van het Afsprakenstelsel.

14.2 De Dienstaanbieder maakt kenbaar dat hij de elektronische weg heeft opengesteld en geeft daarbij aan welke diensten langs elektronische weg kunnen worden afgenomen.

14.3 In het openstellingbesluit maakt de Dienstaanbieder een keuze voor één of meer Betrouwbaarheidsniveaus. Bij het maken van de keuze voor één of meer Betrouwbaarheidsniveaus kan de Handreiking Betrouwbaarheidsniveau van het Forum Standaardisatie als handreiking worden gebruikt. De keuze voor een Betrouwbaarheidsniveau is de uitsluitende verantwoordelijkheid van de Dienstaanbieder. De Deelnemer en de Dienstbemiddelaar zijn niet aansprakelijk voor schade die ontstaat ten gevolge van een door de Dienstaanbieder vastgesteld Betrouwbaarheidsniveau. Dit laat de aansprakelijkheid van de Deelnemer voor de eigen dienstverlening onverlet.

Artikel 15. Melding onregelmatigheden

15.1 In het geval de Dienstverlener ten aanzien van aan haar verstrekte herkenningsgegevens onregelmatigheden constateert of een vermoeden daarvan heeft, doet de Dienstverlener hiervan direct melding aan de Herkenningsmakelaar waarmee zij een Overeenkomst heeft afgesloten.

Artikel 16. Beveiliging dienstverlener

16.1 De Dienstverlener is verantwoordelijk voor de beveiliging en controle van de eigen systemen en netwerken die worden gebruikt, de website en de koppeling met de Herkenningsmakelaar. De Dienstverlener voldoet aan de eisen van het Afsprakenstelsel inzake onder meer de beveiliging van de verbinding en haar systemen, de website en de koppeling met de Herkenningsmakelaar.

16.2 Voor zover de Dienstverlener een publiekrechtelijk rechtspersoon is, wordt door deze overheidsdienstverlener – naast de door Elektronische Toegangsdiensten in het Afsprakenstelsel bekendgemaakte (technische) eisen en voor geschreven beveiligingsmaatregelen - tevens voldaan aan de door het Nationaal Cyber Security Center vastgestelde eisen ten aanzien van beveiliging voor elektronische dienstverlening.

16.3 Indien naar het oordeel van de Herkenningsmakelaar de Dienstverlener niet voldoet aan de in artikel 16.1 en 16.2 bedoelde beveiligingseisen is de Herkenningsmakelaar, overeenkomstig artikel 23 van deze Gebruiksvoorwaarden gerechtigd de Dienstverlener af te sluiten. Het nemen van een dergelijke maatregel wordt door de Herkenningsmakelaar met redenen omkleed.

16.4 De Dienstverlener geeft toestemming tot een controle door een door de Herkenningsmakelaar aan te wijzen auditeur bij het redelijke vermoeden of na het veroorzaken van een Beveiligingsincident.

Artikel 17. SSO

17.1 Het Netwerk voor Elektronische Toegangsdiensten ondersteunt SSO. De Dienstverlener is verantwoordelijk voor de keuze om SSO al dan niet toe te staan voor zijn dienstverlening.

17.2 De Dienstverlener geeft bij registratie van de dienst in de dienstencatalogus op of deze SSO toestaat.

17.3 De Dienstverlener zorgt voor laagdrempelige en adequate informatieverstrekking over het gebruik en de werking van SSO aan de Dienstafnemer.

Artikel 18. Beveiliging

18.1 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de netwerkverbindingen, native apps en systemen die hij gebruikt in het kader van Elektronische Toegangsdiensten. De Deelnemer voldoet daarbij aan de eisen van het Afsprakenstelsel.

Artikel 19. Betrouwbaarheidsniveaus

1.1 De Deelnemer ondersteunt de Betrouwbaarheidsniveaus zoals vastgelegd in de Overeenkomst.

Artikel 20. Informatieverplichting

20.1 De Deelnemer is verplicht alle informatie, waaronder informatie over de Overeenkomst, te verstrekken aan de Toezichthouder voor zover deze informatie voor de Toezichthouder noodzakelijk is om (voortzetting van) deelname aan het Netwerk voor Elektronische Toegangsdiensten te kunnen beoordelen, naleving van de afspraken van het Afsprakenstelsel te kunnen controleren, dan wel indien dit noodzakelijk is vanwege een klacht of een handhavingsverzoek.

Artikel 21. Privacy

21.1 De Deelnemer gebruikt aan hem verstrekte informatie slechts voor het doel waarvoor deze informatie aan hem is verstrekt. De Deelnemer verstrekt geen informatie aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst informatie mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken.

21.2 De Deelnemer verwerkt uitsluitend persoonsgegevens indien en voor zover dit noodzakelijk is ter uitvoering van de Overeenkomst.

21.3 De Deelnemer verstrekt geen persoonsgegevens die betrekking hebben op de gebruiker, tenzij:

- de Dienstverlener of de Dienstafnemer deze gegevens opvraagt in het kader van een juridische procedure; of
- er sprake is van een vordering van een bevoegde opsporingsinstantie of toezichthouder; en
- een en ander geschiedt conform de geldende rechtsregels inzake de verstrekking van persoonsgegevens.

21.4 De verwerking van persoonsgegevens in het kader van uitvoering van de Overeenkomst, geschiedt door de Deelnemer overeenkomstig de bepalingen van de AVG.

Artikel 22. Cookies

22.1 Bij bepaalde instellingen die de Gebruiker zelf kiest, wordt gebruik gemaakt van functionele cookies, dat wil zeggen cookies waarvoor geen expliciete toestemming vereist is. Deze cookies worden niet gebruikt voor andere doeleinden dan het faciliteren van de door de Gebruiker gekozen instelling.

Artikel 23. Toezicht

23.1 De Toezichthouder houdt toezicht op de Deelnemers, de Beheerorganisatie, de centrale voorzieningen die noodzakelijk zijn om het Netwerk van elektronische toegangsdiensten te laten functioneren en behandelt handhavingsverzoeken, meldingen en klachten over de veilige en betrouwbare werking van het Afsprakenstelsel.

23. 2 De Deelnemer schorst de toegang tot zijn dienst in geval van acuut gevaar voor de veilige en betrouwbare werking van het Afsprakenstelsel en overlegt met de Toezichthouder over verder te ondernemen stappen.

23.3 De Toezichthouder behandelt geen zakelijke geschillen tussen Deelnemers of Dienstafnemers.

Organisatie

Hier vindt u de organisatorische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: het operationele handboek, de service level, het businessmodel en het handboek huisstijl. Deze documenten bevatten informatie over de stelselbrede beheerprocessen, de algemene service level die Elektronische Toegangsdiensten hanteert en het gebruik van het beeldmerk van eHerkenning bij externe communicatie.

Deze categorie bevat de volgende onderdelen:

- Operationeel handboek — Dit document beschrijft de operationele beheerprocessen voor het Netwerk. Deze processen hebben als doel om het merk Elektronische Toegangsdiensten te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.
- Businessmodel — Dit document beschrijft het businessmodel voor Elektronische Toegangsdiensten. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het Netwerk (voor Elektronische Toegangsdiensten) invullen. Het is bedoeld voor deelnemers en dienstverleners.
- Service level — Dit document beschrijft de Service Level afspraken die gelden voor deelnemers en de beheerorganisatie van Elektronische Toegangsdiensten. Het betreft een beschrijving van het minimale Service Level dat de deelnemers moeten leveren aan elkaar en hun dienstafnemers en het minimale Service Level dat de beheerorganisatie levert aan de deelnemers.
- Communicatie — Dit document beschrijft de richtlijnen voor naam en merkgebruik, huisstijl afspraken en communicatierichtlijnen voor de merken eHerkenning en eIDAS. Het is bedoeld voor alle betrokken partijen: deelnemers en dienstverleners. De beheerorganisatie levert richtlijnen, standaard tekst- en beeldmateriaal en andere tools die de deelnemers en dienstverleners dienen te gebruiken.

Operationeel handboek

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Dit document beschrijft de operationele beheerprocessen voor het Netwerk. Deze processen hebben als doel om het merk Elektronische Toegangsdiensten te beheren. Onder merkbeheer valt onder andere het beheren van de documentatie van het afsprakenstelsel, de relaties in het netwerk, het technische netwerk, digitale sleutels, toetreding en wensen of wijzigingen.

De juridische afbakening van de beheerorganisatie staat beschreven in Juridisch kader.

Dit document is primair geschreven voor de beheerorganisatie en de deelnemers. Daarnaast is het ook ter inzage voor het Ministerie van Binnenlandse Zaken (opdrachtgever voor Elektronische Toegangsdiensten) en iedere andere organisatie die interesse heeft in Elektronische Toegangsdiensten.

Leeswijzer

- Helpdesk — De beheerorganisatie beschikt over een helpdesk specifiek voor de deelnemers van Elektronische Toegangsdiensten. Deze helpdesk is het eerste meldpunt in geval van vragen, issues of andere problemen binnen het netwerk.
- Proces aanvragen BSNk-sleutelmateriaal
- Proces attribuutcatalogus
- Proces beheren simulator — De simulator is door de beheerorganisatie ontwikkeld om deelnemer en dienstverleners een simulatortest te laten uitvoeren. Hiermee worden koppelvlakken gesimuleerd.
- Proces beheren testnetwerk — Het testnetwerk is een netwerk van alle deelnemers. Het heeft als functie om nieuwe systemen van nieuwe toetreders of deelnemers te kunnen onderwerpen aan ketentesten. Hiermee kan in een netwerk, dat zich op hoofdlijnen gedraagt als het productienetwerk, worden gecontroleerd of aan alle eisen wordt voldaan.
- Proces certificaatwissel — In de metadata zijn één of meer actuele certificaten per deelnemer opgenomen. De deelnemers en de beheerorganisatie hebben de mogelijkheid om uit voorzorg ook certificaten op te geven die gebruikt (kunnen) gaan worden bij het wisselen van een certificaat. Dit maakt het netwerk minder kwetsbaar wanneer een certificaat gewisseld moet worden.
- Proces change en release — Het Afsprakenstelsel Elektronische Toegangsdiensten is dynamisch. Het change en releaseproces beschrijft het proces van het ontstaan van een wijziging, de toetsing en de besluitvorming en het verwerken van de wijziging in het Afsprakenstelsel (AS). Het Proces implementatie koppelvlakrelease beschrijft de implementatie van een change in het Netwerk (voor Elektronische Toegangsdiensten) door een betrokken partij.
- Proces contentmanagement
- Proces distributie en publicatie van documenten — De beheerorganisatie verricht algemene communicatie activiteiten voor Elektronische Toegangsdiensten. Een van die activiteiten is het publiceren van het Afsprakenstelsel Elektronische Toegangsdiensten en andere bij Elektronische Toegangsdiensten berustende informatie (dit betekent documenten met de classificatie 'Elektronische Toegangsdiensten openbaar'). De deelnemers en de beheerorganisatie gebruiken de documentatie voor het beheer van Elektronische Toegangsdiensten. Andere geïnteresseerde par
- Proces doorvoeren nieuwe dienstencatalogus — In de dienstencatalogus zijn alle diensten van aangesloten dienstverleners opgenomen die worden onderscheiden binnen Elektronische Toegangsdiensten. De beheerorganisatie beheert de geaggregeerde dienstencatalogus. Dit proces beschrijft hoe wijzigingen op de dienstencatalogus worden doorgevoerd.
- Proces implementatie koppelvlakrelease
- Proces incidentmanagement
- Proces informeren Toezichthouder
- Proces instandhouding en naleven — Een goede naleving van het afsprakenstelsel is onontbeerlijk voor de veiligheid, betrouwbaarheid, geloofwaardigheid en het vertrouwen in het stelsel. Zowel de Deelnemers aan het Afsprakenstelsel als de Beheerorganisatie, BSNk en de Toezichthouder hebben een rol bij de instandhouding van het netwerk en de borging van het naleven van het Afsprakenstelsel. In eerste instantie gebeurt het toezien op de naleving zo veel mogelijk vanuit een zelfregulerend systeem en in goed onderling overleg tussen pa
- Proces managementrapportage
- Proces meldingenbeheer — De beheerorganisatie is aanspreekpunt voor zaken met betrekking tot de ontwikkeling en implementatie van het Afsprakenstelsel Elektronische Toegangsdiensten. snippet.issues functioneert als portaal voor het maken van meldingen. Bij het melden van een incident moet het proces incidentmanagement als basis genomen worden.
- Proces migratie sleutelmateriaal voor polymorfe pseudonimisering
- Proces netwerkmetadata
- Proces onderhoud cookieserver — Voor de werking van Single Sign On heeft iedere Herkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein snippet.url.sso. De DNS van het gezamenlijke domein wordt beheerd door beheerorganisatie.
- Proces toetreden — Het afsprakenstelsel van Elektronische Toegangsdiensten, waaronder het merk eHerkenning valt, staat open voor deelname door nieuwe geïnteresseerde partijen. Het Proces Toetreden beschrijft de stappen die genomen moeten worden om toe te treden tot het afsprakenstelsel Elektronische Toegangsdiensten. Na ondertekening van de Deelnemersovereenkomst, als sluitstuk van het toetredingsproces, mag het merk eHerkenning gevoerd worden. Bij bepaalde wijzigingen, bijvoorbeeld wanneer een deelnemer zijn dien
- Proces uittreden
- Proces uitvoeren centrale penetratietest
- Proces wijziging rechtspersoon — Wanneer een deelnemer de rechtspersoon wil wijzigen, maakt hij dit kenbaar aan de beheerorganisatie door middel van het formulier Template wijziging rechtspersoon deelnemer. mailto:info@eherkenning.nl.

Helpdesk

De beheerorganisatie beschikt over een helpdesk specifiek voor de deelnemers van Elektronische Toegangsdiensten. Deze helpdesk is het eerste meldpunt in geval van vragen, issues of andere problemen binnen het netwerk.

De helpdesk kan in principe niet gebruikt worden door gebruikers van Elektronische Toegangsdiensten. Zij wenden zich tot de dienstverlener of tot de deelnemer waarmee zij een relatie hebben.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Melding helpdesk

Toelichting processtappen

1. Melding helpdesk	
Input	Vraag, probleem, issue van een deelnemer
Activiteit	1. De deelnemer meldt zijn vraag, probleem of issue aan de helpdesk van de beheerorganisatie per e-mail: *info@eherkenning.nl*. 2. De beheerorganisatie formuleert indien mogelijk direct een oplossing. Indien dit niet mogelijk is, wordt de vraag verder in de beheerorganisatie uitgezet. 3. De beheerorganisatie beantwoordt de vraag van de deelnemer of verstuurt een voortgangsbericht.
Output	Oplossing voor vraag, probleem of issue van de deelnemer
Wie?	• Beheer officer van de beheerorganisatie • Indien nodig, andere experts in de beheerorganisatie • Deelnemers

Proces aanvragen BSNk-sleutelmateriaal

Voor het decrypten van het (polymorf) versleutelde BSN en PseudoID heeft de DV speciaal BSNk-Sleutelmateriaal nodig. Dit moet door haar Herkenningsmakelaar (HM) aangevraagd worden bij het BSNk

Dit proces beschrijft hoe dat aanvraagproces verloopt..

Verantwoordelijkheden

De HM is verantwoordelijk dat het proces wordt uitgevoerd conform de procesbeschrijving.

Toelichting processtappen

Het BSNk beheert en verstrekt cryptografisch sleutelmateriaal aan elke Dienstverlener (DV) die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal (extra) BSN Sleutelmateriaal anders alleen sleutelmateriaal waarmee een PseudoID ontsleuteld kan worden. Ter ontzorging van de DV verzorgt de HM deze aanvraag. Hiervoor implementeert de HM de Interface specifications aux HM-BSNk - ProvideDVkeys.

Het proces volgt de stappen zoals beschreven bij AUC9 Verstrekken sleutelmateriaal Dienstverleners.

Proces attribuutcatalogus

In het Netwerk wordt de Attribuutcatalogus gebruikt voor het beschrijven van de beschikbare attributen en de toegestane bronnen binnen het Afsprakenstelsel Elektronische Toegangsdiensten.

> De attribuutcatalogus wordt gebruikt in zowel het productie- als het testnetwerk. Dit proces beschrijft hoe de attribuutcatalogus eerst in test, en vervolgens in productie wordt doorgevoerd.

Doelstelling

De doelstelling van het proces attribuutcatalogus is tweeledig:

1. Waarborgen dat de attribuutcatalogus op correcte wijze tot stand komt;
2. Waarborgen dat alle deelnemers de actuele attribuutcatalogus in hun systemen gebruiken.

Verantwoordelijkheden

- De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving;
- De technisch beheerder zorgt tevens dat de procesbeschrijving actueel blijft en coördineert de verschillende stappen in het proces;
- De deelnemers zijn verantwoordelijk voor het tijdig verwerken van de attribuutcatalogus.

Overzicht processtappen

- 1. Attribuut toevoegen aan attribuutcatalogus
- 2. Publiceren attribuutcatalogus in het testnetwerk
- 3. Doorvoeren attribuutcatalogus in het testnetwerk
- 4. Publiceren attribuutcatalogus in het productienetwerk
- 5. Doorvoeren attribuutcatalogus in het productienetwerk

Toelichting processtappen

1. Attribuut toevoegen aan attribuutcatalogus

Input	Middels het Proces change en release is een nieuw attribuut toegevoegd aan het Afsprakenstelsel
Activiteit	De technisch beheerder voegt het attribuut met alle kenmerken toe aan de attribuutcatalogus 1. De vorige versie van de attribuutcatalogus wordt handmatig opgehaald vanaf de gepubliceerde locatie; 2. Het nieuwe attribuut, met alle kenmerken zoals beschreven in de RFC, wordt toegevoegd; 3. De change manager (of een tweede technisch beheerder) controleert dit; 4. De attribuutcatalogus wordt voorzien van een digitale handtekening met het certificaat van de Beheerorganisatie (conform Digital signature); 5. De nieuwe versie van de attribuutcatalogus wordt handmatig gepubliceerd.
Output	• Een nieuwe attribuutcatalogus
Wie?	• De technisch beheerder voert deze stap uit • De change manager controleert de wijziging

2. Publiceren attribuutcatalogus in het testnetwerk

Input	De nieuwe attribuutcatalogus
Activiteit	1. De technisch beheerder publiceert de nieuwe attribuutcatalogus op https://extranet.eherkenning.nl/1.11/test/attribuutcatalogus.xml; 2. Middels een bericht op Mantis wordt dit aangekondigd.
Output	Gepubliceerde attribuutcatalogus in het testnetwerk
Wie?	De technisch beheerder van de beheerorganisatie voert deze stap uit

3. Doorvoeren attribuutcatalogus in het testnetwerk

Input	Gepubliceerde attribuutcatalogus
Activiteit	De deelnemers pakken de nieuwe attribuutcatalogus op en voeren deze door binnen 24 uur.
Output	Geïmplementeerde nieuwe attribuutcatalogus in het testnetwerk
Wie?	De deelnemers implementeren de nieuwe attribuutcatalogus

4. Publiceren attribuutcatalogus in het productienetwerk	
Input	De nieuwe attribuutcatalogus
Activiteit	1. De technisch beheerder publiceert de nieuwe attribuutcatalogus op https://extranet.eherkenning.nl/1.11/attribuutcatalogus.xml; 2. Middels een bericht op Mantis wordt dit aangekondigd.
Output	Gepubliceerde attribuutcatalogus in het testnetwerk
Wie?	De technisch beheerder van de beheerorganisatie voert deze stap uit

5. Doorvoeren attribuutcatalogus in het productienetwerk	
Input	Gepubliceerde attribuutcatalogus
Activiteit	De deelnemers pakken de nieuwe attribuutcatalogus op en voeren deze door binnen 24 uur.
Output	Geïmplementeerde nieuwe attribuutcatalogus in het productienetwerk
Wie?	De deelnemers implementeren de nieuwe attribuutcatalogus

Proces beheren simulator

De simulator is door de beheerorganisatie ontwikkeld om deelnemer en dienstverleners een simulatortest te laten uitvoeren. Hiermee worden koppelvlakken gesimuleerd.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technische beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Beheer simulator

Toelichting processtappen

1. Beheer simulator	
Input	Nieuwe versie afsprakenstelsel
Activiteit	1. De beheerorganisatie past de simulator aan op de nieuwe versie van het afsprakenstelsel 2. Wanneer de nieuwe versie van de simulator beschikbaar is, stelt de beheerorganisatie de deelnemers per e-mail hiervan op de hoogte.
Output	• Nieuwe versie simulator • Bericht aan de deelnemers
Wie?	• Beheerorganisatie, technische beheerder • Deelnemers, technische beheerders
Opmerkingen	De simulator is te vinden op https://simulator.etoegang.nl. De handleiding van de simulator is ook opgenomen op deze website.

Proces beheren testnetwerk

Het testnetwerk is een netwerk van alle deelnemers. Het heeft als functie om nieuwe systemen van nieuwe toetreders of deelnemers te kunnen onderwerpen aan ketentesten. Hiermee kan in een netwerk, dat zich op hoofdlijnen gedraagt als het productienetwerk, worden gecontroleerd of aan alle eisen wordt voldaan.

Uitgangspunten

Een (aspirant) deelnemer zal afhankelijk van zijn rol (Herkenningsmakelaar (HM), Authenticatiedienst (AD) of Middelenuitgever (MU) één of meerdere systemen in het testnetwerk opgenomen hebben. Van elk systeem kan tevens zowel een acceptatie- als een preproductie-versie aanwezig zijn. Een (aspirant) deelnemer test zijn acceptatiecomponenten tegen de preproductiecomponenten van de overige deelnemers.

De voorwaarden om het testnetwerk te laten functioneren, zijn als volgt:

- De staat van de preproductiecomponenten in het testnetwerk benadert zo veel mogelijk het productienetwerk.
- Een herkenningsmakelaar MAG dienstverleners via haar preproductiecomponent toegang verlenen tot AD/MR van andere deelnemers en de simulator, mits dit niet tot overlast leidt.
- Het uitvoeren van stresstesten MAG toestemming vooraf van alle te raken deelnemers.
- Deelnemers MOGEN testmiddelen verschaffen aan dienstverleners die zijn aangesloten via een andere deelnemer.
- De acceptatieomgeving dient om de eigen software te testen tegen de preproductiecomponenten van andere deelnemers.
- Een deelnemer MOET toestemming hebben om te testen tegen de acceptatieomgeving van een andere deelnemer.
- Alle deelnemers hebben de beschikking over testmiddelen, voor de preproductiecomponenten in het testnetwerk, voor elke authenticatiedienst en machtigingenregister, op elk toegetreden (of nog toe te treden) betrouwbaarheidsniveau. De deelnemers leveren deze testmiddelen aan elkaar uit.
- Bij het deployen van een systeem in het testnetwerk dient voor een deelnemer of de beheerorganisatie helder te zijn welke build versie het systeem heeft. (Bijvoorbeeld door naamgeving, het displayen van het build nummer op de pagina of in een afgeleide (file).) Dit zodat kan worden nagegaan tegen welke versie van een systeem aan wordt getest. Bij de toetredingschecklists wordt altijd aangegeven tegen welke build versies is getest.
- Acceptatiecomponenten in het testnetwerk MOETEN herkenbaar zijn aan de toevoeging (acc) in de displayname
- Preproductiecomponenten in het testnetwerk MOETEN herkenbaar zijn aan de toevoeging (preprod) in de displayname
- Voor beschikbaarheid van preproductiecomponenten in het testnetwerk wordt een inspanningsverplichting en een meldplicht van verstoringen afgesproken.
- Verzoeken van deelnemers om meer informatie betreffende een fout (op een systeem) in het testnetwerk ZOU binnen één werkdag beantwoord MOETEN worden.
- Het in bezit hebben van testmiddelen door deelnemers en dienstverleners impliceert dat deze testmiddelen ook te allen tijde kunnen werken. Dat wil zeggen dat de uitgevers van deze middelen zich hiermee verplichten een soortgelijk serviceniveau te leveren als bij productiemiddelen het geval is.
- Issues en verstoringen betreffende het testnetwerk worden gemeld in de issuetracker Mantis.
- De metadata en dienstencatalogus voor het testnetwerk zullen ad hoc verspreid worden, als de noodzaak zich aandient. Deze zullen op dezelfde manier als binnen het productienetwerk worden aangeboden aan de deelnemers.
- Een deelnemer MAG haar acceptatie- en preproductiecomponenten NIET afsluiten voor andere deelnemers.
- De deelnemers MOETEN zowel voor de acceptatie- als de preproductieomgeving gebruik maken van PKIoverheid certificaten. Dit geldt voor zowel het signing- als encryptiecertificaat. Deze omgevingen moeten immers zo veel als mogelijk gelijkwaardig aan de productieomgeving zijn.

Proces certificaatwissel

In de metadata zijn één of meer actuele certificaten per deelnemer opgenomen. De deelnemers en de beheerorganisatie hebben de mogelijkheid om uit voorzorg ook certificaten op te geven die gebruikt (kunnen) gaan worden bij het wisselen van een certificaat. Dit maakt het netwerk minder kwetsbaar wanneer een certificaat gewisseld moet worden.

Dit proces beschrijft hoe het wisselen van certificaten verloopt.

Om het proces van het wisselen van een certificaat succesvol te laten verlopen, is het van belang dat deelnemers meerdere certificaten per deelnemer kunnen verwerken.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Aanleveren nieuwe certificaat
- 2. Verwijderen oude certificaat

Toelichting processtappen

1. Aanleveren nieuwe certificaat	
Input	Geplande certificaatwissel bij een deelnemer
Activiteit	1. De deelnemer informeert de beheerorganisatie tijdig over de geplande certificaatwissel. 2. De deelnemer levert het nieuwe metadatabestand aan bij de beheerorganisatie, voorafgaand aan moment waarop het huidige certificaat verloopt. In deze metadata is opgenomen: • de huidige public key die in gebruik is • de nieuwe public key die de deelnemer wil gaan gebruiken 1. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces netwerkmetadata, en attendeert alle deelnemers op de certificaatwissel. 2. De deelnemers MOETEN de nieuwe versie van de metadata binnen het eerstvolgende gebruikelijke Onderhoudsvenster doorvoeren. 3. Na het onderhoudsvenster MAG de betreffende deelnemer het nieuwe certificaat gebruiken.
Output	Doorgevoerde metadata met oude en nieuwe certificaat
Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

2. Verwijderen oude certificaat	
Input	Doorgevoerde metadata met oude en nieuwe certificaat
Activiteit	1. Wanneer het nieuwe certificaat overal binnen het netwerk is geaccepteerd, kan het oude certificaat uit de metadata worden gehaald. De betreffende deelnemer levert nieuwe metadata aan met daarin alleen de public key van het nieuwe certificaat. 2. De beheerorganisatie aggregeert en publiceert de nieuwe metadata volgens het Proces netwerkmetadata, en attendeert alle deelnemers op de certificaatwissel.
Output	Doorgevoerde metadata met enkel het nieuwe certificaat
Wie?	• Beheerorganisatie, technisch beheerder • Deelnemers, technisch beheerders

Certificaatwissel kan ook voorkomen bij certificaten die niet in de metadata zijn opgenomen. Voor de werking van Single Sign On heeft iedere Herkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.sso.eherkenning.nl. Dit gezamenlijke domein wordt beheerd door de beheerorganisatie.

De cookieservers verzenden geen berichten maar maken wel gebruik van certificaten. Wanneer deze certificaten worden gewisseld, wordt ongeveer hetzelfde proces doorlopen als bij de certificaatwissel in metadata. Dat proces verloopt dan als volgt:

- De deelnemer meldt tijdig (minimaal twee weken van te voren) bij de beheerorganisatie dat het certificaat moet worden gewisseld via de issuetracker Mantis. Hierbij vermeldt de deelnemer de huidige public key die in gebruik is, de nieuwe public key en de termijn waarop de wijziging moet plaatsvinden.
- De beheerorganisatie vervangt de public key van de betreffende deelnemer.
- De deelnemer ontvangt een bevestiging van de beheerorganisatie via Mantis wanneer de vervanging is afgerond.
- De deelnemer KAN nu het nieuwe certificaat gebruiken.

Proces change en release

Het Afsprakenstelsel Elektronische Toegangsdiensten is dynamisch. Het change en releaseproces beschrijft het proces van het ontstaan van een wijziging, de toetsing en de besluitvorming en het verwerken van de wijziging in het Afsprakenstelsel (AS). Het Proces implementatie koppelvlakrelease beschrijft de implementatie van een change in het Netwerk (voor Elektronische Toegangsdiensten) door een betrokken partij.

> Indien een wijziging de juridische of technische strekking van het Afsprakenstelsel niet aantast, dan MAG de wijziging direct worden doorgevoerd in het Afsprakenstelsel. Waaronder begrepen, maar niet beperkt tot herstructureren van content, corrigeren van taal- en stijlfouten, onderhoud aan hyperlinks en labels.

Doelstelling

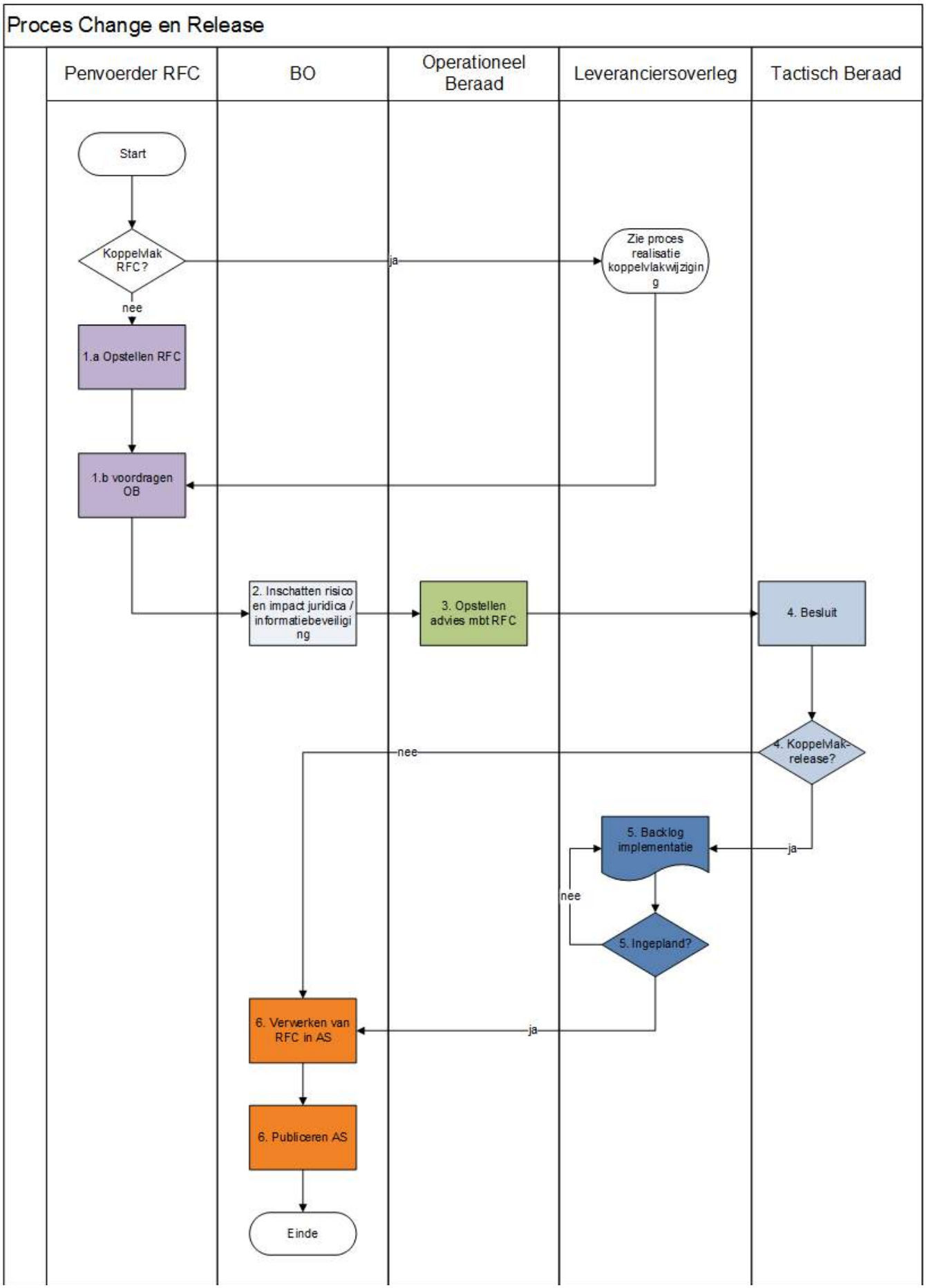
De doelstelling van het change- en releaseproces is tweeledig:

1. Op transparante en zorgvuldig wijze besluiten over welke wijzigingen wel en niet worden doorgevoerd. Alle belanghebbenden moeten invloed kunnen hebben op de wijziging van het Afsprakenstelsel.
2. De release op gestructureerde wijze inbrengen in het Afsprakenstelsel en de productieversie van het netwerk.
    a. volgens de planning;
    b. met minimale verstoringen voor Elektronische Toegangsdiensten.

Verantwoordelijkheden

- In het change- en releaseproces worden de volgende verantwoordelijkheden onderscheiden:
    - Het Strategisch Beraad is verantwoordelijk voor het schetsen van strategische kaders voor de inhoudelijke doorontwikkeling van het Afsprakenstelsel Elektronische Toegangsdiensten in het meerjarenplan;
    - Het Tactisch Beraad besluit over de inhoud van de releases op basis van het advies van het Operationeel Beraad en bij een koppelvlakrelease ook op basis van advies van het Leveranciersoverleg. In het geval van een koppelvlakrelease stelt het Leveranciersoverleg een releasemanager/productowner aan ;
        - De releasemanager en productowner coördineert de totstandkoming van de release
    - Het Operationeel Beraad toetst of een RFC past in de architectuur van het stelsel. Het Operationeel Beraad brengt advies uit over de RFC en samenstelling van een release aan het Tactisch Beraad.
    - Het leveranciersoverleg stelt een advies op ten aanzien van de inhoud van een koppelvlakrelease, de daarbij horende prioriteit en de releasemanager/ productowner voor een koppelvlakrelease. Het leveranciersoverleg is verantwoordelijk voor de backlog rond koppelvlak RFC's, de aangestelde product owner beheert deze backlog met input uit het LO
    - Beheerorganisatie:
        - De change manager is verantwoordelijk dat het proces change en release wordt uitgevoerd volgens de procesbeschrijving. De change manager actualiseert de procesbeschrijving en coördineert de verschillende stappen in het proces.
        - De changemanager organiseert de validatie aan de hand van een demonstratie van de deelnemers van de goede werking van de interoperabiliteit tussen de deelnemers.
        - De jurist, security officer en stelstelarchitect leveren een bijdrage met betrekking tot het uitvoeren van een risico- en impactanalyse op de RFCs.
    - Een RFC kan door een stakeholder worden voorbereid en ingebracht worden voor behandeling. De indiener van een RFC zorgt voor een motivatie en draagvlak waarom een RFC nodig is.

Overzicht processtappen


Proces Change en Release
Penvoerder RFC
BO
Operationeel Beraad
Leveranciersoverleg
Tactisch Beraad
Start
Koppelvlak RFC?
ja
Zie proces realisatie koppelvlakwijziging
nee
1.a Opstellen RFC
1.b voordragen OB
2. Inschatten risico en impact juridica / informatiebeveiliging
3. Opstellen advies mbt RFC
4. Besluit
4. Koppelvlak-release?
nee
ja
5. Backlog implementatie
nee
5. Ingepland?
ja
6. Verwerken van RFC in AS
6. Publiceren AS
Einde

Toelichting processtappen

1a. Opstellen RFC	
Input	Het verzoek van een RFC kan door een stakeholder worden gemeld. Denk hierbij aan de governance, het leveranciersoverleg en de beheerorganisatie. Een RFC kan verschillende aanleidingen hebben, zoals: • Correcties: denk aan tekstuele correcties en patches. Het doorvoeren van correcties heeft geen impact op de inhoud/werking van het Afsprakenstelsel. • Issues: denk aan een (deel van een) functionaliteit die in de praktijk niet goed toepasbaar blijkt. Het oplossen van issues heeft impact op de inhoud/werking van het Afsprakenstelsel. • Nieuwe functionaliteit: het accepteren van nieuwe functionaliteiten heeft impact op de inhoud/werking van het Afsprakenstelsel. • Regelgeving: zorgen dat het AS in lijn blijft met nationale en Europese regelgeving.
Activiteit	De change manager maakt naar aanleiding van het verzoek een dossier voor de RFC aan en deze krijgt een uniek kenmerk. De eigenaar van de RFC is de zogenaamde penvoerder. Hij of zij is het aanspreekpunt voor de RFC en organiseert de activiteiten om de RFC klaar te maken voor behandeling door de governance. Mocht bij het opstellen blijken dat de RFC impact heeft op het koppelvlak dan wordt het Proces realisatie koppelvlak wijzigingen gevolgd. Een RFCs bevat minimaal: • de beschrijving van de concrete gewenste wijziging • een beschrijving van de aanleiding/context, • de oplossingsrichting, • de globale impact per rol in het Afsprakenstelsel • de rechtvaardiging hiervan (toegevoegde waarde, business case). Deze business case moet gedragen zijn door de betrokken partijen. De penvoerder moet hiermee in staat zijn om deze in het Tactisch Beraad te motiveren. De eigenaar van de RFC geeft zelf aan of de inhoud besloten of inzichtelijk is voor de betrokken partijen in de initiële fase. Zodra de RFC gereed is voor toetsing door de governance is deze inzichtelijk voor de betrokken partijen. Deze partijen hebben dan ook de mogelijkheid om voorafgaand aan de behandeling door de governance commentaar te leveren. De penvoerder geeft aan de change manager aan wanneer de RFC gereed is voor de behandeling door de Governance. De change manager organiseert de toetsing op informatiebeveiliging en juridica door de Beheerorganisatie en agendeert de RFC voor behandeling in het Operationeel Beraad.
Output	Opgestelde RFC
Wie?	• Penvoerder RFC • Change manager • Leveranciersoverleg

1b. presentatie oplossingsrichting RFC van werkgroep door penvoerder	
Input	Oplossingsrichting RFC vanuit een werkgroep
Activiteit	De penvoerder en/of sponsor presenteert de gekozen oplossingsrichting aan de leden van het OB met als doel deze te toetsen en te bediscussiëren.
Output	• Verbeterde RFC • Draagvlak voor de RFC bij leden OB
Wie?	Penvoerder en/of sponsor

2. Bepalen impact RFC door BO	
Input	RFC
Activiteit	Vanuit de beheerorganisatie bepaalt de security officer en de jurist de RFCs op het gebied van security en privacy risico's. Bij complexe RFC's voert de stelselarchitect een review uit. De stelselarchitect bepaalt de impact op de architectuur en de conformiteit ten aanzien van de architectuurprincipes.

Output	• Verbetervoorstellen gericht aan de penvoerder • Impact bepaald op het vlak van security en privacy (Actuele risicomatrix) • Eventueel impact bepaald door stelselarchitect • Agendering voor behandeling door OB
Wie?	• Security officer • Jurist • Stelselarchitect

3. Behandeling RFC door het Operationeel Beraad

Input	RFC getoetst door BO
Activiteit	Het Operationeel beraad stelt een advies op voor het Tactisch Beraad of een RFC implementeerbaar is en/of het past het in de architectuur en AS. Het Operationeel Beraad stelt vast of het wel/geen koppelvlakrelease is.
Output	Advies over de RFC als voorbereiding voor de besluitvorming door het Tactisch Beraad.
Wie?	• Operationeel Beraad

4. Besluiten over RFC's

Input	RFC's met advies Operationeel Beraad
Activiteit	De RFC wordt samen met het advies van het Operationeel Beraad doorgeleid naar het Tactisch Beraad. Indien de verzameling bestaat uit administratieve RFC's dan zal de changemanager die aanbieden in een releasebundel. Voor RFC's buiten een koppelvlakrelease kunnen er implementatietermijnen van toepassing zijn. In principe zijn er dan twee vaste momenten in het jaar om een RFC's geïmplementeerd te hebben: 1 juni en 1 december van een betreffend jaar. De koppelvlak RFC's worden los aangeboden en komen na goedkeuring op de backlog van de leveranciers
Output	• Een formeel vastgestelde release (eventueel spoedrelease) • Start Proces implementatie koppelvlakrelease • Aangehouden RFCs
Wie?	• Change manager • Tactisch Beraad

5. Plaatsten van koppelvlak RFC op backlog realisatie

Input	Positief besluit mbt koppelvlak RFC
Activiteit	Het leveranciersoverleg bepaalt aan de hand van de eigen capaciteit en behoeft en marktpotentieel welke koppelvlak RFC's wanneer gerealiseerd worden. Ze informeren het Tactisch Beraad hierover wat op de backlog staat en wat daarbij de prioriteit van realisatie is. Zodra het leveranciersoverleg besloten heeft dat een RFC geïmplementeerd wordt wordt dat doorgegeven aan de changemanager in verband met het verwerken van de aanpassingen in het afsprakenstelsel.
Output	Backlog en prioriteitsstelling en inzicht welke items in een volgende release ingepland zijn.
Wie?	• Leveranciersoverleg • Tactisch beraad

6. Verwerken release in het Afsprakenstelsel	
Input	Vastgestelde release door het Tactisch Beraad.
Activiteit	De Beheerorganisatie verwerkt de wijzigingen in de het Afsprakenstelsel. Bij administratieve RFC's is het moment na de vaststelling door het Tactisch Beraad. Indien er een implementatietermijn van toepassing is zal die worden aangegeven in het afsprakenstelsel zelf. Bij koppelvlak RFC's is het moment zodra de wijziging is ingepland voor realisatie. De penvoerder of Beheerorganisatie voert een review uit of de wijziging correct is doorgevoerd aan de hand van het 4 ogen principe. Na de review publiceert de Beheerorganisatie een nieuwe versie van het afsprakenstelsel
Output	Gepubliceerde nieuwe versie van het afsprakenstelsel
Wie?	• Change manager • Penvoerder

Proces realisatie koppelvlak wijzigingen

Doelstelling

Om tot een soepele implementatie te komen zijn kwalitatief goede specificaties nodig en deelnemers en dienstverleners die de nieuwe functionaliteit willen gebruiken. De ingrediënten voor succes zijn grondige kennis wat er moet gebeuren in combinatie met een heldere bussinesscase.

Door met elkaar (deelnemers, dienstverleners en BO) meer energie te steken in de voorkant van het totstandkomingsproces is het de verwachting dat de kwaliteit van specificaties, use- en testcases en ondersteunde tooling zullen toenemen en de doorlooptijd en impact van de implementatie verkorten.

Door daarnaast gebruik te maken van de Agile/Scrum methodiek bij het schrijven van specificaties is het de verwachting dat vergelijkbare voordelen worden behaald als bij het ontwikkelen van software.

Deze voordelen zijn:

- de nauwe betrokkenheid van de belanghebbenden
- de input vanuit meerdere disciplines
- snel schakelen bij veranderingen
- inzicht in de voortgang en de focus op een werkend product

Het ontwikkelen van testfaciliteiten, testberichten en testcases vormen een integraal onderdeel van het voortbrengingsproces van RFC's. Het doel van deze werkwijze is om te komen tot specificaties van hogere kwaliteit (vooral meer eenduidig en compleet) die testbaar zijn en in kortere cycli opgeleverd kunnen worden.

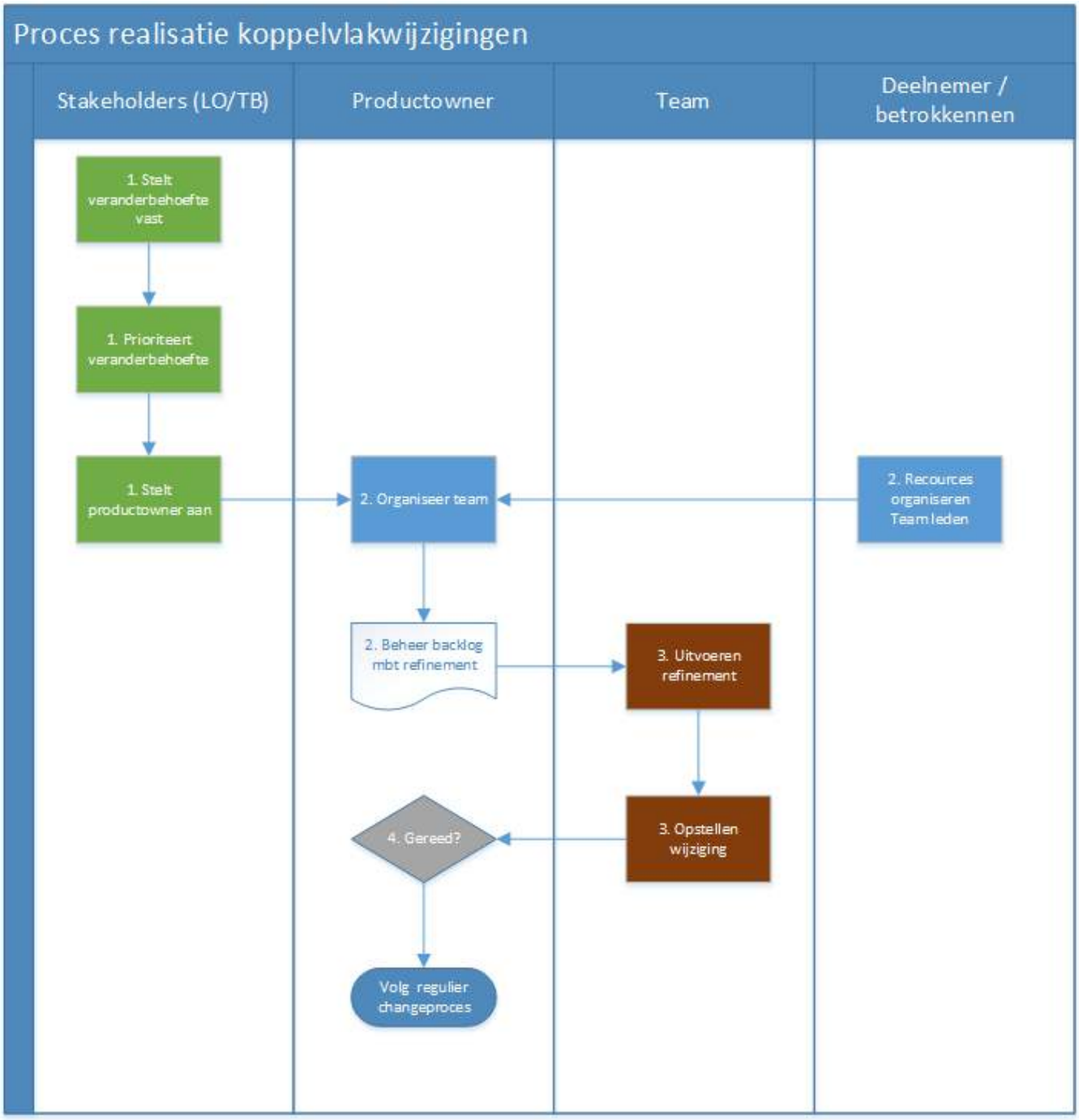
Verantwoordelijkheden

In het worden de volgende verantwoordelijkheden onderscheiden:

- Het Leveranciersoverleg is een stakeholder : Voor aanpassingen in het koppelvlak is dit de initiële plek om veranderbehoefte te agenderen mbt businesscase en prioriteit. De veranderbehoefte is afkomstig van de klant, de dienstverlener, waar een leverancier een relatie mee heeft. De leverancier en dienstverlener stellen samen de behoeftestelling op en die wordt door de overige deelnemers besproken op haalbaarheid en marktpotentie. Het leveranciersoverleg beslist of een werkgroep start met het uitwerken van de oplosrichting. Het leveranciersoverleg benoemt de productowner om een deel van de veranderbehoefte klaar te maken voor bouw.
- De productowner is verantwoordelijk voor het beheer van de productbacklog. Deze persoon geeft met input van het LO aan welke RFC's het refinementteam oppakt en bepaalt of deze producten gereed zijn voor implementatie door de deelnemers. De productowner handelt met een zekere zelfstandigheid om de snelheid van bouw optimaal te laten verlopen. De rol van de governance is het meedenken en helpen bij het weghalen van belemmeringen.
- Het refinementteam bestaat uit belanghebbenden (o.a. dienstverleners, deelnemers en BO) waarbij het principe geldt dat diegene die het ook wil de inspanning levert om het te realiseren en daarbij draagvlak organiseert bij de betrokken. De samenstelling ligt niet vast en is afhankelijk van de fase waarin het zich bevindt of het onderwerp wat besproken wordt. Het team bestaat uit specialisten vanuit verschillende disciplines: architect, security officer, tester, jurist, ontwerper, bouwer en projectleiding. De agile /scrum methodiek wordt toegepast om de producten te realiseren.
- Het Operationeel Beraad is een stakeholder en toetst of de initiële oplosrichtingen qua functionaliteit past in de bestaande architectuur en bepaalt eventueel de impact. Het Operationeel beraad geeft hierover advies aan het Tactisch Beraad.
- Het Tactisch Beraad is een stakeholder en beoordeelt of het voorstel past bij de ambitie en strategie van het stelsel.

Proces ontwerp koppelvlak RFC

Dit proces is van toepassing op RFC's die deel uit maken van een koppelvlakrelease en implementatie vanuit een duidelijke behoeftestelling en opdracht van het leveranciersoverleg. Het moet worden gezien als een voortraject op het Proces change en release.



Toelichting processtappen

1. Veranderbehoefte bespreken en actie bepalen	
Input	De stakeholders van het stelsel zijn divers. De praktijk is dat de stakeholders haar weg vinden naar het Tactisch Beraad en/of het Leveranciersoverleg cq dat het Tactisch Beraad en Leveranciersoverleg de rol vervullen van stakeholder. Uit deze gremia komen de plannen wat de ambities zijn van komende periode zoals in een jaarplan. Als de stakeholders de handen op elkaar hebben om een wijziging komende periode te implementeren dan stellen ze hiervoor een productowner aan.

Activiteit	De stakeholders prioriteren en communiceren van de veranderbehoefte. Denk aan een jaarplan en besluiten wat in een komende release als nieuwe functionaliteit gewenst is. De stakeholder leveranciersoverleg stelt een productowner aan.
Output	• Jaarplan • Aanstellen productowner • Backlog met gewenste functionaliteit
Wie?	• Stakeholders (combinatie van Leveranciersoverleg en Tactisch Beraad.

2. Opstarten refinement team	
Input	Backlog met gewenste functionaliteit
Activiteit	De betrokken partijen (waaronder deelnemers en BO) leveren teamleden voor het refinement team. De BO vervult de rol van scrummaster. De productowner vervult zijn/haar rol volgens de definitie genoemd volgens scrum.
Output	• Team • Backlog voor team
Wie?	• Deelnemers • Productowner

3. Uitvoeren refinement	
Input	Backlog voor team
Activiteit	Bepalen van de definition of done Het team werkt de veranderbehoefte uit in een RFC die klaar is om gebouwd te worden door de deelnemers. Dit is inclusief de beschrijving voor de benodigde veranderingen voor aanpalende systemen zoals de aggregator, simulator etc. en inclusief de beschrijving van testcases.
Output	Een RFC waarbij de deelnemers aangeven dat die voldoet aan de defintion of done.
Wie?	• Team • Operationeel Beraad

4. Opleveren van RFC en doorgeleiden governance via changeproces	
Input	RFC opgesteld door team
Activiteit	De productowner toets de defintion of done en meldt het als gereed. Hij ziet toe dat de RFC wordt doorgeleid aan de governance.
Output	Besluit Tactisch Beraad
Wie?	Operationeel Beraad Tactisch Beraad Voorzitter werkgroep

Proces contentmanagement

Voor een consistente externe communicatie is het van belang om een proces voor contentmanagement te hebben. Hiermee wordt de externe communicatie over eHerkenning structureel inhoudelijk getoetst aan het Afsprakenstelsel en de deelnemersovereenkomst. Bij het opstellen van nieuwe content of het wijzigen van bestaande content is dit proces van toepassing.

Doelstelling

Het proces contentmanagement heeft tot doel het:

1. organiseren van consistente externe communicatie over eHerkenning Consistent betekent in lijn met het Afsprakenstelsel en de deelnemersovereenkomst.
2. op transparante wijze verwerken van aangevraagde wijzigingen, zoals veranderingen in of het verwijderen van bestaande content of het opstellen van nieuwe content.

Classificatie van wijzigingen

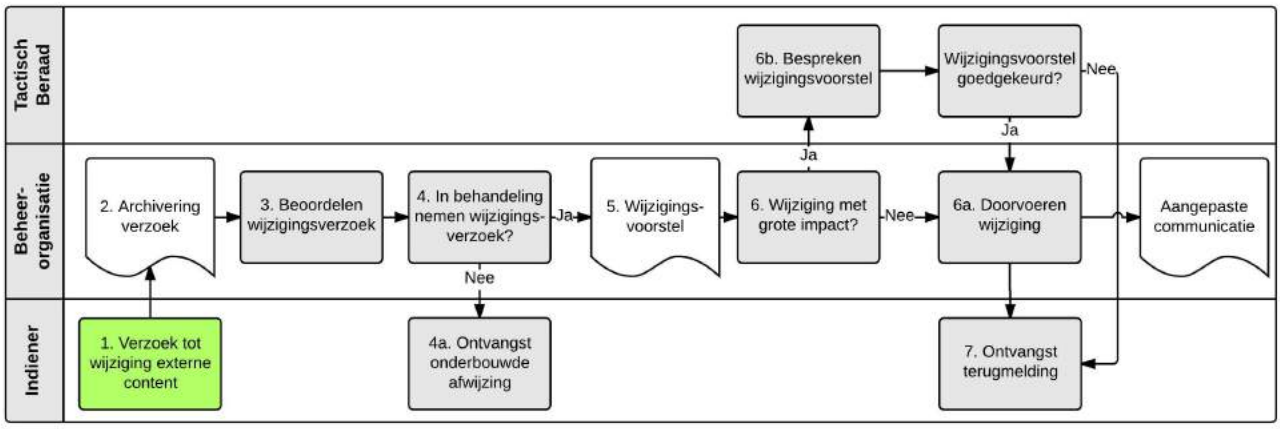
Externe communicatiemiddelen betreft voornamelijk informatie op de website van eHerkenning, maar ook presentaties, factsheets, nieuwsbrieven, artikelen, folders, handleidingen etc.

Impact	Beslissingsbevoegdheid	Voorbeelden
Klein	Beheerorganisatie	Dagelijks beheer, zoals het plaatsen van nieuwsberichten, wijzigen van links en actualiseren van presentaties en factsheets
Groot	Tactisch Beraad	Wijzigingen die van invloed zijn op het merk, het netwerk of de deelnemersovereenkomst, zoals wijzigingen in het aanmeldportaal of de keuzematrix.

Verantwoordelijkheden

- De **deelnemers** zijn verantwoordelijk voor het aanleveren van correcte content voor hun deel in de keuzematrix. Tevens beheren de deelnemers hun eigen communicatiemiddelen omtrent eHerkenning;
- Beheerorganisatie:
    - De **communicatieadviseur** verzorgt namens de beheerorganisatie het dagelijks beheer van de algemene communicatiemiddelen van e Herkenning. De communicatieadviseur voert wijzigingen met een kleine impact door, alsmede wijzigingen met een grote impact nadat hier door het Tactisch Beraad akkoord op is gegeven. Als proceseigenaar is de communicatieadviseur er namens de beheerorganisatie tevens verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving en dat de procesbeschrijving actueel blijft.
- Het **Tactisch Beraad** heeft tot taak te besluiten over wijzigingen met een grote impact.

Overzicht processtappen



Toelichting processtappen

1. Intake en 1e beoordeling	
In put	Verzoek tot wijziging van externe content.

Activiteit	1. Elke partij kan een verzoek tot het wijzigen van externe content indienen bij de beheerorganisatie op `emailadres`. Deelnemers kunnen in plaats daarvan een verzoek indienen in Mantis. Het verzoek bestaat minimaal uit:Alle wijzigingsverzoeken worden door de beheerorganisatie gearchiveerd in Mantis of in de e-mail. • de voorgestelde wijziging; • de reden voor de wijziging; • de urgentie van de wijziging. 2. De beheerorganisatie beoordeelt de impact van het wijzigingsverzoek en of het in lijn is met het Afsprakenstelsel en de deelnemersovereenkomst. 3. De beheerorganisatie neemt het verzoek al dan niet in behandeling. a. In het geval van een afwijzing wordt hiervan een onderbouwde tergmelding gedaan naar de aanvrager.
Output	• Eerste beoordeling verzoek tot wijziging; • In behandeling genomen wijzigingsverzoek of afgewezen wijzigingsverzoek.
Wie?	De secretaris van de beheerorganisatie beoordeelt de impact van het wijzigingsverzoek.

2. Opstellen, doorvoeren en terugmelden	
Input	Eerste beoordeling verzoek tot wijziging.
Activiteit	5. Na een eerste beoordeling formuleert de beheerorganisatie een wijzigingsvoorstel dat in lijn is met het verzoek tot wijziging, het Afsprakenstelsel en de deelnemersovereenkomst. 6. De beheerorganisatie beoordeelt de impact van het opgestelde wijzigingsverzoek. Bij twijfel wordt het verzoek voorgelegd aan inhoudelijke experts uit de beheerorganisatie zodat zij het kunnen toetsen aan het Afsprakenstelsel. a. Bij een wijziging met kleine impact: • De communicatieadviseur van de beheerorganisatie voert de wijziging na eigenstandig door; • Wijzigingen die zijn doorgevoerd op de website zijn terug te vinden in het log van het Content Management Systeem (Typo3), waarmee de website onderhouden wordt. In de praktijk vinden vrijwel alle gezamenlijke communicatie-uitingen ook plaats via de website (ook factsheets, handleidingen etc. worden via de website aangeboden). b. Bij een wijziging met grote impact: • De beheerorganisatie legt het wijzigingsvoorstel voor aan het Tactisch Beraad; • Na goedkeuring wordt de wijziging door de communicatieadviseur van de beheerorganisatie doorgevoerd; • Het goedgekeurde wijzigingsvoorstel is terug te vinden in de besluiten/vergaderstukken van de raad op tactisch niveau. Deze zijn openbaar beschikbaar op de website; 7. De beheerorganisatie doet een terugmelding aan de partij die het wijzigingsverzoek heeft gedaan van het doorvoeren van de wijziging of de afwijzing van het wijzigingsverzoek. • Terugmelding aan een deelnemer kan via Mantis; • Terugmelding aan een andere partij kan via e-mail. Alle terugmeldingen worden door de beheerorganisatie gearchiveerd in Mantis of de e-mail.
Output	• Goedgekeurd of afgekeurd wijzigingsvoorstel; • Beoordeling van de impact van het wijzigingsvoorstel; • Bij goedkeuring, doorvoering van de wijziging; • Terugmelding aan indiener.
Wie?	• De communicatieadviseur van de beheerorganisatie stelt wijzigingsverzoeken op en verwerkt ze (al dan niet na goedkeuring van het Tactisch Beraad); • Verschillende experts uit de beheerorganisatie helpen indien nodig bij het opstellen van het wijzigingsverzoek; • Het Tactisch Beraad besluit over de doorvoering van wijzigingsverzoeken met een grote impact.

Proces distributie en publicatie van documenten

De beheerorganisatie verricht algemene communicatie activiteiten voor Elektronische Toegangsdiensten. Een van die activiteiten is het publiceren van het Afsprakenstelsel Elektronische Toegangsdiensten en andere bij Elektronische Toegangsdiensten berustende informatie (dit betekent documenten met de classificatie 'Elektronische Toegangsdiensten openbaar'). De deelnemers en de beheerorganisatie gebruiken de documentatie voor het beheer van Elektronische Toegangsdiensten. Andere geïnteresseerde partijen kunnen de openbare documenten ook inzien.

Doelstelling

Publiceren van (de actuele versie van) alle documenten van het Afsprakenstelsel Elektronische Toegangsdiensten en andere bij Elektronische Toegangsdiensten berustende openbare documenten zodanig dat informatie over Elektronische Toegangsdiensten kenbaar en vindbaar is voor alle geïnteresseerde partijen. Hiermee wordt de transparantie van het beheer en de governance van Elektronische Toegangsdiensten vergroot.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De secretaris is ervoor verantwoordelijk dat de procesbeschrijving actueel blijft.

Processtappen

Input	• nieuwe versie van het afsprakenstelsel en/of; • bij Elektronische Toegangsdiensten berustende openbare documenten met betrekking tot Elektronische Toegangsdiensten
Activiteit	1. De beheerorganisatie publiceert het nieuwe afsprakenstelsel en andere openbare stukken aangaande Elektronische Toegangsdiensten in pdf formaat op de gezamenlijke digitale documentatieomgeving van Elektronische Toegangsdiensten en de website Elektronische Toegangsdiensten. 2. De deelnemers, de beheerorganisatie en sommige aangesloten overheidsdienstverleners hebben een gepersonaliseerde account met leesrechten voor de documentatieomgeving. Andere geïnteresseerde partijen kunnen via de website de openbare documentatie lezen en downloaden. 3. De openbare documentatie blijft beschikbaar op de documentatieomgeving en de website. De deelnemers, de beheerorganisatie, de overheidsdienstverleners en andere geïnteresseerden kunnen het onbeperkt raadplegen.
Output	Actief gepubliceerde openbare documenten op de website van Elektronische Toegangsdiensten en de gezamenlijke digitale documentatieomgeving van Elektronische Toegangsdiensten.
Wie?	Secretaris van de beheerorganisatie

Proces doorvoeren nieuwe dienstencatalogus

In de dienstencatalogus zijn alle diensten van aangesloten dienstverleners opgenomen die worden onderscheiden binnen Elektronische Toegangsdiensten. De beheerorganisatie beheert de geaggregeerde dienstencatalogus. Dit proces beschrijft hoe wijzigingen op de dienstencatalogus worden doorgevoerd.

Voor de publicatie van de dienstencatalogus in de testomgeving is geen formeel proces afgesproken buiten het feit dat deze op de, in het proces hieronder beschreven, URL wordt gepubliceerd. In de dienstencatalogus in de testomgeving worden de testdiensten van de simulator gepubliceerd, alsmede testomgevingen van dienstverleners indien en voor zover deze testmiddelen en -machtigingen van andere deelnemers willen gebruiken..

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Overzicht processtappen

- 1. Aanleveren nieuwe dienstencatalogusinformatie
- 2. Aanleveren nieuwe dienstencatalogus
- 3. Controleren en aggregeren dienstencatalogus
- 4. Nieuwe dienstencatalogus doorvoeren
- 5. Terugkoppeling onjuistheden dienstencatalogus

Toelichting processtappen

1. Aanleveren nieuwe dienstencatalogusinformatie	
Input	Wens tot registreren van nieuwe dienst of aanpassen bestaande dienst.

Activiteit	De aangeleverde informatie is afhankelijk van het type: een Dienst of een Dienst welke Dienstbemiddeling toepast. De dienstverlener levert informatie over de dienst aan bij de (primaire) Herkenningsmakelaar. Deze informatie over de dienst MOET het volgende bevatten: In het geval van een Dienst die niet zelf Dienstbemiddeling toepast (de dienst mag wel Dienstbemiddeling accepteren): 1. Of de dienst/dienstverlener al publiek beschikbaar is (op een publiek toegankelijke webpagina) voor IsPublic; 2. De precieze URL waar de dienst beschikbaar is (alleen voor diensten die al publiek beschikbaar zijn); 3. De precieze URL waar de voor de dienst geldende privacy policy beschikbaar is (alleen voor diensten die attributen uitvragen); 4. Een correcte, voor gebruikers te begrijpen beschrijving van de dienstverlener (voor OrganizationDisplayName); 5. Een correcte, voor gebruikers te begrijpen naam van de dienst (voor Servicename) en beschrijving (voor ServiceDescription); 6. De gewenste ServiceID en ServiceUUID (kunnen in overleg met de Herkenningsmakelaar worden afgestemd); 7. Het betrouwbaarheidsniveau wat door de dienst wordt gevraagd (voor AuthnContextClassRef). Dit MOET het standaard betrouwbaarheidsniveau zijn voor de dienst, zoals in de Dienstencatalogus (DC) beschreven. Een bestaande dienst MAG op deze wijze NIET van betrouwbaarheidsniveau gewijzigd worden. Indien een dienst van betrouwbaarheidsniveau wijzigt MOET deze opgevoerd worden als nieuwe dienst; 8. De soorten dienstafnemer die de dienst kunnen gebruiken (voor EntityConcernedTypesAllowed); 9. De beperkingen die de dienst kan verwerken (voor ServiceRestrictionsAllowed); 10. Indien er een internetpagina is met uitgebreidere beschrijving van de dienst: een URL van die internetpagina (voor ServiceDescriptionURL); 11. Het certificaat waarmee te ontvangen identiteiten en attributen versleuteld moeten worden (voor ServiceCertificate); 12. Als een HM een nieuwe DV aansluit die voor zijn dienstverlening intermediaire CA's wil gebruiken die niet op https://cert.pkioverheid.nl/ vermeld zijn, dan moet de HM dit in Mantis melden. De overige deelnemers dienen de CA conform Service level toe te voegen aan hun systemen. 13. Indien er attributen voor de dienst uitgevraagd (kunnen) worden, MOET ieder attribuut aangemeld worden inclusief doelverantwoording (voor het vullen van RequestedAttribute en PurposeStatement); 14. Indien de dienst via meer dan één Herkenningsmakelaar wordt gekoppeld aan Elektronische Toegangsdiensten: de namen en/of OINs van de verschillende alternatieve Herkenningsmakelaars (voor AdditionalHerkenningsmakelaarID). N.B. de alternatieve Herkenningsmakelaars leveren verder geen informatie over de dienst aan de beheerorganisatie, alleen de primaire Herkenningsmakelaar; 15. Aangeven of voor deze dienst Dienstbemiddeling is toegestaan en zo ja, of toestemming nodig is. Bij vereiste toestemming geldt dit ook voor toevoegen/intrekken van toestemming voor een specifieke bemiddeling, door het OIN van de betreffende dienstbemiddelaars door te geven. 16. Indien de Dienstinstantie (ServiceInstance) in aanmerking komt voor één of meer classificaties dan worden deze doorgegeven. Zie 'Classifiers' onder Service catalog. 17. De RecipientKeySetVersion (Sleutelsetversie voor ontsleutelen van versleutelde pseudoniemen, afgeleid van geldigheidsdatum PKIo-certificaat). In het geval een Dienst met toepassing van Dienstbemiddeling wordt aangesloten/aangepast: 1. De bovenstaande punten 1, 3, 4, 6, 11 en 14. 2. Welke Dienst instantie wordt bemiddeld, door het ServiceUUID van de betreffende dienst instantie (ServiceInstance) uit de dienstencatalogus op te geven. 3. De dienstinstantie mag verder niet opnieuw bemiddeld worden.
Output	1. Aangeleverde nieuwe / gewijzigde dienstinformatie van dienstverlener 2. Geïnformeerde Herkenningsmakelaar
Wie?	Dienstverlener

2. Aanleveren nieuwe dienstencatalogus

Input	Aangeleverde nieuwe/gewijzigde dienstinformatie van dienstverlener
Activiteit	Deelnemers (in de rol van Herkenningsmakelaar) vullen de door de dienstverlener geleverde informatie zonodig nog aan met het ServiceID, ServiceUUID, het HerkenningsmakelaarID en AdditionalHerkenningsmakelaarID en stellen de, door de dienstverlener beschikbaar gestelde, wijziging op de dienstencatalogus binnen twee werkdagen na ontvangst ter beschikking aan bij de beheerorganisatie door deze te publiceren op een URL (deze URL verwijst naar een dienstencatalogusbestand met daarin alle diensten van de klanten van deze HM). Een Herkenningsmakelaar neemt Diensten die gebruik maken van Dienstbemiddeling alleen op indien toestemming aan de Dienstbemiddelaar is verleend door de Dienstaanbieder (indien van toepassing). Indien voor een Dienst het urn:etoegang:1.12:EntityConcernedID:BSN als identificerend kenmerk wordt gevraagd, MOET een Herkenningsmakelaar controleren of de Dienstverlener vermeld staat op de Autorisatielijst BSN . Als de Dienstverlener vermeld staat op de Autorisatielijst dan MAG de Dienst het urn:etoegang:1.12:EntityConcernedID:BSN vragen; anders niet.
Output	1. Beschikbare nieuwe/gewijzigde dienstencatalogusentries van deelnemer 2. Geïnformeerde collega deelnemers in het stelsel
Wie?	Technisch beheerders deelnemers

3. Controleren en aggregeren dienstencatalogus

Input	Aangeleverde nieuwe dienstencatalogus van deelnemer
Activiteit	• De beheerorganisatie verwerkt één keer per kwartier de wijzigingen in de dienstencatalogi van de deelnemende HM's door middel van een automatisch proces. • Dit proces controleert de aangeleverde dienstencatalogus wijziging(en) op conformiteit en verwijdert de handtekeningen. Als een wijziging niet door de controle komt, dan wordt de betreffende deelnemer via mail op de hoogte gebracht en worden wijzigingen van deze deelnemer niet verder verwerkt tot een correcte dienstencatalogus wordt aangeleverd. • Vervolgens aggregeert dit proces de dienstencatalogi van de verschillende deelnemers tot één nieuw bestand. • Vervolgens wordt de nieuwe dienstencatalogus gepubliceerd op een publieke URL: https://aggregator.etoegang.nl/1.13/servicecatalog.xml. • De dienstencatalogus van de testomgeving wordt gepubliceerd op de publieke URL: https://aggregator.etoegang.nl/test/1.13/servicecatalog.xml . • Tevens wordt de nieuwe dienstencatalogus voor productie gearchiveerd.
Output	Gepubliceerde geaggregeerde nieuwe dienstencatalogus
Wie?	Technisch beheerder van de beheerorganisatie

4. Nieuwe dienstencatalogus doorvoeren

Input	Gepubliceerde geaggregeerde nieuwe dienstencatalogus
Activiteit	De deelnemers halen de nieuwe dienstencatalogus op vanaf de publieke URL en voeren deze door in hun systeem door middel van een automatisch proces. Deelnemers moeten een gewijzigde dienstencatalogus uiterlijk twee uur na publicatie doorvoeren.
Output	Doorgevoerde nieuwe dienstencatalogus.
Wie?	• Technisch beheerder beheerorganisatie • Technisch beheerders deelnemers

5. Terugkoppeling onjuistheden dienstencatalogus

Input	Feedback op dienstencatalogus entries uit de praktijk
Activiteit	1. Indien een deelnemer tijdens de uitvoering van zijn werkzaamheden constateert dat een dienstencatalogus entry onjuist is, MOET hij dat melden aan de desbetreffende Herkenningsmakelaar (direct of via een issue in Mantis). 2. Voorbeelden van onjuiste dienstencatalogus entries zijn onder andere: • Structureel andere betrouwbaarheidsniveaus uitgevraagd dan beschreven; • Dienst ondersteunt andere dienstafnemers dan beschreven; • Dienst staat beschreven als 'IsPublic=true' maar er is geen internetpagina voor de dienst; • Beschrijving van dienst is onjuist of onbruikbaar voor het kunnen uitgeven van machtigingen. • Dienstbemiddeling zonder toestemming Bij meldingen aan de Herkenningsmakelaar (direct of via Mantis) neemt deze contact op met de dienstverlener om wijzigingen te vragen van de dienstbeschrijving (keer terug naar stap 1 van dit proces).
Output	Input voor nieuw proces doorvoeren nieuwe dienstencatalogus.
Wie?	• Technisch beheerder deelnemer • Technisch beheerder beheerorganisatie

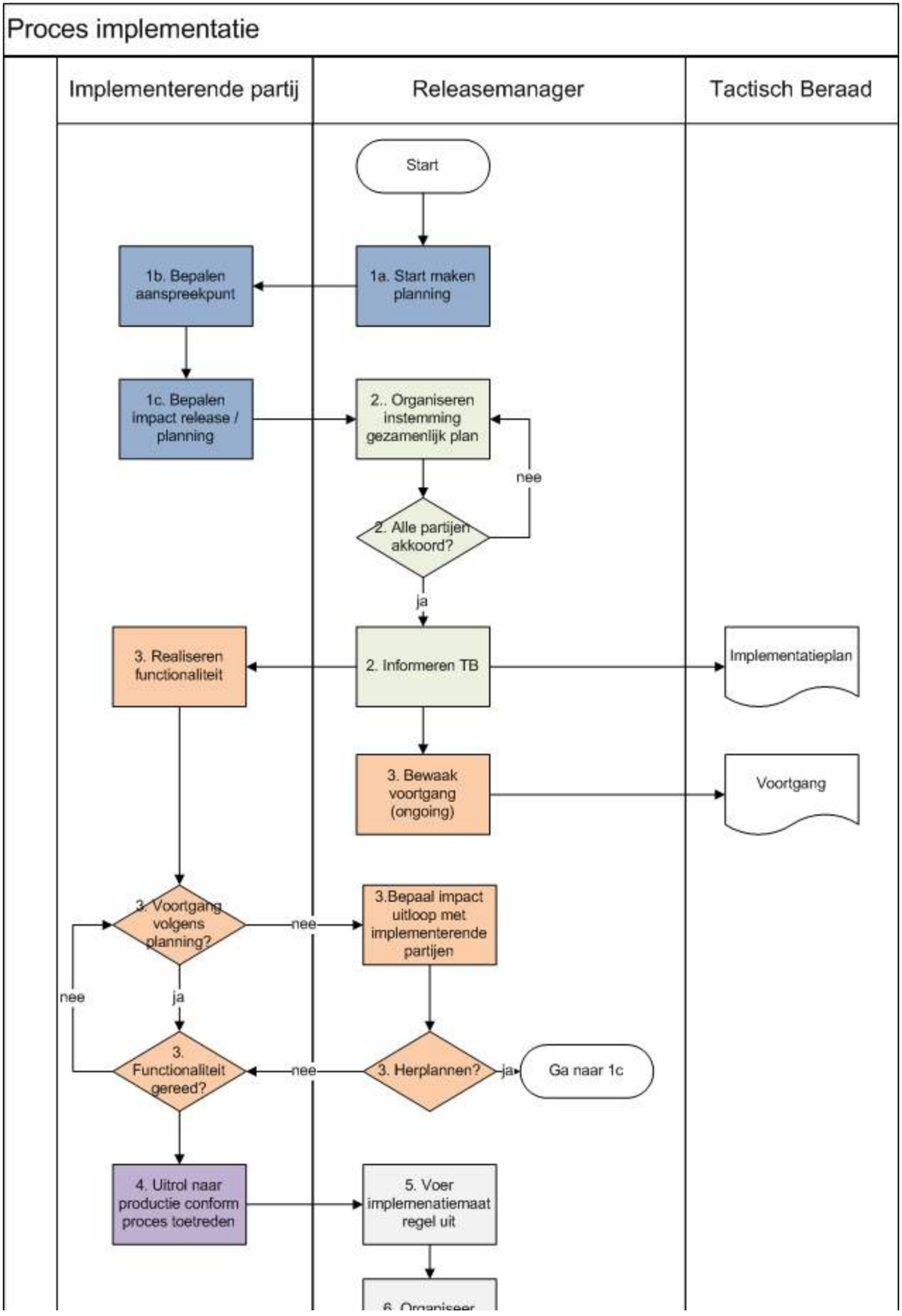
Proces implementatie koppelvlakrelease

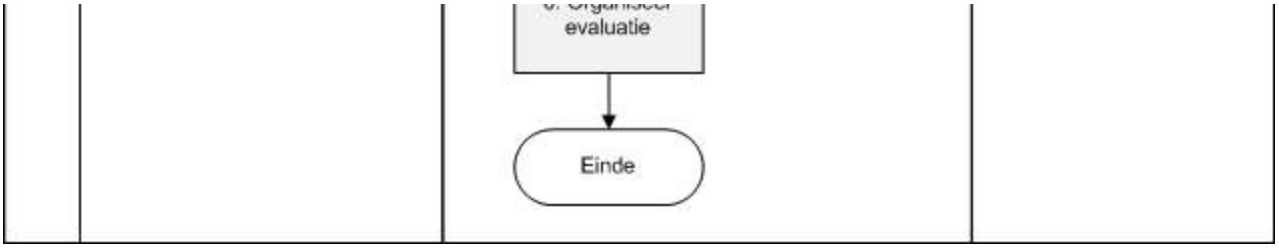
Doelstelling

Het realiseren van een nieuwe versie van een release door alle betrokken partijen is complex vanwege de onderlinge afhankelijkheden. Het eindresultaat hiervan is dat de nieuwe functionaliteit op een afgesproken moment voor alle gebruikers en dienstverleners in het stelsel beschikbaar is. Samenwerking vanuit alle betrokken partijen is nodig om de implementatie een succes te maken in een omgeving waarbij de marktpartijen ook concurrenten van elkaar zijn.

Een implementatie vergt daarom goede coördinatie en goede afspraken van wat partijen van elkaar mogen verwachten. De release manager heeft de taak om dit te organiseren; de betrokken partijen zelf zijn verantwoordelijk voor de invulling daarvan.

Overzicht processtappen


Proces implementatie
Implementerende partij
Releasemanager
Tactisch Beraad
Start
1a. Start maken planning
1b. Bepalen aanspreekpunt
1c. Bepalen impact release / planning
2.. Organiseren instemming gezamenlijk plan
2. Alle partijen akkoord?
nee
ja
2. Informeren TB
Implementatieplan
3. Realiseren functionaliteit
3. Bewaak voortgang (ongoing)
Voortgang
3. Voortgang volgens planning?
nee
ja
3.Bepaal impact uitloop met implementerende partijen
3. Functionaliteit gereed?
nee
3. Herplannen?
ja
Ga naar 1c
4. Uitrol naar productie conform proces toetreden
5. Voer implemenatiemaat regel uit



1. Opstellen implementatieplan	
Input	Vastgestelde release
Activiteit	De releasemanager stelt in afstemming met de aanspreekpunten per implementerende partij een implementatieplan op in het geval de release ketenafhankelijkheden bevat. Het proces om te komen tot een concreet en duidelijk afgebakend en gezamenlijk vastgesteld implementatieplan waaraan alle implementerende partijen zijn gebonden, is als volgt: 1. De implementerende partij (hierna partij) benoemt een verantwoordelijke voor de realisatie van een release. Deze persoon is voor die partij het aanspreekpunt tijdens de gehele implementatie. 2. Iedere partij maakt een impactanalyse en stelt een planning op. 3. De releasemanager stelt aan de hand van deze planningen en in samenwerking met deze aanspreekpunten, een concept implementatieplan op. In het concept implementatieplan wordt een voorstel gedaan voor: a. de concrete maatregelen die de verschillende partijen moeten nemen; b. de bijbehorende milestones en deadline(s).
Output	• Concept implementatieplan
Wie?	• Release manager • Bevoegde vertegenwoordigers van de implementerende partijen. • Aanspreekpunt van de implementerende partijen. • Tactisch Beraad

2. Vaststellen implementatieplan	
Input	Concept implementatieplan
Activiteit	De releasemanager organiseert dat de betrokken partijen met het concept implementatieplan kunnen instemmen. Het instemmen vindt plaats door het ondertekenen van het implementatieplan door een daartoe bevoegde vertegenwoordiger. Zodra alle implementerende partijen hebben getekend is het implementatieplan van kracht. De releasemanager communiceert het implementatieplan aan het Tactisch Beraad.
Output	Goedgekeurd en door de implementerende partijen ondertekend implementatieplan.
Wie?	• Implementerende partijen • De release manager

3. Realiseren release	
Input	Goedgekeurd implementatieplan

Activiteit	Na het vaststellen van het release- en implementatieplan start de realisatie en implementatie door de betrokken partijen. De implementatie bestaat uit één of meer van de volgende stappen: • De implementerende partijen realiseren de functionaliteit zoals afgesproken in het implementatieplan; • De Beheerorganisatie levert een communicatieplan op voor communicatie rondom de nieuwe implementatie; • De deelnemers treden toe tot de nieuwe versie van het Afsprakenstelsel conform het Proces toetreden. • De partijen voeren hun acties uit het communicatieplan uit. De partijen stemmen hun activiteiten af tijdens de implementatie onder regie van de releasemanager. De releasemanager monitort de voortgang van de gehele release en rapporteert tussentijds over de voortgang aan het Tactisch Beraad.
Output	Gerealiseerde functionaliteit
Wie?	• Implementerende partijen • De release manager

4. Uitrol release	
Input	Gerealiseerde functionaliteit
Activiteit	De uitrol van de release gaat conform het Proces netwerkmetadata. Het is van belang dat de activiteit en planning afgestemd wordt met de beheerorganisatie.
Output	Werkende functionaliteit in het productienetwerk.
Wie?	• Implementerende partijen • De releasemanager

5. Uitvoering evaluatie	
Input	De ervaringen van betrokken partijen bij het realiseren van de release.
Activiteit	De release manager organiseert binnen twee maanden nadat de implementatie gereed is een evaluatie met de betrokken partijen.
Output	• Evaluatie.
Wie?	• De release manager; • De implementerende partijen.

Proces incidentmanagement

Het afsprakenstelsel heeft een proces om incidenten binnen het Netwerk op te lossen.

Doelstelling

Het Proces Incidentmanagement heeft als doel om verschillende typen incidenten op gestructureerde wijze af te handelen binnen het stelsel. Daarbij dient de dienstverlening zo min mogelijk te worden verstoord.

Classificatie van incidenten

Incident	Een gebeurtenis die niet tot de standaardoperatie van een elektronische toegangsdienst behoort en die mogelijk impact c.q. risico oplevert ten aanzien van de kwaliteit, beschikbaarheid, integriteit en/of vertrouwelijkheid van (informatie binnen) het afsprakenstelsel. Incidenten kunnen bijvoorbeeld gaan om • Verstoringen: dit zijn gebeurtenissen die er toe leiden dat (onderdelen van) de dienstverlening van eHerkenning beperkt of niet beschikbaar zijn; • Informatiebeveiligingsincidenten: waaronder verlies van USB stick, laptop, losse harde schijf en ook signaleringen van hackpogingen, pogingen tot binnendringen in het systeem of malware; • Fraude of vermoeden van fraude door bijvoorbeeld een medewerker of hacker.
Calamiteit	Een incident waarvoor aan één van de volgende voorwaarden is voldaan: • Verwachte verstoringsduur overstijgt de afgesproken Responsetijden binnen het Beschikbaarheidsvenster; • Betrokkenheid van tenminste twee deelnemers; • Directe en ernstige hinder; • Impact op vertrouwelijkheid en integriteit; • Meldplichtig datalek als bedoeld in de Meldplicht datalekken.
Crisis	Een incident waarvoor aan één van de volgende voorwaarden is voldaan: • De calamiteit heeft een grote impact op de uitstraling/imago van eHerkenning en het vertrouwen van bedrijven en overheidsdienstverleners in het stelsel; • De verwachte verstoring i.e. onbeschikbaarheid van het stelsel duur langer dan 48 uur; • Bij de calamiteit spelen politieke beslissingen/implicaties; • De calamiteit betreft een fundamentele juridische of technische kwetsbaarheid (dus betrekking hebbend op opzet of structuur van Elektronische Toegangsdiensten).

Uitgangspunten

- Bij de oplossing van operationele of technische issues zijn alleen die personen/partijen betrokken die een directe operationele bijdrage kunnen leveren aan het oplossen van het probleem;
- Bij het noemen van een rol of functies in verband met het uitvoeren van een taak geldt dat bij afwezigheid van die functionaris standaard de plaatsvervanger van die rol of functie de taak overneemt;
- Als er besluiten met een grotere reikwijdte moeten worden genomen kunnen mogelijk andere partijen in de governance een rol gaan spelen.

Verantwoordelijkheden

De behandeling van incidenten is primair een operationele verantwoordelijkheid in de lijn Stelselpartij (Deelnemer, BO, BSNk of eIDAS berichtenservice) en de Beheerorganisatie.

- De **Stelselpartij** is verplicht om alle incidenten in het netwerk bij de Beheerorganisatie te melden en op aangeven van de incidentmanager, acties uit te zetten om het incident op te lossen.
- De Beheerorganisatie coördineert de afhandeling van het incident. De volgende rollen zijn daarbij van belang:
    - De **incidentmanager** is het eerste aanspreekpunt voor incidenten en coördineert en volgt de acties die genomen worden om incidenten op te lossen. De incidentmanager is verantwoordelijk dat het Proces Incidentmanagement wordt uitgevoerd conform de procesbeschrijving.
    - De **calamiteitenmanager** van Logius staat de incidentmanager bij (tijdens kantooruren) of vervangt deze (buiten kantooruren)
    - De **security officer** van de beheerorganisatie beslist of incidenten buiten Mantis om (ivm vertrouwelijkheid) behandeld moeten worden.

Vertrouwelijke incidenten

Een Deelnemer kan de Beheerorganisatie verzoeken een incident als vertrouwelijk te behandeelen. Indien het verzoek wordt gehonoreerd, wordt het niet opgenomen in Mantis. Reikt de impact van het incident niet verder dan de meldende Deelnemer dan controleert en volgt de Beheerorganisatie de voortgang van de oplossing. Een incident met een stelselbrede impact wordt altijd geregistreerd in Mantis en wordt, door de incidentmanager van de Beheerorganisatie, direct gemeld aan de Toezichthouder via het secretariaat van de Commissie van Deskundigen.

Overzicht processtappen incident

- 1. Intake incident
- 2. Beoordeling
    - 3a. Behandelen incident
    - 3b. Behandelen calamiteit
    - 3c. Behandelen crisis
- 4. Monitoren, informeren en ondersteunen
- 5. Sluiten incident
- 6. Opstellen rapportage derden

Toelichting processtappen

1. Intake incident	
Input	Een incident
Activiteit	Een Stelselpartij meldt het incident conform het Proces meldingenbeheer. Hierdoor kunnen alle Deelnemers en de Beheerorganisatie kennisnemen van het incident. ⚠ Bij (het vermoeden van) een calamiteit dient de melding ook per telefoon gedaan te worden bij de incidentmanager van de Beheerorganisatie. Buiten kantoortijd kan de standby manager bereikt worden via het Logius servicecentrum (0900 555 4555). Meldingen waarbij de melder vindt dat die vertrouwelijk moeten worden behandeld worden telefonisch én per mail bij de security officer van de beheerorganisatie gemeld. Bij het maken van de incidentmelding moeten de volgende gegevens worden opgenomen door de melder: • Een overzicht van de stappen die genomen moeten worden om het incident te reproduceren; • Indien van toepassing: het laatste bericht dat verstuurd werd voordat een incident optrad;
Output	Melding van een incident bij de Beheerorganisatie.
Wie?	• Meldende partij • Beheerorganisatie

2. Beoordeling	
Input	Melding van een incident bij de Beheerorganisatie
Activiteit	De Incidentmanager beoordeelt aan de hand van de classificatietabel de impact en urgentie van het incident.
Output	Beoordeeld incident.
Wie?	Beheerorganisatie

3a. Behandelen incident	
Input	Beoordeeld incident
Activiteit	1. Er worden één of meerdere oplossende partij(-en) aangewezen die verantwoordelijk zijn voor het verhelpen van het incident onder regie van de beheerorganisatie. 2. De Beheerorganisatie coördineert de acties en het contact met andere partijen. De incidentmanager is hierbij het eerste aanspreekpunt en is verantwoordelijk voor de communicatie tussen betreffende partijen. De incidentmanager heeft de beschikking over de inzet van de Beheerorganisatie. De incidentmanager is niet verantwoordelijk voor de externe communicatie van de deelnemers.
Output	Een oplossende partij; verantwoordelijk voor de acties om het incident op te lossen

Communicatie	Ondervindt de gebruiker hinder bij de dienstverlening? Zo ja, dan communiceren de deelnemers zelf via hun eigen kanalen richting de aangesloten dienstverleners en gebruikers. Alle deelnemers hebben hiervoor een eigen publiek toegankelijke webpagina met informatie over actuele (on)beschikbaarheid (onderhoud en storingen). Op deze pagina staat in elk geval: 1. Type situatie (beschikbaar/normale situatie, onbeschikbaarheid n.a.v. incident/calamiteit/crisis en onbeschikbaarheid n.a.v. onderhoud); 2. Toelichting bij de situatie (soort incident, reden onderhoud). Dit in voor de eindgebruiker begrijpelijke taal; 3. Datum en tijd start onbeschikbaarheid (ook toekomstig, gepland onderhoud); 4. Indicatie van de duur van de onbeschikbaarheid; 5. Handelingsperspectief (waar kan men terecht met vragen, verwijzing naar de klantenservice, etc.); 6. Datum en tijd einde onbeschikbaarheid (een melding blijft staan tot minimaal 24 uur nadat de onbeschikbaarheid is opgelost). Op de website www.eherkenning.nl wordt standaard verwezen naar de publiek toegankelijke webpagina's met actuele beschikbaarheidsinformatie van de deelnemers. Indien mogelijk wordt daar ook verwezen naar beschikbaarheidsinformatie van externe Componenten die onderdeel zijn van de primaire functionaliteit: EB, BRPk en BSNk. Aanvullend op de communicatie van de deelnemers kan eventueel door de beheerorganisatie gecommuniceerd worden, door het publiceren van een klein bericht over verstoring op de website www.eherkenning.nl, maar in principe doen we dit niet. Vaak staat de aard van de verstoring niet in verhouding tot de aandacht die een nieuwsbericht kan genereren. In principe communiceren de deelnemers zelf via de eigen kanalen richting de aangesloten dienstverleners en gebruikers als dat nodig wordt geacht. De deelnemers herhalen in hun berichtgeving dan de strekking van het nieuwsbericht dat de beheerorganisatie heeft geplaatst.
Wie?	• De incidentmanager van de Beheerorganisatie • De incidentmanager van de oplossende partij

3b. Behandelen calamiteit

Input	Het incident is ingeschat als calamiteit
Activiteit	De Beheerorganisatie coördineert het contact met andere betrokken partijen, bewaakt de acties en biedt indien nodig ondersteuning. Dit betekent dat de Beheerorganisatie met enige regelmaat de oplossende partij benadert voor informatie. Als een incident langer dan 4 uur duurt dan stelt de Beheerorganisatie de deelnemers minimaal 1 keer per 4 uur op de hoogte van de status. 1. De betrokken Stelselpartij(en) lossen in principe zelf de calamiteit op. Zij zijn zelf eerste verantwoordelijke voor het organiseren van een operationele oplossing; 2. De calamiteitenmanager informeert: a. De verantwoordelijke beleidsmedewerker bij BZK b. De directeuren van de deelnemers c. Naar eigen oordeel eventueel andere personen/organisaties (bijvoorbeeld NCSC of BZK) 3. De calamiteitenmanager organiseert binnen 24 uur een telefonische conferentie met alle betrokken partijen en zit deze voor. In deze conference call wordt in ieder geval over de interne en externe communicatie afspraken gemaakt; 4. De Beheerorganisatie draagt zorg voor de opstelling van een actieplan om risico's en schade te mitigeren; 5. De Beheerorganisatie[1] geeft advies aan BZK om te escaleren naar **crisis (3c)**. BZK neemt zelf dit besluit en komt daarmee "in the lead";
Output	Bijgewerkt incident
Communicatie	Ondervindt de gebruiker hinder bij de dienstverlening? Zo ja, dan moet er gecommuniceerd worden, zowel intern als extern via het volgende proces: 1. **Interne informatievoorziening**. Alle interne betrokkenen (beheerorganisatie, voorzitters Tactisch Beraad of Strategisch Beraad, BZK en deelnemers) moeten worden voorzien van dezelfde informatie. 2. **Vaststellen boodschap**. De communicatie adviseurs van de beheerorganisatie doen een voorstel voor de inhoud van het nieuwsbericht. De inhoud van het bericht moet afgestemd worden met de coördinator van de beheerorganisatie en indien nodig de betrokken deelnemers. Belangrijk is om afstemming van de inhoud te krijgen: a. Van wie komt het bericht en met wie moet het afgestemd worden? b. Het bepalen van de tijdslijn van het bericht: is berichtgeving van korte/lange duur, is de calamiteit maar één dag. Of moet de berichtgeving meerdere dagen herhaald worden? 3. **Publicatie**. Het nieuwsbericht over de calamiteit wordt gepubliceerd op de website www.eherkenning.nl. De beheerorganisatie wijst de betrokken partijen in het netwerk vervolgens op deze publicatie via e-mail of telefoon 4. **Verspreiding**. De betrokken partijen (zowel deelnemers als dienstverleners) in het netwerk kunnen dit nieuwsbericht overnemen op hun eigen websites. 5. **Informeren klanten**.De deelnemers informeren hun klanten (dienstverleners en gebruikers) in principe zelf. De beheerorganisatie heeft geen contactgegevens van de klanten en kan slechts de deelnemers hierbij ondersteunen. De deelnemers herhalen in hun berichtgeving de strekking van het nieuwsbericht dat de beheerorganisatie heeft geplaatst.

Wie?	• De incidentmanager BO • De calamiteitenmanager • De oplossende partij(en) • De communicatieadviseur adviseert over interne en externe communicatie (boodschap, kanalen, frequentie en doelgroep) en voert dit zo nodig uit via de diverse middelen en kanalen; • De jurist adviseert waar nodig of gewenst; • BZK • (De voorzitter van) het Tactisch Beraad

3c. Behandelen crisis

Input	Het incident is inschat als crisis
Activiteit	Het crisisteam van het Ministerie van BZK is in the lead, de betrokken personen vanuit de beheerorganisatie staan desgevraagd bij. De beheerorganisatie kondigt intern in het netwerk (alle Stelselpartijen, het Tactisch Beraad, het Operationeel Beraad, het Strategisch Beraad) direct een communicatiestop af.
Output	Bijgewerkt incident
Communicatie	Er geldt een communicatiestop. Stelselpartijen staan media niet zelf te woord maar verwijzen door naar de persvoorlichter/woordvoerder van BZK. BZK kan communicatieboodschappen opstellen en betrokken partijen opdragen deze over te nemen.
Wie?	• BZK • De incidentmanager BO • De calamiteitenmanager • De oplossende partij(en) • De communicatieadviseur, jurist en incidentmanager

4. Monitoren, informeren en ondersteunen

Input	Acties om het incident op te lossen
Activiteit	De Incidentmanager en/of calamiteitenmanager coördineert het contact met andere betrokken partijen, bewaakt de acties en biedt indien nodig ondersteuning. Dit betekent dat de Beheerorganisatie met enige regelmaat de oplossende partij benadert voor informatie. Indien het betreffende incident niet conform de afgesproken Responsetijden is opgelost bepaalt de Beheerorganisatie[1] of het incident geëscaleerd moet worden naar een **calamiteit (3b)**. Bij een calamiteit bepaalt BZK of er opgeschaald moet worden naar **crisis (3c)**. De Beheerorganisatie stelt de deelnemers minimaal 1 keer per 4 uur op de hoogte van de status in geval van crisis. In het geval dat de BO het incident niet escaleert naar een calamiteit dan kan de melder de BO vragen om een gesprek te organiseren om de impact en hinder te bespreken met de veroorzakende partij. Dit gesprek heeft als doel om afspraken te maken zodat het incident wordt opgelost inclusief de termijn en inzicht te krijgen of escalatie naar calamiteit van toepassing is. Het gesprek wordt georganiseerd binnen 5 werkdagen na binnenkomst van het verzoek. De uitkomst van het gesprek wordt gedeeld met de Toezichthouder .
Output	• Bijgewerkt incident • Op- of afschaling van het incident
Wie?	• De incidentmanager BO • De calamiteitenmanager • De oplossende partij

5. Sluiten incident

Input	Melding opgelost incident
Activiteit	De oplossende partij geeft een signaal aan de incidentmanager van de Beheerorganisatie zodra het incident is opgelost. De incidentmanager van de Beheerorganisatie meldt dit aan de overige deelnemers via Mantis. Indien het incident impact heeft op deelnemers in het stelsel, wordt dit door de incidentmanager als kenmerk toegevoegd aan de betreffende melding.

Output	Opgelost incident
Wie?	• De incidentmanager van de Beheerorganisatie • De oplossende partij

6. Opstellen rapportage derden	
Input	Mantismeldingen met specifiek kenmerk voor stelselincidenten

Activiteit	1. Voorafgaand aan het Security Officers overleg maakt de incidentmanager aan de hand van meldingen met specifiek kenmerk van stelselincident een samenvatting, met daarin:
	  • De aard van de incidenten;
	  • De oorzaak van de incidenten;
	  • Eventuele trends in aard en oorzaak van incidenten.
	2. In het Security Officers overleg wordt deze samenvatting geëvalueerd.
	3. De incidentmanager verwerkt de conclusies en aanbevelingen in de samenvatting.
	4. De Beheerorganisatie rapporteert de volledige samenvatting aan het Tactisch Beraad, de Eigenaar en de Toezichthouder.

Output	Algemeen periodiek evaluatierapport
Wie	Beheerorganisatie, leden van het Security Offers overleg.

Voetnoten

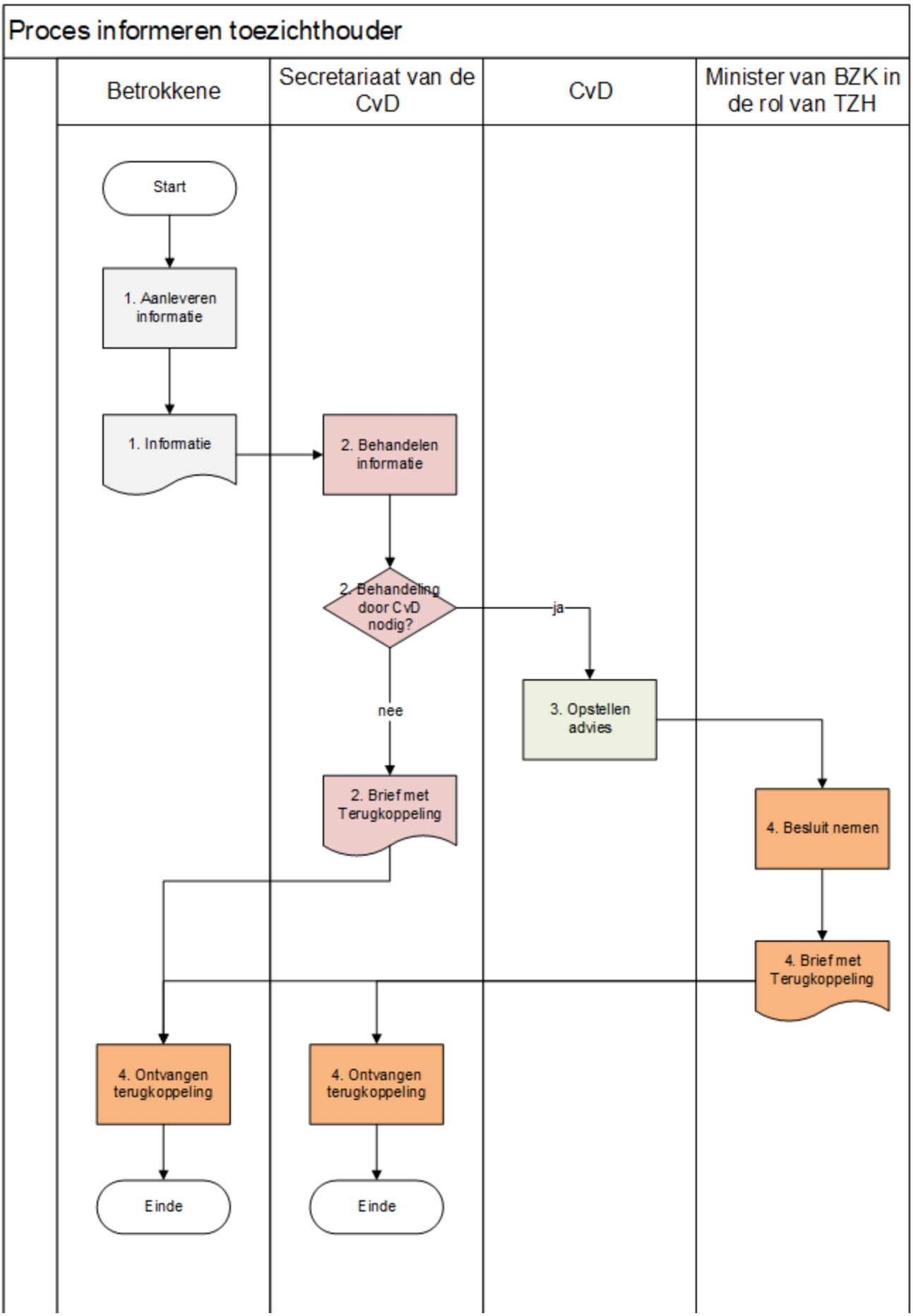
1. Deze beslissing wordt genomen door de coördinator van de Beheerorganisatie, zijn vervanger, of diens meerderen in lijn. Indien deze niet tijdig beschikbaar zijn, mag de beslissing ook worden genomen door twee andere medewerkers die betrokken zijn bij het behandelen van het incident, bijvoorbeeld de security officer en de incidentmanager. Zij dienen hierover later verantwoording af te leggen.

Proces informeren Toezichthouder

Doelstelling

Dit hoofdstuk geeft aan hoe informatie geleverd moet worden aan de Toezichthouder. Dat gaat via een aantal stappen, zoals hieronder is geschetst.

Overzicht processtappen


Proces informeren toezichthouder
Betrokkene
Secretariaat van de CvD
CvD
Minister van BZK in de rol van TZH
Start
1. Aanleveren informatie
1. Informatie
2. Behandelen informatie
2. Behandeling door CvD nodig?
ja
nee
3. Opstellen advies
2. Brief met Terugkoppeling
4. Besluit nemen
4. Brief met Terugkoppeling
4. Ontvangen terugkoppeling
4. Ontvangen terugkoppeling
Einde
Einde



Toelichting processtappen

1. Aanleveren informatie	
Input	• Leveren conform Afsprakenstelsel • Leveren op verzoek van Toezichthouder in het kader van de taak van CvD
Activiteit	**1.** Betrokkene (Deelnemer, Beheerorganisatie, BSNk) levert de informatie aan zoals is gevraagd dan wel is aangegeven in het Afsprakenstelsel. Dit doet de betrokkene door een mailbericht te sturen naar het secretariaat van de CvD of de stukken per post te versturen. **2.** Het secretariaat maakt een dossier op.
Output	Bevestiging van ontvangst van de secretariaat van de CvD.
Wie?	• Betrokkene • Secretariaat van de CvD

2. Behandeling door het secretariaat van de Commissie van Deskundigen	
Input	Informatie mbt verzoek
Activiteit	Het secretariaat behandelt de informatie en geleid het dossier door aan de Commissie van Deskundigen. Indien er geen besluit van de Toezichthouder nodig is geeft het secretariaat terugkoppeling aan de betrokkene met betrekking tot het dossier.
Output	• Dossier voor de CvD • Terugkoppeling aan de betrokkene
Wie?	• Secretariaat van de CvD • Betrokkene • CvD

3. Behandeling door de Commissie van Deskundigen	
Input	Dossier van het secretariaat
Activiteit	De CvD behandelt de informatie en stelt een advies op naar de Toezichthouder.
Output	Advies voor de Toezichthouder
Wie?	• Toezichthouder • CvD

4. Besluit door de Toezichthouder	
Input	Advies van de CvD

Activiteit	1. De Toezichthouder maakt een besluit naar aanleiding van het advies van de CvD en deelt die mee aan de betrokkene 2. Het secretariaat van de CvD ontvangt een kopie van het besluit
Output	Besluit
Wie?	• Toezichthouder • Betrokkene

Proces instandhouding en naleven

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor de veiligheid, betrouwbaarheid, geloofwaardigheid en het vertrouwen in het stelsel. Zowel de Deelnemers aan het Afsprakenstelsel als de Beheerorganisatie, BSNk en de Toezichthouder hebben een rol bij de instandhouding van het netwerk en de borging van het naleven van het Afsprakenstelsel. In eerste instantie gebeurt het toezien op de naleving zo veel mogelijk vanuit een zelfregulerend systeem en in goed onderling overleg tussen partijen in het Afsprakenstelsel. Om de veiligheid, betrouwbaarheid, geloofwaardigheid van en het vertrouwen in het Afsprakenstelsel te waarborgen kan het echter noodzakelijk zijn een correcte naleving te bewerkstelligen door middel van een interventie. De Toezichthouder houdt toezicht op de naleving van stelselafspraken door de Deelnemers, Beheerorganisatie en BSNk voor zover die betrekking hebben op de veilige en betrouwbare werking van het Afsprakenstelsel.

Meldingen en klachten van Deelnemers, Beheerorganisatie, BSNk, Dienstverleners en Dienstafnemers ten aanzien van de veilige en betrouwbare werking van het Afsprakenstelsel worden aan de Toezichthouder gedaan.

Doelstelling

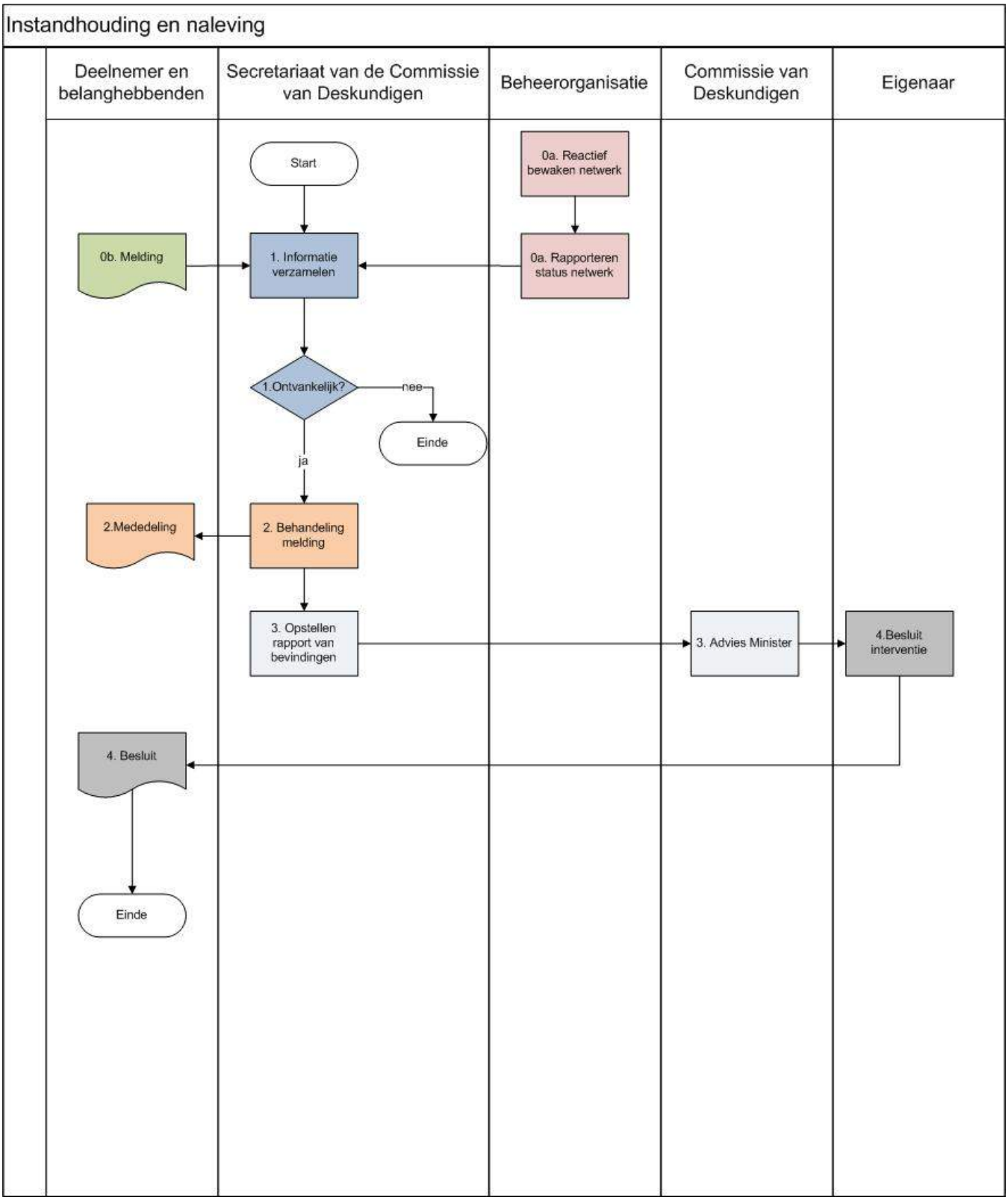
Het Proces instandhouding en naleving heeft als doel de veilige en betrouwbare werking, de geloofwaardigheid van en het vertrouwen in het gehele Afsprakenstelsel te borgen door middel van:

- het behandelen van signalen van Deelnemers, Beheerorganisatie, BSNk, Dienstverleners en Dienstafnemers.
- het behandelen van signalen vanuit de Beheerorganisatie omtrent de technische operationele status en de werking van het netwerk
- het beoordelen of afspraken genoemd in het Afsprakenstelsel (inzake de veilige en betrouwbare werking) naar behoren worden uitgevoerd
- het bewerkstelligen van naleving door middel van interventies

Verantwoordelijkheden

- De Eigenaar is eindverantwoordelijk voor de veilige en betrouwbare werking van het Afsprakenstelsel.
- Het toezicht op de veilige en betrouwbare werking van het Afsprakenstelsel is belegd bij de Toezichthouder. Om de Toezichthouder te adviseren is een Commissie van Deskundigen (CvD) ingesteld. De CvD wordt ambtelijke ondersteund door het Secretariaat van de Commissie van Deskundigen gevestigd bij Agentschap Telecom. Meldingen en klachten, voor zover deze betrekking hebben op de betrouwbaarheid en veilige werking van het Afsprakenstelsel, worden door Deelnemers, Beheerorganisatie, BSNk, Dienstverleners en Dienstafnemers gedaan aan de Toezichthouder.
- De Beheerorganisatie is verantwoordelijk voor de instandhouding van de goede technische werking van de gemeenschappelijke voorzieningen in het Afsprakenstelsel, zoals de metadata- en dienstencatalogusaggregator, Mantis en de website eherkenning.nl. De Beheerorganisatie controleert reactief, voornamelijk vanuit meldingen die conform het incidentmanagementproces worden gedaan en rapporteert aan de Toezichthouder omtrent de technische operationele status en werking van het netwerk.
- De Deelnemer heeft zich verplicht tot het naleven van de stelselafspraken voor specifieke stelselrollen via de ondertekende Deelnemersovereenkomst.
- De Dienstverlener (DV) is zelf verantwoordelijk voor de veilige en betrouwbare werking van de online dienst die hij aanbiedt. Voor aansluitingen op het Afsprakenstelsel sluit de Dienstverlener een contract met de Herkenningsmakelaar waarmee de Dienstverlener zich verplicht tot het nakomen van de Gebruiksvoorwaarden Elektronische Toegangsdiensten . Daarnaast ondertekent de Dienstverlener een zelfverklaring (Template zelfverklaring Dienstverlener). In het kader van indirecte controle is de Dienstverlener verplicht om een zelfverklaring af te leggen aan de Deelnemer over de naleving van de voor hem geldende stelselafspraken.
- De Dienstafnemer (burgers, werknemers, consumenten) sluit een contract met de Middelenuitgever/ Authenticatiedienst en/of Machtigingenregister waarmee de Dienstafnemer zich verplicht tot het nakomen van voorwaarden voor het gebruik.

Overzicht processtappen



Toelichting processtappen

0a. Reactief bewaken netwerk en rapportage status van het netwerk	
Input	Reguliere beheerprocessen

Activiteit	De Beheerorganisatie bewaakt de operationele werking van de eigen beheerobjecten. Deelnemers rapporteren periodiek aan de Beheerorganisatie over het gebruik van het afsprakenstelsel. Zie hiervoor het Proces managementrapportage. De beheerorganisatie aggregeert deze informatie en rapporteert die aan de Toezichthouder en het Tactisch Beraad. De Beheerorganisatie rapporteert over informatiestromen die uit de stelselbeheerprocessen komen en betrekking hebben op de veilige en betrouwbare werking van het afsprakenstelsel aan de Toezichthouder. Voorbeelden hiervan zijn: • administraties in het kader van stelselwijzigingen, incidenten, managementinformatie, toetredingen en uittredingen, • administraties van zowel de uitvoering als de uitkomsten van controles, zoals de rapporten van technische testen, penetratietesten en merkbescherming.
Output	Reguliere informatiestromen en rapportage over de werking van het afsprakenstelsel.
Wie?	• Beheerorganisatie • Toezichthouder

0b. Melding of klacht	
Input	Een vermoeden of feitelijke constatering van Deelnemers, Beheerorganisatie, BSNk, Dienstverleners en Dienstafnemers over niet-naleving van de stelselafspraken inzake de veilige en betrouwbare werking van het Afsprakenstelsel
Activiteit	Deelnemers, Beheerorganisatie, BSNk, Dienstverleners en Dienstafnemers in het Afsprakenstelsel kunnen een melding doen of een klacht indienen bij het secretariaat van de CvD als er een vermoeden van niet-naleving inzake de veilige en betrouwbare werking van het Afsprakenstelsel is. Informeren van de Toezichthouder vindt plaats via het secretariaat van de CvD conform het Proces informeren Toezichthouder.
Output	Een melding of klacht
Wie?	• Deelnemer, Beheerorganisatie, BSNk, Dienstverlener of Dienstafnemer die meldt • Toezichthouder

1. Informatie verzamelen	
Input	De Toezichthouder voert eigenstandig onderzoek uit ter toetsing van de conformiteit met het Afsprakenstelsel van Deelnemers, Beheerorganisatie en BSN-Koppelregister. Meldingen of klachten van Deelnemers, Beheerorganisatie, BSNk, Dienstverleners of Dienstafnemers kunnen naast eigen bevindingen van de Toezichthouder aanleiding zijn voor het starten van een onderzoek. Voorbeelden zijn: • Melding over het niet-naleven van de stelselafspraken • Meldingen van dienstverleners en dienstafnemers over de betrouwbaarheid en veiligheid van de geleverde stelseldiensten • Persistente verschillen van inzicht tussen stelselpartijen over de interpretatie van het afsprakenstelsel voor zover deze de veiligheid van en het vertrouwen in het Afsprakenstelsel (kunnen) raken
Activiteit	Een Deelnemer, de Beheerorganisatie, BSNk, Dienstverlener of Dienstafnemer in het Afsprakenstelsel informeert de Toezichthouder via het secretariaat van de CvD via een melding of klacht. Het secretariaat van de CvD ontvangt de melding of klacht en toetst de ontvankelijkheid en communiceert de uitkomst aan de betrokken partij(-en). De Toezichthouder start uit eigen beweging een onderzoek.
Output	Mededeling over behandeling
Wie?	• Deelnemer, Beheerorganisatie, BSNk, Dienstverlener of Dienstafnemer • Toezichthouder • Secretariaat van de Commissie van Deskundigen

2. Analyseren informatie	
Input	Melding, klacht, bevinding
Activiteit	Het Secretariaat van de Commissie van Deskundigen analyseert de informatie en stelt een analyse op van de verzamelde informatie. Bij het onderzoek wordt indien opportuun hoor en wederhoor toegepast.
Output	Analyserapport
Wie?	• Secretariaat van de Commissie van Deskundigen • Deelnemer, Beheerorganisatie, BSNk, Dienstverlener of Dienstafnemer

3. Adviseren Toezichthouder	
Input	Analyse
Activiteit	De Commissie van Deskundigen adviseert de Toezichthouder.
Output	Advies aan de Toezichthouder
Wie?	• CvD • Toezichthouder

4. Aanwijzing van de Toezichthouder	
Input	Advies aan de Toezichthouder
Activiteit	De Toezichthouder geeft al dan niet een aanwijzing, zoals genoemd in Inrichting toezicht. De betrokken Deelnemer(s), Beheerorganisatie, BSNk, Dienstverlener(s) of Dienstafnemer(s) worden door de Toezichthouder geïnformeerd. Merk op: Dit is niet een besluit in de zin van de Algemene wet bestuursrecht (Awb) en de Awb is in dit geval dan ook niet van op toepassing. Hier staat de civiele rechtsgang voor open.
Output	Aanwijzing
Wie?	• Toezichthouder • Betrokken Deelnemer, de Beheerorganisatie, BSNk, Dienstverlener of Dienstafnemer

Proces managementrapportage

Managementinformatie over het gebruik van het Netwerk en de werking van het Afsprakenstelsel wordt door middel van rapportages verzameld en verspreid. De rapportages worden o.a. gebruikt om de groei van het netwerk te monitoren.

Doelstelling

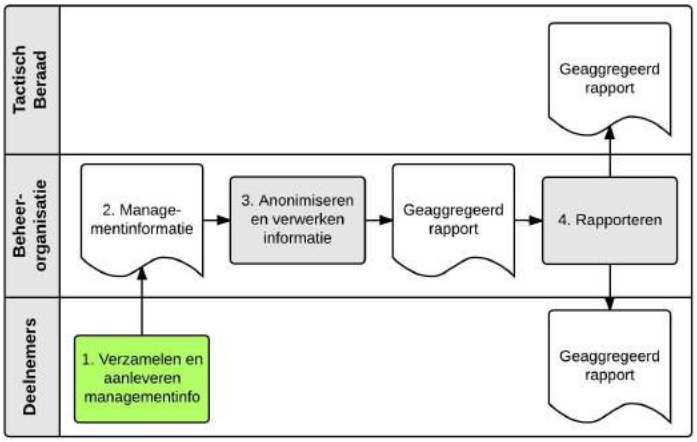
De doelstellingen van het proces managementinformatie zijn:

1. Zorgvuldig opstellen van de managementrapportage;
2. Verzamelen en verstrekken van informatie over de groei van het netwerk en de Service Level afspraken.

Verantwoordelijkheden

- De deelnemers zijn verantwoordelijk voor het aanleveren van managementinformatie conform de hiervoor opgestelde termijnen in het Service level.
- De Beheerorganisatie zorgt voor de verwerking van de gegevens tot een geaggregeerde rapportage. Hierbij is het van belang dat de concurrentiegevoelige informatie zoveel mogelijk verborgen blijft. Als proceseigenaar is de beheerorganisatie tevens verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving en dat de procesbeschrijving actueel blijft.

Overzicht processtappen



Toelichting processtappen

1. Aanleveren informatie	
Input	Rapportagetool. De beheerorganisatie stelt een tool beschikbaar voor het valideren en samenvoegen van de managementinformatie.
Activiteit	1. De deelnemers en de beheerorganisatie verzamelen de eigen managementinformatie van de rapportageperiode (zoals gedefinieerd in het Service Level Managementrapportage) in xml-formaat. Dit betreft: a. Informatie omtrent het gebruik van het Netwerk b. Informatie over de Service level afspraken. 2. De deelnemers en de beheerorganisatie leveren de eigen rapportage in xml-formaat aan bij de beheerorganisatie, bij voorkeur zo snel mogelijk maar in ieder geval zoals afgesproken in het Service Level Managementrapportage. De rapportage wordt geüpload met behulp van de daartoe ter beschikking gestelde rapportagetool. Bij het uploaden van de rapportage in xml-formaat wordt een aantal gestandaardiseerde checks uitgevoerd door de rapportagetool. 3. De deelnemers leveren een additionele rapportage per e-mail aan bij de beheerorganisatie zoals afgesproken in het Service Level Managementrapportage. De rapportage wordt verstuurd naar Logius Ketenbeheer en bevat cijfers over: a. Aantal ketenmachtigingen (van toepassing voor de rol Machtigingenregister (MR) b. Aantal belastingdienstmiddelen (van toepassing voor de rol Middelenuitgever (MU)
Output	Geüploade managementinformatie in xml-formaat per deelnemer volgens onderstaand XML schema. • E-mail richting de beheerorganisatie met rapportage over ketenmachtigingen en belastingdienstmiddelen

Wie?	• De deelnemers leveren de gevraagde gegevens voor de managementrapportage aan. • De beheerorganisatie levert de gevraagde gegevens voor de managementrapportage aan.

2. Verwerken informatie

Input	Managementinformatie per deelnemer.

Activiteit	3. De beheerorganisatie levert op:
	
	a. een geaggregeerde rapportage met daarin de geanonimiseerde en gebundelde gegevens van de deelnemers.
	
	• Er vindt een aantal aanvullende controles plaats nadat alle gegevens van deelnemers zijn ontvangen:
	  • Controle op aantallen middelen: komt de opgegeven groei/krimp overeen met de aantallen van voorgaande maand.
	  • Controle op aantallen aangesloten bedrijven: komt de opgegeven groei/krimp overeen met de aantallen van voorgaande maand.
	  • Controle op aantallen transacties:
	  • Komen bij de transacties tussen HM en AD de aantallen opgegeven door de HM overeen met de aantallen opgegeven door de AD.
	  • Komen bij de transacties tussen HM en MR de aantallen opgegeven door de HM overeen met de aantallen opgegeven door het MR.
	• Zonder geconstateerde fouten bij aangeleverde gegevens zal de beheerorganisatie trachten de rapportage daags na de laatst opgeleverde gegevens geanonimiseerd en geaggregeerd gereed te hebben, maar uiterlijk binnen de in het Service level gestelde termijn.
	• Indien fouten in aangeleverde gegevens geconstateerd zijn, zal de beheerorganisatie dit via Mantis melden aan de betrokken deelnemer(s) en trachten binnen de genoemde periode juiste gegevens van de betrokken deelnemer(s) te verkrijgen en te verwerken.
	• De beheerorganisatie zal via Mantis aan de deelnemers melden als de managementrapportage niet binnen de afgesproken termijn opgeleverd kan worden met vermelding van de oorzaak ervan.
	• Indien het niet mogelijk is om geconstateerde fouten binnen 10 werkdagen in samenspraak met de betreffende deelnemer(s) op te lossen, zal alsnog de geaggregeerde managementrapportage gemaakt worden, met vermelding welke fouten in de rapportage aanwezig zijn (foutmarges + betrokken deelnemer(s)).
	• Indien nieuwe (betere) gegevens worden aangeleverd nadat de managementrapportage is samengesteld, zal de beheerorganisatie deze opnieuw samenstellen (indien er impact is op nieuwere managementrapportage zal de wijziging ook daar doorgevoerd worden). Na 3 maanden worden geen wijzigingen meer gedaan.
	
	Indien de beheerorganisatie bijzonderheden heeft te melden, worden deze bijgevoegd.

Output	Geaggregeerde rapportage managementinformatie over de laatste 12 maanden met onderstaande inhoud: **Overzicht aantallen dienstverleners (uit dienstencatalogus)**: Maand - Totaal aantal dienstverleners - Aantal nieuwe dienstverleners - Aantal verdwenen dienstverleners - Groei aantal aangesloten dienstverleners **Overzicht aantallen diensten (uit dienstencatalogus)**: Maand - Totaal aantal diensten - Aantal nieuw aangesloten diensten - Aantal verdwenen diensten - Groei aantal aangesloten diensten **Overzicht aantallen aangesloten bedrijven**: Maand - Totaal aantal aangesloten bedrijven - Aantal nieuw aangesloten bedrijven - Aantal afgesloten bedrijven - Groei aantal aangesloten bedrijven **Overzicht aantallen middelen**: Maand - Totaal aantal middelen - Aantal nieuw uitgegeven middelen - Aantal ingetrokken middelen - Groei uitgegeven middelen **Overzicht aantallen belastingdienstmiddelen:** Maand - Totaal aantal belastingdienstmiddelen- Aantal nieuw uitgegeven belastingdienstmiddelen- Aantal ingetrokken belastingdienstmiddelen- Groei uitgegeven belastingdienstmiddelen **Overzicht aantallen ketenmachtigingen (MR1):** Maand - Totaal aantal ketenmachtigingen (MR1) - Aantal nieuwe ketenmachtigingen (MR1) - Aantal ingetrokken ketenmachtigingen (MR1) - Groei uitgegeven ketenmachtigingen (MR1) **Overzicht aantallen ketenmachtigingen (MR2):** Maand - Totaal aantal ketenmachtigingen (MR2) - Aantal nieuw uitgegeven ketenmachtigingen (MR2) - Aantal ingetrokken ketenmachtigingen (MR2) - Groei uitgegeven ketenmachtigingen (MR2) **Overzicht aantallen transacties (DV-HM) (gegevens van HM's)**: Maand - Aantal AuthnRequest berichten - Aantal Response berichten- Aantal AuthnFailed response berichten **Overzicht aantallen transacties (HM-AD) (gegevens van HM's)**: Maand - Aantal AuthnRequest berichten - Aantal Response berichten- Aantal AuthnFailed response berichten **Overzicht aantallen transacties (HM-AD) (gegevens van AD's)**: Maand - Aantal AuthnRequest berichten - Aantal Response berichten- Aantal AuthnFailed response berichten **Overzicht aantallen transacties (HM-MR) (gegevens van HM's)**: Maand - Aantal XACMLAuthzDecisionQuery berichten - Aantal Response berichten - Aantal XACMLDeny response berichten **Overzicht aantallen transacties (HM-MR) (gegevens van MR's)**: Maand - Aantal XACMLAuthzDecisionQuery berichten - Aantal Response berichten - Aantal XACMLDeny response berichten

Wie?	De beheerorganisatie aggregeert de gegevens en levert de managementrapportage op.

3. Verspreiden informatie	
Input	Geaggregeerde rapportage managementinformatie.
Activiteit	4. De beheerorganisatie verzendt de geaggregeerde rapportage naar het Tactisch Beraad en stelt deze tevens ter beschikking op Confluence. De beheerorganisatie gebruikt de gegevens tevens voor eventuele periodieke rapportages.
Output	Verspreiding van de geaggregeerde rapportage.
Wie?	De beheerorganisatie stelt de rapportage ter beschikking.

Schema

XML schema

```
<?xml version="1.0"?>
<xs:schema
        xmlns="urn:nl:eherkenning:rapport:1.5"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="urn:nl:eherkenning:rapport:1.5" elementFormDefault="qualified" attributeFormDefault="
unqualified">
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="xmldsig-core-schema.xsd"/>
    <xs:simpleType name="BerichtCategorieType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="AuthnRequest"/>
            <xs:enumeration value="Response"/>
            <xs:enumeration value="Authnfailed response"/>
            <xs:enumeration value="XACMLAuthzDecisionQuery"/>
            <xs:enumeration value="XACMLDeny response"/>
            <xs:enumeration value="XACMLPermit response"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="NiveauType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"/>
            <xs:enumeration value="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"/>
            <xs:enumeration value="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"/>
            <xs:enumeration value="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"/>
            <xs:enumeration value="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="AantallenType">
        <xs:sequence>
            <xs:element name="NieuwDezePeriode" type="xs:integer" minOccurs="1" maxOccurs="1"/>
            <xs:element name="AfgeslotenDezePeriode" type="xs:integer" minOccurs="1" maxOccurs="1"/>
            <xs:element name="TotaalDezePeriode" type="xs:integer" minOccurs="1" maxOccurs="1"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AantallenPerNiveauType">
        <xs:sequence>
            <xs:element name="Niveau" minOccurs="1" maxOccurs="unbounded">
                <xs:complexType>
                    <xs:complexContent>
                        <xs:extension base="AantallenType">
                            <xs:attribute name="niveau" type="NiveauType"/>
                        </xs:extension>
                    </xs:complexContent>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AantalBerichtenPerKoppelvlakType">
        <xs:sequence>
```

```
            <xs:element name="AantalBerichten" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                    <xs:simpleContent>
                        <xs:extension base="xs:integer">
                            <xs:attribute name="berichtCategorie" type="BerichtCategorieType"/>
                        </xs:extension>
                    </xs:simpleContent>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
        <xs:attribute name="entityID" type="xs:string"/>
    </xs:complexType>
    <xs:element name="Rapport">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ds:Signature" minOccurs="1" maxOccurs="1"/>
                <xs:element name="Opmerking" type="xs:string" minOccurs="0"/>
                <xs:element name="HMRol" minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="AantalDienstverleners" type="AantallenType" minOccurs="1"
maxOccurs="1"/>
                            <xs:element name="AantalBerichtenDienstverlener" type="
AantalBerichtenPerKoppelvlakType" minOccurs="0" maxOccurs="unbounded"/>
                            <xs:element name="AantalBerichtenAuthenticatieDienst" type="
AantalBerichtenPerKoppelvlakType" minOccurs="0" maxOccurs="unbounded"/>
                            <xs:element name="AantalBerichtenMachtigingregister" type="
AantalBerichtenPerKoppelvlakType" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute name="entityID" type="xs:anyURI"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="ADRol" minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="AantalBerichtenHerkenningsmakelaar" type="
AantalBerichtenPerKoppelvlakType" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute name="entityID" type="xs:anyURI"/>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MURol" minOccurs="0" maxOccurs="1">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="AantalMiddelen" type="AantallenPerNiveauType" minOccurs="1"
maxOccurs="1"/>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="MRRol" minOccurs="0" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="AantalBedrijven" type="AantallenType" minOccurs="1" maxOccurs="1"
/>
                            <xs:element name="AantalBerichtenHerkenningsmakelaar" type="
AantalBerichtenPerKoppelvlakType" minOccurs="0" maxOccurs="unbounded"/>
                        </xs:sequence>
                        <xs:attribute name="entityID" type="xs:anyURI"/>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
            <xs:attribute name="oin" type="xs:anyURI"/>
            <xs:attribute name="title" type="xs:string"/>
            <xs:attribute name="datumOpgeleverd" type="xs:dateTime"/>
            <xs:attribute name="rapportPeriodeVan" type="xs:dateTime"/>
            <xs:attribute name="rapportPeriodeTot" type="xs:dateTime"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Rapportage Belastingdienstmiddelen

Er moet worden gerapporteerd over het aantal belastingdienstmiddelen. Het gaat hier per kalendermaand over de volgende getallen:

- Aantal nieuwe belastingdienstmiddelen geregistreerd in deze kalendermaand
- Aantal afgesloten belastingdienstmiddelen in deze kalendermaand
- Totale aantal belastingdienstmiddelen aan het einde van deze kalendermaand (laatste dag om 23.59 Nederlandse tijd)

De definitie van een belastingdienstmiddel is: eHerkenningsmiddel op EH3 waarmee een persoon namens een organisatie kan handelen en dat een specifieke restrictie heeft om enkel bruikbaar te zijn bij de belastingdienst. Het middel komt in aanmerking voor de subsidieregeling uitgevoerd door RVO voor het belastingdienstmiddel. Elke persoon/organisatie combinatie telt als één belastingdienstmiddel.

Template

Maak voor het versturen per e-mail gebruik van de volgende template:

Naam middelenuitgever	
Heeft betrekking op	Maand /Jaar
Aantal nieuwe belastingdienstmiddelen	
Aantal afgesloten belastingdienstmiddelen	
Totale aantal belastingdienstmiddelen	

Rapportage Ketenmachtigingen

Er moet worden gerapporteerd over de het aantal geregistreerde ketenmachtigingen. Omdat een ketenmachtiging uit een MR1 en een MR2 deel bestaat is het moet hier apart over gerapporteerd worden.

Bij alle getallen gaat het om de aantallen per kalendermaand. Onderstaand wordt per MR gedefinieerd waar de op te leveren cijfers aan moeten voldoen.

MR1

- Aantal nieuwe ketenmachtigingen geregistreerd in deze kalendermaand
- Aantal afgesloten ketenmachtigingen in deze kalendermaand
- Totale aantal ketenmachtigingen aan het einde van deze kalendermaand (laatste dag om 23.59 Nederlandse tijd)

Een MR1 machtiging is een machtiging die een intermediair ontvangen heeft om te mogen handelen bij één of meerdere dienstverleners namens een externe organisatie. Elke intermediair/organisatie combinatie telt als één machtiging. Voor welke specifieke diensten en dienstverleners, en welk aantal diensten is niet van belang. Ook het aantal medewerkers van de intermediair dat gebruik mag maken van de machtiging is niet relevant. De machtiging telt als actief als er minimaal één bruikbare machtiging is om bij een dienstverlener te mogen handelen namens een organisatie door een intermediair. Een machtiging telt als inactief als de laatste machtiging voor een dienst is afgesloten en deze dus effectief nergens meer bruikbaar is. Of er wel- of geen MR2 machtiging is (en of men dus praktisch gebruik kan maken van de machtiging), is niet relevant.

MR2

- Aantal nieuwe ketenmachtigingen geregistreerd in deze kalendermaand
- Aantal afgesloten ketenmachtigingen in deze kalendermaand
- Totale aantal ketenmachtigingen aan het einde van deze kalendermaand (laatste dag om 23.59 Nederlandse tijd)

Een MR2 machtiging is een machtiging die een organisatie heeft afgegeven aan een derde partij om namens hem te kunnen handelen. Elke intermediair /organisatie combinatie telt als één machtiging. Voor welke specifieke diensten en dienstverleners, en welk aantal diensten is niet van belang. De machtiging telt als actief als er minimaal één bruikbare machtiging is om bij een dienstverlener te mogen handelen namens de organisatie door een intermediair. Een machtiging telt als inactief als de laatste machtiging voor een dienst is afgesloten en deze dus effectief nergens meer bruikbaar is. Of er wel- of geen MR1 machtiging is (en of men dus praktisch gebruik kan maken van de machtiging), is niet relevant.

Template

Maak voor het versturen per e-mail gebruik van de volgende template:

Naam machtigingenregister	
Heeft betrekking op	Maand /Jaar
Aantal nieuwe ketenmachtigingen MR1	
Aantal afgesloten ketenmachtigingen MR1	
Totale aantal ketenmachtigingen MR1	
Aantal nieuwe ketenmachtigingen MR2	
Aantal afgesloten ketenmachtigingen MR2	
Totale aantal ketenmachtigingen MR2	

Proces meldingenbeheer

De beheerorganisatie is aanspreekpunt voor zaken met betrekking tot de ontwikkeling en implementatie van het Afsprakenstelsel Elektronische Toegangsdiensten. Mantis functioneert als portaal voor het maken van meldingen. Bij het melden van een incident moet het proces incidentmanagement als basis genomen worden.

Deelnemers en de beheerorganisatie gebruiken Mantis voor het aanmaken van meldingen. Bijvoorbeeld voor het melden van problemen met betrekking tot het implementeren van het Afsprakenstelsel, server onderhoud, simulators, metadata en dienstencatalogus, en beveiligingsissues. Opvolging van de meldingen vindt ook in Mantis plaats.

Doelstelling

De doelstelling van het proces meldingenbeheer is enerzijds dat meldingen op de juiste manier aangemaakt worden en anderzijds dat er snel en adequate hierop gereageerd kan worden zodat ontwikkeling en implementatie voorspoedig verloopt en de productieomgeving goed functioneert.

Verantwoordelijkheden

- De technisch beheerder van de beheerorganisatie zorgt ervoor dat het beschreven proces correct wordt uitgevoerd en is eerste aanspreekpunt als het gaat om het gebruik van Mantis
- De change manager van de beheerorganisatie wordt door de technisch beheerder ingeschakeld als deze constateert dat de melding geen incident betreft.
- De deelnemers zijn verantwoordelijk voor het zorgvuldig aanmaken van meldingen en het reageren op meldingen indien nodig.
- De deelnemers zijn verantwoordelijk voor de communicatie over meldingen via de eigen publiek toegankelijke webpagina('s) met actuele beschikbaarheidsinformatie van de betreffende deelnemer(s).

Status van een melding

De status van een melding is relevant voor gebruikers van Mantis. Elke melding start met de status "Nieuw" en moet uiteindelijk de status "Afgesloten" krijgen. Voor elk van de statussen is de betekenis de volgende.

Nieuw	De melding is ingeschoten en nog niet in behandeling genomen door de beheerorganisatie
Toegewezen	Melding is toegewezen aan een persoon. Deze persoon moet de melding in behandeling nemen en een nieuwe status aan de melding toewijzen. Zolang de status op "Toegewezen" blijft staan betekent dit dat de nieuwe verantwoordelijke de melding nog niet in behandeling heeft genomen.
Afgemeld	De beheerorganisatie geeft aan dat melding voldoende is behandeld.
Feedback	De melding die de status opgelost heeft gekregen wordt heropend omdat die bijv. onjuist is.
Afgesloten	De melding is afgesloten en hoeft niet meer ingezien te worden. De aanmelder mag de melding opnieuw openen als hij meent dat de reacties niet voldoende zijn.

Overzicht processtappen

- 1. Melding aanmaken
- 2. Melding behandelen

Toelichting processtappen

1. Melding aanmaken	
Input	Een melding kan door zowel deelnemers als de beheerorganisatie worden aangemaakt. Vaak gebeurt dit door deelnemers van het stelsel, maar de beheerorganisatie kan ook zelf nieuwe meldingen aanmaken. Een persoon die een melding maakt heet een aanmelder.
Activiteit	1. Er wordt ingelogd in Mantis met de verstrekte gebruikersnaam en wachtwoord. 2. Er wordt in Mantis een project gekozen waar de melding bij past 3. De aanmelder geeft een korte samenvatting en omschrijft de melding met relevante details 4. De aanmelder kiest het versienummer van het afsprakenstelsel waar de melding van toepassing op is. Er mag voor n.v.t. gekozen worden als het versienummer niet relevant is. 5. De aanmelder wijst de melding toe aan een individu als de melding specifiek voor die persoon bedoeld is. In het andere geval gaat de melding naar de organisatie. Als de melding door verschillende deelnemers opgepakt moet/kan worden, wijst de aanmelder deze toe aan zijn eigen organisatie en stelt de betreffende deelnemers op de hoogte middels de functie "Herinnering verzenden" in de aangemaakte melding. 6. De toegewezen persoon/organisatie wordt op de hoogte gesteld van de nieuwe melding middels een automatisch verzonden e-mail. Soms kan een melding leiden tot een nieuwe melding. Deze mag niet als reactie in een bestaande melding geplaatst worden, maar dient als nieuwe melding geregistreerd te worden. Als er een relatie bestaat met andere meldingen kan hiervoor de betreffende functionaliteit van Mantis worden gebruikt.

Gerapporteerde melding	Gerapporteerde en toegewezen melding
Wie?	De beheerorganisatie beheert Mantis. Deelnemers en leden van de beheerorganisatie kunnen op Mantis een melding aanmaken.

2. Melding behandelen

Input	Toegewezen melding
Activiteit	Deelnemers en beheerorganisatie behandelen de melding volgens de afspraken in het Service level en controleren regelmatig de aan hen toegewezen meldingen en meldingen die al lange tijd open staan. Ze voeren daarbij de volgende acties uit: 1. Reageer op de melding zodat de aanmelder weet dat die gelezen is. Als de persoon/organisatie extra informatie nodig heeft plaatst deze een reactie op de melding. 2. Behandel de melding. Wanneer de toegewezen persoon/organisatie de melding heeft opgelost/afgehandeld moet de status worden gewijzigd naar "Opgelost" en wijs de melding toe aan de aanmelder zodat die kan controleren of de melding terecht is afgemeld; bijvoorbeeld omdat het probleem is opgelost of omdat er eenvoudigweg geen actie hoeft te worden ondernomen. De aanmelder controleert of de afmelding terecht is en bevestigd dit in de reactie van de melding. De aanmelder sluit de melding door deze de status "Afgesloten" te geven. Alvorens de aanmelder de melding sluit door deze de status "Afgesloten" te geven, moet de melding worden toegewezen aan de organisatie waar het probleem zat. 3. Als de aanmelder/toegewezen persoon niet reageert mag deze herinnerd worden door van de "Herinnering verzenden" mogelijkheid gebruik te maken. In enkele gevallen is het gewenst dat een ander persoon dan de aanmelder reageert op een melding. In dat geval wordt deze persoon op de hoogte gesteld dat hij moet reageren middels een herinnering die door de aanmelder verstuurd wordt met de betreffende functionaliteit van Mantis.
Output	Afgesloten melding
Wie?	De persoon die verantwoordelijk is gemaakt zorgt er voor dat de melding correct wordt behandeld. De beheerorganisatie ziet er op toe dat dit binnen redelijke termijn gebeurt.

Proces migratie sleutelmateriaal voor polymorfe pseudonimisering

Voor polymorfe pseudonimisering beschikken verschillende partijen in het eTD-stelsel over verschillende soorten cryptografisch sleutelmateriaal, meer informatie is op te vragen bij de BSNk beheerpartij. Om verscheidene redenen zal het voor komen dat dit sleutelmateriaal dient te worden vervangen om Polymorfe Pseudoniemen te kunnen blijven genereren en ontsleutelen. Voor de ondersteuning van dergelijke sleutelmigraties worden de volgende processen voorgeschreven.

Er zijn vier scenario's voor sleutelvervanging en sleutelmigratie voorzien. Daarvan zijn de Sleutelmigratie A, B1 en C (resp RecipientKeySet versie, OIN wijziging BSN-Dienstverlener en IdentityProviderKeySet) heel eenvoudig en hebben geen verdere detailering nodig. Sleutelmigratie D betreft de migratie van een SchemeWideKeySet. Die zou alleen bij hoge uitzondering voor moeten komen sleutel compromitatie bij BSNk-SleutelBeheer of een significante aanpassing beleid voor gebruik van het BSNk. Verdere detaillering en planning is afhankelijk van situatie en zal op ad-hoc basis door de BSNk-BeheerOrganisatie uitgewerkt worden. Op dit moment geldt dat ook voor een periodieke vervanging van de SchemeWideKeySet die niet voor 2024 verwacht wordt.

Sleutelmigratie A: RecipientKeySet versie	
Sleutelmigratie	De sleutelset bij een Ontvangende Partij (DV, DB, DA) dient te worden vervangen.
Mogelijke oorzaak	Periodieke vervanging (PKIoverheid certificaat), sleutel compromitatie
Proces	Een Ontvangende Partij initieert een verzoek tot sleutelvervanging. • De Ontvangende Partij geeft een notificatie aan zijn Herkenningsmakelaar of de Beheerorganisatie cf. Operationeel Handboek • De Ontvangende Partij vraagt via zijn Herkenningsmakelaar nieuw sleutelmateriaal op bij het BSNk zie AUC9 Verstrekken sleutelmateriaal Dienstverleners. • Totdat dit nieuwe sleutelmateriaal operationeel is, kan de Ontvangende Partij in de dienstencatalogus (voor DVs), c.q. in de metadata (voor MR), aangeven Versleutelde Pseudoniemen of Versleutelde Identiteiten op basis van een eerdere versie van het sleutelmateriaal te willen ontvangen • De Ontvangende Partij installeert en test dit nieuwe sleutelmateriaal, en wijzigt bij goedkeuring van het BSNk de sleutelversie in de metadata (voor MR), c.q. dienstencaalogus (via HM).
NB	Pseudoniemen die al bekend zijn bij de Ontvangende Partij, kunnen worden omgerekend met behulp van het oude en nieuwe sleutelmateriaal. Machtigingenregisters gebruiken de versie zoals vermeld in de dienstencatalogus of metadata en hebben geen actieve rol in deze migratie.

Sleutelmigratie B1: OIN wijziging Dienstverlener voor BSN dienst	
Sleutelmigratie	De identiteit waarop een sleutelset van een Dienstverlener is gebaseerd wijzigt.
Mogelijke oorzaak	Het OIN van een Dienstverlener ondergaat een organisatorische wijziging (bijvoorbeeld wijziging rechtspersoon, of overdracht van een Dienst aan een andere organisatie)
Proces	De Dienstverleners vragen nieuw sleutelmateriaal op via hun Herkenningsmakelaar, conform sleutelmigratie A.
NB	Feitelijk is hier geen sprake van een echte SleutelMigratie, de waarden van Versleutelde Identiteiten (BSN) wijzigen met het nieuwe Sleutelmateriaal. Dienstverleners ontvangen Versleutelde Identiteiten voor de volgens de dienstencatalogus actieve sleutel.

Sleutelmigratie C: IdentityProviderKeySet	
Sleutel migratie	Wijziging van de sleutelset in de transformatie-HSM bij het BSNk-Transformatie
Mogelijke oorzaak	Periodieke vervanging, sleutel compromitatie, organisationele wijziging (resulterend in bijvoorbeeld wijziging OIN of PKIo certificaat van MU /AD/EB)

Proces	Een Machtigingenregister initieert het verzoek tot sleutelwissel. • Het BSNk-Transformatie vraagt nieuw sleutelmateriaal aan bij het BSNk-Sleutelbeheer en installeert dit nieuwe sleutelmateriaal conform AUC9 Verstrekken sleutelmateriaal Dienstverleners • Het Machtigingenregister kan bestaande Polymorfe Pseudoniemen en Polymorfe Identiteiten blijven gebruiken met oude sleutelmateriaal, afhankelijk van oorzaak. • Het Machtigingenregister kan met oude Polymorfe Identiteit een Versleutelde Identiteit voor het BSNk verkrijgen en op basis hiervan nieuwe Polymorfe Pseudoniemen en Polymorfe Identiteiten aanvragen via de BSNk-activatie (mbv AUC6.1 Activeren BSN mbv VI). • Het Machtigingenregister maakt gebruik van de nieuwe Polymorfe Pseudoniemen en Polymorfe Identiteiten om Versleutelde Pseudoniemen en Versleutelde Identiteiten (BSN) aan Dienstverlener te verstrekken. • Authorisatie kan gedurende een migratieperiode met zowel het oude als het nieuwe sleutelmateriaal plaatsvinden, afhankelijk van welk Polymorfe Pseudoniem of Polymorfe Identiteit beschikbaar is.
NB	De pseudoniemen bij de Ontvangende Partij (DV) worden niet geraakt door wijziging van de IdentityProviderKeySet, net als dat zij ook van verschillende MR's tot hetzelfde Persistente Pseudoniem c.q. identiteit ontsleutelen.

Sleutelmigratie D: SchemeWideKeySet	
Sleutelmigratie	Wijziging van de sleutelset bij het BSNk en daarmee alle afhankelijke sleutels in het stelsel.
Mogelijke oorzaak	Periodieke vervanging, sleutel compromitatie bij BSNk-SleutelBeheer of een significante aanpassing beleid voor gebruik van het BSNk.
Proces	Het BSNk initieert de sleutelwissel. • BSNk-Sleutelbeheer genereert nieuw sleutelmateriaal in zijn HSM(s) en behoudt het oude sleutelmateriaal voor migratie tot een aangekondigde datum. • BSNk-BeheerOrganisatie kondigt een sleutelwissel en een bijbehorende planning aan bij alle betrokken partijen. • BSNk-Transformatie krijgt voor elk MachtigingsRegister nieuw sleutelmateriaal in zijn HSM(s) volgens de daarvoor geldende procedure van het BSNk. • De Dienstverleners vragen nieuw sleutelmateriaal op via hun Herkenningsmakelaar, conform sleutelmigratie A. • De Machtigingenregisters vragen nieuwe Polymorfe Pseudoniemen en Polymorfe Identiteiten op bij het BSN, conform sleutelmigratie C**.** • Gedurende een migratieperiode levert de Machtigingenregisters de Versleutelde Pseudoniemen en Versleutelde Identiteiten op basis van zowel het oude en nieuwe sleutelmateriaal op voor de Ontvangende Partijen.
NB	Deze procedure kent de meeste impact, aangezien deze migratie alle partijen raakt. Goede afstemming is hierbij cruciaal. Omdat alle verklaringen ook ondertekend zijn obv PKIo, zal oud PP-sleutelmateriaal in vrijwel alle gevallen nog geruime tijd bruikbaar blijven, omdat het binnen de context van verklaringen nog vertrouwd kan worden. De migratie kan daarmee afgestemd worden om gefaseerd en gecoördineerd geleidelijk doorgevoerd te worden. Bij het verkrijgen van Polymorfe Pseudoniemen en Polymorfe Identiteiten door het Machtigingenregister, worden deze ondertekend door het BSNk. Deze ondertekening vindt plaats met een ECDSA signature, waarvoor de publieke sleutel in de metadata staat. Deze sleutel kan daarmee los van deze procedure 'Sleutelmigratie D' gewijzigd worden via het reguliere Proces netwerkmetadata. Dienstverleners die PseudoID gebruiken ipv BSN zullen beide Versleutelde Pseudoniemen moeten ontsleutelen (elk met het bijbehorende versie van het sleutelmateriaal) om de PseudoID's te kunnen migreren.

Omdat de oude en nieuwe Versleutelde PseudoID's als een *multi-valued* attribuut gecommuniceerd worden, kunnen meerdere sleutelmigraties gelijktijdig ondersteund worden. Hierdoor hoeft een migratieperiode als gevolg van het ene type sleutelmigratie, een andere sleutelmigratie niet te blokkeren. Voor BSN's is er sowieso geen probleem, tenminste als de DV's in staat zijn om de Versleutelde Identiteit bij hun actuele SleutelVersie te kiezen of met meerdere Sleutels te gelijk kunnen werken.

Proces netwerkmetadata

In het Netwerk wordt SAML metadata gebruikt voor het beschrijven van de URL's en certificaten die worden gebruikt op de verschillende koppelvlakken. Actuele metadata is van belang om twee redenen:

1. De metadata geeft weer voor welke rol en op welk betrouwbaarheidsniveau een deelnemer is toegetreden. Met andere woorden, op basis van de metadata wordt bepaald wie wat mag in het netwerk.
2. De metadata geeft weer hoe systemen van deelnemers kunnen worden benaderd en met welke certificaten deze systemen zijn te authenticeren. Hierdoor speelt de metadata een belangrijke rol in het bewaken van de integriteit en authenticiteit van de verklaringen en gegevens die door het netwerk worden geleverd.

> Netwerkmetadata wordt gebruikt voor zowel het productie- als het testnetwerk. De processen voor productie en test zijn grotendeels gelijk. Dit document beschrijft beide.

Doelstelling

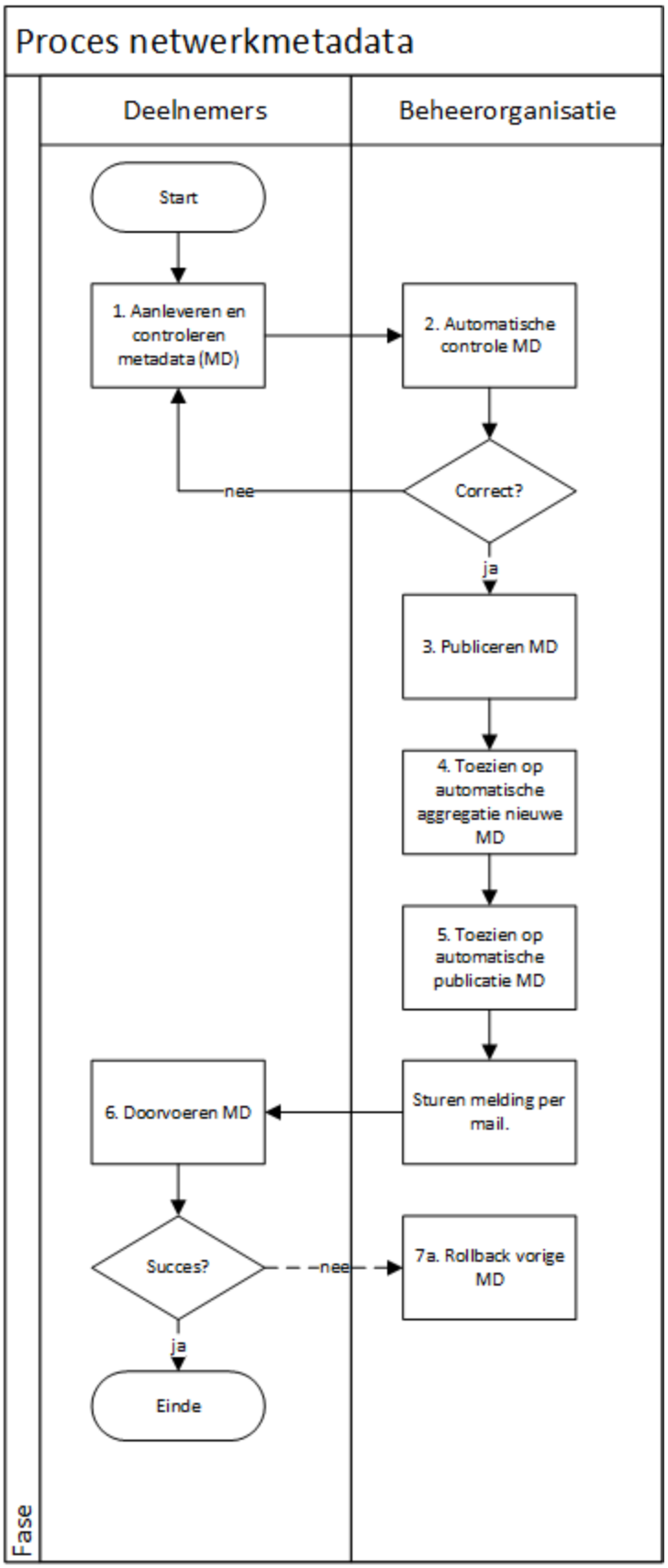
De doelstelling van het metadata proces is tweeledig:

1. Waarborgen dat de netwerkmetadata op correcte wijze tot stand komt;
2. Waarborgen dat alle deelnemers de actuele netwerkmetadata in hun systemen gebruiken.

Verantwoordelijkheden

- Beheerorganisatie:
  - De technisch beheerder is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technisch beheerder zorgt tevens dat de procesbeschrijving actueel blijft en coördineert de verschillende stappen in het proces;
  - De juridisch coördinator bewaakt dat de metadata een correcte weergave is van de contractadministratie en toetredingsbesluiten.
- De deelnemers zijn verantwoordelijk voor het controleren en aanleveren van metadata.

Overzicht processtappen



Toelichting processtappen

1. Controleren en aanleveren metadata

Input	1. Een deelnemer genereert nieuwe metadata conform de technische specificaties en ondertekent deze met zijn valide digitale handtekening. Uiterlijk 7 dagen voor daadwerkelijk doorvoeren van de geplande wijzigingen in zijn infrastructuur, stelt de deelnemer de gecontroleerde nieuwe metadata beschikbaar voor de beheerorganisatie op zijn productionele metadata (HTTPS) URL. Deelnemers publiceren hun productionele metadata op een aparte URL per rol binnen het Netwerk. Nieuwe entities worden hierin toegevoegd met een ValidFrom datum in het beoogde onderhoudswindow waarin de wijziging moet worden doorgevoerd. Overtollige entities worden verwijderd door het toevoegen van een ValidUntil datum in het beoogde onderhoudswindow waarin de wijziging moet worden doorgevoerd. Van gewijzigde entities wordt de oude entry op genomen met een validUntil datum en de nieuwe entry met een validFrom datum. Ook hierbij liggen beide data in het beoogde onderhoudsvenster waarin de wijziging moet worden doorgevoerd. Daarna informeert de deelnemer de andere deelnemers en de beheerorganisatie d.m.v. een Mantis issue. Dit issue bevat minimaal: • Het verwachte tijdstip van doorvoeren • Een beschrijving van de wijzigingen • De URL van de nieuwe metadata
Activiteit	2. Een automatisch controle proces voert de technische controles op de, door de deelnemer gepubliceerde nieuwe, metadata uit. Deze controles bestaan uit: **a.** Validatie van de het metadata bestand tegen de technische specificities **b.** Validatie van de elektronische handtekening van de deelnemer **c.** Controle van de consistentie van het metadata bestand **d.** Controle op juridische inhoud (de rollen en betrouwbaarheidsniveaus die de deelnemer o.b.v. deze metadata claimt te mogen uitvoeren), zoals vooraf gedefinieerd door de juridisch coördinator van de beheerorganisatie. N.B. Deze controlestap wordt voor metadata van het testnetwerk overgeslagen. Hier moeten (aankomende) deelnemers juist kunnen testen als onderdeel van het toetredingsproces. 3. Wanneer één van de genoemde controles geen positief resultaat heeft, wordt geen nieuwe metadata gepubliceerd op de URL van de beheerorganisatie. • De deelnemers worden per e-mail van het resultaat van de controle op de hoogte gebracht, alleen als metadata van de deelnemer gewijzigd is om "spamming" te voorkomen. Bij fouten in de metadata die in stap 1 worden geconstateerd, worden deze via e-mail door het automatisch proces zowel naar de deelnemer als naar de beheerorganisatie verstuurd.
Output	• In behandeling genomen goedgekeurde metadata. • Terugmelding besluit.
Wie?	• De beheerorganisatie beoordeelt de metadata; • De juridisch coördinator beoordeelt de rollen en betrouwbaarheidsniveaus.

2. Genereren en publiceren netwerkmetadata	
Input	Goedgekeurde metadata
Activiteit	4. Het automatisch proces genereert, na stap 1 in de voorgaande activiteit als wijziging in metadata gedetecteerd is, een nieuwe versie van het huidige geaggregeerde metadatabestand met een cacheduration van "PT1H" (één uur). Entries met een ValidUntil datum meer dan 1 maand in het verleden worden hierbij uit het metadata bestand verwijderd. 5. Deze nieuwe netwerkmetadata wordt door het automatisch proces gepubliceerd op https://aggregator.etoegang.nl/test/1.13/networkmetadata.xml (testnetwerk) of https://aggregator.etoegang.nl/1.13/networkmetadata.xml (productie). Deze metadata en het moment waarop deze door het automatisch proces in productie gezet is, wordt tevens door het automatisch proces per email naar de deelnemers gestuurd. Tevens wordt de metadata gearchiveerd conform de werkbeschrijving in Confluence.
Output	Gepubliceerde metadata
Wie?	De technisch beheerder van de beheerorganisatie voert deze stap uit

3. Doorvoeren netwerkmetadata	
Input	Gepubliceerde metadata

Activiteit	6. De automatische processen van de deelnemers pakken de nieuwe metadata op en voeren deze door, waarbij de daadwerkelijke wijzigingen door de gebruikte ValidIUntil/ValidFrom datums direct na het onderhoudswindow daadwerkelijk actief worden. 7. De deelnemer die nieuwe metadata doorvoert controleert, tijdens zijn onderhoudswindow, de werking van de nieuwe metadata. Als de wijzigingen niet goed werken, dan kan de deelnemer tijdens het onderhoudswindow een nieuwe versie van de nieuwe metadata uploaden of de oude versie uploaden. Deze wordt door het automatisch proces gecontroleerd, geaggregeerd en gepubliceerd op de bovengenoemde URLs, waarna deze binnen een uur automatisch door de deelnemers wordt opgepakt en doorgevoerd. a. Zonodig kan de technisch beheerder, bij ernstige verstoringen in het onderhoudswindow, handmatig een rollback naar de originele productionele metadata van voor de wijziging doorvoeren. 8. De deelnemers melden in Mantis het resultaat van de doorvoering indien relevant.
Output	Geïmplementeerde nieuwe metadata
Wie?	• De deelnemers implementeren de nieuwe metadata; • De technisch beheerder monitort en rapporteert aan de deelnemers.

Proces onderhoud cookieserver

Voor de werking van Single Sign On heeft iedere Herkenningsmakelaar een eigen fysieke cookieserver op gezamenlijk domein *.sso.eherkenning.nl. De DNS van het gezamenlijke domein wordt beheerd door beheerorganisatie.

Iedere cookieserver heeft een eigen IP adres gespecificeerd door de betreffende deelnemer. Deze IP-adressen zijn door de beheerorganisatie opgenomen in de DNS van *.sso.eherkenning.nl.

Er moet onderhoud plaatsvinden als een van de deelnemers zijn IP-adres wijzigt. In de praktijk kan dit bijvoorbeeld voorkomen wanneer er een nieuwe deelnemer toetreedt, of wanneer een deelnemer besluit zijn software over te zetten op een nieuwe machine met een ander IP-adres.

Verantwoordelijkheden

De proceseigenaar is er vanuit de beheerorganisatie verantwoordelijk voor dat het proces wordt uitgevoerd conform de procesbeschrijving. De technische beheerder van de beheerorganisatie is er verantwoordelijk voor dat de procesbeschrijving actueel blijft.

Toelichting processtappen

1. Wanneer het IP-adres van de deelnemer wijzigt, dan meldt hij dat tijdig (minimaal twee weken van te voren) via de issuetracker Mantis. Hierbij vermeldt de deelnemer in ieder geval het huidige IP-adres dat nu in gebruik is, het nieuwe IP-adres en de termijn waarop de wijziging plaats moet vinden.
2. De beheerorganisatie vervangt het IP-adres van de betreffende deelnemer in DNS van het gezamenlijke domein in afstemming met de betreffende deelnemer.
3. De deelnemer ontvangt een bevestiging van de beheerorganisatie via Mantis wanneer de vervanging is afgerond.
4. De deelnemer KAN nu het nieuwe IP-adres gebruiken.

Ondertekenen van domein autorisatie formulier voor het aanvragen van een certificaat

Voor het aanvragen/vernieuwen van een certificaat voor het cookiedomein dient men een domein autorisatie formulier te laten ondertekenen door de eigenaar van het domein. Middels dit formulier kan een nieuw certificaat worden aangevraagd door iemand die geen eigenaar is van het betreffende domein. Dit formulier is verkrijgbaar bij de partij waarbij het certificaat wordt aangevraagd. Om dit formulier door Logius ondertekend te krijgen dienen de volgende stappen te worden doorlopen:

1. Meld het verzoek in Mantis;
2. Stuur het ingevulde domein autorisatie formulier naar info@eherkenning.nl;
3. Ketenbeheer zorgt ervoor dat het formulier wordt ondertekend door de domeineigenaar;
4. Ketenbeheer stuurt het ondertekende formulier retour;
5. Nieuw certificaat kan worden aangevraagd;

Proces toetreden

Het afsprakenstelsel van Elektronische Toegangsdiensten, waaronder het merk eHerkenning valt, staat open voor deelname door nieuwe geïnteresseerde partijen. Het Proces Toetreden beschrijft de stappen die genomen moeten worden om toe te treden tot het afsprakenstelsel Elektronische Toegangsdiensten. Na ondertekening van de Deelnemersovereenkomst, als sluitstuk van het toetredingsproces, mag het merk eHerkenning gevoerd worden. Bij bepaalde wijzigingen, bijvoorbeeld wanneer een deelnemer zijn dienstverlening wil uitbreiden of aanpassen, kan er ook sprake zijn van toetreden. In alle gevallen dient de kandidaat toetreder (hierna genoemd: de Toetreder) het Proces Toetreden met goed gevolg te doorlopen.

Er is sprake van toetreding in de volgende situaties:

1. Een nieuwe deelnemer (een partij die nog geen deelnemersovereenkomst heeft getekend) wil één of meer rollen in het stelsel gaan vervullen.
2. Een huidige deelnemer wil zijn rol(len) in het stelsel uitbreiden met één of meer rollen.
3. Een huidige deelnemer wil met één of meer betrouwbaarheidsniveaus uitbreiden op de rol(len) die hij al vervulde in het stelsel.
4. Een huidige deelnemer wil zijn processen voor uitgifte van middelen of registratie van machtigingen aanpassen.
5. Een huidige deelnemer wil één of meer optionele functionaliteiten gaan leveren (of uitbreiden) aan zijn klanten.
6. Verscheidene partijen willen in een combinatie onder een gemeenschappelijke naam Toegangsdiensten verrichten, waarbij ieder van de partijen in de combinatie hoofdelijk aansprakelijk is. In dit geval dienen alle combinanten afzonderlijk toe te treden. Indien er een wijziging is in de samenstelling van de combinatie, moet de nieuwe partij het Proces Toetreden doorlopen.
7. Een huidige deelnemer implementeert een nieuwe koppelvlakrelease van het afsprakenstelsel, zie ook Proces change en release.
8. Een huidige deelnemer wijzigt de rechtspersoon of rechtsvorm. Hij gebruikt dan het formulier Template wijziging rechtspersoon deelnemer.

De Toezichthouder heeft de mogelijkheid om, afhankelijk van de situatie, bepaalde processtappen over te slaan en/of aan te geven wat de op te leveren bewijsstukken zijn. Deze keuze is afhankelijk van de situatie: een nieuwe toetreding verschilt van een wijziging van de rechtspersoon, in het geval van de wijziging van de rechtspersoon heeft de Toezichthouder al de procesbeschrijvingen getoetst. De Toezichthouder bepaalt en communiceert per situatie de te doorlopen stappen en de op te leveren bewijsstukken aan de Toetreder.

Gerelateerde onderdelen van het afsprakenstelsel:

- Toetredingseisen
- Testing
- Beleid voor informatiebeveiliging
- Normenkader betrouwbaarheidsniveaus
- Template deelnemersovereenkomst

Doelstelling

De doelstelling van het Proces Toetreden is om op een zorgvuldige en beheerste wijze nieuwe deelnemers aan te sluiten. Het Proces Toetreden vormt een belangrijke waarborg voor het vertrouwen in het merk eHerkenning. De deelnemers moeten voldoen aan de eisen genoemd in het afsprakenstelsel om dit vertrouwen in het merk te kunnen waarborgen Deze toetsing voert de Toezichthouder uit.

Zorgvuldige en beheerste toetreding betekent o.a.:

- volgens een transparant proces;
- zonder verstoringen;
- dat de Toetreder voldoet aan het afsprakenstelsel.

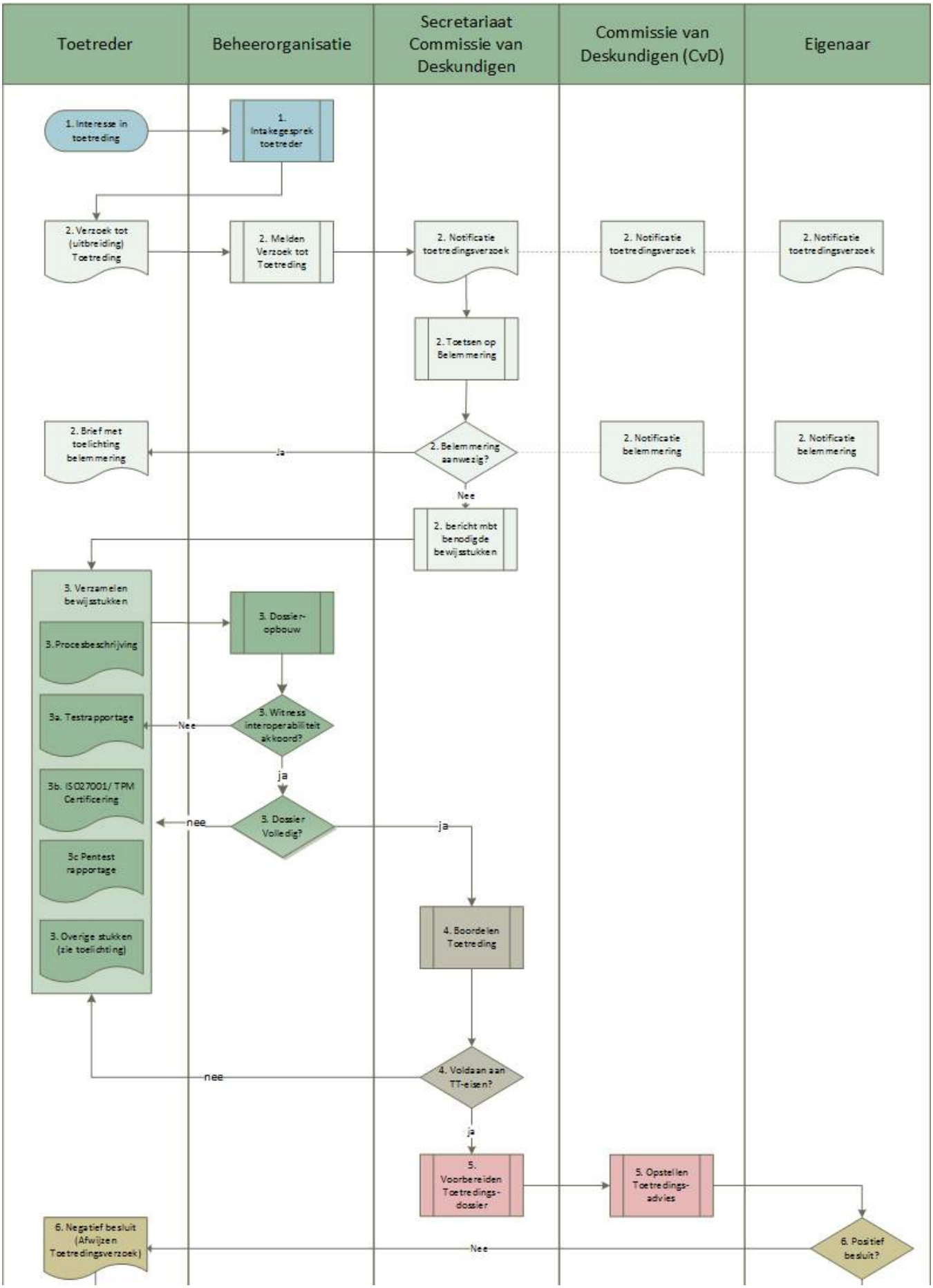
Verantwoordelijkheden

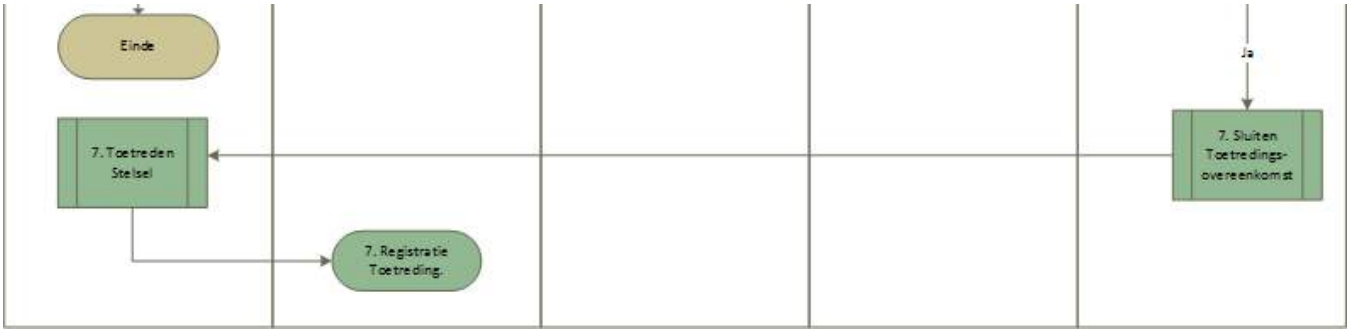
Diverse partijen hebben verantwoordelijkheden en taken in het Proces Toetreden:

- De Toetreder is verantwoordelijk voor het implementeren van de eisen die het afsprakenstelsel stelt. Hij stelt de benodigde documentatie beschikbaar voor de toetsing. De Toetreder stelt tevens een medewerker als aanspreekpunt aan.
- De Beheerorganisatie faciliteert het Proces Toetreden en is verantwoordelijk voor de administratie en de volledigheid van het toetredingsdossier tijdens het Proces Toetreden. De Beheerorganisatie stelt tevens een simulator testtool ter beschikking en heeft de taak om de resultaten van de simulator- en ketentestresultaten cq. de implementatie van de koppelvlakken van de Toetreder steekproefsgewijs te toetsen (zie Testing). De Beheerorganisatie stelt een 'Coördinator Toetreden' aan.
- De Coördinator Toetreden notificeert de Toezichthouder via het secretariaat van de Commissie van Deskundigen (Hierna te noemen: secretariaat van de CvD), de Eigenaar en het Tactisch Beraad wanneer een nieuwe Toetreder zich meldt. Daarnaast administreert de Coördinator Toetreden van de beheerorganisatie het toetredingsdossier en controleert de volledigheid ervan. De Coördinator Toetreden stelt het volledige dossier beschikbaar aan het secretariaat van de CvD met het verzoek de implementatie van een Toetreder te toetsen. De Coördinator Toetreden is verantwoordelijk voor het naleven van het Proces Toetreden conform de procesbeschrijving en houdt de procesbeschrijving actueel.
- De Commissie van Deskundigen (CvD) adviseert de Minister over toetredingen. Het advies bevat informatie of een Toetreder kan toetreden tot het afsprakenstelsel. De Toezichthouder toetst de implementatie van de deelnemer m.b.t. de opzet van de processen voor het uitgeven en registreren van middelen en machtigingen en de vereiste beveiligingsaspecten.
- De CvD wordt ondersteund door het Secretariaat van de Commissie van Deskundigen. Het Secretariaat van de CvD controleert het toetredingsdossier en toetst aan de hand van het controlememorandum of de procesbeschrijvingen van de Toetreder voldoen.
- De Eigenaar sluit, als houder van het merkrecht en politiek verantwoordelijke voor het afsprakenstelsel een deelnemersovereenkomst af met de Toetreder. Daarmee krijgt een partij het recht om deel te nemen in het netwerk en onder het merk eHerkenning de propositie te voeren waarvoor hij is toegetreden.

In het Proces Toetreden spelen concurrentiegevoelige gegevens een rol. Deze gegevens zijn geclassificeerd als 'Vertrouwelijk'.

Overzicht processtappen


Toetreder
Beheerorganisatie
Secretariaat Commissie van Deskundigen
Commissie van Deskundigen (CvD)
Eigenaar
1. Interesse in toetreding
1. Intakegesprek toetreder
2. Verzoek tot (uitbreiding) Toetreding
2. Melden Verzoek tot Toetreding
2. Notificatie toetredingsverzoek
2. Notificatie toetredingsverzoek
2. Notificatie toetredingsverzoek
2. Toetsen op Belemmering
2. Brief met toelichting belemmering
Ja
2. Belemmering aanwezig?
2. Notificatie belemmering
2. Notificatie belemmering
Nee
2. bericht mbt benodigde bewijsstukken
3. Verzamelen bewijsstukken
3. Procesbeschrijving
3. Dossier-opbouw
3a. Testrapportage
Nee
3. Witness interoperabiliteit akkoord?
ja
3b. ISO27001/ TPM Certificering
nee
3. Dossier Volledig?
ja
3c Pentest rapportage
3. Overige stukken (zie toelichting)
4. Boordelen Toetreding
nee
4. Voldaan aan TT-eisen?
ja
5. Voorbereiden Toetredings-dossier
5. Opstellen Toetredings-advies
6. Negatief besluit (Afwijzen Toetredingsverzoek)
Nee
6. Positief besluit?



Toelichting processtappen

1. Intake	
Input	Melding van interesse van een (nieuwe) deelnemer
Activiteit	Een huidige of nieuwe deelnemer meldt zich bij de beheerorganisatie met een verzoek tot (uitbreiding) toetreding. De Beheerorganisatie houdt een intake en informeert de verzoekende partij over: **a.** de rollen waarop kan worden toegetreden; **b.** de procedure voor de toetreding tot de betreffende rol(len); **c.** de voorwaarden voor toetreding waaronder de stelseleisen voor informatiebeveiliging.
Output	Informatie over het Proces Toetreden en over de werking van het afsprakenstelsel.
Wie?	• Coördinator toetreden • Toetreder

2. Formeel verzoek tot toetreding behandelen	
Input	Formulier verzoek tot toetreding
Activiteit	De Potentiële Toetreder (hierna genoemd: Toetreder) dient het ingevulde formulier Template verzoek tot (uitbreiding) toetreding in bij de Beheerorganisatie en benoemt tevens een aanspreekpunt in de eigen organisatie. De Coördinator toetreden controleert het ingevulde formulier op volledigheid. De Beheerorganisatie meldt aan het Secretariaat van de Commissie van Deskundigen dat een verzoek tot toetreding is gedaan. De Beheerorganisatie informeert tevens het Tactisch Beraad over het formele verzoek tot toetreding. Het Secretariaat van de CvD meldt aan de CvD of er vooraf feiten bekend zijn die een succesvolle toetreding van de deelnemer belemmeren**.** Indien er sprake is van belemmerende feiten stelt het Secretariaat van de CvD de Potentiële toetreder op de hoogte. Een voorbeeld van een belemmerend feit is dat de organisatie in het Handelsregister staat met de status surseance. Het is de beslissing van de Toetreder om het toetredingsproces toch voort te zetten. De Toetreder ontvangt een brief met de op te leveren bewijsstukken van het Secretariaat van de CvD. Dat is afhankelijk van de situatie zoals in de inleiding is beschreven.
Output	Brief aan Toetreder (bij belemmering)
Wie?	• Secretariaat van de CvD • Coördinator toetreden • Toetreder

3. Implementatie door deelnemer en leveren bewijsstukken	
Input	Brief met de op te leveren bewijsstukken

Activiteit	De Toetreder start met het implementeren van de voorwaarden genoemd in het afsprakenstelsel. De Toetreder levert de bewijsstukken op aan de Coördinator Toetreden. De Toezichthouder geeft aan welke bewijsstukken van toepassing zijn voor de beoordeling van een nieuwe toetreding. De bewijsstukken zijn afhankelijk van het type verandering: betreft het een kleine wijziging in een procedure of is het een geheel nieuwe toetreding. Bij een geheel nieuwe toetreding bestaat deze documentatie minimaal uit: • Bewijs van inschrijving in het Handelsregister. De Toezichthouder bevraagt met deze informatie het Handelsregister; • Bewijs van een WA verzekering m.b.t. te leveren diensten; • Continuïteitsplan m.b.t. diensten; • ISO27001 certificaat of TPM, inclusief de Verklaring van Toepasselijkheid, waaruit overeenstemming met het Gemeenschappelijk normenkader informatiebeveiliging blijkt; • Resultaten penetratietest; • Resultaten simulator- en ketentest; • Een exitplan. Het staat de Toetreder vrij om de bewijsstukken in delen op te leveren. Ten aanzien van de procesbeschrijving(en) van de uitgifteprocessen voor middelen en machtigingen moet minimaal aangegeven zijn hoe het betrouwbaarheidsniveau kan worden toegekend. Indien een Toetreder alleen als MU toetreedt, dient deze aan te geven met welke authenticatiedienst(en) een overeenkomst is gesloten voor het authentiseren van de uitgegeven middelen. Hierbij dient de Toetreder inzage te geven in de contractuele afspraken tussen MU en AD. Indien de Toetreder als MU en/of AD toetreedt, dient deze een beschrijving van de registratie-, identificatie- en authenticatieprocessen voor gebruikers in te dienen. De Toezichthouder controleert in het toetredingsproces of, in de door de Toetreder gehanteerde modelovereenkomsten, de Gebruiksvoorwaarden van het afsprakenstelsel minimaal van toepassing worden verklaard. Indien de Toetreder het gebruik van Polymorfe Pseudonimisering van het BSN ondersteunt, dan moet hij de "Aansluitovereenkomst MR" en "Bewerkersovereenkomst" van BZK accepteren en hier bewijs van overleggen. Indien de partij als HM toetreedt dient deze een procesbeschrijving in te dienen voor de registratie van de Dienstverlener. Het is gewenst dat de toetsing aan het Normenkader betrouwbaarheidsniveaus efficiënt kan worden uitgevoerd ter beperking van de doorlooptijd. Daarom zijn er criteria gesteld waaraan de op te leveren procesbeschrijvingen moeten voldoen: 1. Voor elke afzonderlijk betrouwbaarheidsniveau dat door de deelnemer wordt geleverd is een beschrijving beschikbaar. 2. De beschrijving is per betrouwbaarheidsniveau en volgt de levenscyclus van middelen en/of machtigingen (van aanvraag tot intrekken). 3. De beschrijvingen voor de uitgifte van middelen en/of machtigingen is als volgt ingedeeld: a. De fase van aanvraag; b. De fase van uitgifte; c. De fase van authenticatie; d. De fase voor intrekking, vernieuwing en eventueel schorsing; e. De communicatie met Gebruikers; f. De technische kwaliteiten van het authenticatiemiddel; g. De procesflow; 4. De specifieke technische en beheersmatige beveiligingsmaatregelen behorende bij het middel en/of de machtiging. 5. Per processtap een beschrijving van de vastlegging (logging) van de input, de verwerking en de output. Het gaat hier vooral om vastlegging van uitgevoerde controles, verificaties en validaties. (specifiek 3a t/m 3d). 6. Beschrijving van de archivering van bewijs dat voortkomt uit punt 5. 7. Verwijzingen naar de relevante voorschriften uit het normenkader betrouwbaarheidsniveaus bij de voorgaande beschrijvingen 3 t/m 6.
Output	Bewijsstukken volgens het controlememorandum
Wie?	• Toezichthouder • Coördinator toetreden • Toetreder

3a. Toelichting technische implementatie	
Input	Gegevens aansluiting testnetwerk en testresultaten

Activiteit	• De Toetreder levert de metadata URL en de public key van het signing certificaat van de acceptatie-systemen. Hiermee wordt vervolgens de metadata geautomatiseerd aangemaakt volgens het Proces netwerkmetadata.
	• De Toetreder betrekt de test authenticatiemiddelen en machtigingen bij andere deelnemers (indien van toepassing).
	• De Toetreder voert een simulator- en ketentest uit en is in staat deze te presenteren en te demonstreren aan BO. De BO maakt hier verslag van en voegt deze toe aan het toetredingsdossier.
	  • De simulator- en ketentests vinden plaats in het testnetwerk (Proces beheren testnetwerk).
	  • De simulatortest wordt uitgevoerd met een simulator, een instrument dat berichten verzendt en de antwoorden beoordeelt op conformiteit aan het afsprakenstelsel.
	  • In de ketentest worden ketens van Dienstverlener (DV), Herkenningsmakelaar (HM), Authenticatiedienst (AD), Machtigingenregister (MR), eIDAS-berichtenservice (EB) en/of BSNk getest, door met een gesimuleerde dienstverlener berichten te versturen naar de verschillende Herkenningsmakelaars in het netwerk. De focus van deze test is interoperabiliteit.
	  • Voor meer informatie over testen voor deelnemers, zie Testing.

Output	Presentatie/demonstratie van de interoperabiliteit in het testnetwerk
Wie?	• Coördinator Toetreden • Toetreder

3b. Toelichting Toets Informatiebeveiliging (ISO27001 audit)	
Input	Formeel verzoek tot toetreding + afspraken over het te doorlopen proces
Activiteit	De Toetreder moet aantonen dat stappen zijn gezet om ISO27001 gecertificeerd te worden en vraagt een Certificerende Instelling (in casu de ISO-auditor) een ISO27001 certificeringsaudit uit te voeren, waarbij de scope van het toepassingsgebied in ieder geval een aanduiding van de rollen bevat die de Toetreder wil gaan uitvoeren in het afsprakenstelsel. Indien de Toetreder al ISO27001 gecertificeerd is kan het zijn dat de scope van het toepassingsgebied wijzigt, waardoor ook nieuwe maatregelen toegevoegd dienen te worden. Bovenstaande kan dan ook van toepassing zijn. Het rapport van de ISO-auditor (waaruit tenminste blijkt dat de opzet en bestaan van alle relevante maatregelen getoetst is) en de bijbehorende Verklaring van Toepasselijkheid wordt vervolgens door de Toetreder aangeleverd bij de Coördinator Toetreden. Zie Beleid voor informatiebeveiliging. Het ISO-certificaat dient binnen 6 maanden na toetreding te worden aangeleverd bij de Toezichthouder via het Secretariaat van de CvD. Zie voor de informatiebeveiligingseisen waaraan de Toetreder moet voldoen om te mogen toetreden: Beleid voor informatiebeveiliging
Output	ISO-certificaat of verklaring
Wie?	• Vanuit de Toetreder de aangestelde contactpersoon • Toetreder

3c. Toelichting Penetratietest	
Input	Formeel verzoek tot toetreding + afspraken over het te doorlopen proces
Activiteit	De Toetreder is verplicht om een penetratietest te ondergaan die overeenkomt met het Beleid voor penetratietesten. De Toetreder levert de resultaten van de penetratietest op bij de Beheerorganisatie.
Output	Gecontroleerde resultaten penetratietest
Wie?	• Coördinator Toetreden • Toetreder

4. Overdracht van dossier Toetreden naar het Secretariaat van de Commissie van Deskundigen	
Input	Dossier van de Beheerorganisatie

Activiteit	De Beheerorganisatie controleert de documentatie op volledigheid en beoordeelt, indien van toepassing, de testresultaten van de Toetreder. De Beheerorganisatie doet een melding aan het Secretariaat van de CvD zodra de bewijsstukken compleet zijn. De beheerorganisatie rapporteert het Secretariaat van de CVD over de uitkomst van de beoordeling van de testresultaten.
Output	Brief met melding een compleet dossier. Overdrachtsdossier met bewijsstukken.
Wie?	• Coördinator Toetreden • Secretariaat van de CvD

5. Toetsing door het secretariaat van de Commissie van Deskundigen	
Input	Overdrachtsdossier met bewijsstukken
Activiteit	Het secretariaat van de CvD toetst of de procesbeschrijvingen behorende bij de rol waarin de Toetreder wil toetreden voldoen aan de eisen zoals gesteld in het Normenkader betrouwbaarheidsniveaus. Het toetsen van de opzet van de processen gebeurt, met het principe van hoor en wederhoor. Dit geldt zowel bij nieuwe toetreding als bij tussentijdse wijziging van deze processen. Het secretariaat van de CvD beoordeelt het toetredingsdossier en stelt een controlememorandum op. Dit memorandum bevat de bevindingen van de procesbeschrijvingen van de Toetreder ten opzichte van het Normenkader Betrouwbaarheidsniveaus.
Output	Gecontroleerde procesbeschrijving(en). Controlememorandum.
Wie?	• Secretariaat van de CvD • Toetreder • Coördinator Toetreden

6. Opstellen advies door Commissie van Deskundigen en besluit toetreding door Eigenaar	
Input	Controlememorandum
Beschrijving	De CvD stelt een advies op basis van de bewijsstukken en de bevindingen uit het controlememorandum. De CvD adviseert de Minister (in zijn rol als Eigenaar) over de toetreding. De Eigenaar neemt een besluit op basis van het advies van de CvD. Een eventueel negatief besluit wordt door de Eigenaar gecommuniceerd naar de Toetreder en daarmee eindigt het proces toetreden. Na een positief besluit wordt een Deelnemersovereenkomst afgesloten. De Eigenaar maakt, gebaseerd op het herstel van bevindingen genoemd in het controlememorandum, afspraken over het oplossen die bevindingen. Het CvD ziet toe op de opvolging van deze afspraken. Na rechtsgeldige ondertekening van de deelnemersovereenkomst heeft de toetredende partij rechten en verplichtingen als deelnemer van het afsprakenstelsel. De Coördinator Toetreden stelt het Tactisch Beraad op de hoogte van de toetreding.
Output	Getekende overeenkomst Besluit aan Toetreder
Wie?	• Commissie van Deskundigen • Eigenaar • Toetreder

7. Toetreden afsprakenstelsel	
Input	Positief besluit voor toetreding Getekende deelnemersovereenkomst

Activiteit	De Deelnemer treedt toe tot het afsprakenstelsel • De Deelnemer geeft de metadata URL en de public key van het signing certificaat aan van de preproductie- en productiesystemen door aan de Beheerorganisatie. De Beheerorganisatie verwerkt de metadata tot nieuwe metadata voor het netwerk en communiceert deze aan alle deelnemers. Nadat de deelnemers de nieuwe metadata hebben verwerkt, is het nieuwe productiesysteem aangesloten op het netwerk. Hierbij wordt het proces gevolgd zoals beschreven in Proces netwerkmetadata. • De Deelnemer geeft informatie over de propositie door aan de beheerorganisatie. Dit wordt op de website van eHerkenning geplaatst. De Deelnemer behaalt zijn ISO-certificering binnen de termijn die daarvoor in het afsprakenstelsel is vastgelegd.
Output	Aangesloten nieuwe deelnemer
Wie?	• Eigenaar • Toetreder • Beheerorganisatie

Proces uittreden

De deelnemersovereenkomst voorziet in artikel 5 het beëindigen van de overeenkomst door zowel de Deelnemer als Eigenaar.

Met het beëindigen van de deelnemersovereenkomst treedt een partij uit het stelsel. De deelnemer heeft na uittreding niet langer het recht om zijn diensten onder het merk eHerkenning aan te bieden en is geen partij meer in het netwerk en het Afsprakenstelsel Elektronische Toegangsdiensten.

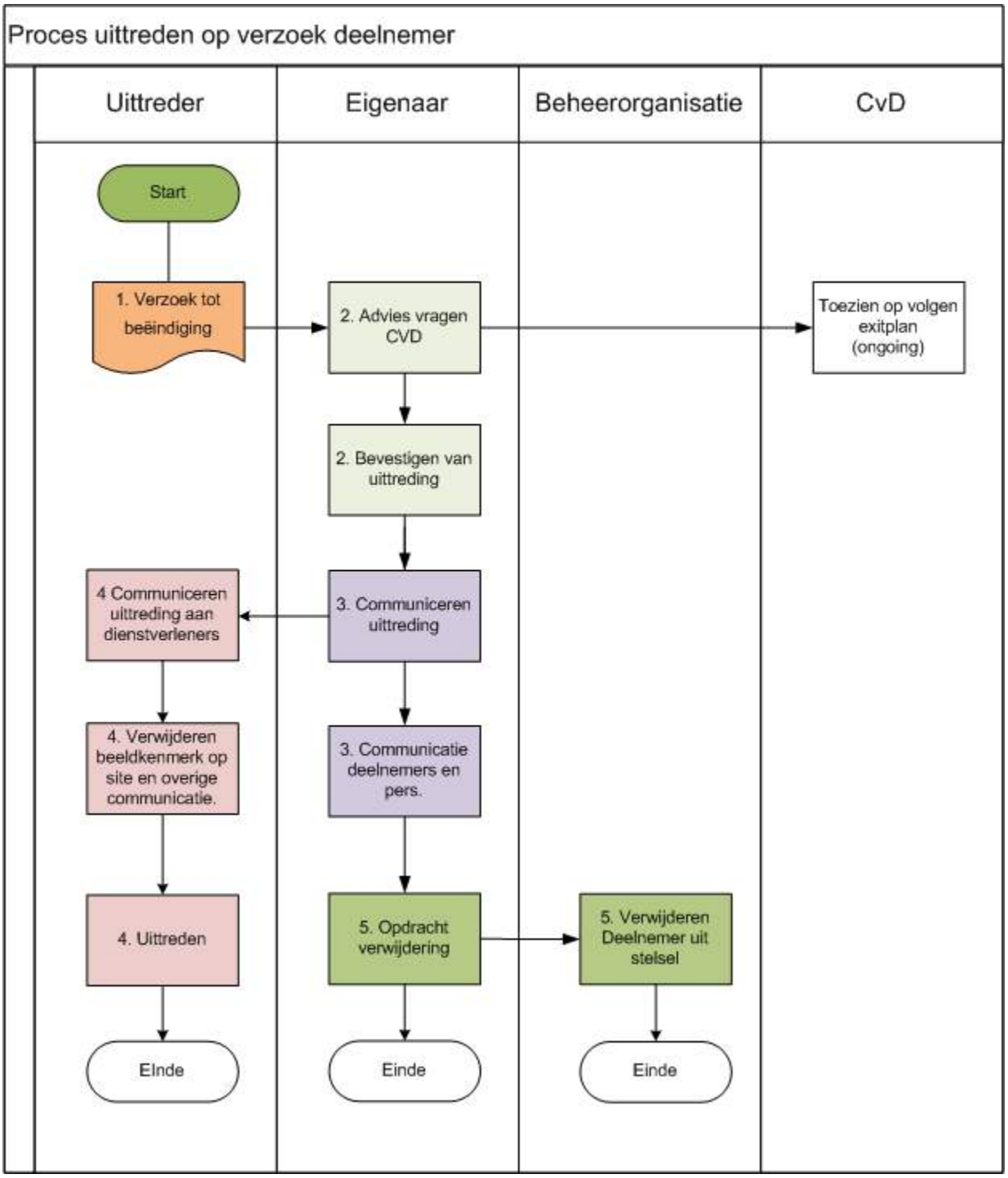
Daarnaast kan zowel de Deelnemer als de Eigenaar besluiten om deelname in een bepaalde rol te beëindigen. Bij het uittreden van een rol bepaalt de Toe zichthouder welke van de onderstaande processtappen van toepassing zijn.

Doelstelling

Het proces uittreden heeft als doel te zorgen voor een ordentelijke uittreding waarbij risico's zoals imagoschade, vertrouwensschade, onderbreking in de continuïteit en beschikbaarheid tot een minimum beperkt worden.

Door toezicht op dit proces te houden wordt gewaarborgd dat de uittredende deelnemer voldoende rekening houdt met de belangen van de in het stelsel actief blijvende gebruikers en dienstverleners.

Overzicht processtappen bij beëindiging door Deelnemer



Processtappen uittreding

1. Verzoek tot beëindiging deelnemersovereenkomst	
Input	Verzoek tot uittreding
Activiteit	De deelnemer meldt het voornemen om uit het stelsel te treden bij de Eigenaar. De schriftelijke opzegtermijn is 3 maanden.
Output	Schriftelijk opzegging van de deelnemersovereenkomst van de deelnemer.
Wie?	• Uittredende deelnemer

2. Behandelen opzegging rol / deelnemersovereenkomst	
Input	Het verzoek tot beëindiging van de deelnemersovereenkomst.
Activiteit	De deelnemers overeenkomst is tussen Deelnemer en Eigenaar. Beide partijen kunnen deze eenzijdig opzeggen. De Eigenaar ontvangt daarom het verzoek tot beëindiging. De Eigenaar vraagt advies aan de CvD inzake de de uittreding.
Output	Adviesverzoek aan de CvD voor de uittreding Bevestiging van het uittredingsverzoek cq beëindigen van de deelnemersovereenkomst.
Wie	• CvD (Secretariaat van de CvD) • Eigenaar

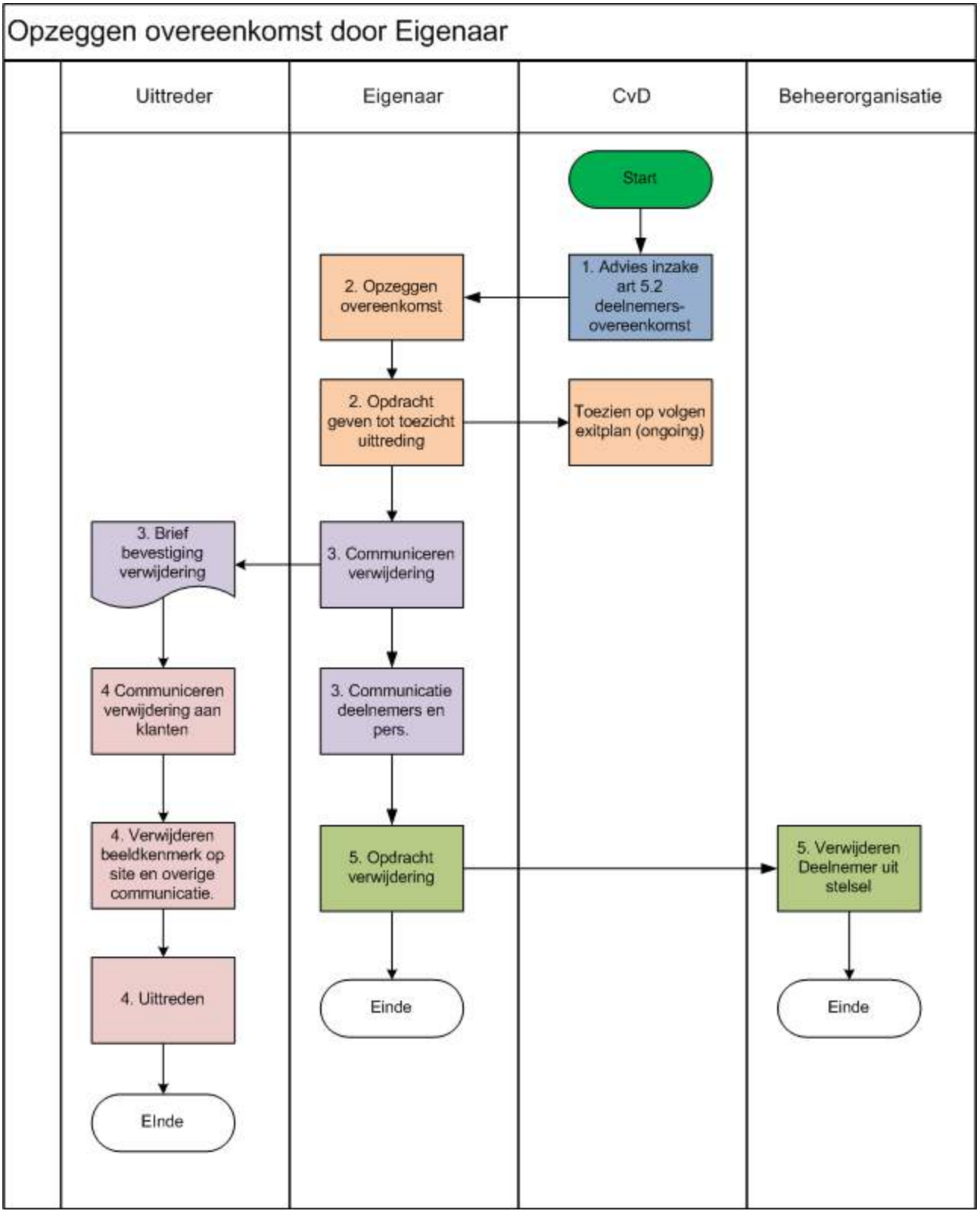
3. Communiceren uittreding	
Input	Het verzoek of besluit tot beëindiging van de deelnemersovereenkomst.
Activiteit	De Eigenaar stuurt de betreffende deelnemer de bevestiging van het verzoek tot uittreding. De Eigenaar informeert de deelnemers in het stelsel over het beëindigen van de deelnemersovereenkomst. De Eigenaar is verantwoordelijk voor communicatie met de pers omtrent de uittreding. De relevante betrokken partijen in het Afsprakenstelsel moeten geïnformeerd worden. Hierbij dienen de verschillende doelgroepen die moeten worden geïnformeerd vooraf te zijn geïdentificeerd en dient de wijze van contact vooraf zijn beschreven. Uitgangspunt hierbij dient te zijn dat dienstverleners en gebruikers zoveel mogelijk tijd krijgen om gestructureerd over te stappen naar een andere deelnemer.
Output	Communicatie richting deelnemers en pers
Wie?	• Eigenaar • Uittredende deelnemer richting haar contractpartijen

4. Uitvoeren handelingen mbt uittreding door deelnemer	
Input	Het verzoek tot beëindiging van de deelnemersovereenkomst.
Activiteit	De uittredende deelnemer voert de maatregelen uit conform het het eigen exitplan (voor een voorbeeld zie handreiking exitplan). De uittredende deelnemer stelt hiervoor een "SMART" actieplan met daarin dwingend opgenomen de volgorde in de tijd waarop activiteiten dienen te worden uitgevoerd. Hieruit moet bijvoorbeeld blijken wanneer de uitgifte van middelen wordt gestopt, wanneer er gecommuniceerd en wanneer de dienstverlening wordt stopgezet enzovoort. De uittredende deelnemer moet zijn contractpartijen (de eindgebruikers en aangesloten dienstverleners) terstond informeren over de opzegging van de deelnemersovereenkomst. De contractpartijen moeten zoveel mogelijk tijd geboden krijgen om over te stappen naar een andere erkende aanbieder. De uittredende deelnemer dient alle beeldmerken van eHerkenning van internetpagina's, websites, apparatuur, reclame-uitingen en andere (communicatie)middelen te verwijderen. De uittredende deelnemer dient alle informatie die niet langer noodzakelijk is, zoals logging, digitale dossiers en fysieke stukken, te verwijderen én veilig te archiveren. Hierbij dient te worden aangegeven of informatie verwijderd kan worden of dat deze bij de beheerorganisatie dient te worden ondergebracht en op welke wijze dit veilig gebeurt. Persoonsgegevens verdienen hierbij bijzondere aandacht.
Output	Actieplan Aangepaste Communicatie Bijgewerkte website van de deelnemer
Wie?	• Deelnemer • CvD met ondersteuning van het secretariaat.

5. Verwijderen deelnemer uit het netwerk	
Input	Communicatie uittreding door Eigenaar Opdracht van de Eigenaar tot verwijdering
Activiteit	De Eigenaar geeft opdracht aan de Beheerorganisatie om alle verwijzingen naar de betreffende deelnemer van de website (uitgezonderd oudere nieuwsberichten) te verwijderen en levert de communicatie aan over de beëindiging van de deelnemersovereenkomst op de website. De Beheerorganisatie verwijdert de informatie van de uittredende partij uit de netwerkmetadata. Deze nieuwe metadata levert de Beheerorganisatie op aan de overige deelnemers conform het Proces metadata. Nadat de deelnemers de netwerkmedata hebben verwerkt is de Deelnemer technisch uit het stelsel verwijderd. De Eigenaar bevestigt de uittreding aan de deelnemer en daarmee de beëindiging van de deelnemersovereenkomst.
Output	Verwijdering van de betreffende deelnemer uit het technische netwerk van het stelsel.
Wie?	• Beheerorganisatie

Overzicht processtappen beëindiging door Eigenaar van de deelnemersovereenkomst

De Eigenaar kan besluiten een deelnemer te verwijderen in zijn rol als Toezichthouder om zo op te kunnen treden tegen Deelnemers die zich niet aan de afspraken houden. De Commissie van Deskundigen geeft advies hoe opgetreden kan worden en verwijdering is hierin een instrument.



Overzicht processtappen

1. Advies over het opzeggen van de overeenkomst door de Eigenaar	
Input	Voorvallen genoemd in artikel 5.2 van de deelnemersovereenkomst

Activiteit	De deelnemersovereenkomst specificeert de redenen om de overeenkomst te beëindigen. Als de Commissie van Deskundigen dergelijke omstandigheden constateert dan zal dat aan de Eigenaar kenbaar worden gemaakt in een advies.
Output	Schriftelijk opzegging van de deelnemersovereenkomst van de deelnemer.
Wie?	• CvD • Eigenaar

2. Opzeggen van de overeenkomst door de Eigenaar	
Input	Advies van de CvD
Activiteit	De Eigenaar zal bij opvolging van het advies de deelnemersovereenkomst met de betreffende deelnemer opzeggen. De Eigenaar vraagt de CvD om toezicht te houden op het uittredingsproces.
Output	Schriftelijk opzegging van de deelnemersovereenkomst van de deelnemer.
Wie?	• Eigenaar • CvD • Uittredende deelnemer

3. Communiceren uittreding	
Input	De beëindiging van de deelnemersovereenkomst.
Activiteit	De Eigenaar brengt de deelnemer schriftelijk op de hoogte van het opzeggen van de overeenkomst en ook overige belanghebbenden zoals overige deelnemers, Goverance, Beheerorganisatie en eventueel de pers.
Output	Brief met de beëindiging van de deelnemersovereenkomst. Communicatieplan
Wie	• Deelnemer • Eigenaar

4. Uitvoeren handelingen mbt uittreding door deelnemer	
Input	De beëindiging van de deelnemersovereenkomst.
Activiteit	De uittredende deelnemer voert de maatregelen uit conform het het eigen exitplan. De uittredende deelnemer stelt hiervoor een "SMART" actieplan met daarin dwingend opgenomen de volgorde in de tijd waarop activiteiten dienen te worden uitgevoerd. Hieruit moet bijvoorbeeld blijken wanneer de uitgifte van middelen wordt gestopt, wanneer er gecommuniceerd en wanneer de dienstverlening wordt stopgezet enzovoort. De uittredende deelnemer moet zijn contractpartijen (de eindgebruikers en aangesloten dienstverleners) terstond informeren over de opzegging van de deelnemersovereenkomst. De contractpartijen moeten zoveel mogelijk tijd geboden krijgen om over te stappen naar een andere erkende aanbieder. De uittredende deelnemer dient alle beeldmerken van eHerkenning van internetpagina's, websites, apparatuur, reclame-uitingen en andere (communicatie)middelen te verwijderen. De uittredende deelnemer dient alle informatie die niet langer noodzakelijk is, zoals logging, digitale dossiers en fysieke stukken, te verwijderen én veilig te archiveren. Hierbij dient te worden aangegeven of informatie verwijderd kan worden of dat deze bij de beheerorganisatie dient te worden ondergebracht en op welke wijze dit veilig gebeurt. Persoonsgegevens verdienen hierbij bijzondere aandacht.
Output	Actieplan Aangepaste Communicatie Bijgewerkte website van de deelnemer
Wie?	• Deelnemer • CvD met ondersteuning van het secretariaat.

5. Verwijderen deelnemer uit het netwerk	
Input	Communicatie uittreding door Eigenaar Opdracht van de Eigenaar tot verwijdering
Activiteit	De Eigenaar geeft opdracht aan de Beheerorganisatie om alle verwijzingen naar de betreffende deelnemer van de website (uitgezonderd oudere nieuwsberichten) te verwijderen en levert de communicatie aan over de beëindiging van de deelnemersovereenkomst op de website. De Beheerorganisatie verwijdert de informatie van de uittredende partij uit de netwerkmetadata. Deze nieuwe metadata levert de Beheerorganisatie op aan de overige deelnemers conform het Proces metadata. Nadat de deelnemers de netwerkmedata hebben verwerkt is de Deelnemer technisch uit het stelsel verwijderd. De Eigenaar bevestigt de uittreding aan de deelnemer en daarmee de beëindiging van de deelnemersovereenkomst.
Output	Verwijdering van de betreffende deelnemer uit het technische netwerk van het stelsel.
Wie?	• Beheerorganisatie

Handreiking exitplan

Inleiding

Deze handreiking geeft aanwijzingen voor een exitplan. De deelnemer kan de aanwijzingen gebruiken als basis voor het opstellen van zijn eigen exitplan.

Het exitplan dient het doel de ordelijke stopzetting van de dienstverlening door de deelnemer, ongeacht de intentie of oorzaak, te waarborgen om daarmee de reputatie van de ETD-merken te beschermen en de veiligheid van en het vertrouwen in het stelsel te borgen. Deze stopzetting is, ofwel een gevolg van een voorziene en geplande situatie, óf het gevolg van een onvoorziene, niet geplande situatie, bijvoorbeeld in geval van een faillissement.

De deelnemer gaat uit van een beslissing tot beëindiging van de dienstverlening en werkt daarbij minimaal één van de volgende scenario's in het exitplan uit.

1. De dienstverlening (van een of meerdere rollen) wordt overgedragen aan een andere deelnemer of;
2. de dienstverlening (van een of meerdere rollen) wordt gestopt zonder overdracht.

Als het stoppen van de dienstverlening slechts een (of meerdere) rol(len) betreft, terwijl de diensten van andere rollen worden voortgezet, dan betekent dit eveneens dat de deelnemersovereenkomst daarop aangepast dient te worden.

In de beschrijving van het gekozen scenario worden de bijzonderheden aangegeven voor het geval het plan in werking moet treden in een onvoorziene situatie. Daarnaast moet het plan aansluiten bij hetgeen in het Operationeel Handboek is opgenomen over het proces uittreden. De deelnemer dient voor toetreding tot het afsprakenstelsel het exitplan uit te werken, waarbij inhoudelijk een detailniveau wordt verlangd dat in lijn is met de op dat moment beschikbare informatie. Als de deelnemer, na toetreding tot het afsprakenstelsel, daadwerkelijk de dienstverlening gaat beëindigen, dan dient het exitplan verder te worden uitgebreid met de dan beschikbare informatie.

De situatie waarbij omgevingsfactoren ongeplande verstoring van de dienstverlening veroorzaken, valt buiten de scope van deze handreiking. Voor het opstellen van klassieke continuïteitsplannen is buiten het ETD-stelsel voldoende informatie beschikbaar.

Het exitplan is een zelfstandig document, of een als zodanig herkenbaar onderdeel van het continuïteit-plan.

Inhoudsopgave van het plan

1. Doel van het exitplan

Kerndoelen van het plan zijn:

1. veiligstellen van de gebruiksgegevens[1], gebruikersgegevens[2] en berichten-logs[3] overeenkomstig in het afsprakenstelsel voorgeschreven bewaartermijnen;
2. veilige en volledige overdracht van gebruikersgegevens, gebruiksgegevens en berichten-logs;
3. waarborgen dat de bedoelde gegevens ook na de overdracht inzichtelijk gemaakt kunnen worden ten behoeve van opvraging door gebruikers, dienstverleners en opsporingsinstanties;
4. waarborgen van mogelijkheden tot het doen van navraag door hierboven genoemde partijen over de hierboven genoemde gegevens;
5. waarborgen van doeltreffende informatie aan klanten (Dienstverleners en Gebruikers), Beheerorganisatie en Toezichthouder, onderaannemers over de stopzetting en overdracht van dienstverlening en data.

2. Scope van het exit-plan

Beschrijft de scope van de dienstverlening waarvoor het exit-plan van toepassing is.

Doel van deze paragraaf is dat de medewerker die verantwoordelijk wordt gesteld voor de uitvoering van het exitplan snel overzicht over het speelveld kan krijgen.

1. Beschrijft de stelsel-rollen waarvoor is toegetreden, inclusief verwijzing naar actuele brongegevens.
2. Beschrijft de diensten, functionaliteiten waarvoor is toegetreden, inclusief verwijzing naar actuele brongegevens.
3. Beschrijft de omvang van de dienstverlening (markt, klanten) of verwijst voor deze informatie naar actuele bedrijfsinterne bronnen.
4. Beschrijft welk scenario voor welke rollen en dienstverlening van toepassing is.

3. Het Exit-scenario

Dit hoofdstuk beschrijft een of meerdere exit scenario's voor de diensten die zijn opgenomen in hoofdstuk 2. Dit hoofdstuk sluit aan bij hetgeen in het Operationeel handboek over het proces uittreden is opgenomen (RFC2041). Daar waar het relevant is, maakt het plan een onderscheid tussen een geplande en ongeplande stop van de dienstverlening.

Doelstelling

- Beschrijft in grote lijnen wat het scenario beoogt te bereiken.

Stappenplan

- Beschrijft de activiteiten die uitgevoerd moeten worden, geeft hierbij aan hoe kerndoelen 1-5 concreet worden ingevuld met welk resultaat en gewenste doorlooptijd. Daarnaast beschrijft het de afhankelijkheden tussen de activiteiten. Dit stappenplan moet door de verantwoordelijke definitief ingevuld kunnen worden op het moment dat het exitplan in werking moet treden.

Verantwoordelijkheden

- Beschrijft de verantwoordelijkheden voor de uitvoering van elke activiteit en ‘wie’ (persoon/afdeling) de activiteit daadwerkelijk uitvoert.

Contact

- Beschrijft de contactgegevens van de relevante personen bij de Toezichthouder en Beheerorganisatie en de contactgegevens van de verantwoordelijke en beheerder voor dit exitplan bij de Deelnemer.

Specifieke aandachtspunten voor de verschillende rollen

- Rol MU/AD:
  - realisatie van privacy-waarborgen die borgen dat gebruikersgegevens en gebruiksgegevens conform gelden privacy wet- en regelgeving worden verwerkt;
  - realisatie van doeltreffende waarborgen voor de communicatie naar gebruikers.
- Rol HM:
  - realisatie van waarborgen voor de communicatie naar Dienstverleners.
- Rol MR:
  - waarborgen voor de communicatie richting Dienstafnemer.
- Alle rollen:
  - het contact met de Toezichthouder en Beheerorganisatie op het moment dat het plan in werking treedt, is gewaarborgd;
  - indien relevant, zijn taken van onderaannemers gewaarborgd.

Uitwerking van de benodigde voorzieningen voor uitvoering van het plan zijn in paragraaf 4 opgenomen.

4. Uitwerking voorzieningen

Beschrijft in elk geval de organisatorische, juridische, technische en financiële waarborgen voor de uitvoering van het exit-plan.

5. Onderhoud

Beschrijft hoe het plan is opgenomen in de risicomanagementcyclus van de onderneming en maakt duidelijk hoe de actualiteit van het exitplan is gewaarborgd.

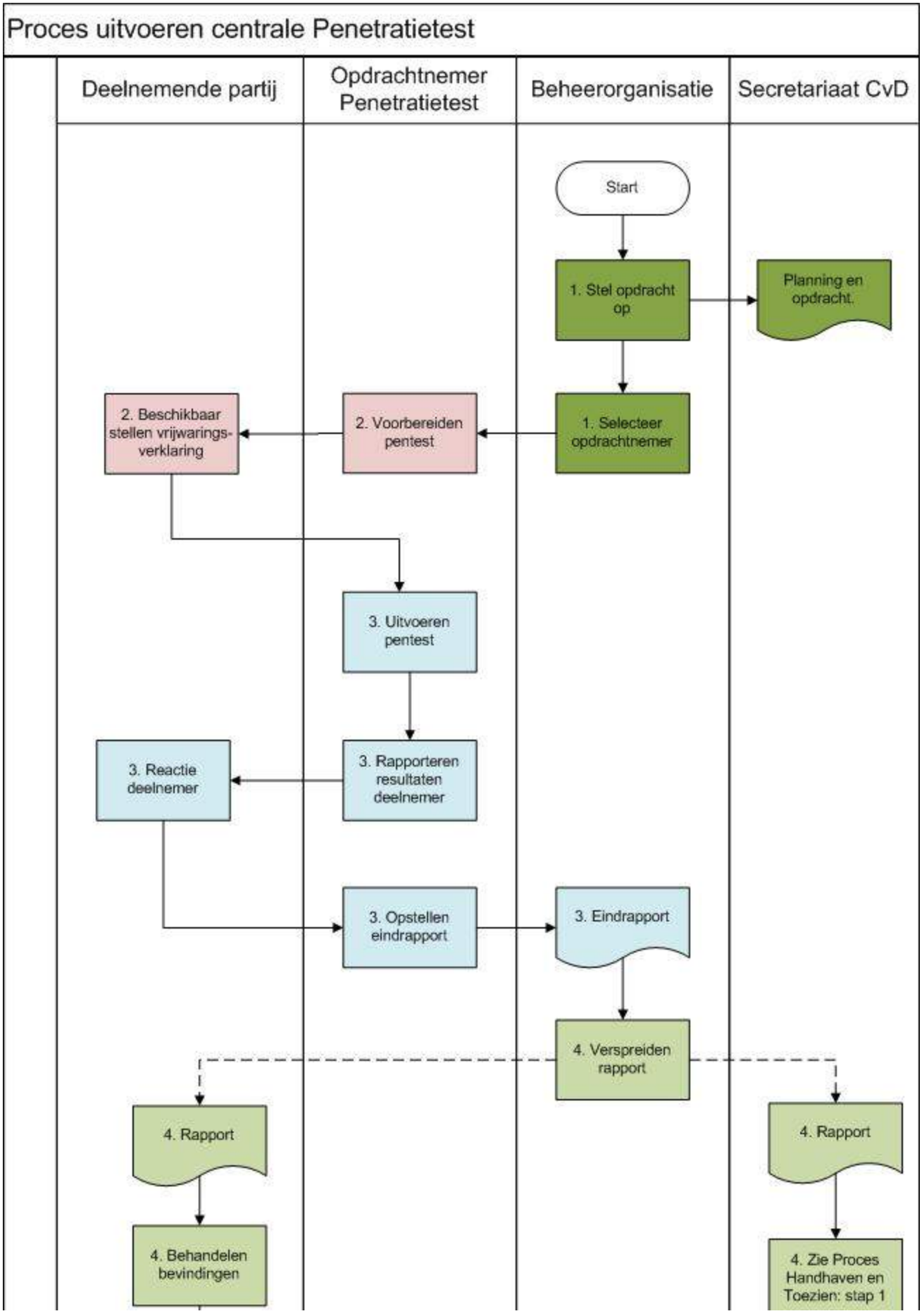
Begrippen

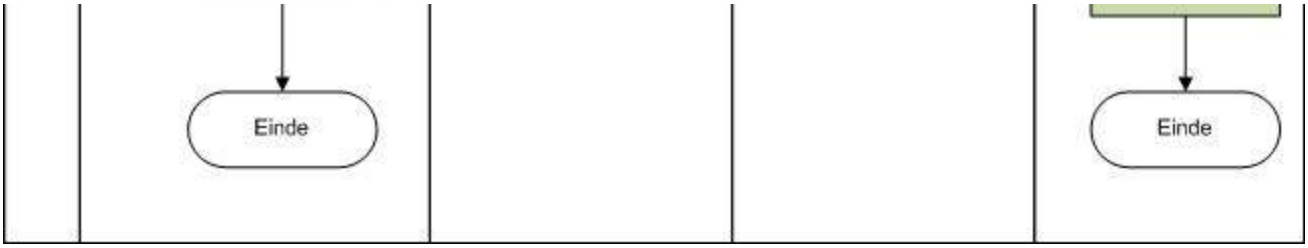
1. Gebruiksgegevens: alle gegevens over het gebruik van een specifiek middel en machtiging.
2. Gebruikersgegevens: alle gegevens die over een gebruiker zijn vastgelegd ten behoeve van de uitgifte van een middel en registratie van een machtiging.
3. Berichten-logs: het betreft hier de verzameling van (technische) ondertekende berichten die de Deelnemer ontvangt en verzendt.

Proces uitvoeren centrale penetratietest

De centrale penetratietest wordt conform het Beleid voor penetratietesten éénmaal per jaar uitgevoerd.

Hieronder staan de processtappen genoemd rondom het uitvoeren van deze test.


Proces uitvoeren centrale Penetratietest
Deelnemende partij
Opdrachtnemer Penetratietest
Beheerorganisatie
Secretariaat CvD
Start
1. Stel opdracht op
Planning en opdracht.
1. Selecteer opdrachtnemer
2. Voorbereiden pentest
2. Beschikbaar stellen vrijwarings-verklaring
3. Uitvoeren pentest
3. Rapporteren resultaten deelnemer
3. Reactie deelnemer
3. Opstellen eindrapport
3. Eindrapport
4. Verspreiden rapport
4. Rapport
4. Behandelen bevindingen
4. Rapport
4. Zie Proces Handhaven en Toezien: stap 1



Toelichting

1. Start opstellen opdracht	
Input	• Bevindingen eerdere penetratietesten • Input vanuit het security officers overleg • Aanbieding externe specialist
Activiteit	De Beheerorganisatie stelt een opdracht voor het uitvoeren van een centrale penetratietest op. In deze opdracht neemt de BO de bevindingen mee van de afgelopen centrale penetratietest en mogelijke input vanuit het security officers overleg. Het Secretariaat van de CvD krijgt een afschrift van de opdracht. De Beheerorganisatie verstrekt de opdracht tot het uitvoeren van een penetratietest aan een onafhankelijke externe specialist (Opdrachtnemer).
Output	Opdracht voor de penetratietest en een opdrachtnemer penetratietest.
Wie?	• Beheerorganisatie • Opdrachtnemer

2. Voorbereiden opdracht	
Input	Opdracht
Activiteit	De opdrachtnemer zorgt dat de Deelnemer een getekende vrijwaringsverklaring overlegt en maakt afspraken over de start van de testen. Zonder deze vrijwaringsverklaring kan de test niet starten en stopt het proces uitvoeren van de penetratietest voor de betreffende Deelnemer.
Output	• Getekende vrijwaringsverklaring • Planning
Wie?	• Opdrachtnemer • Deelnemer

3. Uitvoeren opdracht	
Input	Planning
Activiteit	De Opdrachtnemer voert de penetratietesten uit. De resultaten worden aan de hand van de principes hoor en wederhoor teruggekoppeld aan de Deelnemer. De Deelnemer krijgt hierbij de mogelijkheid om bevindingen toe te lichten en/of op te lossen. De Opdrachtnemer Penetratietest rapporteert integraal over de uitgevoerde penetratietesten aan de beheerorganisatie.
Output	Integraal testrapport
Wie?	• Opdrachtnemer • Deelnemer • Beheerorganisatie

4. Communiceren resultaten penetratietest	
Input	Integraal testrapport
Activiteit	De Beheerorganisatie stelt het individuele rapport beschikbaar aan de Deelnemer en aan het Secretariaat van de CvD. De Beheerorganisatie en Deelnemer gebruikt het rapport als input voor een volgende penetratietest.
Output	Individueel testrapport
Wie?	• Deelnemer • Beheerorganisatie • Secretariaat van de CvD

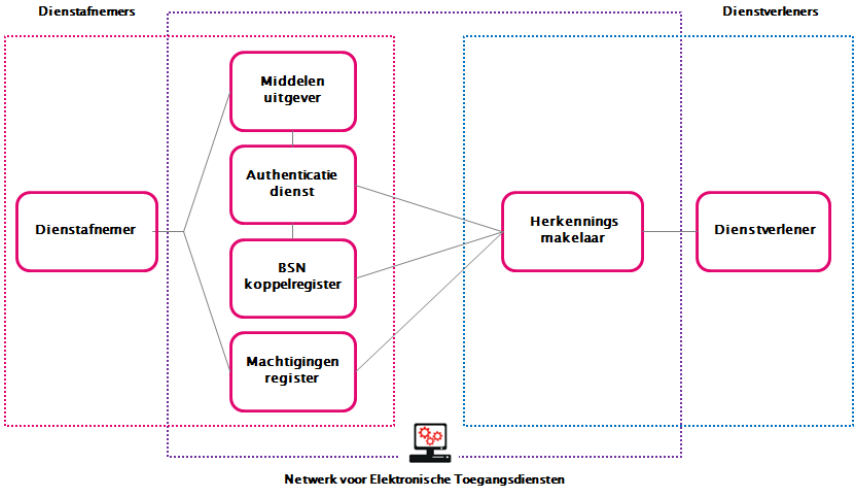
Proces wijziging rechtspersoon

Wanneer een deelnemer de rechtspersoon wil wijzigen, maakt hij dit kenbaar aan de beheerorganisatie door middel van het formulier Template wijziging rechtspersoon deelnemer.De deelnemer retourneert het ingevulde formulier en met bijbehorende bijlagen naar info@eherkenning.nl.

Businessmodel

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Dit document beschrijft het businessmodel voor Elektronische Toegangsdiensten. Onder het businessmodel worden verstaan de afspraken die betrekking hebben op de onderlinge verrekening van kosten en baten tussen verschillende partijen die samen het Netwerk (voor Elektronische Toegangsdiensten) invullen. Het is bedoeld voor deelnemers en dienstverleners.



Het businessmodel gaat uit van de volgende afspraken:

- De kosten voor verplichte functionaliteit worden gedeeld tussen de twee primaire doelgroepen van het Netwerk (voor Elektronische Toegangsdiensten): bedrijven en dienstverleners. De dienstverlener betaalt voor de dienstverlening van de Herkenningsmakelaar, terwijl de bedrijven betalen voor de dienstverlening door de Authenticatiedienst (AD) (inclusief Authenticatiemiddel) en het Machtigingenregister (MR).
- Deelnemers kunnen onderling afspraken maken met betrekking tot de volgende zaken:
  - Onderlinge verrekeningen.
  - Tariefstructuren.
- Onderlinge afspraken moeten altijd voldoen aan de mededingingswetten (ACM als toezichthouder).

Service level

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Dit document beschrijft de Service Level afspraken die gelden voor deelnemers en de beheerorganisatie van Elektronische Toegangsdiensten. Het betreft een beschrijving van het minimale Service Level dat de deelnemers moeten leveren aan elkaar en hun dienstafnemers en het minimale Service Level dat de beheerorganisatie levert aan de deelnemers.

Dit Service Level geldt in aanvulling op de Gebruiksvoorwaarden Elektronische Toegangsdiensten die Deelnemer en zijn Gebruiker zijn overeengekomen en behelst de afspraken over de Beschikbaarheid en het Serviceniveau van Herkenningsdiensten. Gebruikers kunnen slechts rechten ontlenen aan het Service Level dat van kracht was op het moment dat de overeenkomst met de Deelnemer werd gesloten.

Voor de betekenis van en toelichting op de gebruikte begrippen in dit document, zie de Begrippenlijst.

Leeswijzer

- Beschikbaarheid
  - Beschikbaarheidsvenster
  - Onderhoudsvenster
    - Componenten
  - Servicevenster
  - Openstellingsvenster
  - Rekenmethode
- Performance — Performance is datgene wat Elektronische Toegangsdiensten bereikt of levert, uitgedrukt in tijd of aantallen.
- Contentmanagement
- Incidenten — Onder ‘incidenten’ wordt verstaan: elke gebeurtenis die niet tot de standaardoperatie van een dienst behoort en die mogelijk impact c.q. risico oplevert ten aanzien van de kwaliteit, beschikbaarheid, integriteit en/of vertrouwelijkheid van (gegevens binnen) het netwerk.
- Managementrapportage — Managementrapportages zijn bedoeld om de groei van het netwerk en de service level afspraken binnen het netwerk te monitoren. Zie ook Proces managementrapportage.
- Monitoring — De monitoring van de in het service level gemaakte afspraken zal door de beheerorganisatie worden uitgevoerd.
- Ondersteuning — Ondersteuning betreft het afhandelen van zaken als vragen, verzoeken en klachten.
- Responsetijden

Beschikbaarheid

Dit hoofdstuk beschrijft wat het service level voor deelnemers en de beheerorganisatie zijn op het vlak van beschikbaarheid. De beschikbaarheid wordt aan de hand van de volgende vensters gedefinieerd:

- Beschikbaarheidsvenster
- Onderhoudsvenster
- Servicevenster
- Openstellingsvenster
- Rekenmethode

Beschikbaarheidsvenster

Binnen het openstellingsvenster geeft Elektronische Toegangsdiensten aan de hand van het beschikbaarheidsvenster garanties voor de beschikbaarheid van eHerkenning. Deze garanties worden gegeven voor de werking van de primaire en secundaire functionaliteit binnen de productieomgeving van eHerkenning, met als primaire doel een gebruiker in staat te stellen in te kunnen loggen bij een dienst(verlener). Er worden vanuit Elektronische Toegangsdiensten geen garanties gegeven voor de functionele beschikbaarheid van de externe functionaliteit.

Functionaliteit eHerkenning	**Openstellingsvenster**	**Beschikbaarheidsvenster**	**Minimale beschikbaarheid per rol**	**Minimale beschikbaarheid van het stelsel**
Productieomgeving: de primaire functionaliteit is inloggen Onder inloggen wordt verstaan het kunnen kiezen voor eHerkenning bij de Dienstverlener (DV), het kunnen kiezen van leverancier bij de Herkenningsmakelaar (HM), het kunnen invoeren van inloggegevens bij de Authenticatiedienst (AD) en het kunnen selecteren van de juiste machtiging bij het Machtigingenregister (MR), met als resultaat een inlog bij de Dienstverlener. Het betreft hier de primaire functionaliteit die onder beheer van het stelsel van Elektronische Toegangsdiensten valt. *Voor eenmanszaken en eIDAS functionaliteit is Elektronische Toegangsdiensten afhankelijk van overheidsvoorzieningen. Deze overheidsvoorzieningen hanteren eigen serviceniveaus, te weten 99,2% op werkdagen van 8.00 tot 17.00.*	24 uur alle dagen	24 uur alle dagen - onderhoudsvenster	99,5% per maand	99,2 % per maand
Productieomgeving: de secundaire functionaliteit is ondersteunend aan inloggen Onder ondersteunend aan inloggen wordt die functionaliteit verstaan die nodig is om beheer te kunnen uitoefenen op de productieomgeving, waarbij deze functionaliteit niet vereist is om in te kunnen loggen. Het betreft hier de secundaire functionaliteit die onder beheer van het stelsel van Elektronische Toegangsdiensten valt.	24 uur alle dagen	24 uur alle dagen - onderhoudsvenster	99,5% per maand	99,2 % per maand
Productieomgeving: de externe functionaliteit Onder externe functionaliteit wordt die functionaliteit verstaan waarbij het beheer niet onder het beheer van het stelsel van Elektronische Toegangsdiensten valt.	24 uur alle dagen	*Geen garanties vanuit Elektronische Toegangsdiensten*	-	-
Pre-Productieomgeving: de functionaliteit is het bieden van een testnetwerk. Onder het testnetwerk wordt die functionaliteit bedoeld nodig voor het uitvoeren van ketentesten.	24 uur alle dagen	24 uur alle dagen - onderhoudsvenster	Best effort	Best effort

Componenten

De op deze pagina beschreven functionaliteiten eHerkenning worden gerealiseerd middels één of meerdere componenten. Een overzicht van de onderliggende componenten is opgenomen onder Componenten.

Onderhoudsvenster

Het onderhoudsvenster stelt partijen in staat op vooraf vastgestelde tijden regulier onderhoud uit te voeren. Tijdens het onderhoudsvenster kan het voorkomen dat eHerkenning niet beschikbaar is, of onderdelen van eHerkenning niet beschikbaar zijn. Deze periode wordt niet meegenomen in de beschikbaarheidsprestaties, zie Beschikbaarheidsvenster.

De mogelijke onderhoudsvensters zijn:

Maandag t/m zaterdag	00:00 - 06:00
Zaterdag t/m zondag	20:00 - 06:00

Publicatie

- De beheerorganisatie publiceert het onderhoud op www.eherkenning.nl/onderhoud.
- Indien de dienstverlening door het onderhoud wordt verstoord, dient het onderhoud gelijktijdig met de melding in Mantis door de betreffende deelnemer(s) te worden aangekondigd via de eigen kanalen. Alle deelnemers hebben hiervoor een eigen publiek toegankelijke webpagina met informatie over actuele (on)beschikbaarheid (onderhoud en storingen). Op deze pagina staat in elk geval:
    1. Type situatie (beschikbaar/normale situatie, onbeschikbaarheid n.a.v. incident/calamiteit/crisis en onbeschikbaarheid n.a.v. onderhoud);
    2. Toelichting bij de situatie (soort incident, reden onderhoud). Dit in voor de eindgebruiker begrijpelijke taal;
    3. Datum en tijd start onbeschikbaarheid (ook toekomstig, gepland onderhoud);
    4. Indicatie van de duur van de onbeschikbaarheid;
    5. Handelingsperspectief (waar kan men terecht met vragen, verwijzing naar de klantenservice, etc.);
    6. Datum en tijd einde onbeschikbaarheid (een melding blijft staan tot minimaal 24 uur nadat de onbeschikbaarheid is opgelost).

  Op de website www.eherkenning.nl wordt standaard verwezen naar de publiek toegankelijke webpagina's met actuele beschikbaarheidsinformatie van de deelnemers. Indien mogelijk wordt daar ook verwezen naar beschikbaarheidsinformatie van externe Componenten die onderdeel zijn van de primaire functionaliteit: EB, BRPk en BSNk.

Bepalingen

Bepaling primaire functionaliteit

Definitie

- Wijzigingen aan de primaire Componenten worden gezien als onderhoud als er een productieonderbreking wordt verwacht.

Regels

- Onderhoud is gebonden aan onderhoudsvensters.
- Onderhoud MOET worden aangekondigd.
- Aankondiging van onderhoud MOET tenminste 5 werkdagen van tevoren worden gedaan via Mantis onder vermelding van datum, tijdslot en dienst.
- Als er op kortere termijn onderhoud noodzakelijk is, MOET de beheerorganisatie toestemming geven. In overleg wordt dan het tijdstip vastgesteld.
- Indien de dienstverlening door het onderhoud wordt verstoord, dient het onderhoud gelijktijdig met de melding in Mantis te worden aangekondigd via de webpagina('s) met actuele beschikbaarheidsinformatie van de betreffende deelnemer(s).

Bepaling secundaire functionaliteit

Definitie

- Wijzigingen aan de secundaire Componenten worden gezien als onderhoud als er een productieonderbreking wordt verwacht.

Regels

- Onderhoud is gebonden aan onderhoudsvensters.
- Onderhoud MOET worden aangekondigd.
- Aankondiging van onderhoud MOET tenminste op de dag van het onderhoud gedaan worden via Mantis onder vermelding van datum, tijdslot en dienst.
- Indien de dienstverlening door het onderhoud wordt verstoord, dient het onderhoud gelijktijdig met de melding in Mantis te worden aangekondigd via de webpagina('s) met actuele beschikbaarheidsinformatie van de betreffende deelnemer(s).

Bepaling externe functionaliteit

Er kunnen geen garanties worden afgegeven voor de functionele beschikbaarheid van onderdelen buiten ETD en van individuele diensten (of middelen) die afhankelijk zijn van externe Componenten.

- Neem contact op met de beheerorganisatie BSNk voor informatie over haar SNO.

Bepaling testnetwerk functionaliteit

Definitie

- Wijzigingen aan testnetwerk Componenten worden niet gezien als onderhoud (gaat niet gepaard met productieonderbrekingen).

Regels

- Onderhoud MAG plaatsvinden buiten het onderhoudsvenster.
- Onderhoud MAG worden aangekondigd.

Componenten

Het Beschikbaarheidsvenster geeft een overzicht van de functionaliteiten eHerkenning en de definitie hiervan. Deze functionaliteiten bestaan uit de componenten zoals hier weergegeven.

Componenten primaire functionaliteit productieomgeving

Componenten noodzakelijk voor de primaire functionaliteit:

- Authenticatiedienst Authenticatiedienst (AD)
- Machtigingenregister Machtigingenregister (MR)
- Herkenningsmakelaar Herkenningsmakelaar (HM)
- Cookieservers
- Endpoints voor dienstencatalogus en attribuutcatalogus *
- Endpoint voor netwerkmetadata *

De functionaliteit die is gebaseerd op verwerking BSN voor eenmanszaken en eIDAS en gezien wordt als primair, maar valt onder de verantwoordelijkheid van externe overheidsvoorzieningen buiten ETD, worden bij de componenten apart beschouwd onder componenten externe functionaliteit productieomgeving.

* Noodzakelijke ondersteunende diensten voor de productieomgeving tbv de primaire functionaliteit in beheer bij de beheerorganisatie

Componenten secundaire functionaliteit productieomgeving

Componenten noodzakelijk voor de secundaire functionaliteit:

- Confluence
- Managementrapportage
- Metadata-aggregator
- Dienstencatalogus-aggregator
- eHerkenning website
- Mantis

Componenten externe functionaliteit productieomgeving

Noodzakelijke componenten behorend bij externe functionaliteit: Dit zijn partijen buiten ETD die net als ETD deel uitmaken van een keten van organisaties die gezamenlijk dienstverlening leveren voor polymorfe pseudonymering voor gebruik van BSN en dienstverlening voor Europees inloggen onder eIDAS.

Dit zijn:

- eIDAS-berichtenservice (EB) - RVO
- eIDAS attributendienst (BRPk) - RvIG
- BSNk - Logius

Deze componenten zijn onderdeel van primaire functionaliteit voor authenticatie tbv eenmanszaken en tbv eIDAS, maar hanteren eigen richtlijnen voor beschikbaarheid, onderhoud, en service.

Er kunnen geen garanties worden afgegeven voor de functionele beschikbaarheid van individuele diensten (of middelen), aangezien configuratie en inrichting bij de dienstverlener, werkgever of gebruiker buiten het beschikbaarheidsvenster van eHerkenning valt.

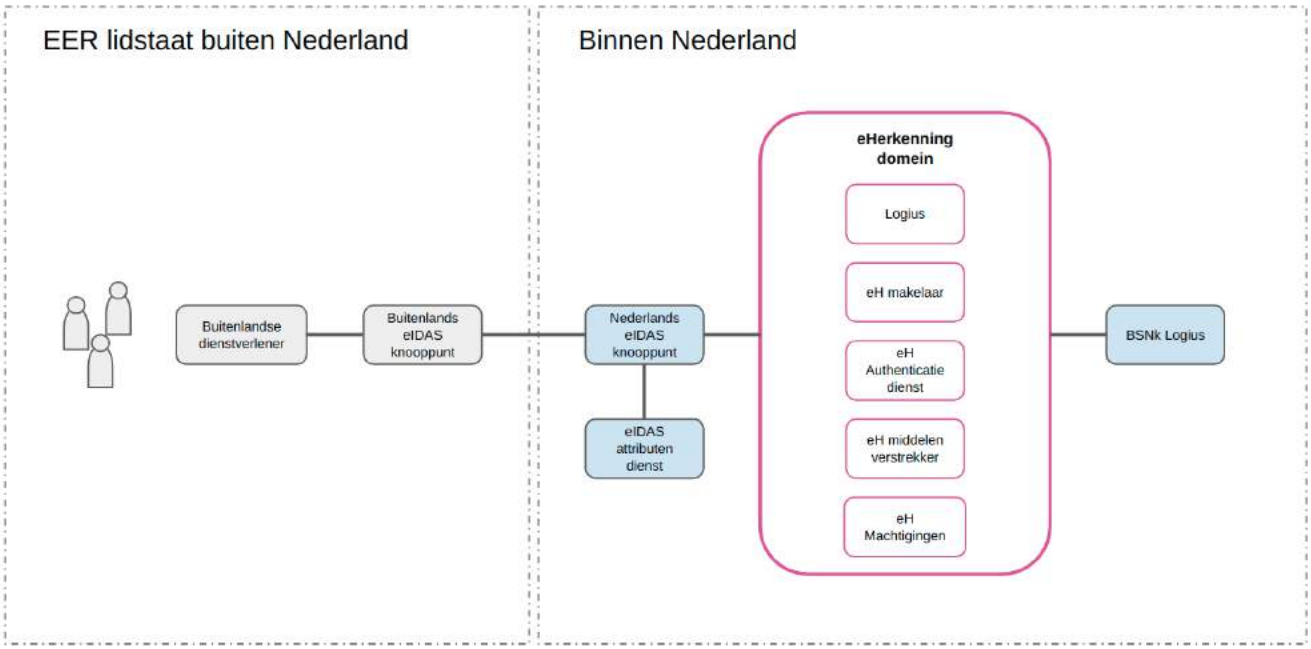
Componenten testnetwerk fuctionaliteit pre-productieomgeving

Componenten noodzakelijk voor het testnetwerk:

- Simulator
- Dienstencatalogus pre-productie
- Metadata-aggregator pre-productie
- test-systemen van de deelnemers

Voorbeeld externe functionaliteit

Het voorbeeld schetst dienstverlening voor Europees inloggen onder eIDAS waarbij de componenten buiten het eHerkennings domein worden geillustreerd (componenten buiten het roze kader). De componenten zoals gebruikt voor een eIDAS outbound flow waarbij wordt ingelogd met eHerkenning bij een buitenlandse dienstverlener.



Inloggen bij een buitenlandse dienstverlener kan met eHerkenning. Gegevens worden daarbij opgehaald in Nederland. Na authenticatie met eHerkenning wordt het versleutelde BSN m.b.v. de BSNk service via eHerkenning geleverd aan het eIDAS knooppunt waar na controle eIDAS attributen worden gekoppeld en geleverd aan de dienstverlener.

Servicevenster

Het servicevenster is de tijd waarbinnen eindgebruikers deelnemers en de beheerorganisatie Elektronische Toegangsdiensten kunnen benaderen voor ondersteuning. Het onderstaand servicevenster, is het minimale servicevenster waarbinnen deelnemers en de beheerorganisatie beschikbaar moeten zijn. Deelnemers en beheerorganisatie dienen duidelijk te communiceren richting eindgebruikers welke service varianten ze aanbieden en hoe eindgebruikers in contact kunnen treden. Tijdens het servicevenster zijn deelnemers en beheerorganisatie bereikbaar voor meldingen over de dienstverlening en de producten. Denk daarbij aan incidenten, vragen en/of klachten.

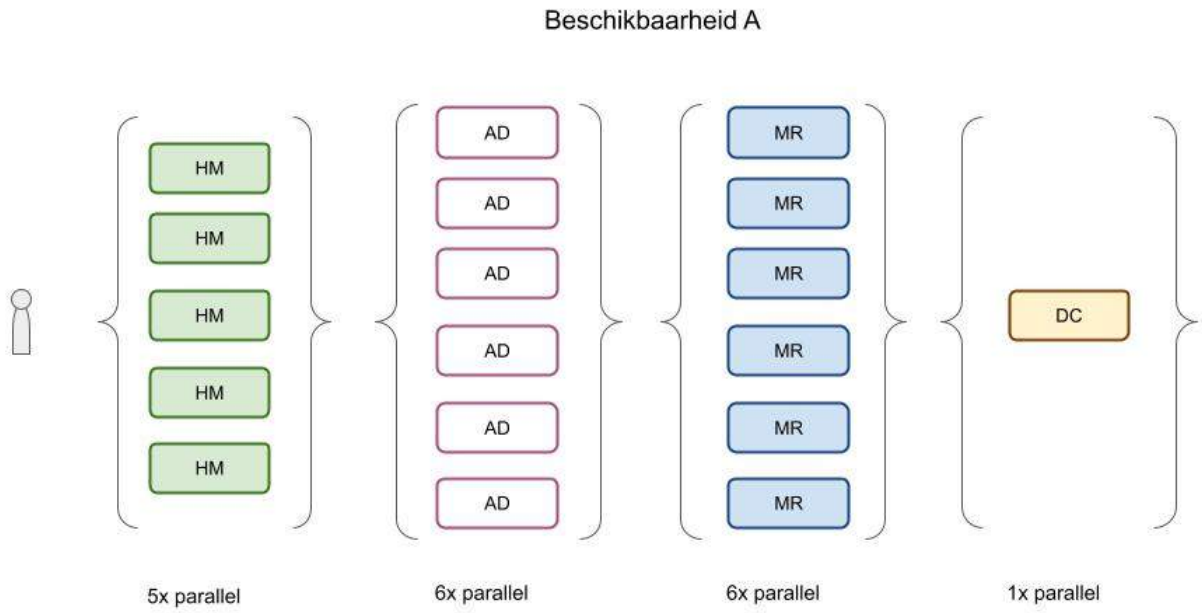
Bereikbaarheid deelnemers en beheerorganisatie	Minimale servicevenster
Voor ondersteuning en het melden van incidenten	Werkdagen tussen 09:00 - 17:00

Openstellingsvenster

Elektronische Toegangsdiensten hanteert een openstellingsvenster van 24 uur voor alle dagen van het jaar. Tijdens dit openstellingsvenster is alle functionaliteit van eHerkenning te gebruiken door alle betrokkenen. Er worden geen garanties gegeven voor de werking van eHerkenning binnen het openstellingsvenster. Het openstellingsvenster is het beschikbaarheidsvenster plus het onderhoudsvenster.

Rekenmethode

Het Beschikbaarheidsvenster geeft een minimale beschikbaarheid in procenten weer. Partijen MOETEN rapporteren over de beschikbaarheid volgens de hier vastgestelde rekenmethode. De rekenmethode is gebaseerd op het principe van parallel en serieel geschakelde componenten. Hierbij worden de parallel geschakelde componenten gemiddeld en worden de seriële geschakelde componenten gelijk gewogen.



De seriële en parallele componenten schematisch weergegeven.

Definities rekenmethode

Rapportage periode	Per kalendermaand
Totaal tijd	Dagen in de maand x uren per dag (24 uur)
Incident tijd	Tijd dat een rol niet operationeel is door een incident (in uren)
Onderhoudstijd	Tijd dat een rol niet operationeel is door onderhoud (in uren)
Beschikbaarheidstijd	Tijd dat een rol operationeel moet zijn (totaal tijd - onderhoudstijd)
Operationeel tijd	Tijd dat een rol operationeel is (totaal tijd - incident tijd - onderhoudstijd)
Beschikbaar (A)	percentage dat rol operationeel is
Niet beschikbaar (NA)	percentage dat een rol niet operationeel is
Formule beschikbaarheid	(Operationeel tijd / Beschikbaarheidstijd) x 100 = (in procenten)
HM	Rol Herkenningsmakelaar
AD	Rol Authenticatiedienst
MR	Rol Machtigingenregister
DC	Rol Dienstencatalogus, attribuutcatalogus en netwerkmetadata

Formule beschikbaarheid per rol

Een leverancier dient de beschikbaarheid per rol als volgt te berekenen; (Operationeel tijd / Beschikbaarheidstijd) x 100 = (in procenten). Voor de bepaling van de operationeel tijd en de beschikbaarheidstijd dienen de definities zoals onder definities rekenmethode weergegeven te worden gehanteerd.

Formule stelselbeschikbaarheid

De gemiddelden voor de parallelle componenten dient als volgt te worden berekend:

Beschikbaarheid (A) HMs = (A HM1 + A HM2+ A HM3 + A HM...) / Totaal aantal HMs;

Beschikbaarheid (A) ADs = (A AD1 + A AD2+ A AD3 + A AD...) / Totaal aantal ADs;

Beschikbaarheid (A) MRs = (A MR1 + A MR2+ A MR3 + A MR...) / Totaal aantal HMs;

Beschikbaarheid (A) DCs = (A DC1 + A DC2+ A DC3 + A DC...) / Totaal aantal DCs.

Met deze beschikbaarheidscijfers dient de stelselbeschikbaarheid als volgt te worden berekend:

Beschikbaarheid As = (A HMs) (A ADs) (A MRs) (A DCs)

Voorbeeld berekening

Dit voorbeeld is gebaseerd op fictieve leveranciers en cijfers en dient slecht als voorbeeld te worden gezien.

Maand	**Dagen**	**Uren per dag**	**Totaaltijd**			
Maart	31	24	744			
HM	**Totaal tijd**	**Onderhoudstijd**	**Incident tijd**	**Operationeel tijd**	**Beschikbaarheidstijd**	**Beschikbaarheid (A)**
Leverancier 1	744	0	0	744	744	100
Leverancier 2	744	0	2	742	744	99,73
Leverancier 3	744	4	0	740	740	100
AD	**Totaal tijd**	**Onderhoudstijd**	**Incident tijd**	**Operationeel tijd**	**Beschikbaarheidstijd**	**Beschikbaarheid (A)**
Leverancier 1	744	0	0	744	744	100
Leverancier 2	744	0	2	742	744	99,73
Leverancier 3	744	2	2	740	742	99,73
MR	**Totaal tijd**	**Onderhoudstijd**	**Incident tijd**	**Operationeel tijd**	**Beschikbaarheidstijd**	**Beschikbaarheid (A)**
Leverancier 1	744	0	2	742	744	99,73
Leverancier 2	744	4	0	740	740	100
Leverancier 3	744	0	0	744	744	100
DC	**Totaal tijd**	**Onderhoudstijd**	**Incident tijd**	**Operationeel tijd**	**Beschikbaarheidstijd**	**Beschikbaarheid (A)**
Leverancier 1	744	0	0	744	744	100

Beschikbaarheid (A) HMs = (A HM1 + A HM2+ A HM3) / Totaal aantal HMs = (100 + 99,73 + 100) / 3 = 99,91%

Beschikbaarheid (A) ADs = (A AD1 + A AD2+ A AD3) / Totaal aantal ADs = (100 + 99,73 + 99,73) / 3 = 99,82%

Beschikbaarheid (A) MRs = (A MR1 + A MR2+ A MR3) / Totaal aantal HMs = (99,73 + 100 + 100) / 3 = 99.91%

Beschikbaarheid (A) DCs = (A DC1) / Totaal aantal DCs = (100) / 1 = 100%

Beschikbaarheid As = (A HMs) (A ADs) (A MRs) (A DCs) = (0,9991) (0,9982) (0,9991) (1) = 99,64%

Performance

Performance is datgene wat Elektronische Toegangsdiensten bereikt of levert, uitgedrukt in tijd of aantallen. Doel van het stellen van performancenormen is het waarborgen van een goede gebruikersbeleving op piekmomenten.

Voor deelnemers	Norm
Verwerking van berichten	• 95% van de berichten MOET binnen 2 seconden worden beantwoord • 99% van de berichten MOET binnen 5 seconden worden beantwoord • Elke deelnemer MOET ten minste 100 gelijktijdige berichten kunnen verwerken terwijl nog wordt voldaan aan de performance-eisen

Contentmanagement

De beheerorganisatie MOET verzoeken tot wijzigen van content vanuit het Proces contentmanagement binnen 3 werkdagen afhandelen.

De beheerorganisatie MOET maximaal 10 dagen na het afronden van gepland onderhoud de publicatie hiervan op www.eherkenning.nl/onderhoud verwijd eren.

Incidenten

Onder ‘incidenten’ wordt verstaan: elke gebeurtenis die niet tot de standaardoperatie van een dienst behoort en die mogelijk impact c.q. risico oplevert ten aanzien van de kwaliteit, beschikbaarheid, integriteit en/of vertrouwelijkheid van (gegevens binnen) het netwerk.

Zie ook Proces incidentmanagement.

Prioritering incidenten

Voor de prioritering van incidenten bestaan verschillende escalatieniveaus.

Escalatieniveau	Impact en urgentie
Incident	• Verwachte verstoringsduur <4 uur; • Betrokkenheid van één deelnemer.
Calamiteit	• Verwachte verstoringsduur > 4 uur en/of; • Betrokkenheid van tenminste twee deelnemers en/of; • Directe en ernstige hinder en/of; • Impact op vertrouwelijkheid en integriteit.
Crisis	• Verwachte verstoringsduur > 48 uur en/of; • Betrokkenheid van meerdere deelnemers en/of; • Grote impact op imago en vertrouwen van eHerkenning en/of; • Politieke implicaties en/of; • Fundamentele juridische of technische kwetsbaarheid.

Melden van incidenten

Elke deelnemer moet incidenten direct na ontdekking melden bij de beheerorganisatie.

Type incident	Melding
Incident	• Via de issuetracker Mantis.
Calamiteit	• Telefonisch bij de incidentmanager van de beheerorganisatie; • Na overleg met de beheerorganisatie via de issuetracker Mantis.
Crisis	• Telefonisch bij de incidentmanager van de beheerorganisatie; • Na overleg met de beheerorganisatie via de issuetracker Mantis.

De prioritering van het incident wordt bepaald door de melder. De beheerorganisatie mag de prioriteit van een gemeld incident wijzigen.

Oplossen van incidenten

Indien een incident niet binnen de gestelde Responsetijden opgelost is, maakt de BO de afweging of er opgeschaald moet worden conform het Proces incidentmanagement.

In het geval van een calamiteit of een crisis moet elke deelnemer 24x7 een contactpersoon beschikbaar hebben.

Managementrapportage

Managementrapportages zijn bedoeld om de groei van het netwerk en de service level afspraken binnen het netwerk te monitoren. Zie ook Proces managementrapportage.

De deelnemers en de beheerorganisatie verzamelen de eigen managementinformatie van de rapportageperiode (deze loopt van de eerste dag van een kalendermaand 0:00 uur tot de laatste dag 24:00 uur).

Elke deelnemer moet uiterlijk de 5e van elke kalendermaand de rapportage over de voorafgaande rapportageperiode aan de beheerorganisatie opleveren voor 24:00 uur. Hiertoe moet de deelnemer de door de beheerorganisatie beschikbaar gestelde rapportagetool gebruiken. De rapportage over ketenmachtigingen en belastingdienstmiddelen moet per e-mail verstrekt worden. De regels om rapportages via email te verzenden zijn als volgt:

1: De rapportage MOET als encrypted bestand verstuurd. Dit mag middels extern vertrouwde websites of middels het versleutelen van de rapportage zelf

2: De decryptiesleutel, of wachtwoord, MOET out-of-band worden verstuurd.

De beheerorganisatie zal de geaggregeerde informatie binnen 5 werkdagen delen met alle deelnemers en dienstverleners.

Monitoring

De monitoring van de in het service level gemaakte afspraken zal door de beheerorganisatie worden uitgevoerd. Zij doet dit in de eerste plaats door het analyseren van de door deelnemers opgeleverde rapportages, maar ook het uitvoeren van steekproeven behoort tot de mogelijkheden.

Ondersteuning

Ondersteuning betreft het afhandelen van zaken als vragen, verzoeken en klachten.

Beschikbaarheid deelnemers	**Norm**
Voor service en support aan elkaar, dienstverleners, eindgebruikers en de beheerorganisatie bij onder andere het: • ondersteunen bij het gebruik van Elektronische Toegangsdiensten; • verstrekken van informatie; • aannemen en beantwoorden van vragen (ook van gebruikers); • in behandeling nemen van storingen en klachten over Elektronische Toegangsdiensten en de dienstverlening daarover; • (helpen) testen en hertesten van aansluitingen; • aanmaken, toewijzen en sluiten van door de deelnemer aangemaakte meldingen.	Zie Servicevenster
Beschikbaarheid beheerorganisatie	**Norm**
Voor service en support aan deelnemers bij onder andere het: • verstrekken van informatie; • in behandeling nemen van storingen en wensen m.b.t. systemen van de Beheerorganisatie; • (helpen) aansluiten op Elektronische Toegangsdiensten; • hulp bij technische implementatie; • uitvoeren van certificaatwissels; • aankondiging van onderhoud; • DAL aanvragen en DNS wijzigingen cookie domeinen.	Zie Servicevenster

Responsetijden

Voor de verschillende activiteiten van de Deelnemers, Beheerorganisatie en BSNk kunnen andere responsetijden gelden.

Activiteit	Norm
Voor Ondersteuning	Ontvangstbevestiging binnen 4 werkuren Oplossing/antwoord binnen 5 werkdagen
Afhandeling van incidenten	Oplossing binnen 4 uur

Communicatie

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Dit document beschrijft de richtlijnen voor naam en merkgebruik, huisstijl afspraken en communicatierichtlijnen voor de merken eHerkenning en eIDAS. Het is bedoeld voor alle betrokken partijen: deelnemers en dienstverleners. De beheerorganisatie levert richtlijnen, standaard tekst- en beeldmateriaal en andere tools die de deelnemers en dienstverleners dienen te gebruiken.

Eisen communicatie bij samenwerking met externe verkoopkanalen

Wat betreft het gebruik van het beeld- en woordmerk van eHerkenning door externe verkoopkanalen, gecontracteerd door Deelnemers, MOETEN Deelnemers zich houden aan de volgende afspraken:

- De beeld- en woordmerken eHerkenning zijn eigendom van de Eigenaar. Gebruik buiten de vastgelegde afspraken is NIET toegestaan;
- Deelnemers zijn NIET bevoegd derden toestemming te geven het beeld- of woordmerk eHerkenning te gebruiken, tenzij de samenwerking met het externe verkoopkanaal voldoet aan het Afsprakenstelsel en voldaan is aan de meldplicht;
    - Het gebruik van het woord- en beeldmerk van eHerkenning in domeinnaam/naamvoering door deze derden is NIET toegestaan.

De volgende eisen ten aanzien van communicatie door externe verkoopkanalen gelden:

Deelnemers MOETEN er op toezien dat de externe verkoopkanalen waar zij mee samenwerken:

- De verplichte kernboodschap voor externe verkoopkanalen opnemen, nl: " <naam externe verkoopkanaal> is wederverkoper van de erkende leverancier van eHerkenning <Naam erkende leverancier>..." Deze moet gebruikt worden bij alle communicatie middelen;
    - Voor websites specifiek moet deze op de homepage staan;
- Naast het logo van eHerkenning, het logo van de Deelnemer tonen waarmee zij samenwerken bij alle communicatie middelen;
- Het externe verkoopkanaal mag de Deelnemer, waarmee zij een contract hebben afgesloten, niet positioneren als enige verkoper van inlogmiddelen voor eHerkenning;
- De termen en/of beeldmerken "erkend" of "leverancier" zoals gebruikt in het Afsprakenstelsel in samenhang met eHerkenning zijn exclusief voorbehouden aan Deelnemers;
- Geen commerciële uitingen doen over eHerkenning en/of de Deelnemers die de beleving van het merk eHerkenning negatief kunnen beïnvloeden.
- De Deelnemer ziet erop toe dat het externe verkoopkanaal duidelijk is in de communicatie over de kosten voor de diensten i.h.k.v. eHerkenning en overige (additionele) dienstverlening.

Richtlijnen naam- en merkgebruik eHerkenning

Algemeen

Wat betreft logo, beeldelementen en terminologie MOETEN alle deelnemers en dienstverleners zich houden aan de volgende richtlijnen:

- Alle betrokken partijen (deelnemers en dienstverleners) maken gebruik van dezelfde beeldelementen en logo's (zoals beschreven in de regels en richtlijnen opgenomen in het Huisstijlhandboek eHerkenning) en passen dezelfde schrijfwijze en terminologie toe (zoals beschreven in de Begrippenlijst). Dit zorgt voor eenduidigheid in de communicatie en uitstraling van het merk eHerkenning richting gebruikers.

Deelnemers

Wat betreft naam- en merkgebruik MOETEN deelnemers zich houden aan de volgende richtlijnen:

- De naam eHerkenning wordt als merk gebruikt voor dienstverlening met eHerkenning binnen het B2B, B2G, B2C en G2G domein. eHerkenning is een merk dat binnen het overkoepelende Afsprakenstelsel Elektronische Toegangsdiensten valt.
- In algemene zin kan er gesproken worden over eHerkenningsmiddel of eHerkenningsmiddelen.
- Partijen die toegetreden zijn tot het afsprakenstelsel, mogen onder de noemer 'erkend aanbieder' het merk eHerkenning gebruiken ter ondersteuning van de branding van hun diensten/middelen. Het gebruik van het logo 'erkend aanbieder' is voorbehouden aan partijen die erkende aanbieder zijn binnen eHerkenning. Andere partijen mogen dit logo niet voeren, ook niet voor verwijzingen. Om eenduidige gebruikersinteractie te waarborgen, hanteren makelaars eenzelfde standaard keuzescherm van eHerkenning.
- De makelaars verstrekken de Handleiding Communicatie en de Toolkit (logo eHerkenning, betrouwbaarheidsvignetten en inlogbuttons) aan de dienstverleners en informeren en adviseren de dienstverleners bij de toepassing van de verplichte alsook optionele merkrichtlijnen.

Eisen met betrekking tot de communicatie-uitingen op dialoogvensters tijdens het herkenningsproces worden beschreven in het onderdeel Use cases.

Dienstverleners

De dienstverlener heeft zich te houden aan de richtlijnen voor naam- en merkgebruik eHerkenning. Zie Handleiding Communicatie Versie 4 [webrichtlijnen].pdf

Richtlijnen communicatie eHerkenning

Deelnemers

- Deelnemers MOETEN zichzelf positioneren als deelnemer binnen eHerkenning. Er dient altijd te worden gerefereerd aan het afsprakenstelsel en de deelnemer dient zich te positioneren als 'onderdeel' van dit stelsel.
- Deelnemers dienen zelf richting dienstverleners en gebruikers sales-activiteiten ontplooien.
- Indien deelnemers informatie over eHerkenning op hun website publiceren MOGEN zij daarvoor gebruik maken van de standaardteksten, kernboodschappen of elementen daarvan, zoals die in de communicatie toolkit beschikbaar zijn gesteld door de beheerorganisatie.
- Deelnemers MOGEN voor hun communicatie-uitingen over eHerkenning gebruik maken van de standaardteksten, kernboodschappen en andere elementen zoals die in de communicatie toolkit beschikbaar zijn gesteld door de beheerorganisatie.

Dienstverleners

- Dienstverleners MOGEN voor veel gestelde vragen (FAQ) over eHerkenning op hun site doorverwijzen naar de actuele veel gestelde vragen op e Herkenning.nl.
- Indien dienstverleners informatie over eHerkenning op hun website publiceren MOGEN zij daarvoor gebruik maken van de standaardteksten, kernboodschappen en andere elementen, zoals die in de communicatie toolkit beschikbaar zijn gesteld door de beheerorganisatie.
- Dienstverleners MOGEN voor hun communicatie-uitingen over eHerkenning gebruik maken van de standaardteksten, kernboodschappen en andere elementen zoals die in de communicatie toolkit beschikbaar zijn gesteld door de beheerorganisatie.

Huisstijlhandboek eHerkenning

Regels en Richtlijnen van de visuele identiteit eHerkenning.pdf

Huisstijlhandboek eIDAS

Op de volgende internetpagina is de handreiking communiceren over eIDAS beschikbaar. Hierin staat hoe Europese bedrijven en burgers kunnen inloggen met een Europees erkend inlogmiddel bij dienstverleners. Deze pagina bevat ook de communicatietoolkit met tekstmogelijkheden en beeldsuggesties (inlogknop). Zie https://magazines.logius.nl/eidas/2017/01/communiceren-met-europese-gebruikers.

Richtlijnen communicatie eIDAS

Deelnemers

- Deelnemers MOETEN zich onthouden van uitingen m.b.t. eIDAS tijdens het inlogproces.
- Indien deelnemers informatie over eIDAS en Europees inloggen op hun website publiceren MOGEN zij daarvoor gebruik maken van de beeldmerken, standaardteksten, kernboodschappen of elementen daarvan, zoals die in de communicatie toolkit beschikbaar zijn gesteld via de pagina Communicatietoolkit eIDAS.
- Deelnemers MOGEN voor hun communicatie-uitingen over eIDAS gebruik maken van de beeldmerken, standaardteksten, kernboodschappen en andere elementen zoals die in de communicatie toolkit beschikbaar zijn gesteld via de pagina Communicatietoolkit eIDAS.

Dienstverleners

- Dienstverleners MOETEN voor "eIDAS inkomend" een aparte inlogknop tonen, die verwijst naar de "eIDAS Berichtenservice" (EB). Uitsluitend deze EB toont het landenkeuze scherm. Dienstverleners MOGEN zelf GEEN landkeuze tonen.
    - Indien dezelfde service ook in het bedrijvendomein wordt aangeboden, wordt los hiervan de eHerkennings inlogknop getoond volgens de Richtlijnen communicatie eHerkenning.
    - De EU-vlag MOET als visual marker bij de inlogknop voor Europees inloggen gebruikt worden. De vlag zelf mag niet als inlogknop gebruikt worden. Meer informatie is te vinden in: Algemene richtlijnen stijlelementen eIDAS.pdf.
- Dienstverleners MOGEN voor veel gestelde vragen (FAQ) over eIDAS op hun site doorverwijzen naar de actuele veel gestelde vragen op Communicatietoolkit eIDAS.
- Indien dienstverleners informatie over eIDAS en Europees inloggen op hun website publiceren MOETEN zij daarvoor gebruik maken van de beeldmerken, standaardteksten, kernboodschappen en andere elementen, zoals die in de communicatie toolkit beschikbaar zijn gesteld via de pagina Communicatietoolkit eIDAS.
- Dienstverleners MOETEN voor hun communicatie-uitingen over eIDAS gebruik maken van de beeldmerken, standaardteksten, kernboodschappen en andere elementen zoals die in de communicatie toolkit beschikbaar zijn gesteld door de beheerorganisatie.

Techniek en functionaliteit

Hier vindt u de technische documenten van het Afsprakenstelsel Elektronische Toegangsdiensten: de koppelvlakspecificaties, de use cases en testen voor deelnemers. Deze documenten bevatten informatie over welke standaarden worden gehanteerd, de functionaliteit, de berichten en koppelvlakken die Elektronische Toegangsdiensten ondersteunt en de testen die worden uitgevoerd. Deze categorie bevat de volgende onderdelen:

- Use cases — Beschrijft de functionaliteit van Elektronische Toegangsdiensten in detail.
- Gebruikersinterface — Dit hoofdstuk beschrijft eisen die worden gesteld aan de gebruikersinterface met de gebruiker.
- Interface specifications
- Attribuutverstrekking — Een AD, MR of EB kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in de Attribuutcatalogus beschreven worden.
- SAML metadata — This chapter describes the metadata the participants must supply, how the Beheerorganisatie publishes the aggregated metadata, and how it is to be interpreted by the participants.
- Service catalog — This chapter describes the format and publication of the Dienstencatalogus (DC) (service catalog).
- Testing — This document describes the tests that (aspiring) participants should perform.

Bijgevoegd zijn de voorbeelden van de berichten in XML samen met de XSD bestanden die nodig zijn om de berichten te valideren:

Let op: onderstaand .zip bestand bevat verouderde XML-voorbeelden en XSD's. Het is bekend dat ze niet up-to-date zijn, en dat bijv. de XSD's voor de Diensten Catalogus ontbreken. Ze zijn uitsluitend bedoeld als voorbeelden.
Er wordt gewerkt aan een governance proces om in de toekomst correcte, complete, en up-to-date bestanden te kunnen leveren.



Use cases

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Beschrijft de functionaliteit van Elektronische Toegangsdiensten in detail.

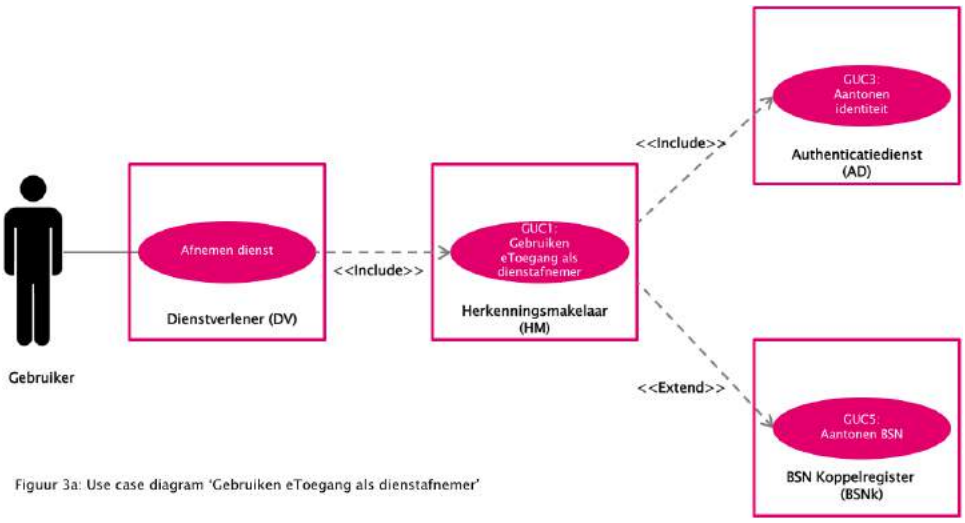
Leeswijzer

- Use cases voor Gebruik
  - GUC1 Gebruiken eToegang als dienstafnemer — In deze use case wordt de identiteit van de dienstafnemer vastgesteld. De Herkenningsmakelaar geeft hierover een verklaring af aan de dienstverlener. De gebruiker voert hiertoe de GUC3 Aantonen identiteit uit.
  - GUC2 Gebruiken eToegang als vertegenwoordiger — In deze use case, die een uitbreiding is op GUC1 Gebruiken eToegang als dienstafnemer, wordt de identiteit van de vertegenwoordigde dienstafnemer, de pseudo-identiteit van de gebruiker en de vertegenwoordigingsbevoegdheid van de gebruiker namens deze vertegenwoordigde dienstafnemer vastgesteld. De Herkenningsmakelaar geeft een nieuwe verklaring af aan de dienstverlener. Deze verklaring is samengesteld uit de verklaringen van de authenticatiedienst en het machtigingenregister. De gebruiker voert
  - GUC3 Aantonen identiteit — In deze use case kiest de Gebruiker een authenticatiedienst en identificeert zich bij die Authenticatiedienst (AD) door het gebruik van een authenticatiemiddel, dat hij eerder heeft verkregen (zie Use cases voor Administratie). De authenticatiedienst stelt het beoogde machtigingsregister vast en authenticeert de gebruiker voor de dienstverlener en het beoogde machtigingenregister en geeft hierover een verklaring af aan de herkenningsmakelaar. Deze use case wordt hieronder in een activity diagram
    - GUC3.3 Authenticatie gebruiker mislukt
    - GUC3.4 Selecteren beoogd machtigingenregister RFC2331
  - GUC4 Aantonen bevoegdheid — In deze use case raadpleegt de gebruiker de machtigingenregister. Het machtigingenregister stelt op basis van de eerder met GUC3 Aantonen identiteit verkregen identiteit van de gebruiker en een eerder geregistreerde bevoegdheid (zie Use cases voor Administratie), de identiteit van de vertegenwoordigde dienstafnemer en de pseudo-identiteit van de gebruiker vast en geeft hierover een verklaring af aan de Herkenningsmakelaar.
    - GUC4.1 Te bevragen machtigingenregister reeds bekend
    - GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet
    - GUC4.3 Portaalfunctie
    - GUC4.4 Verschillende bevoegdheden aanwezig
    - GUC4.5 Ketenmachtiging
      - Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet (stap 4.5c alternatief)
      - Vertegenwoordigde dienstafnemer onbekend (stap 4.5 alternatief)
    - Vaststellen bevoegdheid
  - Use case overschrijdende alternatieve scenario's
    - Alternatief scenario attribuutverstrekking
    - Attributen niet leverbaar of niet toegestaan
    - Attribuut komt niet voor in attribuutcatalogus
    - Dienst of dienstverlener komt niet voor in dienstencatalogus
    - Gebruiker annuleert
    - Soort dienstafnemer kan niet worden geleverd
  - Use cases Single Sign-On
    - Geen reactie bij lezen of schrijven selectie authenticatiedienst
    - Single Log-out
- Use cases voor Administratie
  - AUC1 Aansluiten dienst
  - AUC2 Verkrijgen authenticatiemiddel
  - AUC3 Registreren bevoegdheid
    - AUC3.1 Registreren bevoegdheid eenmanszaken
    - AUC3.2 Registreren status machtigingen eenmanszaken
  - AUC4 Registreren attribuut
  - AUC6 Activeren BSN
    - AUC6.1 Activeren BSN mbv VI — In het kader van sleutelmigratie van de IdentityProviderKeySet en van de SchemeWideKeySet (zie Proces migratie sleutelmateriaal voor polymorfe pseudonimisering) moet een MachtigingsRegister en MiddelenUitgever alle nog active (en dus eerder geactiveerde) BSN's opnieuw activeren bij BSNk-Activeren. Hiervoor stuurt de Machtigingenregister of MiddelenUitgever de BSN in de vorm van een Versleutelde Identiteit naar BSNk-Activeren. Die genereert en verstrekt een Polymorf Pseudoniem en Polymorfe Identi
  - AUC7 Proces verlenen toestemming dienstbemiddeling — Voor Diensten die via Dienstbemiddeling kunnen worden ontsloten, kan toestemming van de Dienstaanbieder (DA) benodigd zijn. Dit proces beschrijft de werkwijze voor het verlenen van toestemming door een Dienstaanbieder aan een Dienstbemiddelaar (DB) om een Dienst te mogen bemiddelen.
  - AUC8 Verkrijgen lijst Authenticatiediensten
  - AUC9 Verstrekken sleutelmateriaal Dienstverleners — Het BSNk beheert en verstrekt via een Herkenningsmakelaar cryptografisch sleutelmateriaal aan elke Dienstverlener (DV) die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het Versleutelde Identiteit of Versleutelde Pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.
  - AUC10 Transformeren
    - AUC10.2 MachtigingsRegister of Authenticatiedienst gebruikt BSNk transformatie functie
    - AUC10.3 HSM transformatie
  - AUC11

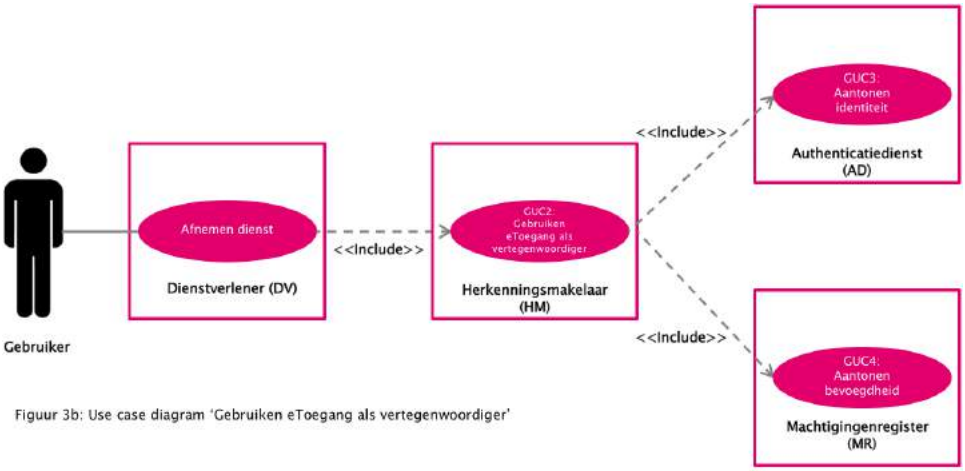
Use cases voor Gebruik

Het gebruik van Elektronische Toegangsdiensten is geen doel op zich. Elektronische Toegangsdiensten wordt gebruikt als bouwsteen in een business use case waarin de business actor Gebruiker een dienst afneemt van een business actor Dienstverlener (DV). Pas wanneer binnen deze dienst behoefte bestaat aan de Herkenning van de Dienstafnemer speelt Elektronische Toegangsdiensten een rol.

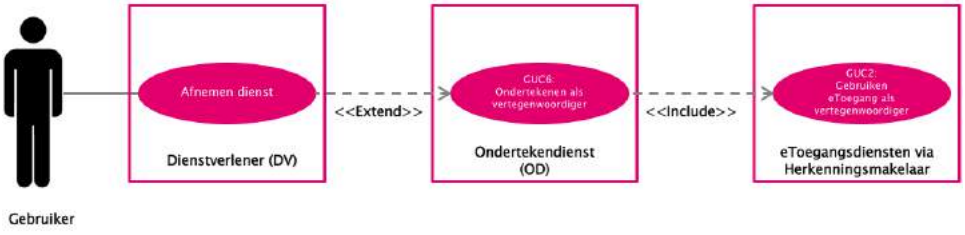
Use case diagrammen voor Gebruik



Figuur 3a: Use case diagram 'Gebruiken eToegang als dienstafnemer'



Figuur 3b: Use case diagram 'Gebruiken eToegang als vertegenwoordiger'



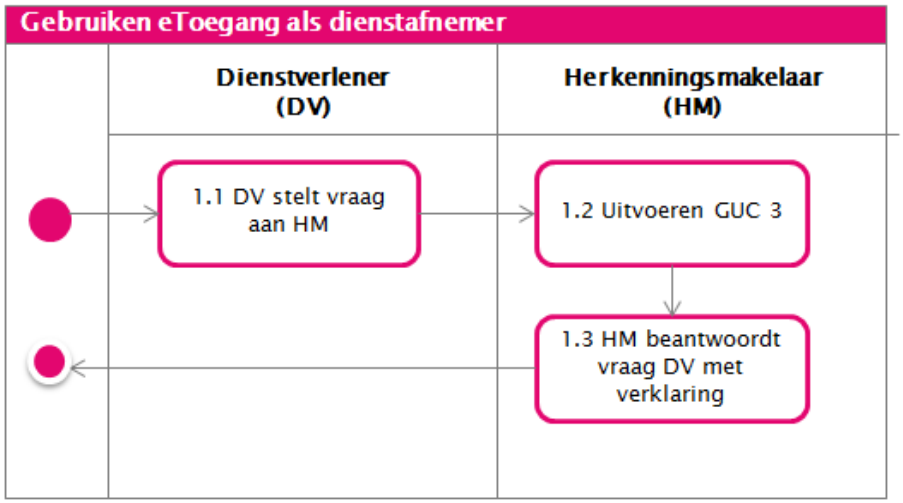
Figuur 3c: Use case diagram 'Gebruiken Ondertekendienst als vertegenwoordiger'

Het use case diagram "Gebruik", hierboven, beschrijft de hoofd use cases waarin de herkenning van de gebruiker of een dienstafnemer binnen Elektronische Toegangsdiensten wordt geïmplementeerd en de sub use cases die daar een rol bij spelen.

Per use case worden verschillende alternatieve scenario's beschreven. Hierin wordt aanvullende functionaliteit, functionaliteit als gevolg van een keuze van de gebruiker of functionaliteit als gevolg van een uitzondering (fout) beschreven. Daarnaast zijn er een aantal Use case overschrijdende alternatieve scenario's.

GUC1 Gebruiken eToegang als dienstafnemer

In deze use case wordt de identiteit van de dienstafnemer vastgesteld. De Herkenningsmakelaar geeft hierover een verklaring af aan de dienstverlener. De gebruiker voert hiertoe de GUC3 Aantonen identiteit uit.De use case wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC1 worden hier in meer detail beschreven. Voor de acties in use case GUC3 wordt verwezen naar GUC3 Aantonen identiteit.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstafnemer gebruikt voor zichzelf een dienst bij een dienstverlener die authenticatie van de dienstafnemer vereist. De dienstafnemer is daarmee tevens gebruiker.
1.1	Dienstverlener stelt vraag aan Herkenningsmakelaar	De dienstverlener stuurt de gebruiker door naar de Herkenningsmakelaar en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst. **Alternatieve scenario's:** • Vóór stap 1.1 MAG de Dienstverlener de gebruiker een keuzescherm bieden voor het kiezen van een eHerkenning Authenticatiedienst. Deze lijst met relevante Authenticatiediensten wordt opgehaald bij de Herkenningsmakelaar en bevat eIDAS NIET als optie. Met de vraag wordt dan ook het identificerende kenmerk van de door de gebruiker gekozen Authenticatiedienst meegegeven in stap 1.1. De gebruiker kan ervoor kiezen deze keuze te bewaren bij de Dienstverlener in geval van succesvolle authenticatie. • In het geval dat de dienst ook toegankelijk is na authenticatie met eIDAS-erkende buitenlandse authenticatie middelen, MOET de Dienstverlener de gebruiker een keuzescherm bieden voor het kiezen van authenticatie via eIDAS of eHerkenning (vóór stap 1.1). Op dit scherm kiest de dienstafnemer tussen authenticeren via eIDAS of via eHerkenning. In het geval dat authenticatie via eIDAS wordt gekozen, wordt het identificerend kenmerk van de eIDAS Berichtenservice (EB) meegegeven in stap 1.1. De gebruiker kan er NIET voor kiezen om deze keuze te bewaren bij de Dienstverlener.
1.2	Uitvoeren GUC3 Aantonen identiteit	Het resultaat is dat de Herkenningsmakelaar een verklaring over de authenticatie van de gebruiker ontvangt met een Pseudo niem. **Alternatieve scenario's:** Wanneer in deze stap geconstateerd wordt dat er sprake is van vertegenwoordiging, wordt de use case vervolgd met stap 2.3 in GUC2 Gebruiken eToegang als vertegenwoordiger.
1.3	Herkenningsmakelaar beantwoordt vraag van dienstverlener met verklaring	De Herkenningsmakelaar beantwoordt de vraag van de dienstverlener. Dit antwoord bevat een verklaring die de Herkenningsmakelaar opstelt op basis van de van de authenticatiedienst ontvangen verklaring over de authenticatie van de gebruiker met daarin het betrouwbaarheidsniveau van de verklaring en Identificerende kenmerken.
	Finale staat	De dienstafnemer is geauthenticeerd en de dienstverlener heeft daar de benodigde informatie over ontvangen. De dienstafname kan worden vervolgd. Informatie over de gebruiker kan benut worden voor personalisatie, logging e.d.

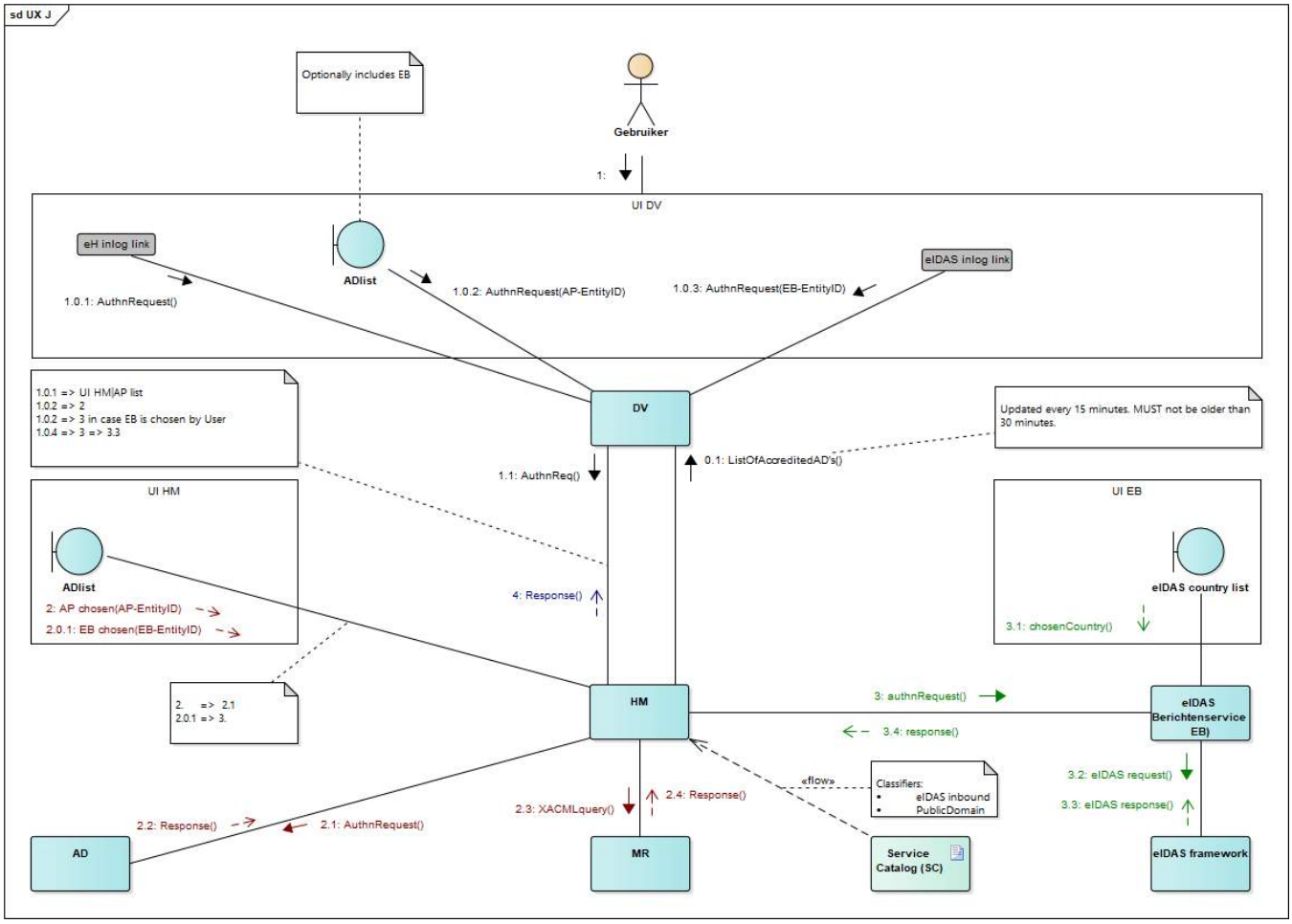
ad actie 1.1: De vraag is als AuthnRequest in detail beschreven in Interface specifications DV-HM.

ad actie 1.3: Het antwoord is als Response in detail beschreven in Interface specifications DV-HM.

In het communication diagram hieronder is aangegeven welke varianten van AD-keuzen een Dienstverlener kan aanbieden en hoe de verwerkings-flow dan wordt:

- eH Inlog link: Dit is de link die de 'normale' flow waarbij de DV geen AD keuze aanbiedt start.
- ADList: Dit is het keuzescherm met eHerkennings authenticatie diensten dat een DV mag aanbieden. Deze lijst MAG de eIDAS-berichtenservice NIET bevatten.
- eIDAS Inlog link: Dit is de link die waarmee de gebruiker aangeeft met een buitenlands middel te willen inloggen. De flow wordt naar de eIDAS-berichtenservice doorgezet. Zie Richtlijnen communicatie eIDAS

> *Note: de genoemde "inlog links" in het lijstje hierboven, vind je o.a. op pagina 6 van het bijgevoegde document ("Klantreis eIDAS–adviesrapport 27082019.pdf").*

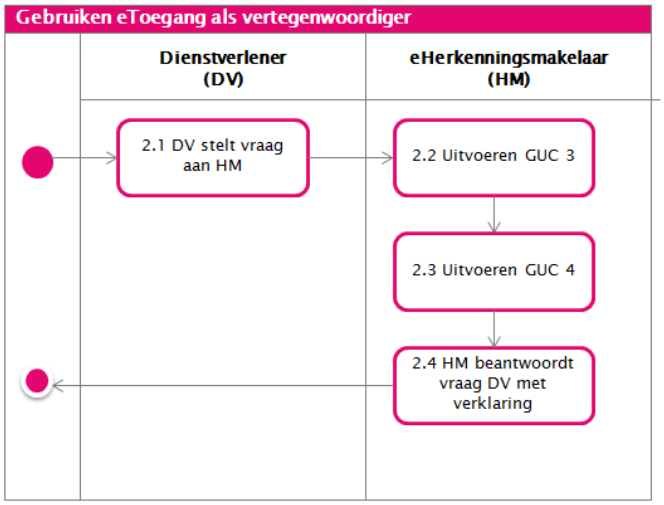


In de figuur is aangegeven volgens welke gebruikersinteractie bepaald wordt welke AD of EB gebruikt gaat worden

GUC2 Gebruiken eToegang als vertegenwoordiger

In deze use case, die een uitbreiding is op GUC1 Gebruiken eToegang als dienstafnemer, wordt de identiteit van de vertegenwoordigde dienstafnemer, de pseudo-identiteit van de gebruiker en de vertegenwoordigingsbevoegdheid van de gebruiker namens deze vertegenwoordigde dienstafnemer vastgesteld. De Herkenningsmakelaar geeft een nieuwe verklaring af aan de dienstverlener. Deze verklaring is samengesteld uit de verklaringen van de authenticatiedienst en het machtigingenregister. De gebruiker voert hiertoe de use cases GUC3 Aantonen identiteit en GUC4 Aantonen bevoegdheid uit.

Deze use case is een uitbreiding op GUC1 Gebruiken eToegang als dienstafnemer en wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC2 worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstafnemer laat zich voor het afnemen van een dienst vertegenwoordigen bij een dienstverlener die authenticatie van de dienstafnemer vereist. De gebruiker handelt als vertegenwoordiger.
2.1	Dienstverlener stelt vraag aan Herkenningsmakelaar	Zie stap 1.1 GUC1 Gebruiken eToegang als dienstafnemer
2.2	Uitvoeren GUC3 Aantonen identiteit	Het resultaat is dat de Herkenningsmakelaar een verklaring over de authenticatie van de gebruiker ontvangt met een de gevraagde identificerende kenmerken van de gebruiker.
2.3	Uitvoeren GUC4 Aantonen bevoegdheid	Het resultaat is dat de Herkenningsmakelaar een verklaring over de bevoegdheid van de gebruiker ontvangt. Indien het een ketenmachtiging betreft verifieert de Herkenningsmakelaar de hele keten alvorens deze te gebruiken in de volgende stap. **Alternatief scenario:** In het geval dat een gebruiker zich heeft geauthenticeerd met een eIDAS-authenticatiemiddel uit een andere eIDAS-lidstaat, ontvangt de Herkenningsmakelaar in het antwoord van de eIDAS-berichtenservice (EB) mogelijk ook een autorisatieverklaring en kan stap 2.3 worden overgeslagen. ⓘ Let op: dit scenario is uitsluitend van toepassing op eIDAS Inkomend, NIET op eIDAS Uitgaand.
2.4	Herkenningsmakelaar beantwoordt vraag van dienstverlener met verklaring	De Herkenningsmakelaar beantwoordt de vraag van de dienstverlener. Dit antwoord bevat een verklaring die de Herkenningsmakelaar opstelt (op basis van én met inbegrip van de authenticatiedienst en van het machtigingenregister/de machtigingenregisters ontvangen verklaringen over de authenticatie en de bevoegdheid van de gebruiker) met daarin het betrouwbaarheidsniveau van de verklaring, de identificerende kenmerken van de vertegenwoordigde dienstafnemer, de identificerende kenmerken van de gebruiker en (indien relevant) informatie over de ketenmachtiging. Het betrouwbaarheidsniveau is gelijk aan het laagste betrouwbaarheidsniveau van de betrouwbaarheidsniveaus van de verklaringen van de authenticatiedienst en het machtigingenregister/de machtigingenregisters.
	Finale staat	De dienstafnemer is geauthenticeerd en de dienstverlener heeft daar de benodigde informatie over ontvangen. De dienstafname kan worden vervolgd ten behoeve van de vertegenwoordigde dienstafnemer. Informatie over de gebruiker en zijn bevoegdheid kan benut worden voor personalisatie, logging e.d.

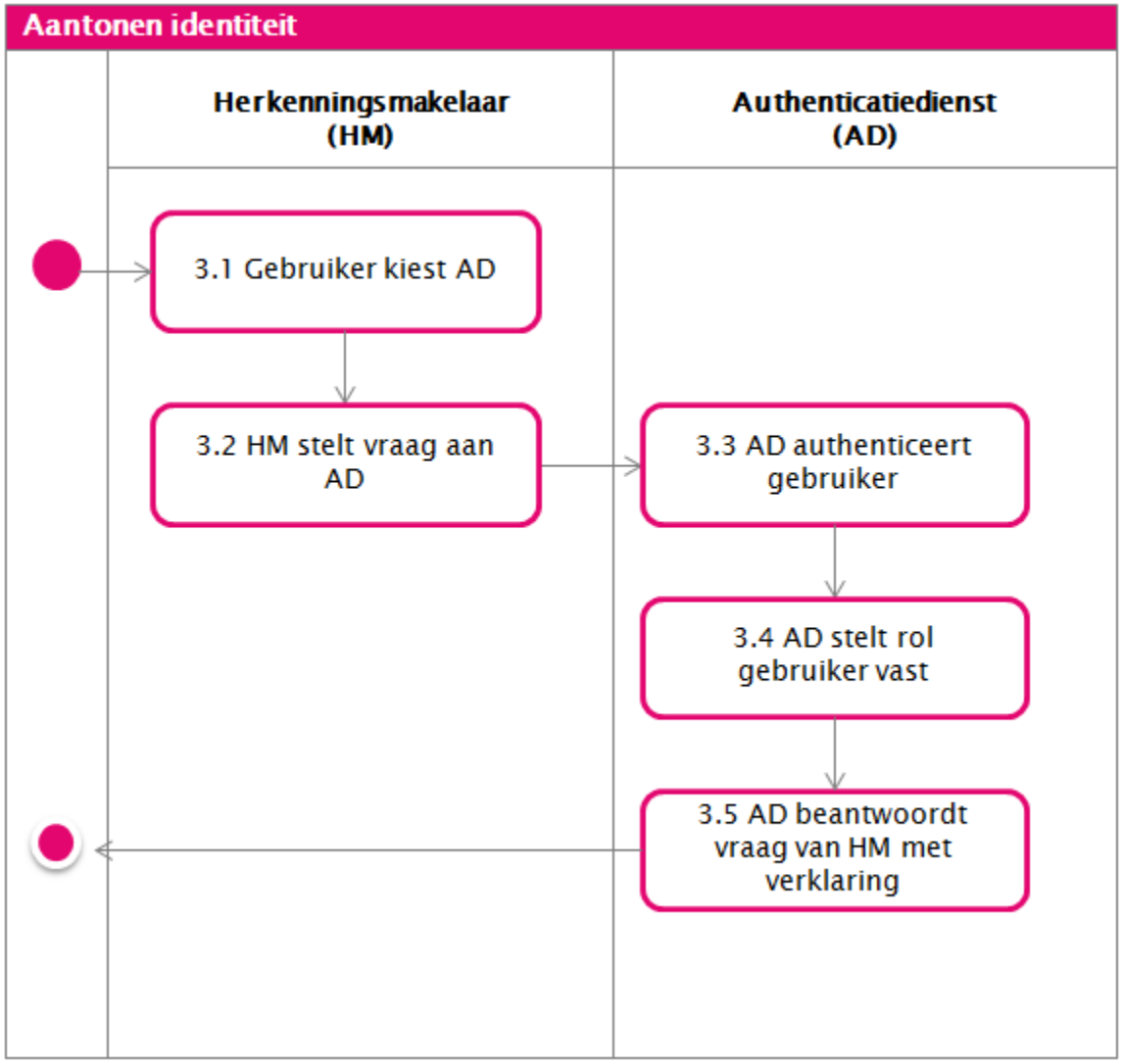
ad actie 2.4: Het antwoord is als Response in detail beschreven in Interface specifications DV-HM.

Alternatieve scenario's

Voor deze use case bestaan geen zelfstandige alternatieve scenario's.

GUC3 Aantonen identiteit

In deze use case kiest de Gebruiker een authenticatiedienst en identificeert zich bij die Authenticatiedienst (AD) door het gebruik van een authenticatiemiddel, dat hij eerder heeft verkregen (zie Use cases voor Administratie). De authenticatiedienst stelt het beoogde machtigingsregister vast en authenticeert de gebruiker voor de dienstverlener en het beoogde machtigingenregister en geeft hierover een verklaring af aan de herkenningsmakelaar. Deze use case wordt hieronder in een activity diagram weergegeven.Deze use case wordt hieronder in een activity diagram weergegeven.



De verschillende acties worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstverlener heeft een vraag gesteld aan de Herkenningsmakelaar.

3.1	De gebruiker kiest authenticatiedienst	Op de website van de Herkenningsmakelaar kiest de gebruiker een authenticatiedienst uit de lijst van authenticatiediensten. De gebruiker kan ervoor kiezen deze keuze te bewaren. Zie Dialoogbeschrijving Herkenningsmakelaars. **Alternatieve scenario's:** • Als bij stap 1.1 de gebruiker reeds een keuze voor een Authenticatiedienst heeft gemaakt bij de Dienstverlener, MOET stap 3.1 worden overgeslagen. De Herkenningsmakelaar dient de verkozen Authenticatiedienst over te nemen die in de herkenningsvraag is meegegeven. • Wanneer een Gebruiker in het keuzescherm bij de Herkenningsmakelaar kiest voor een eIDAS-authenticatiedienst en zich dus wenst te authentiseren bij een Authenticatiedienst (AD) uit een andere eIDAS-lidstaat, wordt de Gebruiker een keuzescherm gepresenteerd door de eIDAS-berichtenservice (EB) waarin de Gebruiker een landenkeuze moet maken (als deze keuze niet eerder bij de Herkenningsmakelaar of Dienstverlener (DV) is geregistreerd). In het geval de DV als reeds gekozen Authenticatiedienst de eIDAS-berichtenservice (EB) heeft meegegeven, geldt soortgelijk als bij de vorige bullet. De HM dient de EB als Authenticatiedienst over te nemen. De keuze voor de gewenste EU-lidstaat waar de gebruiker zich wenst te authenticeren, wordt verder gefaciliteerd door de EB. Na het maken van een landenkeuze, wordt de Gebruiker doorgestuurd naar de eIDAS-oplossing van de betreffende eIDAS-lidstaat. Wanneer de gebruiker is geauthenticeerd, stuurt de eIDAS-berichtenservice in zijn rol als Authenticatiedienst een antwoord naar de Herkenningsmakelaar, waarmee het proces vervolgt vanaf stap 3.5. De functionaliteit van de eIDAS-berichtenservice, anders dan het koppelvlak met een Herkenningsmakelaar, wordt niet in het Afsprakenstelsel gespecificeerd en hier uitsluitend vermeld voor volledigheid.
3.2	Herkenningsmakelaar stelt vraag aan authenticatiedienst	De Herkenningsmakelaar stuurt de gebruiker door naar de door de gebruiker geselecteerde authenticatiedienst en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst.
3.3	Authenticatiedienst authenticeert gebruiker	De gebruiker identificeert zich bij de authenticatiedienst door het gebruik van zijn authenticatiemiddel, waarop de authenticatiedienst de gebruiker authenticeert. Zie Verantwoordelijkheden Authenticatiedienst. De gebruiker kan bevraagd worden over de te leveren attributen, bijvoorbeeld voor het geven van toestemming of het verstrekken van een attribuut dat nog niet eerder was vastgelegd. Dit heeft gevolgen voor de gebruikerservaring en de doorlooptijd van het authenticatieverzoek. Partijen dienen hier rekening mee te houden. **Alternatief scenario:** GUC3.3 Authenticatie gebruiker mislukt
3.4	Authenticatiedienst stelt rol gebruiker vast	De authenticatiedienst stelt vast in welke rol de gebruiker acteert. Mogelijke rollen zijn: • Burger/consument • Vertegenwoordiger De authenticatiedienst bepaalt dit op basis van de Dienstencatalogus (DC), de eigen (contract-) administratie, of door de gebruiker te vragen een keuze te maken. Hierbij borgt de authenticatiedienst dat de gebruiker uitsluitend kan acteren als burger/consument als dit door de dienstverlener voor deze dienst is toegestaan en zodanig in de dienstencatalogus is vastgelegd. **Alternatief scenario:** GUC3.3 Authenticatie gebruiker mislukt authenticatie Voor het vervolg van deze use case wordt ervan uitgegaan dat de gebruiker mag acteren en acteert als burger/consument. De andere rollen worden in alternatieve scenario's uitgewerkt.
	Authenticatiedienst stelt het machtigingsregister van de gebruiker vast	Indien de de gebruiker de rol van Vertegenwoordiger heeft stelt de authenticatiedienst vast wat het beoogde 'standaard' machtigingsregister is. Dit 'standaard' machtigingsregister is vastgelegd bij de aanschaf van het authenticatiemiddel (door de werkgever). Indien er geen 'standaard' machtigingsregister is geselecteerd start Alternatief scenario: GUC3.4 Selecteren beoogd machtigingenregister RFC2331.
3.5	Authenticatiedienst vraagt gebruiker om goedkeuring voor het gebruik van BSN gegevens	Indien een dienstverlener een uitvraag doet om BSN gegevens (middels de ASTA urn:etoegang:1.12:EntityConcernedID:BSN) MOET de AD vragen of de gebruiker zijn BSN wil delen met de dienstverlener. Indien de gebruiker geen akkoord geeft, MOET de AD de ASTA urn:etoegang:1.12:EntityConcernedID:BSN beschouwen als niet leverbaar en MOET hij proberen door te gaan met eventueel gedefinieerde ASTA (sets) met een lagere prioriteit. Als er niet voldaan kan worden aan de bij de dienst gedefinieerde ASTA-set, dan stopt de flow en reageert de AD met een Responder Error. Zie Error handling.

3.6	Authenticatiedienst beantwoordt vraag van Herkenningsmakelaar met verklaring	De authenticatiedienst beantwoordt de vraag van de Herkenningsmakelaar. Dit antwoord bevat een verklaring over de authenticatie met daarin het betrouwbaarheidsniveau van de verklaring en de gevraagde identificerende kenmerken van de gebruiker (versleuteld voor de beoogde ontvanger(s)). Indien de gebruiker in stap 3.1 heeft aangegeven zijn keuze voor de authenticatiedienst te willen bewaren dan slaat de Herkenningsmakelaar deze nu op, zodanig dat deze instelling ook voor andere Herkenningsmakelaars toegankelijk is.
	Finale staat	De gebruiker is geauthenticeerd en de Herkenningsmakelaar heeft daar de benodigde informatie over ontvangen.

ad actie 3.2: De vraag is als AuthnRequest in detail beschreven in Interface specifications HM-AD
ad actie 3.5: Het antwoord is als Response in detail beschreven in Interface specifications HM-AD

- GUC3.3 Authenticatie gebruiker mislukt
- GUC3.4 Selecteren beoogd machtigingenregister RFC2331

GUC3.3 Authenticatie gebruiker mislukt

In stap 3.3 kan de authenticatie van de Gebruiker om verschillende redenen mislukken: het authenticatiemiddel is niet van het minimaal door de dienstverlener gewenste betrouwbaarheidsniveau, het authenticatiemiddel is verlopen of ingetrokken, of de gebruiker gebruikt het authenticatiemiddel foutief (verkeerd wachtwoord, verkeerde kaart, et cetera). Deze situaties worden allemaal op dezelfde manier afgehandeld.

- De authenticatiedienst stelt de gebruiker op het scherm op de hoogte van de reden van het mislukken van de authenticatie.
- De authenticatiedienst geeft aan de gebruiker op het scherm een suggestie voor de vervolghandeling die de persoon naar aanleiding van de fout zou kunnen uitvoeren.
- De authenticatiedienst MAG de gebruiker aanbieden het opnieuw te proberen.
- De authenticatiedienst MOET de gebruiker de mogelijkheid bieden te annuleren (zie Gebruiker annuleert).

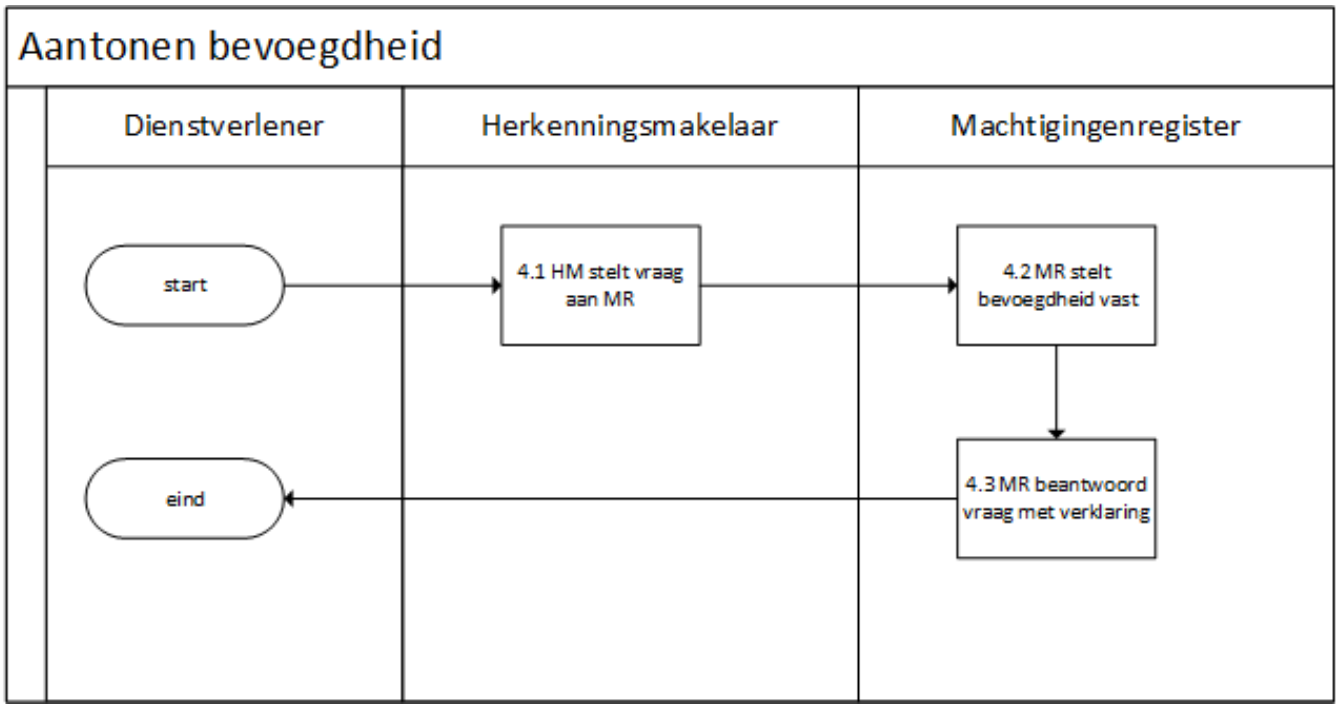
GUC3.4 Selecteren beoogd machtigingenregister RFC2331

Nr.	Actie	Omschrijving
3.4.1	Gebruiker kiest machtigingenregister	De authenticatiedienst laat de gebruiker uit de lijst van machtigingenregisters het beoogde machtigingenregister kiezen. De gebruiker kan aangeven dat dit het 'standaard' machtigingenregister is.

GUC4 Aantonen bevoegdheid

eIn deze use case raadpleegt de gebruiker de machtigingenregister. Het machtigingenregister stelt op basis van de eerder met GUC3 Aantonen identiteit verkregen identiteit van de gebruiker en een eerder geregistreerde bevoegdheid (zie Use cases voor Administratie), de identiteit van de vertegenwoordigde dienstafnemer en de pseudo-identiteit van de gebruiker vast en geeft hierover een verklaring af aan de Herkenningsmakelaar.

De use case wordt hieronder in een activity diagram weergegeven.



De verschillende acties voor use case GUC4 worden hier in meer detail beschreven.

Nr.	Actie	Omschrijving
	Initiële staat	De dienstverlener[1] heeft een vraag gesteld aan de Herkenningsmakelaar. De gebruiker is geïdentificeerd door een authenticatiedienst en de gebruiker heeft bij deze authenticatiedienst het beoogde machtigingsregister geselecteert[2]. Herkenningsmakelaar heeft daarover een verklaring met een identificerend kenmerk ten behoeve van het geselecteerde machtigingsregister ontvangen.
4.2	Herkenningsmakelaar stelt vraag3 aan machtigingenregister	De Herkenningsmakelaar stuurt de gebruiker door naar het door de gebruiker geselecteerde machtigingenregister en stelt daarbij een vraag. Deze vraag bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst, het door de dienstverlener gewenste betrouwbaarheidsniveau en het identificerend kenmerk van de gebruiker. **Alternatieve scenario's:** • GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet • GUC4.3 Portaalfunctie • GUC4.4 Verschillende bevoegdheden aanwezig • GUC4.5 Ketenmachtiging
4.3	Machtigingenregister stelt bevoegdheid gebruiker vast	Het machtigingenregister bepaalt op basis van identificerend kenmerk voor welke dienstafnemer de gebruiker bevoegd is. Zie Verantwoordelijkheden Machtigingenregister. De wijze waarop de MR bepaald welke bevoegdheid van toepassing is wordt beschreven op de pagina Vaststellen bevoegdheid. De gebruiker kan bevraagd worden over de te leveren attributen, bijvoorbeeld voor het geven van toestemming of het verstrekken van een attribuut dat nog niet eerder was vastgelegd. Dit heeft gevolgen voor de gebruikerservaring en de doorlooptijd van het authenticatieverzoek. Partijen dienen hier rekening mee te houden.
4.4	Machtigingenregister beantwoordt[3] vraag van Herkenningsmakelaar met verklaring	Het machtigingenregister beantwoordt de vraag van de Herkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de gebruiker met daarin het betrouwbaarheidsniveau van de verklaring, het identificerend kenmerk van de vertegenwoordigde dienstafnemer desgevraagd het identificerend kenmerk van de gebruiker.

	Finale staat	De bevoegdheid van de gebruiker namens de vertegenwoordigde dienstafnemer is aangetoond en de Herkenningsmakelaar heeft daar de benodigde informatie over ontvangen.

Voetnoten

1. De vraag is als XACMLAuthzDecisionQuery in detail beschreven in Interface specifications HM-MR.
2. De keuze lijst met machtigingsregisters komt nauwelijks voor omdat de gebruiker meestal slechts een machtiging heeft bij dezelfde ETD-Leverancier.
3. Het antwoord is als XACMLAuthzDecision Response in detail beschreven in Interface specifications HM-MR.

GUC4.1 Te bevragen machtigingenregister reeds bekend

Indien al bekend is welk machtigingenregister geraadpleegd moet worden biedt de Herkenningsmakelaar de gebruiker geen lijst van machtigingenregisters aan. Met het bekende machtigingenregister wordt stap 4.2 vervolgd. De opgave van het machtigingenregister kan afkomstig zijn uit de verklaring van de authenticatiedienst (GUC3) of uit een verklaring van een ander machtigingenregister (zie GUC4.5 Ketenmachtiging).

GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet

Er kunnen verschillende redenen zijn waarom een machtigingenregister geen bevoegdheid vindt die aan de vraag voldoet. Voorbeelden hiervan zijn: de geregistreerde bevoegdheid is niet van het minimaal door de dienstverlener vereiste betrouwbaarheidsniveau, de machtiging is verlopen of ingetrokken of de dienst of dienstverlener komt niet (langer) voor in de dienstencatalogus. Deze situaties worden allemaal op dezelfde manier afgehandeld.

- Het machtigingenregister stelt de gebruiker op het scherm op de hoogte van de reden van het mislukken van de raadpleging.
- Het machtigingenregister geeft aan de gebruiker op het scherm een suggestie voor de vervolghandeling die de persoon naar aanleiding van de fout zou kunnen uitvoeren.

De gebruiker kan annuleren (zie Gebruiker annuleert).

GUC4.3 Portaalfunctie

Wanneer een dienstverlener een authenticatie van een uitvoerende dienstafnemer voor dienst 0 vraagt, wijzigen 4.3 en 4.4. Na deze stap wordt GUC4 Aantonen bevoegdheid gewoon met "Finale staat" vervolgd.

Nr.	Actie	Omschrijving
4.3	Machtigingenregister stelt bevoegdheid gebruiker vast	Het machtigingenregister bepaalt op basis van het identificerend kenmerk voor welke uitvoerende dienstafnemer de gebruiker voor tenminste één dienst een bevoegdheid is geregistreerd. Het machtigingenregister volgt de stappen zoals vastgelegd in Vaststellen bevoegdheid. Het machtigingenregister toont alle aanwezige machtigingen voor de uitvoerende dienstafnemer welke voldoen aan het vereiste betrouwbaarheidsniveau. Het machtigingenregister bewaakt hierbij dat het registratieproces waarmee de bevoegdheid is vastgelegd minimaal van het door de dienstverlener vereiste betrouwbaarheidsniveau is. Indien Dienstbemiddeling van toepassing is, mag er slechts 1 dienst worden gekozen.
4.4	Machtigingenregister beantwoordt vraag van eHerkenningsmakelaar met verklaring	Het machtigingenregister beantwoordt de vraag van de Herkenningsmakelaar. Dit antwoord bevat een verklaring over de gekozen bevoegdheden van de gebruiker met daarin het betrouwbaarheidsniveau van de verklaring, het identificerend kenmerk van de vertegenwoordigde dienstafnemer.

GUC4.4 Verschillende bevoegdheden aanwezig

Het is mogelijk dat voor het in de vraag gespecificeerde interne pseudoniem (van de gebruiker) meerdere geldige machtigingen voor dezelfde dienst gevonden worden. Denk hierbij aan situaties bij intermediairs, adviseurs met verschillende opdrachten, eigenaars van verschillende bedrijven, etc. Het is ook mogelijk dat een gebruiker meer (maar niet alle) vestigingen van een dienstafnemer mag vertegenwoordigen.

Het Machtigingenregister vraagt een bevoegdheid te kiezen



I.p.v. stap 4.3 zijn dan de volgende stappen nodig. Na deze stappen wordt GUC4 gewoon met stap 4.4 vervolgd.

Nr.	Actie	Omschrijving
4.3	Machtigingenregister toont mogelijke bevoegdheden	Het machtigingenregister bepaalt op basis van het identficerend kenmerk van de uitvoerende natuurlijke persoon welke mogelijke bevoegdheden bestaan en toont de bijbehorende dienstafnemers in een lijst.
4.3a	Gebruiker selecteert bevoegdheid	De gebruiker selecteert de bevoegdheid op basis waarvan hij ditmaal toegang vraagt uit de getoonde lijst.
4.3b	Machtigingenregister stelt bevoegdheid gebruiker vast	Het Machtigingenregister stelt de bevoegdheid van de gebruiker vast en verklaart hierover.

GUC4.5 Ketenmachtiging

In verschillende situaties moet het machtigingenregister concluderen dat de gevonden bevoegdheid nog niet het volledige antwoord op de gevraagde bevoegdheid compleet maakt. Dit zijn de volgende situaties:

- Vertegenwoordigde dienstafnemer is in de vraag gespecificeerd en is ongelijk aan de partij die als vertegenwoordigde in de gevonden bevoegdheid voorkomt.
- Bij de gevonden bevoegdheid is een beperking vastgelegd die bepaalt dat de bevoegdheid alleen "voor derden" geldt en niet voor de in de bevoegdheid voorkomende vertegenwoordigde partij zelf. Deze derde moet dan als informatie bekend zijn in het betreffende machtigingenregister.
- Het machtigingenregister toont na bepalen van één geldige bevoegdheid (in stap 4.2 of 4.2a) een bevestigingscherm dat de optie bevat om in plaats van het bevestigen van de bevoegdheid een vertegenwoordigde dienstafnemer op te geven namens wie ditmaal toegang gevraagd wordt.
- De flow voor machtigingen wordt gevolgd die is vastgelegd op pagina Vaststellen bevoegdheid.

Vervolgens is het verdere verloop als volgt:

Nr.	Actie	Omschrijving
4.4	Machtigingenregister beantwoordt vraag van Herkenningsmakelaar met verklaring en specificeert volgende machtigingenregister.	Het machtigingenregister beantwoordt de vraag van de Herkenningsmakelaar en stuurt de gebruiker terug naar de Herkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de gebruiker met daarin het betrouwbaarheidsniveau van de verklaring en desgevraagd het identificerend kenmerk van de gebruiker. Daarnaast wordt een bevoegdheidsketen meegegeven, wordt de aanduiding van het volgende machtigingenregister meegegeven. De bevoegdheidsketen bevat de specificatie van de vertegenwoordigde dienstafnemer (hetzij uit de vraag, hetzij zoals in dit machtigingenregister vastgelegd). De verklaring specificeert alleen dat het machtigingenregister voor de gevraagde schakel het bestaan van een machtiging heeft geverifieerd. Voor de rest van de bevoegdheidsketen wordt alleen informatief aangegeven hoe deze eruit ziet en waar deze geverifieerd kan worden.
4.4a	Herkenningsmakelaar ontvangt incomplete keten.	De Herkenningsmakelaar voert controles uit op de ontvangen verklaring en constateert dat de keten incompleet is.
4.4b	Herkenningsmakelaar bevraagt volgend machtigingenregister.	De Herkenningsmakelaar bevraagt het in voorgaande verklaring aangeduide machtigingenregister. De vraag daarbij bevat het identificerend kenmerk van zowel de betreffende dienstverlener als de betreffende dienst, het door de dienstverlener gewenste betrouwbaarheidsniveau en deze MOETEN identiek zijn aan hetgeen in de vraag bij stap 4.2 gespecificeerd was. Daarnaast bevat de vraag het identificerende kenmerk van de intermediaire partij waarvoor aan het machtigingenregister een bevoegdheid gevraagd wordt en de bevoegdheidsketen van de gebruiker tot aan deze intermediaire partij. De vraag bevat tevens alle andere gegevens die van het voorgaande machtigingenregister ontvangen zijn en die in de initiële vraag aan de Herkenningsmakelaar gespecificeerd zijn.
4.4c	Machtigingenregister bepaalt machtiging aan intermediaire partij.	Het machtigingenregister bepaalt op basis van het identificerende kenmerk van de intermediaire partij of er inderdaad een bevoegdheid voor betreffende dienst is geregistreerd en controleert of deze het minimaal vereiste betrouwbaarheidsniveau heeft.
4.4d	Machtigingenregister verstrekt gevraagde verklaring aan Herkenningsmakelaar.	Het machtigingenregister levert een verklaring met het gevraagde antwoord aan de Herkenningsmakelaar. Dit antwoord bevat een verklaring over de bevoegdheid van de vertegenwoordigde dienstafnemer aan de in de vraag gespecificeerde intermediaire partij met daarin het betrouwbaarheidsniveau van de verklaring. Daarnaast wordt een bevoegdheidsketen meegegeven die volledig is van vertegenwoordigde dienstafnemer tot aan de intermediaire partij namens w de gebruiker bevoegd is.
4.4e	Herkenningsmakelaar concludeert dat keten volledig is.	De Herkenningsmakelaar voert controles uit op de ontvangen verklaring en constateert dat de keten compleet is (identiek aan stap 4.4a met ander resultaat).
	Finale staat	De finale staat conform use case GUC4 is bereikt met dien verstande dat daarbij nu ook informatie over een complete ketenmachtiging bij de Herkenningsmakelaar bekend is.

Varianten bij Ketenmachtiging

Als onderdeel van de alternatieve flow voor ketenmachtiging kunnen de volgende varianten voorkomen (die hier dus als alternatieve flow binnen de alternatieve flow van GUC4.5 Ketenmachtiging beschreven worden).

Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet (stap 4.5c alternatief)

Indien geen geldige bevoegdheid gevonden wordt, of indien meerdere bevoegdheden gevonden worden zonder dat op basis van gespecificeerde vertegenwoordigde dienstafnemer bepaald kan worden welke bevoegdheid gevraagd wordt (m.a.w. er is geen eenduidig antwoord te geven) dan wordt de bevraging afgebroken met foutmelding aan de Herkenningsmakelaar en deze geeft een foutmelding aan de gebruiker conform alternatief scenario GUC4.2 Machtigingenregister vindt geen bevoegdheid die aan de vraag voldoet, met dien verstande dat de Herkenningsmakelaar de foutmelding aan de gebruiker moet tonen en de afhandeling moet uitvoeren.

Vertegenwoordigde dienstafnemer onbekend (stap 4.5 alternatief)

Indien de vertegenwoordigde dienstafnemer niet is gespecificeerd in de vraag en niet aanvullend bij de gevonden bevoegdheid is opgenomen wordt de gebuiker gevraagd deze te specificeren. Deze vraag kan gecombineerd worden met de selectie voor het geval dat er verschillende bevoegdheden aanwezig zijn.

Dat wil zeggen dat de gebuiker op dit punt gevraagd wordt alle informatie aan te vullen die nodig is om de rest van de keten zonder gebruikersinteractie door Herkenningsmakelaar middels bevraging van machtigingenregisters te laten verifiëren. De happy flow blijft de situatie waarbij al deze informatie reeds bij de bevoegdheid is vastgelegd tijdens de registratie. Belangrijk is dat alle aanvullende informatie als attribuut wordt doorgegeven en dus geen verklaring over geldigheid inhoudt, de verdere schakels van de keten MOETEN daadwerkelijk geverifieerd worden in het machtigingenregister waar ze geregistreerd zijn.

Vaststellen bevoegdheid

In the paragraphs below is an example implementation of all the functionality which a MR must support, this is not the required implementation, other implementations are allowed as long as they deliver the same result.

Process to find applicable authorisation

1: Check LOA levels

1A: If the level of assurance is included in XACMLAuthzDecisionQuery request Resource LevelOfAssurance

- The LOA of the authentication means in the AD assertion MUST BE equal or greater than the LOA which is requested included in the XACMLAuthzDecisionQuery request Resource LevelOfAssurance
- The LOA which is included in the DC MUST BE equal or greater than the LOA which is requested included in the XACMLAuthzDecisionQuery request Resource LevelOfAssurance.
- The LOA of the Machtiging (machtigen) MUST be equal or greater than the LOA included in XACMLAuthzDecisionQuery request Resource LevelOfAssurance.

1B: If the level of assurance is NOT included in XACMLAuthzDecisionQuery request Resource Level of assurance.

- Continue the process with the LOA which is specified in the Service Catalog.

2: Check ServiceUUID

2A: If the requested service is NOT a portal service:

- The ServiceUUID at XACMLAuthzDecisionQuery request Resource ServiceUUID MUST match the serviceUUID (of the ServiceDefinition) which is part of the Machtiging (machtigen).

3: Choose (Dienstafnemer)

3A Generate List of Dienstafnemers for which the user has Authorizations (Machtigingen)

3B Remove Authorizations that are for other DV

3B1 In case of a specific service request (ServiceID Index > 0): Remove the Dienstafnemers where the user does not have an Authorization for the requested Service.

3B2 In case of a Portaalfunctie request (ServiceID Index = 0): Remove the Dienstafnemers where the user does not have an Authorization for any service of the Dienstverlener

3C Filter based on ECTA

3C1 In case of a specific service request: Filter the Dienstafnemers where the available EntityConcernedTypes of a Dienstafnemer cannot fulfill any ECTA set of the requested service

3C2 In case of a Portaalfunctie request: Remove the Dienstafnemers from the list where the available EntityConcenedTypes of a Dienstafnemer cannot fulfill any ECTA set of any service of the Dienstverlener. Note: Here a Dienstverlener/Dienst combination can occur that later when filtering on Service Restriction turns out not to be usable.

3D Alternative flow: No Dienstafnemers

If the user does not have any authorizations left, the MR MUST inform the user and offer the option to cancel the login process (link to cancel flow)

3E Let user select the Dienstafnemer he wants to represent

Note: MR MAY skip this step is the user can represent exactly one (1) Dienstafnemer.

4. In case of a Chain authorization and multiple Intermediairy organizations, let user select the Intermediary organization.

5. Determine the list of services

5A if the request is for a portal service

5A1 create a list of all services of the DV

5B If the Dienstafnemer selected is a Location (the authorization is limited to a Location), remove the services that do not indicate that they can respect restricted authorizations.

Note that there is multiple negative logic here. If the service specifies ServiceRestriction=Vestigingnummer it indicates that it can handle restricted authorisations and unrestricted authorizations.

6. Alternative flow : no applicable services

If the user does not have any authorizations left (the services list is empty), the MR MUST inform the user and offer the option to cancel the login process (link to cancel flow).

7. Determine the LoA

7A If the request is for a specific service

Select the specific authorization of the highest LoA.

7B If the request is for a portal service, from the list of services take the lowest LoA of all authorizations.

Use case overschrijdende alternatieve scenario's

Een aantal alternatieve scenario's heeft impact op meer dan één use case. Deze scenario's worden hier beschreven. De volgende alternatieve scenario's worden onderscheiden:

- Alternatief scenario attribuutverstrekking
- Attributen niet leverbaar of niet toegestaan
- Attribuut komt niet voor in attribuutcatalogus
- Dienst of dienstverlener komt niet voor in dienstencatalogus
- Gebruiker annuleert
- Soort dienstafnemer kan niet worden geleverd

Alternatief scenario attribuutverstrekking

In stap 1.1 van GUC1 Gebruiken eToegang als dienstafnemer en stap 2.1 van GUC2 Gebruiken eToegang als vertegenwoordiger kan de dienstverlener wanneer de Herkenningsmakelaar dit ondersteunt optioneel om aanvullende attributen vragen. Dit kan impliciet door met de Herkenningsmakelaar af te spreken dat voor een bepaalde dienst altijd een bepaalde set attributen wordt uitgevraagd. De gevraagde attributen worden opgenomen in de DV-HM SAML metadata en de Service catalog (Dienstencatalogus). Een dienstverlener kan verschillende metadata profielen hanteren voor verschillende sets met uit te vragen attributen.

In stap 3.2 van GUC3 Aantonen identiteit neemt de Herkenningsmakelaar, wanneer de dienstverlener om aanvullende attributen vraagt, de attributen die de authenticatiedienst zou kunnen leveren in de vraag op.

Na stap 3.4 van GUC3 Aantonen identiteit toont de authenticatiedienst, wanneer aanvullende attributen van de authenticatiedienst worden gevraagd, de authenticatiedienst dit ondersteunt en de attributen in de Dienstencatalogus voor de gevraagde dienst vermeld staan, de beschikbare attributen en de waarden van de attributen en vraagt de gebruiker goedkeuring om deze attributen te verstrekken (User consent). In het geval van Dienstbemiddeling levert de authenticatiedienst de attributen versleuteld aan alleen de dienstaanbieder op. De authenticatiedienst MOET de display name van de attributen uit de Attribuutcatalogus op eenvoudige wijze tonen. De authenticatiedienst MOET de doelbinding uit de Dienstencatalogus op eenvoudige wijze tonen. Indien de gebruiker al eerder doorlopende user consent heeft gegeven dan kan deze stap achterwege worden gelaten.

In stap 3.5 van GUC3 Aantonen identiteit worden, wanneer aanvullende attributen worden gevraagd en de authenticatiedienst dit ondersteunt, in het antwoord ook de beschikbare en waarvoor de gebruiker user consent heeft verleend, opgenomen in versleutelde vorm.

Na stap 4.3 van GUC4 Aantonen bevoegdheid toont het machtigingenregister, wanneer aanvullende attributen van het machtigingenregister worden gevraagd, het machtigingenregister dit ondersteunt en de attributen in de Dienstencatalogus voor de gevraagde dienst vermeld staan, de beschikbare attributen en de waarden van de attributen en vraagt de gebruiker goedkeuring om deze attributen te verstrekken (User consent). In het geval van Dienstbemiddeling levert het machtigingenregister de attributen versleuteld aan alleen de dienstaanbieder op. Het Machtigingenregister MOET de display name van de attributen uit de Attribuutcatalogus op eenvoudige wijze tonen. Het Machtigingenregister MOET de doelbinding uit de Dienstencatalogus op eenvoudige wijze tonen. Indien de machtigingenbeheerder van de vertegenwoordigde dienstafnemer/intermediaire partij al eerder (bijvoorbeeld bij registratie van de machtiging) doorlopende user consent heeft gegeven dan kan deze stap achterwege worden gelaten.

In stap 4.4 van GUC4 Aantonen bevoegdheid worden, wanneer aanvullende attributen worden gevraagd en het machtigingenregister dit ondersteunt, in het antwoord ook de beschikbare en waarvoor de gebruiker user consent heeft verleend, opgenomen in versleutelde vorm. Vestigingsspecifieke attributen worden alleen verstrekt indien ze als zodanig gevraagd worden.

In stap 1.3 van GUC1 Gebruiken eToegang als dienstafnemer en stap 2.4 van GUC2 Gebruiken eToegang als vertegenwoordiger worden, wanneer aanvullende attributen door de dienstverlener zijn gevraagd en deze attributen door authenticatiedienst en/of machtigingenregister zijn geleverd, deze in versleutelde vorm aan het antwoord toegevoegd.



Bij Dienstbemiddeling worden attributen alleen geleverd aan de Dienstaanbieder, de Dienstbemiddelaar ontvangt dus geen attributen. Een Dienstbemiddelaar kan deze attributen wel verkrijgen door voorafgaand aan de Dienstbemiddeling de attributen zelf uit te vragen voor een eigen dienst (en treedt dan direct als dienstverlener op).

Attributen niet leverbaar of niet toegestaan

Indien AD of MR één of meer van de gevraagde attributen, waarvan in de SAML metadata of het verzoek is aangegeven dat deze niet Required zijn, niet kunnen leveren (hetzij omdat zij deze gegevens niet registeren, hetzij omdat er geen User consent gegeven wordt) wordt in stap 5 van GUC3 Aantonen identiteit, respectievelijk stap 4 van GUC4 Aantonen bevoegdheid een authenticatieverklaring afgegeven die enkel de authenticatie en gegevens die wel leverbaar zijn bevat. De Use case wordt vervolgens normaal vervolgd. In stap 3 van GUC1 Gebruiken eToegang als dienstafnemer of stap 4 van GUC2 Gebruiken eToegang als vertegenwoordiger levert de HM de gevraagde attributen die geleverd konden worden, de andere attributen worden niet meegezonden.

Indien AD of MR één of meer van de gevraagde attributen, waarvan in de Dienstencatalogus of het verzoek is aangegeven dat deze Required zijn, niet kunnen leveren (hetzij omdat zij deze gegevens niet registeren, hetzij omdat er geen user consent gegeven wordt) of omdat voor de gevraagde dienst de attributen niet in de Dienstencatalogus vermeldt staan, wordt na stap 5 van GUC3 Aantonen identiteit, respectievelijk stap 4 van GUC4 Aantonen bevoegdheid de Use case niet vervolgd (zie Error handling).

Dienstverlener MOET er rekening mee houden dat gevraagde optionele attributen niet geleverd kunnen worden. Dit kan betekenen dat bepaalde dienstverlening niet mogelijk is.

Attribuut komt niet voor in attribuutcatalogus

Zowel de Herkenningsmakelaar (in stap 1 van GUC1 Gebruiken eToegang als dienstafnemer en stap 1 van GUC2 Gebruiken eToegang als vertegenwoordiger) als de authenticatiedienst (in stap 2 van GUC3 Aantonen identiteit) als het machtigingenregister (in stap 2 van GUC4 Aantonen bevoegdheid) dienen te controleren of het attributen betreft die voorkomen in de attribuutcatalogus. Indien dit niet het geval is dienen zij een fout met die strekking te tonen (zie Error handling) en wordt de use case niet vervolgd.

Dienst of dienstverlener komt niet voor in dienstencatalogus

In stap 1.1 van GUC1 Gebruiken eToegang als dienstafnemer, stap 2.1 van GUC2 Gebruiken eToegang als vertegenwoordiger, stap 3.2 van GUC3 Aantonen identiteit, stap 4.2 van GUC4 Aantonen bevoegdheid of stap 5.1 van GUC5 Aantonen BSN kan worden geconstateerd dat de dienst of dienstverlener niet voorkomt of het gebruik van dienstbemiddeling niet is toegestaan voor de dienst in de door de betreffende deelnemer gehanteerde versie van de dienstencatalogus. De betreffende deelnemer MOET het bericht afwijzen, zoals beschreven Error handling.

Gebruiker annuleert

De gebruiker kan de authenticatie op elk gewenst moment annuleren.

Wanneer het annuleren plaatsvindt bij de Herkenningsmakelaar (HM) MOET deze het proces afbreken en naar de Dienstverlener (DV) antwoorden met een foutmelding die is beschreven in Error handling.

Wanneer het annuleren plaatsvindt bij de Authenticatiedienst (AD) MOET deze het proces afbreken en naar de DV antwoorden met een foutmelding die is beschreven in Error handling. De HM MOET de gebruiker dan aanbieden een andere authenticatiedienst te kiezen. Indien er een selectie van een authenticatiedienst bewaard is moet deze worden genegeerd. Indien vervolgens opnieuw een authenticatiedienst geselecteerd wordt moet de vraag of deze instelling bewaard moet worden opnieuw getoond worden met default "leeg". De nieuwe keuze overschrijft de oude.

Wanneer het annuleren plaatsvindt bij het Machtigingenregister (MR) MOET deze het proces afbreken en naar de HM antwoorden met een foutmelding die is beschreven in Error handling. De HM MOET de gebruiker dan aanbieden opnieuw een AD te kiezen of de Herkenning te annuleren.

Soort dienstafnemer kan niet worden geleverd

In stap 3.3 van GUC3 Aantonen identiteit kan een authenticatiedienst (en in stap 4.3 van GUC4 Aantonen bevoegdheid een machtigingenregister) vaststellen dat de voor het antwoord benodigde soort dienstafnemer niet kan worden geleverd. Dit kan bijvoorbeeld komen doordat de gebruiker niet behoort tot de gevraagde beroepsgroep, of doordat de authenticatiedienst of machtigingenregister niet gerechtigd is de gevraagde gegevens vast te leggen. In dat geval MOET de betreffende deelnemer het bericht weigeren, zoals beschreven in Error handling.

Use cases Single Sign-On

In stap GUC1 Gebruiken eToegang als dienstafnemer of GUC2 Gebruiken eToegang als vertegenwoordiger kan de dienstverlener in de vraag specificeren dat single sign-on is toegestaan of dat een hernieuwde authenticatie wordt afgedwongen.

> Voor diensten die betrouwbaarheidsniveau 4 vereisen is single sign-on nooit toegestaan.

In stap GUC3 Aantonen identiteit wordt door een authenticatiedienst die SSO ondersteunt als volgt gehandeld:

- Indien door de dienstverlener een hernieuwde authenticatie wordt afgedwongen en er al eerder een aanlog door de gebruiker heeft plaatsgevonden waarvan de authenticatie bewaard is gebleven, MOET de nog niet verlopen authenticatie worden beëindigd. Daarnaast MAG na succesvolle authenticatie de optie worden geboden aan de gebruiker om aangelogd te blijven. Indien de gebruiker deze optie selecteert, wordt deze bewaard en kan vanaf dat moment SSO plaatsvinden. Tevens MOET de authenticatiedienst vanaf dit moment de timer van het maximum authenticatiedienst tijdsverloop starten;
- Indien SSO is toegestaan en er al eerder een aanlog door de gebruiker heeft plaatsgevonden waarvan de authenticatie bewaard is en die nog niet verlopen is, wordt deze hergebruikt zonder interactie met de gebruiker en gaat het authenticatiedienst tijdsverloop opnieuw in;
- Indien er geen eerdere (nog) geldige authenticatie is, MAG de optie worden geboden aan de gebruiker om aangelogd te blijven. Indien de gebruiker deze optie selecteert, wordt deze bewaard en kan vanaf dat moment SSO plaatsvinden. Tevens zal de authenticatiedienst vanaf dit moment de timer van het maximum authenticatiedienst tijdsverloop starten.

Na het succesvol uitvoeren van GUC1 Gebruiken eToegang als dienstafnemer of GUC2 Gebruiken eToegang als vertegenwoordiger MOET de dienstverlener die SSO toepast lokaal de sessie bijhouden. Indien SSO wordt toegepast moet de dienstverlener een logoutfunctie aanbieden.

Varianten bij Single Sign-On

Als onderdeel van de alternatieve flow voor Single Sign-On kunnen de volgende varianten voorkomen (die hier dus als alternatieve flow binnen de alternatieve flow van Use cases Single Sign-On beschreven worden).

- Geen reactie bij lezen of schrijven selectie authenticatiedienst
- Single Log-out

Geen reactie bij lezen of schrijven selectie authenticatiedienst

Als het cookie niet gelezen kan worden, dan moet het proces doorgaan alsof er geen selectie gemaakt is. Als het cookie niet geschreven kan worden, dan moet het proces doorgaan zonder een foutmelding aan de eindgebruiker te tonen.

Single Log-out

De volgende specifieke use case (Single log-out) MOET door alle authenticatiediensten en Herkenningsmakelaars ondersteund worden, ook door authenticatiediensten die geen Single Sign-On ondersteunen. Zij MOGEN logoutberichten NIET afkeuren en MOETEN de melding tonen zoals beschreven in stap 2 hieronder.

Nr.	Actie	Omschrijving
	Initiële staat	Een uitvoerende natuurlijke persoon heeft op basis van één of meer verklaringen toegang bij een dienstverlener en deze houden lokaal een sessie bij. Mogelijk is er ook bij andere dienstverleners nog een geldige sessie aanwezig.
1	gebruiker selecteert "logout" binnen de website van de dienstverlener.	De uitvoerende persoon wordt lokaal uitgelogd bij de dienstverlener conform de eisen in Single sign-on and user sessions en daarna doorgestuurd naar de Herkenningsmakelaar met een logoutbericht (zie Interface specifications DV-HM).
2	HM ontvangt logoutbericht en stuurt dit naar geselecteerde authenticatiedienst	De Herkenningsmakelaar stuurt het logoutbericht door naar de authenticatiedienst. Op basis van het ontvangen bericht beëindigt de authenticatiedienst de eventueel nog geldige bewaarde authenticatie en toont daarna in browserwindow een bericht "uitgelogd bij [naam dienstverlener] en [naam authenticatiedienst]. Als u van andere Herkenningsdiensten gebruik heeft gemaakt, moet u daar zelf nog uitloggen. U kunt ook alle browservensters sluiten" (of een andere tekst met gelijke strekking).
	Finale staat	De gebruiker heeft bij de authenticatiedienst geen geldige sessie meer, maar mogelijk nog wel bij de andere dienstverleners waarbij eerder is ingelogd. Indien de browser wordt afgesloten verdwijnen ook die sessies.

Wanneer de Herkenningsmakelaar geen geldige authenticatiedienst vindt om het logoutbericht naar toe te sturen, dan toont de Herkenningsmakelaar een scherm met de tekst "Uitloggen is momenteel niet mogelijk. Sluit alle [naam browser*]vensters om de beveiliging van uw informatie te waarborgen."

*naam browser bepaald op basis van browserdetectie, of alleen 'browservensters' als detectie niet mogelijk is.

Use cases voor Administratie

De volgende processen onderscheiden waarin uitvoerende natuurlijke personen, dienstafnemers en dienstverleners voorbereidingen treffen voor het gebruik van Elektronische Toegangsdiensten.

- AUC1 Aansluiten dienst
- AUC2 Verkrijgen authenticatiemiddel
- AUC3 Registreren bevoegdheid
    - AUC3.1 Registreren bevoegdheid eenmanszaken
    - AUC3.2 Registreren status machtigingen eenmanszaken
- AUC4 Registreren attribuut
- AUC6 Activeren BSN
    - AUC6.1 Activeren BSN mbv VI — In het kader van sleutelmigratie van de IdentityProviderKeySet en van de SchemeWideKeySet (zie Proces migratie sleutelmateriaal voor polymorfe pseudonimisering) moet een MachtigingsRegister en MiddelenUitgever alle nog active (en dus eerder geactiveerde) BSN's opnieuw activeren bij BSNk-Activeren. Hiervoor stuurt
      de Machtigingenregister of MiddelenUitgever de BSN in de vorm van een Versleutelde Identiteit naar BSNk-Activeren. Die genereert en verstrekt een Polymorf Pseudoniem en Polymorfe Identi
- AUC7 Proces verlenen toestemming dienstbemiddeling — Voor Diensten die via Dienstbemiddeling kunnen worden ontsloten, kan toestemming van de Dienstaanbieder (DA) benodigd zijn. Dit proces beschrijft de werkwijze voor het verlenen van toestemming door een Dienstaanbieder aan een Dienstbemiddelaar (DB) om een Dienst te mogen bemiddelen.
- AUC8 Verkrijgen lijst Authenticatiediensten
- AUC9 Verstrekken sleutelmateriaal Dienstverleners — Het BSNk beheert en verstrekt via een Herkenningsmakelaar cryptografisch sleutelmateriaal aan elke Dienstverlener (DV) die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het Versleutelde Identiteit of Versleutelde Pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.
- AUC10 Transformeren
    - AUC10.2 MachtigingsRegister of Authenticatiedienst gebruikt BSNk transformatie functie
    - AUC10.3 HSM transformatie
- AUC11

AUC1 Aansluiten dienst

In deze use case wordt een dienst van een dienstverlener aangesloten op Elektronische Toegangsdiensten. De invulling van deze use case is onderdeel van het competitieve domein van Elektronische Toegangsdiensten en wordt in zijn geheel overgelaten aan de Herkenningsmakelaar. Hierbij dient een Herkenningsmakelaar in elk geval te voldoen aan de in AUC1 Aansluiten dienst gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- De Herkenningsmakelaar MOET een overeenkomst met de dienstverlener sluiten. Zie ook Juridisch kader. Deze overeenkomst MOET in lijn zijn met de Gebruiksvoorwaarden Elektronische Toegangsdiensten.
- De Herkenningsmakelaar MOET waarborgen dat de dienstverlener het koppelvlak DV-HM zoals beschreven in Interface specifications of een gelijkwaardig koppelvlak correct heeft geïmplementeerd. In het geval van Dienstbemiddeling MOET de Herkenningsmakelaar ook waarborgen dat de bij die Herkenningsmakelaar aangesloten dienstaanbieder/dienstbemiddelaar het koppelvlak DB-DA zoals beschreven in Interface specifications correct heeft geïmplementeerd.
- De Herkenningsmakelaar MOET waarborgen dat de dienst(en) van de dienstverlener, het bijbehorende betrouwbaarheidsniveau, toestemming voor dienstbemiddeling en de toegestane typen dienstafnemers correct, voorzien van een uniek nummer in een dienstencatalogus worden beschreven en dat deze dienstencatalogus wordt aangeleverd bij de beheerorganisatie. Zie Operationeel handboek en Interface specifications.
- In het geval de aan te sluiten dienst van een Dienstbemiddelaar is, MOET de Herkenningsmakelaar vooraf in de dienstencatalogus controleren of toestemming voor de dienst van de dienstaanbieder vereist is en zo ja, controleren of de dienstaanbieder in de dienstencatalogus controleren de dienstbemiddelaar toestemming heeft verstrekt. Indien de toestemming na aansluiting komt te vervallen, is dat reden om de aansluiting van de dienst op te schorten.
- De Herkenningsmakelaar MOET voor de Dienstverlener sleutelmateriaal ophalen bij BSNk voor het ontsleutelen van DV-specifieke Versleutelde Pseudoniemen c.q. Versleutelde Identiteiten en leveren aan een ontvangende partij, zie AUC9 Verstrekken sleutelmateriaal Dienstverleners.
- De Herkenningsmakelaar MOET controleren of een Dienstverlener gerechtigd is het BSN te ontvangen bij de autorisatielijst BSN, wanneer een Dienstverlener in de dienstencatalogus een EntityConcernedTypeAllowed EncryptedBSN registreert.
- De Herkenningsmakelaar MOET de legitimiteit controleren door middel van een controle op de authorisatielijst BSN wanneer een dienst DeprecatedServiceProviderID toepast.

N.B. Een dienstverlener ZOU een uniek nummer voor een dienst NIET MOETEN hergebruiken voor andere diensten. Wanneer een dienstverlener een dienst of de beschrijving van een dienst wijzigt MOET de dienstverlener waarborgen dat de betekenis van de dienst gelijk blijft en daarmee geregistreerde bevoegdheden geldig blijven. In het geval dat de dienstverlener dit niet kan of wil waarborgen MOET een nieuw uniek nummer worden toegekend.

Alternatieve scenario's

Voor deze use case zijn geen alternatieve scenario's gedefinieerd.

AUC2 Verkrijgen authenticatiemiddel

In deze use case verkrijgt de gebruiker een voor Elektronische Toegangsdiensten geschikt authenticatiemiddel. Dit kan op verschillende manieren: Het kan zijn dat de gebruiker een eigen (privé) middel verkrijgt, maar het kan ook zijn dat de gebruiker het middel op initiatief van, of door zijn werkgever krijgt uitgereikt of dat de gebruiker een eerder verkregen authenticatiemiddel registreert bij een middelenuitgever voor gebruik binnen Elektronische Toegangsdiensten. Bij de registratie kan een middel worden gekoppeld aan één of meer identificerende kenmerken van beroepsbeoefenaren. De invulling van deze use case is onderdeel van het competitieve domein van Elektronische Toegangsdiensten en wordt grotendeels overgelaten aan de middelenuitgever. Hierbij dient een middelenuitgever in elk geval te voldoen aan de in AUC2 Verkrijgen authenticatiemiddel gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- De middelenuitgever MOET alle processen beschrijven en inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in Normenkader betrouwbaarheidsniveaus. De beschrijvingen MOETEN via de website van de middelenuitgever worden gepubliceerd.
- De middelenuitgever MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- De middelenuitgever MOET een overeenkomst met de gebruiker en/of de dienstafnemer sluiten. Zie ook Juridisch kader.
- De middelenuitgever MOET waarborgen dat het authenticatiemiddel te gebruiken is bij ten minste één authenticatiedienst en daar uniek is te authenticeren.
- De middelenuitgever MOET waarborgen dat voor het authenticatiemiddel bevoegdheden kunnen worden geregistreerd in een machtigingenregister.
- De middelenuitgever MAG het BSN van de gebruiker eenmalig gebruiken om deze te activeren bij BSNk zodat het eHerkenningsmiddel gebruikt kan worden voor diensten die zijn polymorfe pseudoniem en/of polymorfe identiteit vereisen. Hiervoor MOET de middelenuitgever expliciete toestemming hebben van de gebruiker in kwestie.

Alternatieve scenario's

Voor deze use case zijn geen alternatieve scenario's gedefinieerd.

AUC3 Registreren bevoegdheid

In deze use case legt de dienstafnemer de bevoegdheid van een gebruiker vast in een machtigingenregister. Deze bevoegdheid kan voortvloeien uit een machtiging of een wettelijke vertegenwoordigingsbevoegdheid (de gebruiker is bijv. eigenaar van een eenmanszaak). De invulling van deze use case is onderdeel van het competitieve domein van Elektronische Toegangsdiensten en wordt in zijn geheel overgelaten aan het machtigingenregister. Hierbij dient een machtigingenregister in elk geval te voldoen aan de in AUC3 Registreren bevoegdheid gestelde eisen.

Bij de implementatie van deze use case gelden de volgende eisen:

- Het machtigingenregister MOET alle processen beschrijven en inrichten volgens de eisen voor het betreffende betrouwbaarheidsniveau zoals beschreven in document Normenkader betrouwbaarheidsniveaus. De beschrijvingen MOETEN via de website van het machtigingenregister worden gepubliceerd.
- Het machtigingenregister MAG NIET betrouwbaarheidsniveaus voeren of gebruiken waarvoor hij geen expliciete toestemming heeft van de beheerorganisatie.
- Het machtigingenregister MOET een overeenkomst met de dienstafnemer sluiten. Zie ook Juridisch kader.
- Het machtigingenregister MOET bevoegdheden zo vastleggen dat voor elke dienst in de dienstencatalogus een eenduidige uitspraak is te doen over de bevoegdheid van de gebruiker.
- Het machtigingenregister MOET vastleggen wat het betrouwbaarheidsniveau van een vastgelegde bevoegdheid is.
- Het machtigingenregister MAG mogelijkheden bieden voor het beperken van een bevoegdheid tot een bepaalde vestiging van de dienstafnemer. Daarentegen MAG het machtigingenregister een beperking van de bevoegdheid tot een vestiging NIET afdwingen.
- Het machtigingenregister MOET waarborgen dat bij het vastleggen van een bevoegdheid de aanvrager voldoende geïnformeerd is over de betekenis van die bevoegdheid.
- Het machtigingenregister MOET duidelijk onderscheid maken tussen dienstverleners en diensten die live danwel in test/pilot fase zijn.
- Het machtigingenregister MOET de mogelijkheid bieden voor het registreren van een algemene bevoegdheid. Een registratie van een dergelijke bevoegdheid betekent dat de gebruiker alle huidige en toekomstige diensten in de dienstencatalogus mag afnemen.
- Het machtigingenregister MAG in aanvulling op de registratie van een algemene bevoegdheid ook een registratieproces voor een algemene bevoegdheid met beperkingen voor geselecteerde diensten aanbieden.
- Het registreren van machtigingen voor bedrijven en organisaties die niet in het Nederlandse handelsregister zijn ingeschreven vereist verificatie van identificatie van de dienstafnemer en vertegenwoordigingsbevoegdheid in buitenlandse handelsregisters of daarmee vergelijkbare openbare registers. Deelnemers zijn niet verplicht deze functionaliteit aan te bieden, het is een Optionele functionaliteit.
- Het machtigingenregister MOET de machtigingenbeheerder op enig moment informeren over het feit dat een machtiging voor een dienst ook geldig is indien deze dienst nu of in de toekomst door andere Dienstverleners wordt aangeboden. Het moment hiervoor is vrij, dit kan vooraf (op het moment van machtiging) of achteraf (wanneer op een later moment één of meerdere geregistreerde machtigingen door een andere Dienstverlener worden gebruikt).

Alternatieve scenario's

Deze scenario's zijn terug te vinden onder AUC3.1 Registreren bevoegdheid eenmanszaken en AUC3.2 Registreren status machtigingen eenmanszaken

AUC3.1 Registreren bevoegdheid eenmanszaken

Voor het initieel registreren van bevoegdheden rondom eenmanszaken gelden aanvullende eisen ten opzichte van AUC3 Registreren bevoegdheid. Dit is in verband met de wijze waarop de eenmanszaak geregistreerd is bij de kamer van koophandel in het handelsregister. De kamer van koophandel gebruikt in het geval van een eenmanszaak niet het RSIN om de juridische identiteit te bepalen, maar de BSN gegevens van de eigenaar van de eenmanszaak. Om de veiligheid van BSN gegevens te garanderen moet voldaan worden aan de volgende aanvullende eisen:

- Het machtigingenregister MOET controleren of de gebruiker eigenaar is van de eenmanszaak.
- Het machtigingenregister MAG NIET de BSN gegevens opslaan van de eigenaar van de eenmanszaak.
- Het machtigingenregister MOET het BSN van de eigenaar van de eenmanszaak polymorf encrypted opslaan.
- BSN gegevens moeten op dezelfde manier worden verwerkt als BSN gegevens die zijn verstrekt om een natuurlijk persoon te identificeren.

Een voorbeeld use case om deze gegevens te registreren is als volgt:

1: Een gebruiker meldt zich aan bij het machtigingsregister.

2: De gebruiker levert een kopie aan van het uittreksel van de KVK waar het KVK nummer op staat van de eenmanszaak.

3: De gebruiker levert een WID document waar het BSN nummer op staat van de gebruiker.

4: Het machtigingenregister controleert de geldigheid van beide documenten.

5: Het machtigingenregister controleert of de NAW gegevens op de beide documenten overeenkomen.

6: Indien deze gegevens correct zijn en overeenkomen wordt de gebruiker aangewezen als de beheerder van de machtigingen voor de eenmanszaak.

7: Het machtigingenregister registreert de BSN gegevens bij het BSNk en slaat zelf de polymorfe identiteit op van de eigenaar van de eenmanszaak mbv A UC6 Activeren BSN

8. Het MachtigingsRegister registeert de machtiging(en) van de eenmanszaak voor specifieke Gebruikers

9: Het machtigingenregister registreert de status van de machtigingen bij het BSNk mbv AUC3.2 Registreren status machtigingen eenmanszaken

AUC3.2 Registreren status machtigingen eenmanszaken

Voor het registreren van de status van machtigingen rondom eenmanszaken gelden aanvullende eisen ten opzichte van AUC3 Registreren bevoegdheid, die zijn opgelegd vanuit het BSNk.

- Een MachtigingsRegister MOET de status van elke 'verzameling van machtigingen' registeren en actueel houden bij het BSNk-InzageRegister (met een beschrijving) die zinvol is voor de eigenaar van de eenmanszaak.
- Een MachtigingsRegister MAG NIET de status registreren van elke individuele machtiging.
- Een MachtigingsRegister moet als een minimum onderscheid maken tussen machtigingen voor de (eigennaar van de) eenmanszaak als Vertegenwoordigde en Vertegenwoordiger. Op dit moment is de eenmanszaak als Vertegenwoordiger nog niet ondersteund in ETD!
- Een MachtigingsRegister MAG als een maximum onderscheid maken tussen meerdere 'verzameling van machtigingen' elk met een specifiek doel en bijbehorende beschrijving als dit zinvol is voor de eenmanszaak, bijv "Bedrijfsmachtigingen voor de administratie afdeling"
- Een MachtigingsRegister MAG in de beschrijving van de 'verzameling van machtingen' geen gegevens opnemen die gebruikt kunnen worden om de eenmanszaak of de gemachtigde te identificeren

Stap	Actie	Omschrijving
	Initiële staat	Een MachtigingsRegister heeft de BSN van de Zelfstandige Ondernemer eerder geactiveerd bij BSNk-Activeren. En de het MachtigingsRegiser wil een status van (een verzameling) machtigingen bij het BSNk Inzageregister registreren of een eerder geregistreerde status moet aan gepast worden..
2.1	MR identificeert het Authenticatiemiddel en de Gebruiker	Het MachtigingsRegister identificeert de Zelfstandige Ondernemer volgens de eisen die het normenkader stelt (minimaal) op betrouwbaarheidsniveau 3 en identif (verzameling van) machtigingen waarvan een statusgegevens geregistreerd moeten worden bij het BSNk-Inzageregister
		Het MachtigingsRegister doorloopt AUC10 Transformeren functie. Daar wordt het (niet naar BSN te herleiden) Versleuteld Pseudoniem van het Inzageregister vastgesteld (VP@IR).
2.2	De MR stuurt de nieuwe status naar het BSNk Inzageregister	Het MachtigingsRegister stuurt de nieuwe status naar bij het BSNk Inzageregister met het zojuist verkregen Versleuteld Pseudoniem van de Gebruiker (VP@IR) en het volgnummer van de (verzameling van) machtigingen.
2.3	BSNk Inzageregister valideert de aanvraag	Het BSNk Inzageregister controleert of het MachtigingsRegister gemachtigd is om een BSN te activeren en of de aanvraag daadwerkelijk en ongewijzigd van het MachtigingsRegister afkomstig is en ontsleutelt de BSNk Inzageregister specifieke pseudoniem van de Gebruiker uit de Versleutelde Pseudoniem (VP@IR).
2.4	BSNk Inzageregister versleutelt en registreert de nieuwe status	Het BSNk Inzageregister registreert de nieuwe status voor de combinatie van specifieke pseudoniem van de Gebruiker, het MachtigingsRegister en het volgnummer van de (verzameling van) machtigingen. Deze registratie gaat met [interface spec BSNk: registerStatusEIM
	Finale staat	de verzameling van machtigingen heeft een nieuwe status bij het BSNk Inzageregister

AUC4 Registreren attribuut

In deze use case wordt een attribuut geregistreerd voor gebruik binnen Elektronische Toegangsdiensten. De invulling van deze use case wordt verder uitgewerkt in Proces change en release en hier verder niet beschreven.

AUC6 Activeren BSN

Deze Use Case wordt gerealiseerd door de BSNk Use Case AUC1 Activeren BSN. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.

AUC6.1 Activeren BSN mbv VI

In het kader van sleutelmigratie van de IdentityProviderKeySet en van de SchemeWideKeySet (zie Proces migratie sleutelmateriaal voor polymorfe pseudonimisering) moet een MachtigingsRegister en MiddelenUitgever alle nog active (en dus eerder geactiveerde) BSN's opnieuw activeren bij BSNk-Activeren. Hiervoor stuurt de Machtigingenregister of MiddelenUitgever de BSN in de vorm van een Versleutelde Identiteit naar BSNk-Activeren.
Die genereert en verstrekt een Polymorf Pseudoniem en Polymorfe Identiteit met het nieuwe sleutelmateriaal voor betreffende BSN specifiek voor de betreffende Machtigingenregister of MiddelenUitgever.

Deze Use Case wordt gerealiseerd door de BSNk Use Case AUC1 Activeren BSN. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.

AUC7 Proces verlenen toestemming dienstbemiddeling

Voor Diensten die via Dienstbemiddeling kunnen worden ontsloten, kan toestemming van de Dienstaanbieder (DA) benodigd zijn. Dit proces beschrijft de werkwijze voor het verlenen van toestemming door een Dienstaanbieder aan een Dienstbemiddelaar (DB) om een Dienst te mogen bemiddelen.

Diensten krijgen bij aansluiting vier opties om via Dienstbemiddeling ontsloten te mogen worden:

- Niet bemiddelbaar;
- Bemiddeling door derden niet toegestaan;
- Vrij bemiddelbaar (geen toestemming vereist);
- Toestemming vereist

Wanneer een Dienstaanbieder voor een van de eerste drie opties kiest, is er geen (expliciete) toestemming benodigd en daarmee is er geen proces nodig. Indien een DA aangeeft toestemming te vereisen, moet toestemming kenbaar worden gemaakt zodat dit in het netwerk gecontroleerd en erkend kan worden.

Het proces voor het verlenen van toestemming verloopt als volgt:

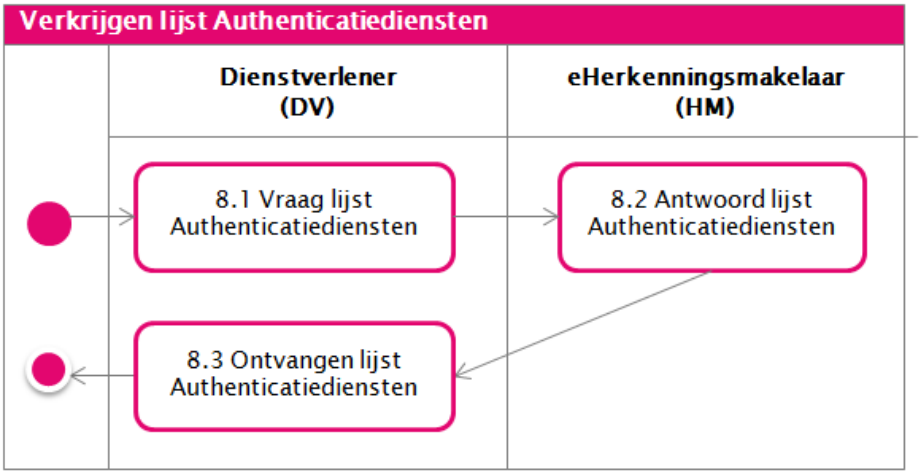
1. DB geeft bij DA aan dat deze een dienst van de betreffende Dienstaanbieder wil gaan ontsluiten op basis van Dienstbemiddeling.
2. DA neemt aanvraag in behandeling en kan/mag daarbij een aanvullend toestemmingsproces – zoals het toepassen van toestemmingscriteria of een testtraject – toepassen.
3. DA verleent toestemming aan de DB; de DA deelt dit mee aan zijn eigen HM en aan de DB.
4. De HM van de DA registreert de erkenning voor bemiddeling in de dienstencatalogus (in ServiceIntermediationAllowed) welke aan de beheerorganisatie wordt aangeleverd volgens Proces doorvoeren nieuwe dienstencatalogus.
5. De DB vraagt aan zijn eigen HM om de bemiddeling te activeren.
6. De HM van de DB controleert in de nieuwe dienstencatalogus of toestemming door de DA voor de DB is opgenomen en alleen als dit zo is mag de DB aansluiten voor Dienstbemiddeling van de betreffende dienst.

Alternatief scenario

De DA verleent geen toestemming. In dit geval dient de DA dit zelf aan de DB mee te delen, breekt af voor stap 3 en wijzigt er voor het netwerk niets.

AUC8 Verkrijgen lijst Authenticatiediensten

In deze use case vraagt een Dienstverlener (DV) de meest recente lijst met gecertificeerde ADs voor een dienst op bij de HM. Deze lijst dient om de gebruiker een AD te laten kiezen bij de DV, zie alternatief scenario 1.1 (GUC1 Gebruiken eToegang als dienstafnemer) en alternatief scenario 3.3 (GUC3 Aantonen identiteit).



Nr.	Actie	Omschrijving
8.1	Vraag lijst Authenticatiediensten	De Dienstverlener vraagt een lijst op van relevante Authenticatiediensten via een door de Herkenningsmakelaar verstrekte URL. De URL bevat een parameter voor de betreffende dienst (ServiceUUID).
8.2	Antwoord lijst Authenticatiediensten	Een Herkenningsmakelaar levert hierop een lijst met relevante informatie van alle van toepassing zijnde Authenticatiediensten voor de dienst (op basis van ServiceUUID) van een Dienstverlener. 'Van toepassing zijnde' is hierbij een Authenticatiedienst welke minimaal het gevraagde betrouwbaarheidsniveau en het gevraagde identificerende kenmerk kan leveren volgens de Network metadata. De lijst wordt door de Herkenningsmakelaar op alfabetische volgorde (OrganizationDisplayName) gesorteerd. Een Herkenningsmakelaar ondertekent deze lijst met een geldig PKIo-certificaat voor signing zoals vermeldt voor de HM in de Network metadata.
8.3	Ontvangen lijst Authenticatiediensten	De DV controleert de handtekening en bewaart de lijst met relevante Authenticatiediensten. De Dienstverlener toont alle relevante Authenticatiediensten in dezelfde volgorde als aangeleverd door de Herkenningsmakelaar en in gelijke weergave aan de gebruiker, wanneer de gebruiker een selectie kan maken zoals beschreven in alternatief scenario 1.1 (GUC1 Gebruiken eToegang als dienstafnemer).

AUC9 Verstrekken sleutelmateriaal Dienstverleners

Het BSNk beheert en verstrekt via een Herkenningsmakelaar cryptografisch sleutelmateriaal aan elke Dienstverlener (DV) die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal.
De Dienstverlener ontsleutelt met dit Sleutelmateriaal het Versleutelde Identiteit of Versleutelde Pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.

Voor eIDAS Outbound acteert de eIDAS Berichtenservice als Dienstverlener, die dienstbemiddelaar is voor de BRP. Daarom moet in deze use case het gebruik van de term "Dienstverlener", worden geïnterpreteerd als "Dienstaanbieder (hier: BRP) en/of eIDAS Berichtenservice (EB)".

Deze use case is een variant op de BSNk use case <AUC5>.

Stap	Actie	Omschrijving
	Initiële staat	Een Dienstverlener heeft Sleutelmateriaal nodig om de identiteit (bijv BSN) en/of pseudoniem uit de Versleutelde Identiteit/Pseudoniem te halen en vraagt zijn Herkenningsmakelaar om hem hierbij te ondersteunen.
9.1	De Herkenningsmakelaar valideert het verzoek.	De Herkenningsmakelaar valideert dat het verzoek afkomstig is van bevoegd medewerker van de Dienstverlener, of een door deze geautoriseerde derde of zijn systeem.
9.2	De Herkenningsmakelaar stuurt een aanvraag naar het Sleutelbeheer	De Herkenningsmakelaar stuurt een aanvraag voor Sleutelmateriaal naar het BSNk Sleutelbeheer met daarin het PKIoverheid-certificaat van betreffende Dienstverlener.
9.3	Sleutelbeheer valideert de aanvraag	BSNk Sleutelbeheer controleert of de aanvraag daadwerkelijk en ongewijzigd van een erkende Herkenningsmakelaar afkomstig is en of het meegeleverde PKIoverheid-certificaat van de Dienstverlener geldig is.
9.4	Sleutelbeheer controleert of Dienstverlener BSN mag ontvangen	BSNk Sleutelbeheer controleert of het OIN van de Dienstverlener zoals deze op het meegeleverde PKIoverheid-certificaat voorkomt op de Autorisatielijst BSN en ook Sleutelmateriaal mag ontvangen om een BSN te ontsleutelen.
9.5	Sleutelbeheer genereert Sleutelmateriaal	BSNk Sleutelbeheer genereert het Sleutelmateriaal voor het OIN van de Dienstverlener inclusief het BSN-Sleutelmateriaal indien diens OIN inderdaad voorkomt op de Autorisatielijst BSN
9.6	Sleutelbeheer versleutelt Sleutelmateriaal	BSNk Sleutelbeheer versleutelt Sleutelmateriaal obv de publieke sleutel op het meegeleverde PKIoverheid-certificaat van de Dienstverlener
9.7	Sleutelbeheer verstrekt Sleutelmateriaal aan de Herkenningsmakelaar en registreert de verstrekking	BSNk Sleutelbeheer verstrekt Sleutelmateriaal ten behoeve van de Dienstverlener aan de aanvragende Herkenningsmakelaar en registreert de verstrekking in een publiekelijk toegankelijke Sleutelverstrekkingslijst .
9.8	Herkenningsmakelaar verstrekt Sleutelmateriaal aan de Dienstverlener	De Herkenningsmakelaar verstrekt Sleutelmateriaal aan de betreffende Dienstverlener.
9.9	Dienstverlener ontsleutelt en installeert Sleutelmateriaal	De Dienstverlener ontsleutelt Sleutelmateriaal en installeert dit op zijn toegangssystemen.
	Finale staat	De Dienstverlener kan BSN en Pseudoniem uit een Versleutelde Identiteit/Pseudoniem halen. En de sleutelverstrekking is geregistreerd in het Sleutelverstrekkingslijst. De Dienstverlener kan via zijn HM diensten aansluiten en is klaar om gebruikers voor die dienst obv Persistent Pseudoniem of BSN te ontvangen.

NB: deze use case wordt gerealiseerd mbv Interface specifications MR-BSNk

AUC10 Transformeren

Deze Use Case wordt gerealiseerd door de BSNk Use Case AUC2 Transformeren. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.

AUC10.2 MachtigingsRegister of Authenticatiedienst gebruikt BSNk transformatie functie

Uitwerking van stap 2.2 van AUC10 Transformeren

Stap	Actie	Omschrijving
	Initiële staat	het MachtigingsRegister of AuthenticatieDienst heeft de benodigde Polymorfe Identiteit/Pseudoniem (PP@MU of PI@MU) van de betreffende Gebruiker en weet ten behoeve van welke Ontvangende Partij transformatie nodig is.
2.2.1	MachtigingsRegister of AuthenticatieDienst randomiseert PI@MU of PP@MU	het MachtigingsRegister of AuthenticatieDienst randomiseert de Middelenuitgever specifieke Polymorfe identiteit /pseudoniem (PP@MU of PI@MU) zodat het BSNk deze niet meer kan herkennen.
2.2.2	MachtigingsRegister of AuthenticatieDienst vraagt het BSNk om de PI@MU of PP@MU te transformeren	het MachtigingsRegister of AuthenticatieDienst stuurt de gerandomiseerde Middelenuitgever specifieke Polymorfe identiteit/pseudoniem (PP@MU of PI@MU) samen met de identiteit (OIN), en BSNk-sleutelversie (BSNk-recipientKeySetVersion in de Dienstcatalogus) van de beoogde Ontvangende Partij(-en) naar het BSNk volgens BSNk: transform. De BSNk-structuur versie (BSNk-structureVersion in de Dienstcatalogus) bepaalt welke BSNk-Transformatieservice gebruikt moet worden. In het geval van DienstBemiddeling waarbij beide ontvangers een polymorf pseudoniem of polymorfe identiteit vereisen: • MOET de BSNk-structuurversie "2" zijn voor beide partijen • MOET in het transform request bij de RelyingParty van de dienstbemiddelaar het LinkVerification element worden toegevoegd Indien de BSNk-structuurversie "1" is, of niet is ingevuld MOET de BSNk-transformatieservice V1 aangeroepen worden. Indien de BSNk-structuurversie "2" is MOET de BSNk-transformatieservice V2 aangeroepen worden.
2.2.3	BSNk valideert de aanvraag	Het BSNk controleert dat de aanvragende partij geautoriseerd is als MachtigingsRegister of AuthenticatieDienst en of de aanvraag daadwerkelijk en ongewijzigd van die partij afkomstig is.
2.2.4	BSNk transformeert de PI@MU VI@OP of PP@MU VP@OP	Het BSNk transformeert met zijn HSM de Middelenuitgever specifieke Polymorfe Identiteit/Pseudoniem met behulp van de identiteit (OIN) en sleutelversie van de Ontvangende Partij naar een specifieke Versleutelde Identiteit /Pseudoniem (PP@MU VP@OP of PI@MU VI@OP).
2.2.5	BSNk verstrekt de VI@OP of VP@OP aan het MachtigingsRegister of de Authenticatiedienst	Het BSNk verstrekt de voor de Ontvangende Partij specifieke Versleutelde Identiteit/Pseudoniem (VP@OP of VI@OP) aan het MachtigingsRegister of AuthenticatieDienst en logt de aanvraag ten behoeve van audit-doeleinden.
	Finale staat	Het MachtigingsRegister of AuthenticatieDienst kan de Gebruiker identificeren voor de betreffende Ontvangende Partij.

AUC10.3 HSM transformatie

NB Deze interface naar de HSM wordt door de HSM (en/of bijbehorende firmware-) leverancier gespecificeerd.

Nr.	Actie	Omschrijving
2.3.1	HSM valideert de aanvraag	Het HSM controleert of de aanvragende applicatie geauthenticeerd en geautoriseerd is en of de aanvraag correct aan de specificatie voldoet.
2.3.2	HSM genereert het VP@OP of VI@OP	De HSM transformeert één of meerdere Polymorfe identiteit(en)/pseudoniem(en) met behulp van de identiteit (OIN) en sleutelversie van de Ontvangende Partij naar één of meer Ontvangende Partij(en) specifieke Versleutelde Identiteit(en) /Pseudoniem(en) (PP@MU VP@OP of PI@MU VI@OP).
2.3.3	HSM verstrekt het VP@OP of VI@OP	De HSM verstrekt de voor de Ontvangende Partij specifieke Versleutelde Identiteit(en)/Pseudoniem(en) (VP@OP of VI@OP) aan de aanvrager en logt de aanvraag ten behoeve van auditing.

AUC11

Op dit moment is Dienstbemiddeling functionaliteit beperkt tot de eIDAS BerichtenService (EB) van de RVO als Dienstbemiddeling voor de BRP-Attributendienst van de RvIG. Deze beperking wordt afgedwongen op basis van de OIN van de EB. Om een eventuele OIN-migratie van de EB te kunnen faciliteren moet de EB ook meerdere geautoriseerde OIN's kunnen hebben. Hiertoe zal de Logius Beheerorganisatie een lijst van toegestane Dienstbemiddelaars (Allowed4ServiceIntermediation) publiceren via email en Leveranciersoverleg.

Overige 'instellingsparameters voor Dienstbemddeling' zijn *IntermediatedService* and *ServiceIntermediation (@intermediationAllowed, ServiceIntermediationAllowed*) en staan in de DienstCatalogus. De AD/MR MAG deze instellingsparameters tijdens het authenticatieproces uit de ServiceCatalogus halen en toepassen. Maar een AD/MR mag deze instellingsparameters ook handmatig uit de DienstCatalogus overnemen en in een 'configuratie-bestand' afhandelen.

Via het Leveranciersoverleg wordt per aanpassing van Allowed4ServiceIntermediation of overige instellingsparameters een implementatietermijn afgesproken.

Gebruikersinterface

Dit hoofdstuk beschrijft eisen die worden gesteld aan de gebruikersinterface met de gebruiker.

Voor eisen in dit hoofdstuk waaraan middelen en of kanalen door hun opzet niet of zeer lastig kunnen voldoen geldt de verplichting in overleg met de beheerorganisatie een acceptabele oplossing te realiseren.

Dialoogbeschrijving

Alle dialoogvensters die door partijen in het herkenningsproces worden ingezet om met de gebruiker te communiceren ZOUDEN MOETEN voldoen aan de volgende eisen:

- De naam van de partij die het dialoogvenster presenteert (en op dat moment een rol in het herkenningsproces vervult) wordt duidelijk getoond.
- De naam van de dienst, dienstverlener (of dienstbemiddelaar en dienstaanbieder) alsmede de extra beschrijving van de dienst (indien beschikbaar) worden duidelijk aan de gebruiker getoond, bij voorkeur zoals beschreven onder Dialoogbeschrijving Herkenningsmakelaars
- Het dialoogvenster MAG NIET informatie bevatten die niet rechtstreeks van toepassing is op, of bijdraagt aan het herkenningsproces. Reclame-uitingen of links naar andere webpagina's die buiten het herkenningsproces vallen MOGEN NIET worden opgenomen.
- Het beeldmerk van het product (eHerkenning en eIDAS) wordt getoond en wel volgens de daarvoor geldende richtlijnen. Zie Communicatie.
- De gebruiker moet in staat zijn de URL en het gepresenteerde SSL certificaat te controleren. Dientengevolge MOGEN schermen NIET ingebed worden, bijvoorbeeld in een mobiele app of een (i)frame. Partijen MOETEN hierop controleren en zonodig het herkenningsproces afbreken.
- Een partij MAG naast bovengenoemde gebruik maken van haar eigen logo's en huisstijl.
- Het ontwerp MOET bruikbaar zijn op schermen met lage resolutie of hoge pixeldichtheid, bijvoorbeeld mobiele apparaten. Hiervoor kan gebruik worden gemaakt van responsive webdesign-technieken.
- In het geval van Error handling of een normale fout (bv LoA te laag, geen machtiging en dergelijke) MOET de gebruiker handelingsperspectief worden geboden. Hierin ZOU minimaal MOETEN zijn opgenomen:
    - Relevante informatie in relatie tot de foutmelding (bv toelichting op de aard van de foutmelding, error codes), op basis waarvan de leverancier onderzoek kan doen naar de fout.
    - Generieke stappen die een gebruiker zelf uit zou kunnen voeren. Bijvoorbeeld het sluiten van alle browserschermen, verwijderen cookies, en dergelijke.
    - Contactinformatie van de leverancier die de foutmelding toont, waar de gebruiker een melding kan doen.

Naast dialoogschermen worden ook "URL-redirections" uitgevoerd (o.a. vaak door de HM).

De gebruikte redirect-schermen MOETEN voldoen aan de volgende eisen:

- De laadtijd van het redirect-scherm wordt tot een minimum beperkt en moet voldoen aan de eisen m.b.t. Performance.
- Bij succesvolle redirects merkt de gebruiker zo min mogelijk van het redirect scherm. Ideaal gezien is het scherm wit.
- In het geval dat de redirect poging niet succesvol is voldoen de huidige maatregelen m.b.t. Error handling.
- Bovenstaande punten functioneren zonder afhankelijkheden van "scripts" (bijv. mag het uitschakelen van JavaScript in de browser deze functionaliteit niet belemmeren).

Voor details in relatie tot de dialoogbeschrijving per rol zie pagina's:

- Dialoogbeschrijving Authenticatiedienst
- Dialoogbeschrijving Authenticatiedienst

Dialoogbeschrijving Authenticatiedienst

De Authenticatiedienst ZOU in het kader van gebruik aan de algemene eisen MOETEN voldoen zoals beschreven in de Dialoogbeschrijving, maar ZOU ook aan de volgende aanvullende eisen MOETEN voldoen:

Alle dialoogvensters die door partijen in het herkenningsproces worden ingezet om met de gebruiker te communiceren ZOUDEN MOETEN voldoen aan de volgende eisen:

- In het geval van dienstbemiddeling wordt zowel de dienstaanbieder als de dienstbemiddelaar genoemd VOOR het inloggen. Bijvoorbeeld: "U wilt inloggen bij DienstBemiddelaar.serviceProviderName voor DienstBemiddelaar.serviceName (ProviderName) en bij DienstAanbieder. serviceProviderName voor DienstAanbieder.serviceName."
- In geval veld @ProviderName in het AD request gevuld is, ZOU deze informatie VOOR het inloggen getoond moeten worden aan de gebruiker
    - Eventuele scripting MOET verwijderd worden

Dialoogbeschrijving Herkenningsmakelaars

De Herkenningsmakelaar MOET in het kader van gebruik aan de volgende aanvullende eisen voldoen:

- Indien het een "eIDAS Inkomend" verzoek betreft:
  - Laat geen scherm zien, maar stuur het verzoek direct door naar de eIDAS Berichtenservice (EB)
- De opsomming van deelnemers in de keuzelijst van de Herkenningsmakelaar MOET in alfabetische volgorde worden getoond volgens de naam die is opgenomen in het veld "displayname" dat is opgenomen in de metadata, ongeacht hoofd- of kleine letters. Zie Interface specifications.
- Deze opsomming MOET alleen de deelnemers tonen die het door de dienstverlener gevraagde Identificerende kenmerk kan leveren. Zie Metadata for participants.
- De Herkenningsmakelaar MOET voor stap 3.1 uit GUC3 Aantonen identiteit en stap 4.1 uit GUC4 Aantonen bevoegdheid twee aparte gestandaardiseerde schermen implementeren. De beheerorganisatie stelt hiervoor templates ter beschikking (20210709 schermen eherkenning versie 16.zip). De template MOET als volgt worden gevuld:
  - Tenzij dienst 0 (GUC4.3 Portaalfunctie) wordt *naam_dienst* gevuld met *"voor ServiceName*"
  - In geval veld @ProviderName in het SAML-bericht wordt *naam_dienst* aangevuld met "*(@ProviderName)*"
  - In het geval van dienstbemiddeling wordt *naam_dienst* aangevuld met "en bij *naam_dienstaanbieder voor naam_dienstaanbieder_dienst"*
  - De namen van de dienst en dienstverlener (dan wel dienstbemiddelaar) en dienstaanbieder zijn afkomstig uit de dienstencatalogus.
  - De namen van de authenticatiediensten en machtigingenregisters zijn afkomstig uit de metadata.
  - @ProviderName is afkomstig uit de DV-Request
- Op het scherm van de Herkenningsmakelaar wordt vermeld wat het door de dienstverlener minimaal vereiste betrouwbaarheidsniveau is.
- Het vakje "Onthoud deze keuze" is default aangevinkt, ook indien na annuleren er hernieuwde selectie plaatsvindt. Als gebruiker dit vakje uitvinkt, moet deze selectie onthouden worden door het plaatsen van een cookie. Zie Single sign-on and user sessions.
- Deelnemers die ETD voorzieningen gerealiseerd hebben m.b.v. een subsidie uit Europa moeten dit vanwege de subsidie regeling vermelden. Omdat standaardisatie van de HM look & feel gewenst is MOETEN die deelnemers dit vermelden onderaan de template met de voorgeschreven logo, zie template cef voor HM.zip.

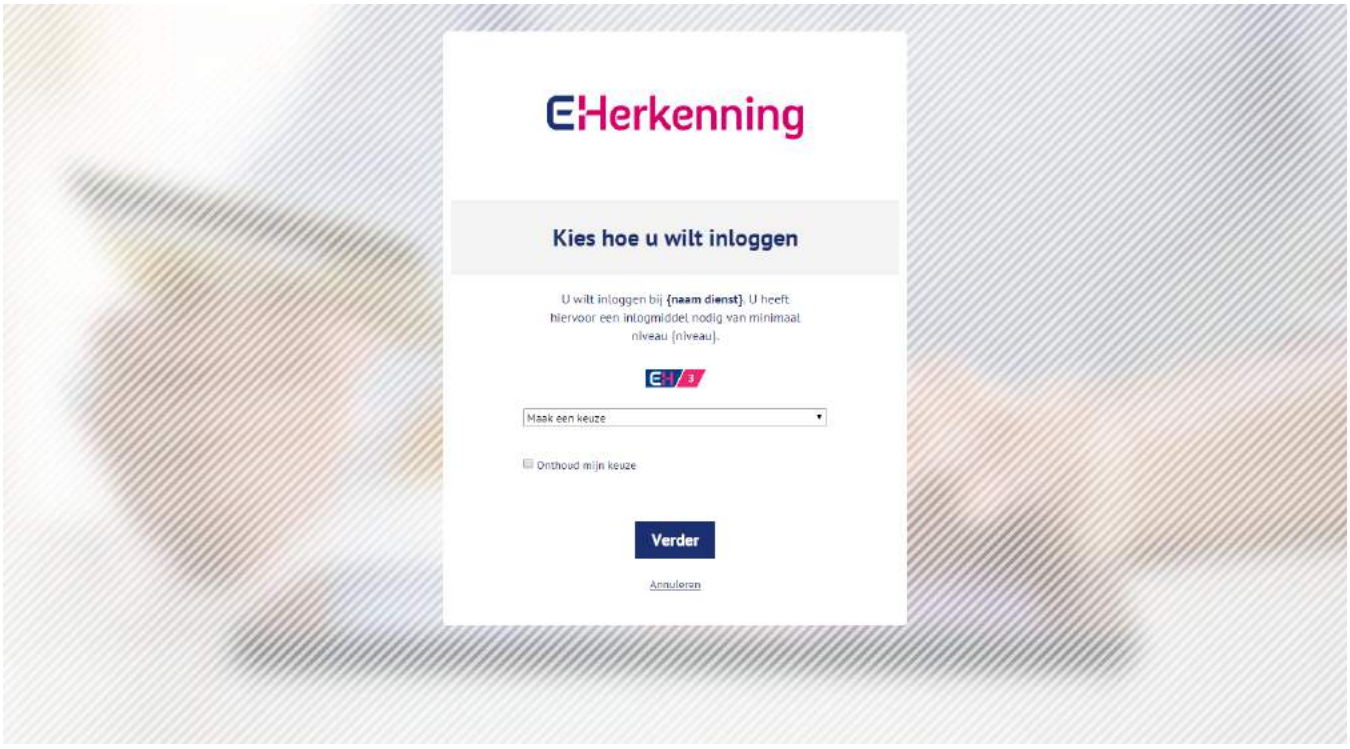
Note: At this moment the use of ASTA-sets and Service Intermediation is limited to the EB for eIDAS Outgoing.

Voorbeelden

Een voorbeeld voor eIDAS-outbound (dienstbemiddeling):

U wilt inloggen bij **Authenticatie buitenlandse dienstverlener** voor **Publieke dienst in Duitsland** (Finanzamt) en bij **Rijksdienst voor Identiteitsgegevens** voor **Ophalen persoonsgegevens voor EU inlog**. U heeft hiervoor een inlogmiddel nodig van minimaal **betrouwbaarheidsniveau EH3.**

eHerkenning template:



Toegankelijkheid

Alle dialoogvensters die door partijen in het herkenningsproces worden ingezet MOETEN voldoen aan de eisen die worden gesteld aan niveau 1 (" Toegankelijkheid prioriteit 1") van het Waarmerk drempelvrij.nl (www.drempelvrij.nl). Partijen MOETEN dit aantonen door middel van een zelfverklaring en MOGEN dit verder aantonen door middel van certificering.

Alle dialoogvensters die door partijen in het registratieproces van middelen worden ingezet MOETEN voldoen aan de eisen die worden gesteld aan niveau 1 ("Toegankelijkheid prioriteit 1") van het Waarmerk drempelvrij.nl. Partijen MOETEN dit aantonen door middel van een zelfverklaring en MOGEN dit verder aantonen door middel van certificering.

Alle webpagina's in het herkenningsproces MOETEN ten minste in het Nederlands als in het Engels beschikbaar zijn. Voor alle rollen geldt dat er naar de Browser taal gekeken moet worden. Als de rol (HM,AD,MR,EB,BSNk) niet de door de gebruiker gewenste taal kan weergeven MOET de rol Nederlands gebruiken. Een rol MAG ook een functie aanbieden om de gebruiker een andere taal te laten selecteren. De registratieprocessen MOGEN ook alleen in het Nederlands worden aangeboden.

Alle webpagina's die door partijen in het herkenningsproces worden ingezet MOETEN functioneren zonder het gebruik van client-side scripting.

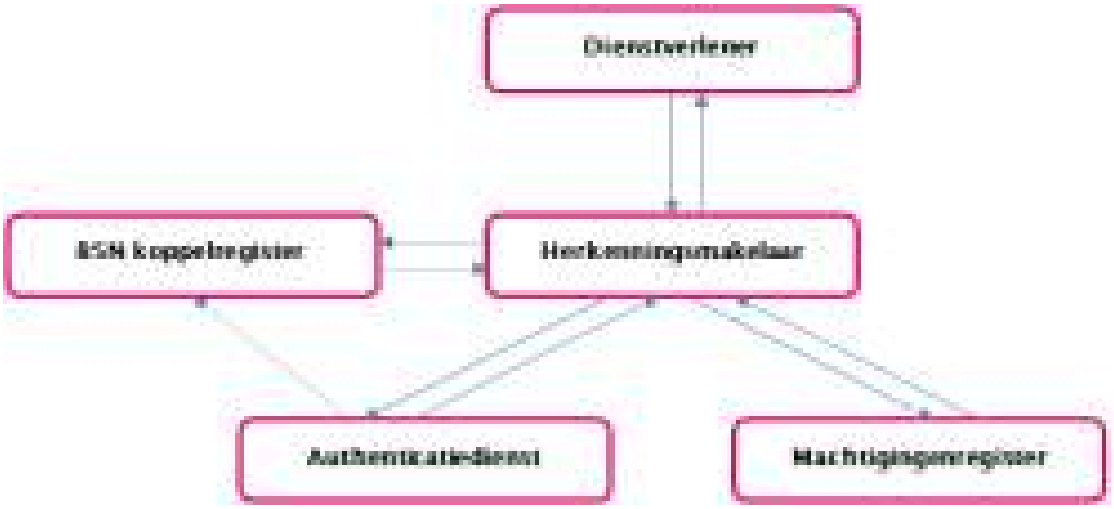
Interface specifications

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Interface specifications web

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

This section describes the interface specifications for the traffic between all roles in the network. The messages are based on SAML 2.0, or XACML where applicable.



General requirements

The following requirements are valid for all interfaces.

SAML Web Browser SSO Profile

The SAML Web Browser SSO Profile MUST be used for the interface described in this document. Optionally, an extension can be used for retrieving attributes.

Relay State

Every SAML request message MAY contain RelayState data. The response to an SAML request with RelayState data MUST also contain this RelayState data. The content of the RelayState MUST NOT exceed 80 byte and MUST be protected against changes by the party creating the RelayState.

Namespace aliases

Perhaps superfluously, it must be said that the parties are free to choose the aliases they use for the abbreviations of namespaces in tags.

HTTP Headers

The following HTTP headers MUST be used for all content that is sent to the browser of a user:

- Cache-Control with value "no-cache, no-store"
- Pragma with value "no-cache"

Optional elements and attributes

Optional elements and attributes MAY be included in the messages. These elements MUST be populated according to the specifications and MUST NOT be empty.

Versioning

Because different versions of the interface specifications (e.g. 1.9 and up) must be distinguished from each other at the interface level, message versioning MUST be used in the implemented interface. Because SAML 2.0 messages do not have a field for this and it is not desirable to use an extension in the messages, participants MUST link the URL on which SAML messages can be offered to a version of the framework in the published metadata. For example, https://www.deelnemer.nl/SAML-endpoint/v1.0/.

The same URL MUST NOT be used for two different versions of the framework. See also SAML metadata.

Language preference

The language preference of the user can be specified, so the dialogue can take place in that language. Because SAML 2.0 messages do not have a field for this and it is not desirable to use an extension in the messages, EherkenningPreferredLanguage MAY be used as query variable in the URL or provided as POST variable. See also section SAML attribute elements.

Character set and encoding

All message MUST the Unicode character set. All characters MUST be UTF-8 encoded.

Contents of this chapter

- Interface specifications HM-EB — This page describes the interface between a Herkenningsmakelaar (HM) and the eIDAS-berichtenservice (EB)
- Interface specifications HM-MR — This page describes the messages for the interface between an Herkenningsmakelaar (HM) (broker) and a Machtigingenregister (MR) (authorization information provider).
- Interface specifications HM-AD — This page describes the messages that are exchanged between an Herkenningsmakelaar (HM) and an Authenticatiedienst (AD) (identity provider).
- Interface specifications DB-DA — This paragraph describes the (guidelines for) interface(s) between the Dienstbemiddelaar (DB) (Service Intermediary) and the Dienstaanbieder (DA) (Service Supplier). The interface between a DB and a DA is considered a machine to machine interface. The implementation details of this interface will always be specified by the Dienstaanbieder. In order to facilitate adoption, Elektronische Toegangsdiensten aims to deliver an Authorization Solution compatible not only with green field implementation,
    - Reference Architecture DB-DA SOAP — This paragraph describes a reference architecture and specification of Interface specifications DB-DA, for use with a machine-to-machine interface using WebServices (SOAP).
- Interface specifications DV-HM — This page describes the messages for the interface specification between a Dienstverlener (DV) (service provider) and an Herkenningsmakelaar (HM) (broker).

Interface specifications HM-EB

This page describes the interface between a Herkenningsmakelaar (HM) and the eIDAS-berichtenservice (EB)

Note: The eIDAS-berichtenservice does not support a portal service.

This interface is exclusively applicable to eIDAS Inbound, and NOT to eIDAS Outbound.

Incoming authentication

When the EB serves as an Authenticatiedienst (AD) and Machtigingenregister (MR) for eIDAS-users from a different eIDAS member state; the HM will request the EB for both authentication and authorization information (machtiging) in one request. The eIDAS specifications transfer both in one message, thus separating these in two calls is deemed ineffective.

Request

A HM MUST request the EB with an AuthnRequest, identical to the AuthnRequest of the Interface specifications HM-AD. All processing rules MUST be adhered to.

Rules for procesing request

- If a request is received for ECTA urn:etoegang:1.12:EntityConcernedID:BSN the EB must check if the Service Provider is entitiled to receive the BSN by checking if the Service Provider is listed on the Autorisatielijst BSN.
    - If the Service Provider is not listed the EB must handle the error as an unrecoverable error (: urn:oasis:names:tc:SAML:2.0:status: RequestUnsupported.).
- In case a portal service request is made at the eIDAS-berichtenservice, the HM MUST return a error message containing ResultMajor "RequesterError" and ResultMinor "NotSupported".

Additional processing rules for request

A receiving EB

- if the ServiceInstance belonging to the ServiceUUID in the AuthnRequest is NOT classified as 'eIDAS-inbound', MUST handle this as a non-recoverable error (see Error handling).

The EB (in case of inbound authentication requests) MUST process the EntityConcernedTypesAllowed list

Response

The EB MUST construct an Assertion identical to the Assertion of an AD as defined in the Interface specifications HM-AD. In case an authentication in another eIDAS member state uses representation, the EB MUST construct an Assertion identical to the Assertion of an MR as defined in the Interface specifications HM-MR.

The EB MUST respond to the AuthnRequest in a single SAML Response message (transferred via Artifact binding), using the following structure:

@ID	1	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	SAML: Unique attribute of the AuthnRequest for which this Response message is the answer.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the Response.
@Destination	1	SAML: URL of the endpoint of the HM on which the message is offered. MUST match the HM's metadata.
@Consent	0	Elektronische Toegangsdiensten: MUST NOT be present
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the eIDAS-berichtenservice.
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.

@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	0 .. 1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloping message. When communicated within a ArtifactResolveResponse the signature on the SAML:Response MAY be omitted, since the parent message already guarantees the integrity.
Extensions	0	Elektronische Toegangsdiensten: MUST NOT be included.
Status	1	Elektronische Toegangsdiensten: MUST contain a StatusCode element with the status of the authentication. See Error handling.
StatusCode	1	SAML: MUST be present in a Status element.
@Value	1	If not 'success' additional information should be provided. (conform Elektronische Toegangsdiensten specifications).
StatusCode	0 .. 1	Only present if top-level StatusCode is not 'success'.
@Value	1	In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See Error handling.
StatusMessage	0 .. 1	Only present if top-level StatusCode is not 'success'.
StatusDetail	0	Elektronische Toegangsdiensten: MUST NOT be included.
Assertion	0 .. 2	Elektronische Toegangsdiensten: MUST contain the <Assertion> that is delivered in the response, if the request was processed successfully. In case of representation MUST contain a second, linked Assertion, containing the <Assertion> with the authorization information. See below.
EncryptedAssertion	0	Elektronische Toegangsdiensten: MUST NOT be included.

Processing rules for responses

A responding EB

- MUST provide an Assertion identical to that of an AD and apply all processing rules for a responding AD in Interface specifications HM-AD.
- In case of representation by the user from another eIDAS member state:
  - MUST also provide an Authorization Assertion containing a XACMLDecisionStatement identical to that of an MR and apply all processing rules for a responding MR in Interface specifications HM-MR.
  - MUST ensure the AD-assertion and MR-assertion originate from the same authentication and are properly linked.
- MAY provide attributes that have 'eIDAS' as source. These attributes MUST be translated from the corresponding eIDAS messages.
- MUST NOT provide any other attributes or use other attribute sources.

MUST respond with the identifier(s) using the following rules:

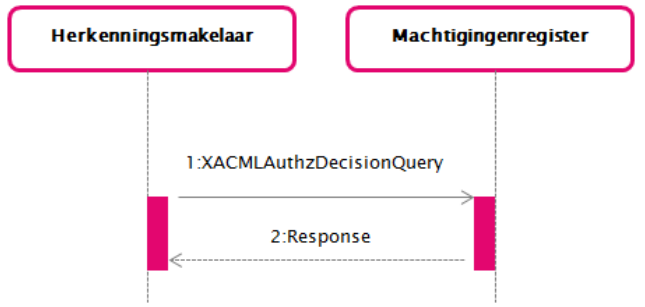
- MUST respond with all the EntityConcernedTypes in an Identifier Set.
  - An identifier set is a cluster of EntityConcernedTypes with the same set number in the Service catalog.
  - If no set numbers are used, only one EntityConcernedType is allowed, which MUST be handled as if it was in 1 set.
- MUST respond with all the EntityConcernedTypes in the identifier set with the lowest set number.
  - If the EB cannot respond with all the EntityConcernedTypes the set, the next set with the lowest number MUST be used, until all sets are proven to be impossible. Only then an error MUST be returned.

A receiving HM

- MUST validate the response and signature.
- MUST validate and process the message according to the processing rules in Interface specifications HM-AD and – if applicable – those in Interface specifications HM-MR.
- MUST accept and process both Assertions as if they were received from any other AD and MR (if applicable).
- MUST include both messages in its response to the initiating DV/OD.

Interface specifications HM-MR

Sequence diagram HM-MR



disclaimer

The example messages below need adjusment because of RFC2134. Contact the beheerorganisatie for more info.

This page describes the messages for the interface between an Herkenningsmakelaar (HM) (broker) and a Machtigingenregister (MR) (authorization information provider).In the interface described here, the use case GUC4 Aantonen bevoegdheid consists of an SAML 2.0 XACMLAuthzDecisionQuery and Response.

A column in a message description that starts with 'SAML:' or 'XACML:' indicates that this is the standard value. A value that starts with 'Elektronische Toegangsdiensten' indicates that the value is specific to Elektronische Toegangsdiensten.

[XACMLAuthzDecisionQuery (1)] [Rules for processing request] [Response (2)] [Rules for processing responses] [Authorization assertion]

XACMLAuthzDecisionQuery (1)

@ID		SAML: Unique message attribute
@Version		SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant		SAML: Time at which the message was created.
@ReturnContext		Elektronische Toegangsdiensten: The value MUST be 'true'.
@Destination		SAML: URL of the MR on which the message is offered. MUST match the MR's SAML metadata.
@Consent		Elektronische Toegangsdiensten: MUST NOT be included.
@InputContextOnly		Elektronische Toegangsdiensten: MUST NOT be included
Issuer		Elektronische Toegangsdiensten: MUST contain the EntityID of the HM. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature		Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloped message.
Extensions		Elektronische Toegangsdiensten: • MUST contain an XACML Attribute-element with AttributeId AssertionConsumerServiceIndex • MUST contain the attribute IntendedAudience. • MUST contain an <Assertion> element that contains the AD Assertion in a XACML Attribute-element with AttributeId Assertions. If the DV queries additional attributes, they MUST be included here by the HM. To this extent, one Elektronische Toegangsdiensten specific RequestedAttributes (see schema) element MUST be included containing the RequestedAttribute elements reflecting the DV's request. The requested attribute(s) MUST be defined in the Attributcatalogus and MUST be declared as RequestedAttribute in the Service catalog entry for the requested service. An MR not able to provide these attributes MUST act as specified in the alternative use case described in Attributen niet leverbaar of niet toegestaan. In case of chain authorization, different rules apply with regards to additional attributes, see Vervallen_Interface specifications HM-MR chain authorization. Other elements MUST NOT be included.
Request	**Subject**	Elektronische Toegangsdiensten: MUST contain a transient identifier which must be the same as the one contained in the <Assertion> element.

	Resource	Elektronische Toegangsdiensten: MUST contain the XACML attributes ServiceID and the corresponding ServiceUUID and MAY contain a XACML attribute LevelOfAssurance. When LevelOfAssurance is included in the request, it must contain the same or lower LevelOfAssurance (AuthnContextClassRef) as included in the Service catalog for the requested service. Other XML attributes MUST NOT be included. Other elements MUST NOT be included. An MR MAY ignore requests for additional attributes, but MUST NOT reject the message.
	Action	Elektronische Toegangsdiensten: MUST contain the XACML attribute Action-ID.
	Environment	Elektronische Toegangsdiensten: MUST be empty.

Rules for processing request

The MR MUST process the EntityConcernedTypesAllowed list.

A requesting HM:

- MUST include a copy of the AD Assertion for the authenticated User under Assertions in the extensions of the request.

IF ketenmachtiging see Vervallen_Interface specifications HM-MR chain authorization.

A receiving MR MUST provide an Assertion:

```
Determine required data for processing rules:
        USE (AD-Assertion) AttributeStatement.Attribute.ActingSubjectID.EncryptedID@MR TO determine
ActingSubject
        USE Authentication-LoA, Requested.Minimum-LoA, Requested.ServiceRestrictions, ActingSubject
and User input TO determine the response.LegalSubject, response.LOA, response.ServiceIDs and response.
ServiceRestrictions accoording         to Use Case Vaststellen bevoegdheid (or proces with similar result).
        USE ActingSubject TO create response.SpecificPseudoniem@SP
        USE Requested.EntityConcernedTypesAllowed and response.LegalSubject TO determine response.
EntityConcernedTypes and corresponding response.LegalSubject.Identities
        USE ActingSubject TO create response.SpecificPseudoniem@SP and response.SpecificPseudoniem@SI
        USE XACMLAuthzDecisionQuery.Request.Resource.ServiceUUID TO determine  ServiceCatalog.Minimum-LoA,
Requested.Attributes, Requested.EntityConcernedTypesAllowed, Requested.ServiceRestrictions,
ServiceIntermediation, SP-certificate from the Service Catalog
        USE XACMLAuthzDecisionQuery.Request.Resource.ServiceID (<index>=0) TO determine PortalRequest
        IF available XACMLAuthzDecisionQuery.Request.Resource.LevelOfAssurance THEN copy this
value to Requested.Minimum-LoA ELSE copy ServiceCatalog.Minimum-LoA to Requested.Minimum-LoA.
        Copy AD-Assertion - AuthnStatement.LevelOfAssurance to Authentication-LoA
        IF (NOT Ketenmachtiging) OR (Ketenmachtiging AND last-MR) THEN
         IF (any of the response.EntityConcernedTypes > r1.09 OR any Requested.Attributes) AND no available
DV-certificate THEN start Error Handling
     MUST provide an <XACMLAuthz-Decision> containing in <Subject> a <LinkedDeclarationSignatureValue> (see
Linking of Assertions) with value:
            AD-Assertion: Signature
     MUST provide a <XACMLAuthz-Decision> containing
            IF available SP-certificate THEN
                Copy response.SpecificPseudoniem@SP as an EncryptedID@SP in <Subject> to <ActingSubjectID>
                Copy all response.LegalSubject.Identities as EncryptedID@SP in <Subject> to <LegalSubjectID>
                    IF any requested.ServiceRestrictions THEN copy all requested.ServiceRestrictions in
<Resource> to <ServiceRestriction> (eg ServiceRestriction:Vestigingsnr)
            IF PortalRequest THEN copy all the response.ServiceID's and response.ServiceUUID's in <Resource>
to (a multi valued XACML attribute) <ServiceID> respectively <ServiceUUID> (See  GUC4.3 Portaalfunctie for
more details).
            IF requested.attributes AND User consent THEN in <Resource>
                IF available SP-certificate THEN copy attributesvalue(s) to an EncryptedAttribute@SP
            ------- For backward compatibility -------
            Copy response.SpecificPseudoniem@SP in <Subject> to <ActingEntityID>
            IF NOT eIDAS-BS THEN FOR all EntityConcernedTypes in response.EntityConcernedTypes:
                IF EntityConcernedType < r1.11 THEN copy response.EntityConcernedTypes with corresponding
response.LegalSubject.Identifier (<value>)in <Resource> to <EntityConcernedID>
            ------------------------------------------------
```

Determine appropriate ECTA and Identifiers:

- all the EntityConcernedTypes in an Identifier Set of EntityConcernedTypes with the same set number in the Service catalog.
- IF no set numbers are used, only one EntityConcernedType is allowed THEN handle this EntityConcernedType as if it was in 1 set.
- all the EntityConcernedTypes in the identifier set with the lowest possible set number the MR can provide for this response.LegalSubject.
- IF MR can't provide for any Identifier Set THEN start Error Handling
- Determine the response.EntityConcernedTypes and the corresponding response.LegalSubject. Identifiers for the selected identifier set

User consent for providing additional attributes can be granted the user OR by the authorization manager of the represented service consumer/intermediary (during the transaction or through prior consent)

All encryption is done using the DV-certificate from the Service Catalog.

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml-samlp:XACMLAuthzDecisionQuery xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os" xmlns:
samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " Version="2.0" IssueInstant=" " ReturnContext="true"
Destination=" ">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    </saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI=" ">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>
                </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>
        </ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Extensions>
        <xacml-context:Attribute name="AssertionConsumerServiceIndex" DataType="http://www.w3.org/2001
/XMLSchema#unsignedShort" Issuer=" ">
            <xacml-context:AttributeValue> </xacml-context:AttributeValue>
        </xacml-context:Attribute>
        <xacml-context:Attribute AttributeId="urn:etoegang:core:Assertions" DataType="urn:oasis:names:tc:
SAML:2.0:assertion:Assertion" Issuer=" ">
            <xacml-context:attributevalue>
                <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="_abc123">
                    <saml2:Issuer>urn:etoegang:AD:...</saml2:Issuer>
                    ...
                </saml2:Assertion>
            </xacml-context:Attributevalue>
        </xacml-context:Attribute>
        <saml:Attribute Name="urn:etoegang:core:IntendedAudience">
            <saml:AttributeValue>urn:etoegang:DV:OIN:entities:index</saml:AttributeValue>
        </saml:Attribute>
        <esp:RequestedAttributes>
            <md:RequestedAttribute Name="urn:etoegang:1.11:attribute-represented:CompanyName" IsRequired="
```

```
false" />
        </esp:RequestedAttributes>
    </samlp:Extensions>
    <xacml-context:Request xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
        <xacml-context:Subject>
            <xacml-context:Attribute AttributeId="urn:oasis:names:tc:SAML:2.0:assertion:NameID" DataType="
urn:oasis:names:tc:SAML:2.0:nameid-format:transient" Issuer=" ">
                <xacml-context:AttributeValue> </xacml-context:AttributeValue>
            </xacml-context:Attribute>
        </xacml-context:Subject>
        <xacml-context:Resource>
            <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceID" DataType="http://www.w3.org
/2001/XMLSchema#string">
                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
            </xacml-context:Attribute>
            <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceUUID" DataType="http://www.w3.org
/2001/XMLSchema#string">
                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
            </xacml-context:Attribute>
            <xacml-context:Attribute AttributeId="urn:etoegang:core:LevelOfAssurance" DataType="http://www.
w3.org/2001/XMLSchema#string">
                <xacml-context:AttributeValue>
                </xacml-context:AttributeValue>
            </xacml-context:Attribute>
    </xacml-context:Resource>
        <xacml-context:Action>
            <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="
http://www.w3.org/2001/XMLSchema#string">
                <xacml-context:AttributeValue>Authenticate</xacml-context:AttributeValue>
            </xacml-context:Attribute>
        </xacml-context:Action>
        <xacml-context:Environment>
        </xacml-context:Environment>
    </xacml-context:Request>
</xacml-samlp:XACMLAuthzDecisionQuery>
```

Response (2)

@ID	SAML: Unique message attribute
@InResponseTo	SAML: Unique attribute of the XACMLAuthzDecisionQuery to which this response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the HM on which the message is offered. MUST match the SAML metadata.
@Consent	Elektronische Toegangsdiensten: MUST NOT be included
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the MR. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the MR for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included
Status	Elektronische Toegangsdiensten: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	Elektronische Toegangsdiensten: MUST contain an assertion about the authorization (see the next section).

Rules for processing responses

A receiving HM:

- MUST verify the structure and contents of the response.

A responding MR MUST:

- The MR MUST communicate the Level of Assurance of the registered authorization. A MR MUST NOT communicate a level for which it is not certified.
  - In case of a chain of authorizations, the MR MUST communicatie the minimum of the LoA of all Representation authorizations in the applicable chain (so far).
  - In case of a request for a portal service, a MR MUST communicate the Level of Assurance as the minimum Level of Assurance of all applicable service authorizations chosen by the user.

Authorization assertion

Assertion	**@Version**	SAML: Version of the SAML protocol. The value MUST be '2.0'.
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the MR. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
	Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the MR for the enveloped assertion.
	Subject	Elektronische Toegangsdiensten: MUST contain a different transient <NameID> from the AD Assertion as received in the Request or preceding MR assertion in case of chain authorization. Each assertion MUST contain a new transient identifier, that is unique for the issuer during at least the past 12 months.
	Conditions	Elektronische Toegangsdiensten: MAY be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. Other conditions MUST NOT be included.
	Advice	Elektronische Toegangsdiensten: MUST be included, containing an AssertionIDRef referencing the Assertion this declaration is directly linked to.
	XACMLAuthz-Decision Statement	Elektronische Toegangsdiensten: MUST contain an SAML Statement of the type XACMLAuthzDecisionStatementType. See below.

XACMLAuthzDecision Statement	**Response**	**Result**	**@ResourceID**	Elektronische Toegangsdiensten: MUST NOT be included
			Decision	XACML: One of the values allowed in XACML 2.0. In the event of a cancellation or error, the element MUST be populated with the value 'Deny'. See also Error handling.
			Status	XACML: must be filled with one of the values that are allowed according to the XACML 2.0 specifications
			Obligations	Obligation urn:etoegang:core:RequireConfirmationFromNextMR FulfillOn=Permit AttributeAssignment urn:etoegang:core:AuthorizationRegistryID = <MR2> (see EntityID) Elektronische Toegangsdiensten: In the event of chain authorization, such is established by the first MR, which then specifies, by means of an Obligation, that the second link MUST be verified or Decision = 'Permit' is otherwise invalid.
	Request		**Subject**	Elektronische Toegangsdiensten: Any received AuthenticationMeansID MUST be deleted and not returned in the response to the HM. If the Decision is 'Permit' THEN Depending on the Rules for processing request: • an ActingEntityID • an ActingSubjectID.EncryptedID@SP • one LegalSubjectID with one or more AttributeValues with an EncryptedID@SP • a LinkedDeclarationSignatureValue

		Resource	Elektronische Toegangsdiensten: MUST contain the attribute-elements contained in the resource element from the request.
			
			If the Decision is 'Permit'
			
			• ServiceID MUST be included as multi-valued XACML attribute
			• ServiceUUID MUST be included as multi-valued XACML attribute
			• LevelOfAssuranceUsed MUST be included. See Level of assurance
			• Depending on the Rules for processing request:
			  ◦ an EntityConcernedID
			  ◦ one or more ServiceRestrictions
			  ◦ an IntermediateEntityID.EncryptedID
			  ◦ one or more Encrypted Attributes
			
			NextAuthorizationRegistryID MAY be included. See EntityID.
			
			Other attributes MUST NOT be included.

		Action	Elektronische Toegangsdiensten: MUST be the same as the Action element in the request. See XACMLAuthzDecisionQuery (above).
		Environment	Elektronische Toegangsdiensten: MUST be empty.

Example message

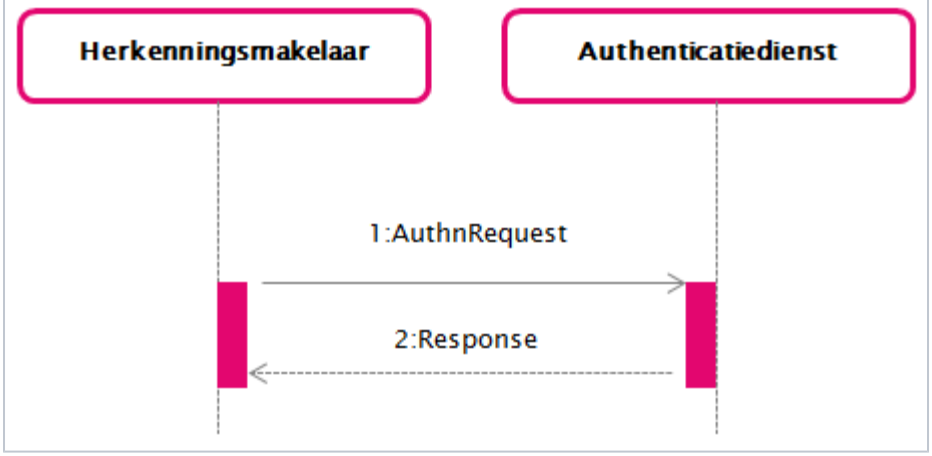
```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " InResponseTo=" " Version="2.0"
IssueInstant=" " Destination=" ">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> </saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI=" ">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue> </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue> </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName> </ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"> </samlp:StatusCode>
    </samlp:Status>
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID=" " IssueInstant=" ">
        <saml:Issuer> </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                <ds:Reference URI=" ">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue> </ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue> </ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName> </ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"> </saml:NameID>
        </saml:Subject>
```

```
        <saml:Conditions NotBefore=" " NotOnOrAfter=" "> </saml:Conditions>
        <saml:Statement xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" xmlns:xsi="
http://www.w3.org/2001/XMLSchema-instance" xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
            <xacml-context:Response xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <xacml-context:Result>
                    <xacml-context:Decision>Permit</xacml-context:Decision>
                    <xacml-context:Status>
                        <xacml-context:StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"> </xacml-
context:StatusCode>
                    </xacml-context:Status>
                </xacml-context:Result>
            </xacml-context:Response>
            <xacml-context:Request xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <xacml-context:Subject>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ActingEntityID" DataType="
http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Subject>
                <xacml-context:Resource>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceID" DataType="http://www.
w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceUUID" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:LevelOfAssurance" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:LevelOfAssuranceUsed" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:1.9:EntityConcernedID:KvKnr"
DataType="http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:ResourceContent>
                        <saml:EncryptedAttribute>
                            <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" Id="
_DE46C6F5E2E3111255D3A715C4760656">
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
                                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                    <xenc:EncryptedKey>
                                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04
/xmlenc#rsa-oaep-mgf1p"/>
                                        <ds:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                                            <ds:KeyName>62355fbd1f624503c5c9677402ecca00ef1f6277</ds:KeyName>
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>.....</xenc:CipherValue>
                                        </xenc:CipherData>
                                    </xenc:EncryptedKey>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>.......</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                        </saml:EncryptedAttribute>
                    </xacml-context:ResourceContent>
                </xacml-context:Resource>
                <xacml-context:Action>
                    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue>Authenticate</xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Action>
```

```
                <xacml-context:Environment> </xacml-context:Environment>
            </xacml-context:Request>
        </saml:Statement>
    </saml:Assertion>
</samlp:Response>
```

Interface specifications HM-AD

Sequence diagram HM-AD



This page describes the messages that are exchanged between an Herkenningsmakelaar (HM) and an Authenticatiedienst (AD) (identity provider).In the interface described here, the use case GUC3 Aantonen identiteit consists of an SAML 2.0 AuthnRequest and Response. The specific content of these messages is described below. Detailed information about the value of fields can be found in Attribute elements.

For eIDAS Outbound, the eIDAS Berichtenservice acts as a DV, and as Dienstbemiddelaar (DB) for the BRP. Any statement in this page about the DV should therefore be interpreted as "DV and/or EB".

A column in a message description that starts with 'SAML' indicates that this is the standard value. A value that starts with 'Elektronische Toegangsdiensten' indicates that the value is specific to Elektronische Toegangsdiensten.

[Rules for processing requests] [Response (2)] [Authentication assertion] [AttributeStatement] [Rules for processing response] [ ] [Determine appropriate ECTA and Identifiers:] [LogoutRequest]

AuthnRequest (1)

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the AD on which the message is offered. MUST match the AD's metadata.
@Consent	Elektronische Toegangsdiensten: MUST NOT be included.
@ForceAuthn	The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the AD MAY use an existing SSO session if one is open.
@IsPassive	Elektronische Toegangsdiensten: MAY be included. If IsPassive is included, the value MUST be 'false'.
@ProtocolBinding	SAML: MUST NOT be included because AssertionConsumerServiceIndex is required in Elektronische Toegangsdiensten.
@AssertionConsumerServiceIndex	Elektronische Toegangsdiensten: This attribute element indicates the URL to which the response must be sent. The value of AssertionConsumerServiceIndex MUST match an index at the assertion consumer service in the HM's metadata.
@AssertionConsumerServiceURL	SAML: MUST NOT be included because AssertionConsumerServiceIndex is required in Elektronische Toegangsdiensten.
@AttributeConsumingServiceIndex	Elektronische Toegangsdiensten: The value MUST be '4'. Indicates that it is about the interface described in this document.
@ProviderName	Elektronische Toegangsdiensten: MAY contain a more detailed description of the provider.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.

Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloping message.
Extensions	Elektronische Toegangsdiensten: MUST contain the attributes IntendedAudience, ServiceID and the corresponding ServiceUUID. If the DV queries additional attributes (via an AttributeConsumingService as described in Interface specifications DV-HM and the DV metadata for HM), they MUST be included here by the HM. To this extent, one Elektronische Toegangsdiensten specific RequestedAttributes (see schema below) element MUST be included containing the RequestedAttribute elements reflecting the DV's request. The requested attribute(s) MUST be defined in the Attribuutcatalogus and MUST be declared as RequestedAttribute in the Service catalog entry for the requested service. An AD not able to provide these attributes MUST act as specified in the alternative use case described in Attributen niet leverbaar of niet toegestaan. Other XML attributes MUST NOT be included. Other elements MUST NOT be included.
Subject	Elektronische Toegangsdiensten: MUST NOT be included
NameIDPolicy	Elektronische Toegangsdiensten: MUST NOT be included.
Conditions	Elektronische Toegangsdiensten: MUST NOT be included.
RequestedAuthnContext	Elektronische Toegangsdiensten: MAY contain an attribute Comparison='minimum' and an element AuthnContextClassRef that contains the minimum Level of assurance required by the DV. When RequestedAuthnContext is included in the request, then it must contain a Level of assurance (AuthnContextClassRef) equal to or lower than the level of assurance included in the Service catalog for the requested service.
Scoping	Elektronische Toegangsdiensten: MUST NOT be included

XML schema saml protocol extensions

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:etoegang:1.9:samlp-extension"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:element name="RequestedAttributes">
          <xs:complexType>
               <xs:sequence>
                    <xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
               </xs:sequence>
          </xs:complexType>
     </xs:element>

</xs:schema>
```

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:esp="urn:etoegang:1.9:samlp-extension"
    ID="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
    Destination="https://..."
    ForceAuthn="true"
    AssertionConsumerServiceIndex="1"
    AttributeConsumingServiceIndex="4"
    ProviderName="DV Name"
    IssueInstant="2015-04-10T12:30:03Z"
    Version="2.0">
    <saml:Issuer/>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference URI="#_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Extensions>
                <saml:Attribute Name="urn:etoegang:core:IntendedAudience">
            <saml:AttributeValue>urn:etoegang:DV:...:entities:...</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceID">
            <saml:AttributeValue>urn:etoegang:DV:...:services:...</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:AttributeValue>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:AttributeValue>
        </saml:Attribute>
        <esp:RequestedAttributes>
            <md:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" IsRequired="false" />
        </esp:RequestedAttributes>
    </samlp:Extensions>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Rules for processing requests

A requesting HM:

- MUST propagate @ProviderName of the party initiating the Request.

A receiving AD:

- MUST verify a requested service is defined in the Service Catalog and requested accordingly.
- MUST sanitize @ProviderName to remove any script or formatting before displaying.
- In case of Dienstbemiddeling (service intermediation), MUST verify the Dienstbemiddelaar (Service Intermediary) is still authorized by the Dienstaanbieder (Service Supplier) by verifying the authorization status of the mediated service in the Service Catalog.
- The AD MUST determine the branding to be used.
    - If IntendedAudience is eIDAS Berichtenservice, use eIDAS Outbound branding as described in Richtlijnen communicatie eIDAS.
    - Else, base the branding on the information elements listed in the table below.

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

* Citizen: r1.12 only EU-citizens via eIDAS BerichtenService

- The AD MUST process the ActingSubjectTypesAllowed list AND the EntityConcernedID:Pseudo.

If one of the criteria is not met, the AD MUST handle this as a non-recoverable error (see Error handling).

Note: When an AD specifies a MR for the HM to use as the next hop, the AD may only specify a MR of the same version.

Response (2)

@ID	SAML: Unique message characteristic.
@InResponseTo	SAML: Unique attribute of the AuthnRequest for which this response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the HM on which the message is offered. MUST match the HM's metadata.
@Consent	Elektronische Toegangsdiensten: MUST NOT be included.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the AD. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the AD for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included
Status	Elektronische Toegangsdiensten: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	Elektronische Toegangsdiensten: MUST contain an assertion about the authentication (see the next section).

Example AD Response

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    Destination="https://..."
    ID="_62619615-e452-47d3-a44b-93da2d5a76f9"
    InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_62619615-e452-47d3-a44b-93da2d5a76f9">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de" IssueInstant="2015-04-10T11:16:28Z" Version="
2.0">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:AD:...</saml:Issuer>
        ....
    </saml:Assertion>
</samlp:Response>
```

Note: the above example only provides the response. The response will be sent via an Artifact binding.

Authentication assertion

Assertion	**@Version**	SAML: Version of the SAML protocol. The value MUST be '2.0'
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the AD. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
	Signature	Elektronische Toegangsdiensten: MUST be included
	Subject	Elektronische Toegangsdiensten: MUST contain a <NameID> with a Transient ID. A SubjectConfirmation element that meets the Web Browser SSO profile MUST be included. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.

	Conditions	Elektronische Toegangsdiensten: MUST be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. An Audience element in the AudienceRestriction element that meets the Web Browser SSO profile MUST be included. Other audience elements MUST include relevant parties: EntityIDs of the requesting DV and the MR/KR/HM (if applicable) to whom the assertion will be targeted. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV:<*OIN*>' is to be used. Note that for eIDAS Outbound, the eIDAS Berichtenservice has the role of Dienstverlener. So the notation of the EntityID is identical as for the DV (with ROLE "DV" and not "EB"). Other conditions MUST NOT be included.
	Advice	Elektronische Toegangsdiensten: MUST NOT be included
	AuthnStatement	Elektronische Toegangsdiensten: The attribute AuthnInstant MUST contain the time of authentication. The AuthnContext element MUST contain an AuthnContextClassRef element containing the level of assurance at which authentication took place and an AuthenticatingAuthority element containing the OIN format of the KvK number of the AD. In the case of proxying, AuthenticatingAuthority element MUST be populated with a unique identifying attribute for the party that carried out the authentication. Other attributes and elements MUST NOT be included.
	Optional Attribute-Statement	Elektronische Toegangsdiensten: MUST be included if StatusCode is 'Success'. MUST NOT be included otherwise. In case of representation: • ActingSubjectID (EncryptedID@MR) with the internal pseudonym of the acting user MUST be included. • IF an additional ActingSubjectID is requested by the EB in the servicecatalog, the ASTA will be Encrypted for the EB (as an EncryptedID@EB) and MUST contain all identifiers in ASTA-set as described in the service catalogue for the service. • If the ASTA-set can not be delivered by the AD, the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details.

AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

Element /@Attribute	0..1	Description

Attribute	0..n	Depending on Rules for processing request:
		
		• MUST include:
		  • ActingSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier of the acting (natural) person for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).
		  • LegalSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier(s) of the ServiceConsumer for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).
		  • ServiceID - multi-valued SAML-attribute
		  • ServiceUUID - multi-valued SAML attribute
		• MAY include:
		  • AuthorizationRegistryID (see EntityID).
		
		Other Attribute elements MUST NOT be included.

EncryptedAttribute	0..n	Depending on Rules for processing request • Additional attributes MAY be included here only IF the StatusCode is 'Success'. Other EncryptedAttribute elements MUST NOT be included.

Rules for processing response

A responding AD:

Identifiers:

- MUST include a transient identifier as a <NameID> in Subject; see Linking of Assertions.
- MUST encrypt any other identity according to the rules specified in SAML encryption and added as Attribute in the AttributeStatement.
- MUST ensure that a user consents to authentication for:
    - the ServiceProvider,
    - ServiceName
    - (optional/if applicable) "@ProviderName"
    - Personal attributes and/or BSN of the ActingPerson FOR the Intermediated Service and/or Intermediating Service

- MUST ensure only to provide a BSN to receipients on the BSN AutorisationList otherwise respond with a non-recoverable error. See Error handling for more details
- MUST determine appropriate identity(s) according to Determine appropriate ECTA and Identifiers:
- In case of no representation:
    - An AD MUST include all appropriate (ECTA) identifiers of the acting user for the DV in ActingSubjectID, as described in the service catalogue for the service
    - If an AD can not provide any of these requested ECTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Representation
    - An AD MUST include the internal pseudonym of the acting user for the MR in ActingSubjectID
    - If additional ASTA-identifiers are requested by the EB (in the ServiceCatalog) then an AD MUST include all appropriate ASTA-identifiers of the acting user for the DV* in ActingSubjectID, as described in the service catalogue for the service
        - ActingSubjectID MUST contain an EncryptedID encrypted only for the receiving DA/DB that requested the specific ASTA. The recipient of the ASTA for the DA and DB SHOULD be taken from the IntendedAudience element in the request.
            - In case of a DA for whom only the OIN is known, the notation 'urn:etoegang:DV:*<OIN>*' is to be used as recipient.
    - If an AD can not provide any of these requested ASTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Service Intermediation
    - An AD MUST ensure ServiceProvider is authorised to use service intermediation as stated on the list AllowedForServiceIntermediation IF the AD does not want to use the service catalog to determine that the ServiceProvider is authorised to intermediate the intermediated service
    - If the AD does configure the AllowedForServiceIntermediation list locally, An the AD MUST use the ServiceCatalog to determine that the ensure ServiceProvider is authorised to intermediate the intermediated service as stated in the ServiceCatalog
    - An AD MUST add ASTA- and ECTA-identifiers for the intermediated service as stated in the ServiceCatalog using the same above processing rules as for the DV
- IF non-representation AND NOT service intermediation THEN MUST include the appropriate identity(s) of the user for the Dienstverlener (DV) as an <EncryptedID> in ActingSubjectID
- IF non-representation AND service intermediation THEN MUST include the appropriate identity(s) of the user for both Dienstverleners (DienstBemiddelaar (DB) and Dienstaanbieder (DA)) as an <EncryptedID> in ActingSubjectID

Reference implementation processing rules for Identities

- DV.ServiceProviderID = ServiceCatalog(request.ServiceUUID).ServiceProviderID
- DV.IntermediatedService = ServiceCatalog(request.ServiceUUID).IntermediatedService
- DV.ASTA-sets = ServiceCatalog(DV.ServiceUUID).ActingSubjectTypeAllowed
- DV.ECTA-sets = ServiceCatalog(DV.ServiceUUID).EntityConcernedTypeAllowed
- IF non-representation THEN
    - Determine approperiate.Identities (DV.ECTA-sets, DV.ServiceProviderID, DV.Type)
    - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- IF representation THEN
    - MUST include Internal pseudonym of the user for the appropriate MachtigingRegister as an EncryptedID@MR in ActingSubjectID
    - IF DV.ASTA-sets THEN
        - Determine appropriate.Identities (DV.ASTA-sets, DV.ServiceProviderID, DV.Type)
        - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- **# ico Service Intermediation via service-catalog, DB authorization must be checked in service catalog**
- **IF DV.IntermediatedService AND DV.ServiceProviderID IS IN Config(AllowedForServiceIntermediation) THEN**
    - **DA.ServiceUUID = DV.IntermediatedService**
    - **DA.ServiceProviderID = ServiceCatalog(DA.ServiceUUID).ServiceProviderID**
    - **DA.@intermediationAllowed = ServiceCatalog(DA.ServiceUUID).@intermediationAllowed**
    - **DA.ServiceIntermediationAllowed = ServiceCatalog(DA.ServiceUUID).ServiceIntermediationAllowed**
    - **DA.ASTA-sets = ServiceCatalog(DA.ServiceUUID).ActingSubjectTypeAllowed**
    - **DA.ECTA-sets = ServiceCatalog(DA.ServiceUUID).EntityConcernedTypeAllowed**
    - **IF DA.@intermediationAllowed = “generalAvailable” OR (DA.@intermediationAllowed = “requiresApproval” AND DV. ServiceProviderID IS IN DA.ServiceIntermediationAllowed) THEN**
        - **IF non-representation THEN**
            - **Determine approperiate.Identities (DA.ECTA-sets, DA.ServiceProviderID)**
            - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**
        - **IF representation AND DA.ASTA-sets THEN**
            - **Determine appropriate.Identities (DA.ASTA-sets, DA.ServiceProviderID)**
                - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**

Determine appropriate.Identities for (ECTA- or ASTA-) Sets for Recepient (DV of DA)

DetermineAppropriateIdentifiers (sets, Recipient.ServiceProviderID)

- GROUP ecta/acta-sets BY setNumber in sets
- ORDER sets ASSENDING BY setNumer

- FOR EACH set IN sets
    - # check IF all IdentityTypes in set can and may be provided for het user
    - FOR EACH IdentifierType IN set
        - IF IdentifierType=BSN AND Recipient.ServiceProviderID NOT on the BSN AutorisationList THEN respond with a unrecoverable error (Attributes not supported). See Error handling for more details.
        - IF IdentifierType can not be provided for this user THEN next set
    - # all IdentifierTypes are checked, current Set = *appropriate* set
    - # Add the Identifiers of the user for all IdentifierTypes (Identificerende kenmerken) in the *appropriate set to appropriate.Identities*
    - FOR EACH IdentifierType IN set
        - appropriate.Identities[IdentifierType] = IdentifierValue of IdentifierType for the user and Receipient combination
    - RETURN appropriate.Identities
- # No appropriate Set can be provides for this user - start error handling
- respond with a recoverable error (Attributes not supported). See Error handling for more details.

Note: At this moment the use of ASTA-sets and Service Intermediarion is limited to the EB for eIDAS Outgoing.

Attributes:

- MUST include additional attributes as an AttributeStatement.EncryptedAttribute that are requested by the DV (Dienstaanbieder /DienstBemiddelaar) as specified in the Service catalog and consented by the user.
- IF required attributes cannot be provided (because of consent of not available) MUST act according to UC on not providing Attributes (see Attributen niet leverbaar of niet toegestaan) : stop the authentication flow and start error flow.
- MUST encrypt attributes according to the rules specified in 3. SAML encryption and added as an Encrypted Attribute in the AttributeStatement.
- MUST ensure user consent according to rules of the Attribute Policy (see Attributenbeleid)
- MUST ensure that only attributes are provided that are listed for the requested service in the service catalog
- If additional required atributes are requested by the DV (in the HM-request) then an AD MUST include these Attributes
- If an AD can not provide a requested required atttributes the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- If additional optional atributes are requested by the DV (in the HM-request) then an AD SHOULD include these Attribute

---

Reference Implementation of Processing Rules for Attributes

- IF Request.RequestedAttributes THEN
    - FOR EACH attribute IN Request.RequestedAttributes
        - attribute.isRequired = **ServiceCatalog(DV.ServiceUUID).RequestedAttribute[attribute].isRequired**
        - IF attribute available AND user-consent THEN MUST
            - include attribute as EncryptedAttribute@DV with a unique Encrypted_DATA_ID that is the same as the attribute name in the attribute catalogue (e.g. urn:etoegang:1.9:attribute:FirstName).
        - ELSE IF attribute.isRequired THEN respond with a recoverable error). See Error handling for more details.

LevelOfAssurance:

- An AD MUST include the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied.
- MUST include the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied. An AD MUST NOT include a level for which it is not certified.

Determine appropriate ECTA and Identifiers:

- all the EntityConcernedTypes in an Identifier Set of EntityConcernedTypes with the same set number in the Service catalog.
- IF no set numbers are used, only one EntityConcernedType is allowed THEN handle this EntityConcernedType as if it was in 1 set.
- all the EntityConcernedTypes in the identifier set with the lowest possible set number the AD/MR can provide for this response. LegalSubject.
- IF AD/MR can't provide for any Identifier Set THEN start Error Handling
- Determine the response.EntityConcernedTypes and the corresponding response.LegalSubject.Identifiers for the selected identifier set.
- For ECTA=BSN the applicable service provider MUST be listed on the BSN Autorisation List OTHERWISE start Error Handling

Example attribute after decryption

```
<saml:Attribute Name="urn:etoegang:1.9:attribute:FirstName"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:attrext="urn:oasis:names:tc:SAML:attributes:ext"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    attrext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:NLWID"
    attrext:LastModified="2015-03-31T12:00:00Z">
    <saml:AttributeValue xsi:type="xs:string">...</saml:AttributeValue>
</saml:Attribute>
```

Example AD Assertion - representation

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:EncrypedID>
            <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                Type="http://www.w3.org/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                        URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                Recipient="urn:etoegang:MR:...">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                </xenc:EncryptionMethod>
                <ds:KeyInfo>
                    <ds:KeyName>...</ds:KeyName>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                </xenc:CipherData>
                <xenc:ReferenceList>
                    <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
```

```
                </xenc:ReferenceList>
            </xenc:EncryptedKey>
        </saml:EncrypedID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:MR:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>true</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:MR:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>...</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>

 </saml:AttributeStatement>

</saml:Assertion>
```

Example AD Assertion - citizen domain

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-961e-
cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:KR:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:KR:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
```

```
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>...</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

Example AD Assertion - consumer domain

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-961e-
cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
```

```
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:DV:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>...</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>

        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_FirstName" Type="http://www.w3.org
/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
                    ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>
        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_18OrOlder" Type="http://www.w3.org
/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
                 ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>
```

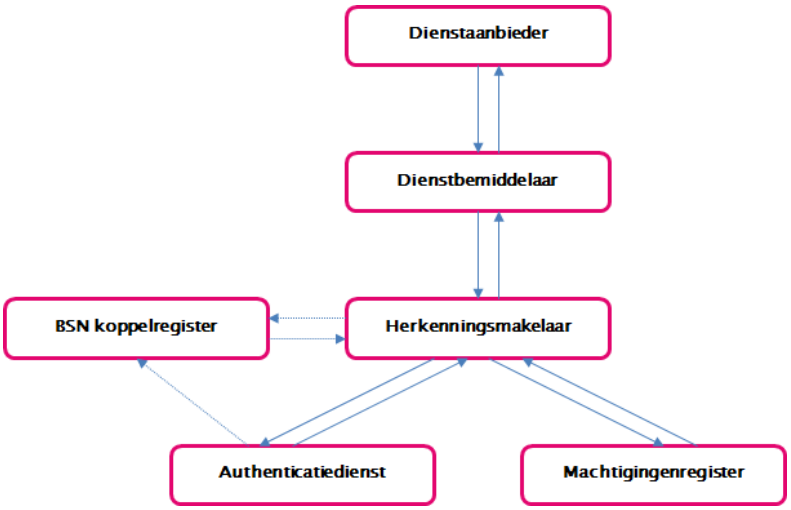
```
    </saml:AttributeStatement>
</saml:Assertion>
```

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied on the understanding that the logout message is sent to the AD through the HM. The interface for this message is described below.

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the AD on which the message is offered.
NameID	Elektronische Toegangsdiensten: MUST contain a NameID element, this MUST NOT contain the Internal pseudonym or Specific pseudonym of the user.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloped message.

Interface specifications DB-DA



This paragraph describes the (guidelines for) interface(s) between the Dienstbemiddelaar (DB) (Service Intermediary) and the Dienstaanbieder (DA) (Service Supplier). The interface between a DB and a DA is considered a machine to machine interface. The implementation details of this interface will always be specified by the Dienstaanbieder. In order to facilitate adoption, Elektronische Toegangsdiensten aims to deliver an Authorization Solution compatible not only with green field implementation, but also with existing services as already consumed in the field today. Thus to be interoperable with the wide variety of implementations that exist. Therefore the machine to machine interface will not specify a technical or protocol specific implementation but rather a set of principles, concepts and requirements. Currently, a reference for the interface DB-DA based on SOAP WebsServices is provided. In a future version these design principles will be further illustrated by including several other reference architectures of common service implementations, and how they map with these specifications and principles.

Concerning association of the Authorization Token with the Service-Request.

Elektronische Toegangsdiensten-Declarations can be used to ‘add’ security (more precise authorization) to a message by applying them as Authorization /Security Tokens. To be considered valid Authorization tokens, these declarations have to conform to certain conditions. These conditions concern the concepts of ‘meaningful consent’ and the proof of this consent (to establish ‘non-repudiation’).
With meaningful consent we mean that the user has to reach a well informed conscience decision concerning whether or not to consume the service. For transactions with high juridical or legal consequences the process to establish this ‘well informedness’ will have to meet higher standards than for user actions with a lower impact. For example, accessing relative harmless information like ‘last time visited’, might require a very implicit informedness like ‘You are logging on to ..’. However, transactions for services with significant implications will require a more formal 'informedness' and might even require independent Signature Services.

When the user has reached an informed decision, **non-repudiation** about this decision has to be achieved. The preferred way to achieve this is to associate;

1. **the Elektronische Toegangsdiensten-Declarations,** with
2. **the specific Request message used to consume the service,** and
3. **the means on how this request message has been established/constructed**
   In a reliable, provable and accountable way.

The Elektronische Toegangsdiensten-Declarations give insight in who is consuming the service, on whose behalf, including information which the Dienstaanbieder can use to conduct its authorization decision.
The specific Request message used to consume the service conforms to the input for the (web) service as specified by the Dienstaanbieder, and therefore does not have to be in a human readable form. This technical message however, should be no more than a perfect transformation of a users intended action into a format as understood by the Dienstaanbieder.

This ‘service’/intended users action could be anything i.e. ‘logging on’, ‘retrieving last time visited’, ‘declare taxes’, ‘request permit’, ‘retrieve information from a portal’ etc. The transformed technical message could be anything from a specific SOAP or REST message, to PDF or ByteArray etc.

The means on how this request message has been established/constructed should be present to provide a provable and accountable link between the first 2 pieces of information; the user and its intended user action, and the resulting technical translation used to consume the service.

The above results in the following requirements:

- A DA MUST provide clear, non-ambiguous documentation for the technical interface for a Service to a DB, to allow proper implementation by the DB.
- A DB MUST make an exact transformation of the user's input and intend into the technical messages sent to the DA. A DB MUST make an exact transformation of the DA's response to the user as well.
- A DB MUST get the user's explicit consent and approval before sending the messages to the DA.
- A DB will receive the identifying attribute of the user; the DB MAY use this identity to verify that the user for approving/sending the request to the DA is the same as the user that prepared the request, in case such a business case or security requirement exists for the service.
- A DB MUST send the Elektronische Toegangsdiensten declarations along with the request to the DA. This MUST be verbatim copies, so that digital signatures are not affected.

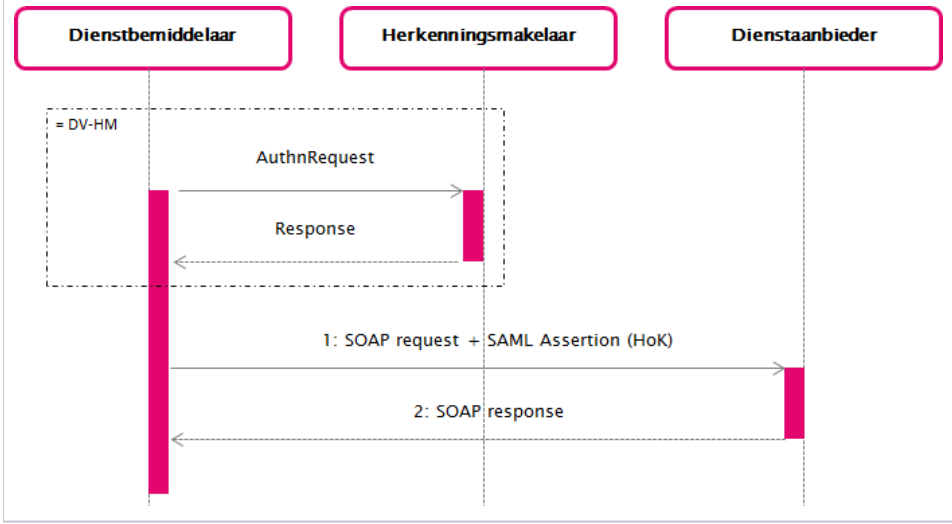
- A DA MUST verify the Elektronische Toegangsdiensten declarations before processing a message and using the identity in its authorization decision.

The DA and DB MUST ensure that security of the interface DB-DA is appropriate for the security needs and risk profile of the service. The security of the interface DB-DA SHOULD ensure confidentiality, integrity and mutual authentication of the communication. It is therefore recommended that:

- Communication between DB and DA SHOULD use a Secure connection or a communication method with at least equivalent security properties.
- A DB SHOULD send the technical messages with all applicable Elektronische Toegangsdiensten declarations, bound together through a digital signature to safeguard integrity and authenticity – both at transmission and for audit purposes afterwards – and as declaration of following the requirements for this interface for the request. The digital signature SHOULD have the same cryptographic strength as specified in Digital signature or a method with at least equivalent security properties.
- A DA SHOULD verify the digital signature of the DB.
- An interface between DA and DB MAY follow one of the reference architectures, these have been verified to fulfil the technical requirements above.

Reference Architecture DB-DA SOAP

DB-DA sequence diagram



This paragraph describes a reference architecture and specification of Interface specifications DB-DA, for use with a machine-to-machine interface using WebServices (SOAP).

This reference architecture describes the interface offered by a Dienstaanbieder (DA)(Service supplier) for use with a Dienstaanbieder (DA) (service intermediary), in case of a Webservice interface based on SOAP in a Dienstbemiddeling use case. By nature, the exact interface specification and its contents depend on the service(s) offered and are specific for its context.

The generic reference architecture for such SOAP WebService with Dienstbemiddeling is described as:

- The DA provides a service interface defined as a documented API, using a WSDL to define the service interface.
- The DB requires recognition of the user, using Interface specifications DV-HM to request the applicable service with Dienstbemiddeling in the Service catalog.
- The DB calls the service confirm this WSDL, adhering to Interface specifications DB-DA.
- The DB provides the Elektronische Toegangsdiensten declarations, by adding the Assertion obtained from the HM as a SOAP-header.
- The DB signs the SOAP-body (or all requests elements thereof) and the Assertion using a WS-Security Signature valid for the DB's own signing certificate.
- The DA verifies upon receipt the SOAP-headers with the signature and Assertion before processing the message. The verification MUST validate the assertion (see processing rules in Interface specifications DV-HM) and the signature.

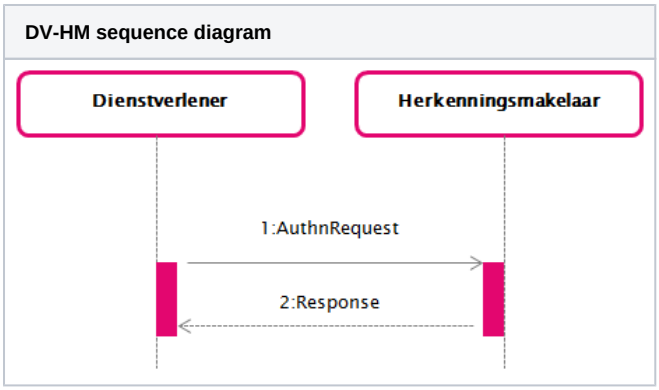
A practical implementation for providing the Assertion and a signature can be done as described in WS-Security SAML Token profile for the holder-of-key Subject Confirmation Method. Next to the SAML token, a WS-Security Signature (can be based on the WS-Security X509 token profile) over the SAML Assertion ***and*** SOAP Body is present to associate the Elektronische Toegangsdiensten Declaration with the request body. The example below is based on these specifications.

Example DB-DA SOAP-request

```
<?xml version="1.0"?>
<soap:Envelope xmlns:soap="..." xmlns:wsse="..." xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:
ds="..." xmlns:wsu="...">

  <soap:Header>

    <wsse:Security>

      <!-- eToegang SAML Assertion applicable to SOAP-request, authenticating the user -->
      <saml:Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc" IssueInstant="2016-02-05-17T10:06:02Z">
        <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
        <!-- Signature over assertion by HM -->
        <ds:Signature>
          ...
        </ds:Signature>
        <saml:Subject>
          <saml:EncryptedID NameQualifier="..." Format="">...</saml:EncryptedID>
          <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_52B816C631C564BACF59E758CBA91718" NotOnOrAfter="2016-
```

```
02-05T10:11:48Z" Recipient="https://..."/>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2016-02-05T10:06:03.173Z" NotOnOrAfter="2016-02-05T10:11:33.173Z"/>
        <saml:AttributeStatement>
          ...
        </saml:AttributeStatement>
      </saml:Assertion>

      <!-- WS-Security Signature by DB over SOAP-Body and eToegang SAML Assertion, to associate message and
assertion and proof authenticity  -->
      <ds:Signature>
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <!-- Signature covers SOAP-body: -->
          <ds:Reference URI="#MsgBody">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
          <!-- Signature covers eToegang SAML Assertion: -->
          <ds:Reference URI="#_a75adf55-01d7-40cc-929f-dbd8372ebdfc">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference>
            <ds:X509IssuerSerial>
              <ds:X509IssuerName>CN=...,...,O=...,C=NL</ds:X509IssuerName>
              <ds:X509SerialNumber>...834756978854956...</ds:X509SerialNumber>
            </ds:X509IssuerSerial>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>

    </wsse:Security>

  </soap:Header>

  <soap:Body wsu:Id="MsgBody">

    <!-- Actual SOAP-request from user to DA -->
    <MyRequest xmlns="...">
      <RequestDetails>...</RequestDetails>
      ...
    </MyRequest>

  </soap:Body>

</soap:Envelope>
```

Interface specifications DV-HM



This page describes the messages for the interface specification between a Dienstverlener (DV) (service provider) and an Herkenningsmakelaar (HM) (broker).

For eIDAS Outbound, the eIDAS Berichtenservice acts as a DV, and as Dienstbemiddelaar (DB) for the BRP. Any statement in this page about the DV should therefore be interpreted as "DA (BRP) and/or EB".

The interface specification described in this document is used to implement the use case GUC1 Gebruiken eToegang als dienstafnemer (Use eToegang as service consumer) and MUST (with the exception of alternative Bindings) be implemented by every Herkenningsmakelaar and offered to their customers, the DVs. This is in order to prevent lock-in and enables middleware suppliers to write generic code that can be used by all Herkenningsmakelaars.

In the interface described here, the use case GUC1 Gebruiken eToegang als dienstafnemer is populated with an SAML 2.0 AuthnRequest and Response.

The specific contents of these messages is described below. A column in a message description that starts with 'SAML:' indicates that this is a standard value within the official SAML specification. A value that starts with 'Elektronische Toegangsdiensten' indicates that the value is specific to Elektronische Toegangsdiensten.

[AuthnRequest (1)] [Rules for processing requests] [Response (2)] [HM Summary assertion] [AttributeStatement] [Rules for processing responses] [LogoutRequest] [ProvideKeyMaterial]

AuthnRequest (1)

This section describes regular Authentication Requests.

Element/@Attribute	0..n	Description
@ID	1	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the request.
@Destination	1	SAML: URL of the HM on which the message is offered. MUST match the HM's metadata.
@Consent	0..1	Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
@ForceAuthn	0..1	Elektronische Toegangsdiensten: The value 'true' indicates that an existing single sign-on session MUST NOT be used for the request in question. If the value is 'false' or empty or the specification is missing, the AD MAY use an existing SSO session if present.
@IsPassive	0..1	Elektronische Toegangsdiensten: MAY be included. If IsPassive is included, the value MUST be 'false'.
@ProtocolBinding	0..1	SAML: Specifies the used binding. MUST only be used when an *@AssertionConsumerServiceURL* is used, MUST NOT be used in combination with an *@AssertionConsumerServiceIndex*.
@AssertionConsumerServiceIndex	0..1	

		Elektronische Toegangsdiensten: This attribute element specifies the URL to which the HM sends the response for the DV. If present this index MUST refer to an endpoint of an AssertionConsumerService in the DV metadata for HM. MUST NOT be present if *@AssertionConsumerServiceURL* is present. If neither *@AssertionConsumerServiceIndex* or *@AssertionConsumerServiceURL* is present, the HM MUST send the response to the endpoint in the metadata that is marked with 'isDefault=true'
@AssertionConsumerServiceURL	0..1	SAML: If present, URL MUST point to a SAML endpoint acknowlegded in the DV metadata for HM . If present, the participant MUST check whether the *@AssertionConsumerServiceUrl* is included in the DV's DV metadata for HM. If it is not included in the metadata, the participant MUST reject the message with the status code RequestDenied. MUST NOT be present if *@AssertionConsumerServiceIndex* is present.
@AttributeConsumingServiceIndex	0..1	SAML: If present, MUST refer to an AttributeConsumingService in the DV's metadata. If absent, the AttributeConsumingService marked as default in the DV metadata for HM SHOULD be used. The AttributeConsumingService MUST contain exactly *one* attribute with a name that is the same as a long formatted ServiceID. The AttributeConsumingService MAY contain attributes to be requested. Multiple AttributeConsumingService elements MAY be present in the DV metadata for HM and can be mapped to the same ServiceID. This allows DVs to request authentication for a single service with varying attributes depending on the context. The union of all attributes that may be queried for a ServiceID MUST be declared in the Service Catalog. An application that cannot pass an AttributeConsumingServiceIndex can now retrieve different services and/or attribute contracts by exchanging metadata between different EntityIDs.
@ProviderName	0..1	Elektronische Toegangsdiensten (DV): MAY contain a more detailed description of the service, complimentary to the entry in the service catalog Elektronische Toegangsdiensten MAY NOT contain personally identifiable information
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the DV.
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the DV for the envelopping message.
Extensions	0	Elektronische Toegangsdiensten: MUST NOT be included.
Subject	0	Elektronische Toegangsdiensten: MUST NOT be included.
NameIDPolicy	0	Elektronische Toegangsdiensten: MUST NOT be included.
Conditions	0	Elektronische Toegangsdiensten: MUST NOT be included.
RequestedAuthnContext	0..1	Elektronische Toegangsdiensten: MAY be used to explicitly request a specific LoA. If specified, the HM summary response will communicate the detailed LoA, rather than SAML 'unspecified'. If present it MUST be used to request a *equal to or lower than the level of assurance* specified in the Service catalog. A lower LoA can for instance be used in requests to allow read-only access to services. If RequestedAuthnContext is absent, then the request will be further processed, using the Level of assurance (AuthnContextClassRef) as specified in the service catalog for the requested service.
@Comparison	1	MUST use the value 'minimum'.

AuthnContextClassRef	1	MUST be one of the following requested Level of assurance.
Scoping	0..1	Elektronische Toegangsdiensten: MUST be included in case an AD is pre-selected by the user at the DV, MUST NOT be included otherwise.
IDPList	1	MUST be present in case of pre-selection of an AD.
IDPEntry	1	MUST be present in case of pre-selection of an AD.
@ProviderID	1	EntityID of the AD selected by the user.
@Name	0	MUST NOT be present.
@Loc	0..1	In case an AD has multiple endpoints in the Network metadata, the endpoint selected by the user MUST be provided.

Rules for processing requests

A requesting DV:

- MUST sign the <AuthnRequest>.
- MUST request a serviceID that is listed for that ServiceProvider itself in the Service Catalog. Requesting services of other Service Providers is not allowed. A Dienstbemiddelaar (DB) (Service Intermediary) can intermediate another service, if permitted by the Dienstaanbieder (Service Supplier), by indicating this in the Service Catalog (@IntermediatedService in ServiceInstance).
- MAY use the *@AttributeConsumingServiceIndex* to reference the service (as specified in the metadata).
- MAY use the <RequestedAuthnContext> to indicate a requested level of assurance, optionally lower than the LoA listed in the Service Catalogue for the requested Service.
  NB. Using the <RequestedAuthnContext> indicates the DV can accept/process the LoA in the <AuthnContextClassRef> in the response as well. (NB. this may restrict out-of-box-processing by appliances!)
- MAY pass AD pre-selected for authentication. In this case:
  - the DV MUST use an authentic list (signed by BO/HM) of accredited ADs. The list SHOULD be updated at least once every 15 minutes, the list MUST NOT be older than 30 minutes.
  - the DV MUST show the OrganizationDisplayName of all valid, applicable ADs, in alphabetic order and equal appearance. Applicable means an AD supporting at least a LevelOfAssurance equal to or greater than the minimum requested level of assurance and the requested NameIDFormat(s) (=EntityConcernedType). The OrganizationDisplayName MUST be taken from the beforementioned list of accredited ADs, which MUST contain an exact copy from the Network metadata.
    - In case of a Portal request the eIDAS-berichtenservice MUST NOT be offered in the list of AD's to be selected.
    - If eIDAS-inbound is supported for the service, the eIDAS-berichtenservice MUST be displayed as a separate option / brand for authentication, next to eHerkenning. The EB MUST NOT be part of the eHerkenning AD list.

    - In case of multiple OrganizationDisplayNames: if a user-specified preference or user interface language is available, the DV MUST present the OrganizationDisplayName with a matching LanguageQualifier; else if an OrganizationDisplayName with LanguageQualifier "nl" is present, this Dutch OrganizationDisplayName MUST be displayed; else if an OrganizationDisplayName with LanguageQualifier "en" is present, this English OrganizationDisplayName MUST be displayed; else, the first OrganizationDisplayName with a different LanguageQualifier MUST be displayed.
  - the DV MUST show the logo of the applicable brand of the service classifier specified by the DV:

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

  * Citizen: r1.12 only EU-citizens via eIDAS BerichtenService
- in case an AD has multiple endpoints (SingleSignOnService elements): the user MUST be allowed to select one of the endpoints, based on the eme:name attribute of applicable SingleSignOnService endpoints, by listing an AD multiple times with the eme:name appended.
- Additionally a DV MUST present A separate "eIDAS" login option , to opt for the eIDAS-berichtenservice as an AD for login with an eIDAS-authentication scheme from another eIDAS-member state:
  - The Dienstverlener MUST use the Richtlijnen communicatie eIDAS to present the eIDAS. Berichtenservice to the user.
  - The Dienstverlener MUST use the EntityID to refer to the EB in the AuthnRequest to the HM.

        - Since this reference is static, a Dienstverlener is not bound to honour the update requirements of a refresh atleast once every 15 minutes as mentioned above.
        - When presenting "eIDAS" link/button the "eHerkenning" button MAY also be presented by the DV to allow access to the full list of regular ADs as specified above.
    - A DV MAY offer the user to save the selection of the AD as default, except for eIDAS. However, if an error occurs when authenticating at a user-preselected default AD, the DV MUST retrieve a current list of accredited AD's from the HM and prompt the user to choose an AD.
    - The ASTA's MUST NOT be requested by DV's, ONLY the EB and BRP MAY request ASTA's

A responding HM:

- MUST only process requests from contracted DVs.
- MUST validate all signatures to be valid before further processing any request. Message (elements) MUST be signed using a certificate as listed in the DV Metadata for HM for the purpose of signing for a SPSSODescriptor of the requesting DV.
- MUST verify the structure and contents of the request.
- MUST request authentication, authorization, sectorIDs and attributes on behalf of the DV, as applicable to the requested Service and User's choices.
- In case of service intermediation the HM MUST verify the Service Intermediary is still authorized by the Dienstaanbieder (DA) (Service Supplier) by verifying the authorization status of the mediated service (@intermediationAllowed) in the Service Catalog.
- MUST support the IDPEntry element from the Scoping element in the AuthnRequest. In case the element Scoping is present, the HM MUST use the IDPEntry as reference for the AD selected by the user, bypassing the AD-selection page (applying use case GUC1-alt and GUC3-alt).
- MUST verify the chosen AD and optional endpoint provided in the IDPEntry element reference a valid AD/EB as listed in the Network metadata.
- MUST sanitize @ProviderName to remove any script or formatting before displaying
- MUST determine the branding to use based on the service classifier specified by the DV.

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

* Citizen: r1.12 only EU-citizens via eIDAS BerichtenService

If one of the criteria is not met, the HM must handle this as a non-recoverable error (see Error handling).

Note: When a HM receives a DV request on a specific version of the DV-HM interface, it should only show AD's that list eme:version in the Metadata with the same, or higher version.

Note: When a HM receives a response from an AD, and the AD specifies an MR that is not of the same version, the HM must handle this as a non-recoverable error.

- In case a portal service request is made at the eIDAS-berichtenservice, the HM MUST return a error message containing ResultMajor "RequesterError" and ResultMinor "NotSupported"

With regards to determining the user's choice of AD/MR, the following processing rules apply;

- A HM MAY maintain user preferences (selected AD and MR, and 'Representation' use), except for eIDAS-inbound requests, and use these values for determining applicable AD/MR queries, else;
- When the EntityConcernedTypesAllowed for the requested service signify a representation scenario (i.e. KVK, RSIN etc.), the HM MUST NOT query the user if it wants to authenticate on behalf of himself or another.
    - In such a scenario a HM MAY opt to only offer a selection list for AD's (GUC3 Aantonen identiteit). This facilitates the current common practice that the AD already knows the MR so that the user will not be confronted with a potential confusing new choice to make whilst this information is already known within the scheme. (However this does invoke the possibility that AD will be confronted with lacking logistic information; see processing rules HM-AD). In case of a Portal request the eIDAS-berichtenservice MUST NOT be offered in the list of AD's to be selected.

Note: The examples below show only the AuthnRequest. Additional wrapping elements can be present in case of HTTP Artifact binding.

Example DV AuthnRequest

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="_6984066c-de03-11e4-a571-080027a35b78"
    ForceAuthn="true"
    IsPassive="false"
    Destination="https://..."
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
```

```
    AssertionConsumerServiceURL="https://"
    AttributeConsumingServiceIndex="1"
    IssueInstant="2015-04-08T16:30:03Z"
    Version="2.0">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:...</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI=" ">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:core:
assurance-class:loa3</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Example DV AuthnRequest - minimal

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="_2962ac7c-de04-11e4-9801-080027a35b78"
    Destination="https://..."
    IssueInstant="2015-04-08T16:30:07Z"
    Version="2.0">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:DV:...</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_2962ac7c-de04-11e4-9801-080027a35b78">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
</samlp:AuthnRequest>
```

Response (2)

For chain authorizations (Vervallen_Interface specifications HM-MR chain authorization), the identification number of the represented service consumer are included in the assertion for the HM in the same way as for single authorizations. The additional information about the chain is stored in a separate attribute.

Note: The HM will not identify the MRs from which the underlying assertions originate. Additional attributes relate to the represented service consumer or the user. There is no mechanism to include an additional attribute that relates specifically to an intermediary.

Element/@Attribute	0..n	Description
@ID	1	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	SAML: Unique attribute of the AuthnRequest for which this Response message is the answer.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the Response.
@Destination	1	SAML: URL of the endpoint of the DV on which the message is offered. MUST match the DV's metadata.
@Consent	0..1	Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM.
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	0..1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloping message. When communicated within a ArtifactResolveResponse the signature on the SAML:Response MAY be omitted, since the parent message already guarantees the integrity.
Extensions	0	Elektronische Toegangsdiensten: MUST NOT be included.
Status	1	Elektronische Toegangsdiensten: MUST contain a StatusCode element with the status of the authentication. See Error handling.
StatusCode	1	SAML: MUST be present in a Status element.
@Value	1	If not 'success' additional information should be provided. (conform Elektronische Toegangsdiensten specifications).
StatusCode	0..1	Only present if top-level StatusCode is not 'success'.
@Value	1	In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See Error handling.
StatusMessage	0..1	Only present if top-level StatusCode is not 'success'.
StatusDetail	0	Elektronische Toegangsdiensten: MUST NOT be included.
Assertion	0..1	Elektronische Toegangsdiensten: MUST contain the <Assertion> that is delivered in the response, if the request was processed successfully. See below.
EncryptedAssertion	0	Elektronische Toegangsdiensten: MUST NOT be included.

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    ID="_5e702d5c-de06-11e4-a5a1-080027a35b78"
    InResponseTo="6984066c-de03-11e4-a571-080027a35b78"
    Version="2.0"
```

```
    Destination="https://..."
    IssueInstant="2015-04-08T16:30:06Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_5e702d5c-de06-11e4-a5a1-080027a35b78">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion Version="2.0"
        ID="_535162e2-de06-11e4-98a2-080027a35b78"
        IssueInstant="2015-04-08T16:30:05Z">
        <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
        ...
    </saml:Assertion>
</samlp:Response>
```

HM Summary assertion

This paragraph describes a HM summary <Assertion>

Element/@Attribute	0..1	Description
@ID	1	SAML: MUST identify the <Assertion> uniquely within the scope of the Issuer for a period of at least 12 months.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the assertion.
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the Issuer (HM) for the enveloping Assertion.
Subject	1	Elektronische Toegangsdiensten: MUST be included.
BaseID	0	Elektronische Toegangsdiensten: MUST NOT be included.
NameID	0..1	Rules for processing request requires NameID to contain a TransientID or an ActingEntityID (DV connects to r1.09 or older, for older specifications see https://afsprakenstelsel.etoegang.nl/display/archief/Archief).
EncryptedID	0..1	Elektronische Toegangsdiensten: MUST NOT be included.
SubjectConfirmation	1...2	SAML: Contains the SubjectConfirmation conform the WebSSO profile.

		Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.
Conditions	1	Elektronische Toegangsdiensten: MUST be included.
@NotBefore	1	Elektronische Toegangsdiensten: MUST be included.
@NotOnOrAfter	0..1	Elektronische Toegangsdiensten: MAY be included.
Condition	0	Elektronische Toegangsdiensten: MUST NOT be used.
AudienceRestriction	1	SAML: MUST be included.
Audience	1	Elektronische Toegangsdiensten: Contains the EntityID(s) for all relevant parties that are intended to receive and process this assertion, as per SAML WebSSO profile. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV:<*OIN*>' is to be used.
ProxyRestriction	0	Elektronische Toegangsdiensten: MUST NOT be included.
Advice	0..1	Elektronische Toegangsdiensten: SHOULD be included. See below under processing rules.
AssertionIDRef	0	Elektronische Toegangsdiensten: MUST NOT be included.
AssertionURIRef	0	Elektronische Toegangsdiensten: MUST NOT be included.
Assertion	1	Elektronische Toegangsdiensten: Contains the original <Assertion> elements this assertion is composed of.
EncryptedAssertion	0	Elektronische Toegangsdiensten: MUST NOT be included.
AuthnStatement	1	Elektronische Toegangsdiensten: MUST be included. The AuthenticatingAuthority element MUST be populated with the EntityID of the AD that performed the authentication.
@AuthnInstant	1	Elektronische Toegangsdiensten: MUST contain the time of authentication.
@SessionIndex	0..1	Elektronische Toegangsdiensten: MAY be included.
AuthnContext	1	Elektronische Toegangsdiensten: MUST be included.
AuthnContextClassRef	1	Elektronische Toegangsdiensten: MUST be included. Contains either the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified' (default) or the obtained effective Level of assurance, see below under "rules for processing responses".
AttributeStatement	1	Elektronische Toegangsdiensten: MUST contain an <AttributeStatement> in accordance with the following section and the rules for processing responses.

Example HM Assertion

```
<saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_535162e2-de06-11e4-98a2-080027a35b78">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
```

```
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for minimal DV request

```
 <saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        ...
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for Representation

```
Vraag het op bij de BO / Ask BO
```

Example HM Assertion for citizen domain

```
 <saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        ...
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer>urn:etoegang:KR:...</saml:Issuer>
            <!-- Verbatim copy of KR declaration of sectoral identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example - HM Assertion - eIDAS-OUT withService Intermediation

```
<saml2:Assertion ID="_67d2200a8bd8401dc1b7274106731ca6" IssueInstant="2019-02-26T10:35:43.000Z" Version="
2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:HM:00000003271247010000:
entities:7611</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_67d2200a8bd8401dc1b7274106731ca6">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue/>
            </ds:Reference>
        </ds:SignedInfo>
```

```
        <ds:SignatureValue/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>f04a58c387f4f8b5f1fa3a614f79f073f3f08953</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" xmlns:saml="urn:oasis:
names:tc:SAML:2.0:assertion">ed3d5655-b6ee-47bf-87d5-fb77302e14b4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" xmlns:saml="urn:oasis:names:
tc:SAML:2.0:assertion">
            <saml:SubjectConfirmationData InResponseTo="_d3fda417414c17b2667995961cf79fc5" NotOnOrAfter="
2019-02-26T10:37:39Z" Recipient="https://brk.eid-tst.ad.nl/brk/HM1CServiceProvider" xmlns:saml="urn:oasis:
names:tc:SAML:2.0:assertion"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml2:Conditions NotBefore="2019-02-26T10:35:43Z" NotOnOrAfter="2019-02-26T10:37:43Z" xmlns:saml2="urn:
oasis:names:tc:SAML:2.0:assertion">
        <saml2:AudienceRestriction>
            <saml2:Audience>urn:etoegang:DV:00000001111111110000:entities:9113</saml2:Audience>
            <saml2:Audience>urn:etoegang:DV:00000002222222220000:entities:9613</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml:AuthnStatement AuthnInstant="2019-04-08T16:30:07Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml2:Advice>
        <saml:Assertion IssueInstant="2019-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78"
Version="2.0">
            <saml:Issuer> urn:etoegang:AD:00000004444444445001:entities:9042</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
        <saml:Assertion IssueInstant="2019-04-08T16:30:07Z" ID="dd4dae83-0f35-4695-b24a-29d470a63ea7"
Version="2.0">
            <saml:Issuer> urn:etoegang:MR:00000005555555555001:entities:9042</saml:Issuer>
            <!-- Verbatim copy of MR declaration of identity contents -->
        </saml:Assertion>
    </saml2:Advice>
    <saml2:AuthnStatement AuthnInstant="2019-02-26T10:35:43Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:
assertion">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml2:AuthnContextClassRef>
            <saml2:AuthenticatingAuthority>urn:etoegang:AD:00000004444444445001:entities:9042</saml2:
AuthenticatingAuthority>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        . . . . .
    </saml2:AttributeStatement>
</saml2:Assertion>
```

Example HM assertion - Attribute Statement - eIDAS-OUT using Service Intermediation

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"
>dafca82e-4806-408e-956e-3a7092643e54</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute Name="urn:etoegang:core:ServiceID">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">urn:
etoegang:DV:00000001111111110000:services:8002</saml2:AttributeValue>
    </saml2:Attribute>
    <saml:Attribute Name="urn:etoegang:core:Representation" xmlns:saml="urn:oasis:names:tc:SAML:2.0:
assertion">
        <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org
/2001/XMLSchema-instance" xsi:type="xs:boolean">true</saml:AttributeValue>
    </saml:Attribute>
    <!-- igv de service via de Service Catalog vraagt om een ServiceRestriction en de MR-->
```

```
    <!-- heeft een service restriction bij de machtiging. Vb restrictie op KvK Vestigingsnr-->
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ActingSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:
assertion">
        <saml:AttributeValue>
            <!-- # ActingSubjectID - BSN:VP@RVO (PseudoID voor de EB) -->
            <saml:EncrypedID>
                <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04
/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="
#_15531f42aa31bbd4" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>...</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:
00000001111111110000:entities:9613">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
        <saml:AttributeValue>
            <!-- # ActingSubjectID - BSN:VI@RVIG (BSN voor BRP-Attributendienst)-->
            <saml:EncrypedID>
                <xenc:EncryptedData Id="_ed3457856888ad576a0aa751725ce76a6b866" Type="http://www.w3.org/2001
/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="
#_4567788aa31bbd4" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>...</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:
00000002222222220000">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>UtEw923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:LegalSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:
assertion">
```

```
        <saml:AttributeValue>
            <!-- # LegalSubjectID - KvK voor de EB)-->
            <saml:EncryptedID>
                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_6bc1c98ef545444da370efd74371ff6f" Type="http://www.w3.org/2001/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:RetrievalMethod URI="#_105e787ebce14ea2b6655adb4d736b86" Type="http://www.w3.org
/2001/04/xmlenc#EncryptedKey" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>lx922tGEfI9T7WgoduHAZ941XA....</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_105e787ebce14ea2b6655adb4d736b86" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.
w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:KeyName>022A8DEA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:
KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>gNDIheioi3mgjeyCTviEXDui3.....</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_6bc1c98ef545444da370efd74371ff6f" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncryptedID>
        </saml:AttributeValue>
        <! # LegalSubjectID - Geen KvK voor de dienstaanbieder.>
    </saml:Attribute>
    <!-- # CompanyName werkgever voor de EB.-->
    <saml:EncryptedAttribute>
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_67947663adfasdf9410780097b9bf2f04fa8" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org
/2000/09/xmldsig#sha1" />
            </xenc:EncryptionMethod>
            <ds:KeyInfo>
                <ds:KeyName>57890EA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>WYuIOsaf1aNbZdRQPXepQjlw4Tg...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
    <!-- # Optionele Bedrijfs attributen (CompanyName) voor de EB.-->
    <saml:EncryptedAttribute>
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_6974a3dsdf9410780097b9bf2f04fa8" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org
/2000/09/xmldsig#sha1" />
            </xenc:EncryptionMethod>
            <!-- # EB should recognise KeyName.-->
            <ds:KeyInfo>
                <ds:KeyName>57890EA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>WYuIOsaf1aNbZdRQPXepQjlw4Tg...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
</saml2:AttributeStatement>
```

AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

Element/@Attribute	0..1	Description
Attribute	0..n	Elektronische Toegangsdiensten: Depending on Rules for processing request: • one or more ActingSubjectID's • one or more LegalSubjectID • one or more EntityConcernedID • ServiceID as multi-valued XACML attribute • exactely one IntermediateEntityID, the identity of Intermediate • one or more ServiceRestrictions, eg ServiceRestriction:Vestigingsnr In case of Ketenmachtiging, MUST contain the attribute IntermediateEntityID.
EncryptedAttribute	0..n	Depending on Rules for processing request • one or more EncryptedAttributes requested by the DV and provided by the AD and/or MR

Example HM AttributeStatement for citizen domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">1ff84f14-df64-11e4-ba1a-080027a35b78</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:AD:...</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for consumer domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">0013c492-84cd-4c4b-8206-b13007ac2a1c</saml:AttributeValue>
    </saml:Attribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_FirstName" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
            <ds:KeyInfo>
                <ds:Keyname>...</ds:Keyname>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_18OrOlder" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
            <ds:KeyInfo>
                <ds:Keyname>...</ds:Keyname>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain with multiple entityconcernedtypes

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:RSIN">
        <saml:AttributeValue xsi:type="xs:string">987654321</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Rules for processing responses

On a successful authentication the HM MUST generate a 'Summary Assertion' based on the Assertions gathered during the authentication process, using the following processing rules.

- MUST sign the enclosed <Assertion> as well as the <Response> (and/or the enclosing <ArtifactResponse>).
- MUST verify each collected assertion has at minimum the Level of Assurance as requested by the DV. If verification fails, MUST handle the received responses as an unrecoverable error.
- MUST provide an <AuthnContextClassRef>:
  - By default fill the AuthnContextClassRef with the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified'.
  - When a DV explicitly requests a detailed LoA by including an AuthnContextClassRef in its AuthnRequest (see above): The HM MUST communicate the effective Level of Assurance of the combined assertions. The effective Level of assurance is the minimum of the LoA of the Authentication assertion and (if applicable) the LoA of the Representation authorization assertion(s).

    The MR communicates two Levels of Assurance in its Assertion. A LevelOfAssurance (requested) and a LevelOfAssuranceUsed (actually obtained). The HM MUST use the LevelOfAssuranceUsed from the MR Assertion as the LoA of the Representation authorization.

    .

- HM MUST provide an <Subject> with the following <NameID>
  - *IF* DV connects to r1.13 (or newer) AND non-represenation THEN copy AD-assertion: Subject.NameID.TransientID
  - *IF* DV connects to r1.13 (or newer) AND representation THEN copy MR-assertion: Subject.NameID.TransientID
  - *IF* DV connects to r1.11 (or older) *THEN* copy MR-assertion: XACMLAuthz-Decision.Subject.ActingEntityID
- HM MUST provide an <AttributeStatement> with the following <Attributes> and <EncryptedAttributes>
  - *IF* DV connects to r1.13 (or newer) *THEN*
    - *the HM must copy all relevant information (see Interface specifications DV-HM) from the below sources to the ActingSubjectID attribute:*
      - MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID (EncryptedID)

        - AD-assertion: Response.Assertion.AttributeStatement.ActingSubjectID.
        - copy all relevant AD-assertion: AttributeStatement.EncryptedAttribute
- IF Representation THEN
    - IF DV connects to r1.13 (or newer) THEN
        - copy all relevant EncryptedID from MR-Assertion: XACMLAuthz-Decision.Subject.LegalSubjectID to <LegalSubjectID>
        - copy all relevant EncryptedID from MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID to <ActingSubjectID>
        - copy all relevant MR-assertion: XACMLAuthz-Decision.Resource.EncryptedAttribute
    - *IF* DV connects to r1.11 (or older) *AND* Representation *THEN* copy MR-assertion: XACMLAuthz-Decision.Resource.EntityConcernedID
    - copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.ServiceID
    - *IF* available copy all MR-assertion: XACMLAuthz-Decision.Resource.ServiceRestrictions
    - *IF* Ketenmachtiging *THEN* copy MR2-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.IntermediateEntityID

- MUST provide an <Advice>, by default filled with verbatim copy of all Assertions – so that original signatures over the assertions remains verifiable – gathered during the authentication process. HM MAY offer their DV to omit this information, if they archive this information and allow for later retrieval.

NOTE: When copying encrypted XML elements (<EncryptedID>, <EncryptedAttribute>) to create the summary declaration the HM MUST substitute used XML identifiers to point at the EncryptedTypes for a guaranteed unique identifier. This MAY be accomplished by pre- or suffixing the used identifier in the copy.

(Rationale: *@ID* values must uniquely identify the elements which bear them. Identifiers that appear once in the summary assertion and once in the advice assertion(s) will break schema validation of assertions).

All relevant

all <EncryptedID> or <EncryptedAttribute> elements except those encrypted for MR

A receiving DV:

- MUST verify the response matches with the Request responded to.
- MUST validate the signature on the Assertion as well as the Response (and/or the enclosing ArtifactResponse). Message (elements) MUST be signed using a certificate as listed in the SAML metadata of the HM for the purpose of signing for an IDPSSODescriptor of the responding HM. (NB this should correspond to the certificate as published in the network metadata).
- MUST be able to process DeprecatedActingSubjectID to facilitate migration or replacements of identifiers.
- SHOULD verify the structure and contents of the Response.
- SHOULD validate the signature and linking of the Evidence assertions.
- In case the receiving DV is a Dienstbemiddelaar, the Dienstbemiddelaar MUST provide a verbatim copy of the assertion – so that original signatures over the assertions remains verifiable – to the Dienstaanbieder (service supplier).
- IF the DV wants to decrypt urn:etoegang:1.12:EntityConcernedID:PseudoID or urn:etoegang:1.12:EntityConcernedID:BSN the DV must use preinstalled BSNk-keymaterial and software to obtain the actual identifier.
- IF the DV receives a pseudonym THEN the DV SHOULD create a mapping from the obtained Pseudonym to a user account, rather than using the obtained pseudoniem directly as unique key for an account.
- MUST decrypt an Encrypted Pseudonym or Encrypted Identity in the EncryptedID in the Attribute Statement of the Assertion using preinstalled keymaterial and software to obtain the actual identifier.
    - SHOULD create a mapping from the obtained identifier to a user account, rather than using the obtained identifier directly as unique key for an account. This so that a Persistent Pseudonym as well as deprecatedID can be in use at the same time to access an account during migrations.

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied, although considering that the logout message is sent to the AD via the HM. Only supported, is the DV's LogoutRequest where the user chooses to log out from the AD. The DV should never expect a LogoutRequest or a LogoutResponse. The interface for this message is described below.

@ID	SAML: Unique message characteristic
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created
@Destination	SAML: URL of the HM on which the message is offered.
NameID	Elektronische Toegangsdiensten: MUST contain a NameID element with the transient from the Subject of the concomitant AD assertion. This MUST NOT contain any identifier of the user.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the DV.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the DV for the envelopping message.

RequestKeyMaterial

The DV may request the HM for DV-specific key material which the DV can use to decrypt the EncryptedPseudonym into a DV-specific pseudonym or BSN, as per AUC9 Verstrekken sleutelmateriaal Dienstverleners. The HM can request the keys at the BSNk (see Interface specifications aux HM-BSNk - ProvideDVkeys).

A PKIo-certificate of the DV is required, the PKIo-certificate MUST have a (extended) key usage that allows for keyEncipherment. If the DV may request a BSN, the PKIo-certificate MUST have a Subject.serialNumber containing the organizations OIN.

ProvideKeyMaterial

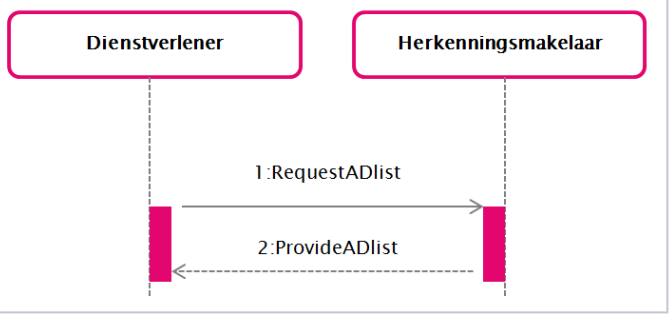
The Herkenningsmakelaar MUST transfer the PKIo-encrypted key material to the DV unaltered. The HM will receive the DV-keys from the BSNk (see I nterface specifications aux HM-BSNk - ProvideDVkeys).

The DV can decrypt the DV-keys using its private key corresponding with the PKIo-certificate used in the request.

Interface specifications DV-HM RequestADlist

For preselection of an AD by the user at the DV, the DV retrieves a list of relevant AD's for that service from the HM (that the HM compiles from network metadata), to complete AUC8 Verkrijgen lijst Authenticatiediensten.

DV-HM sequence diagram



RequestADlist (1)

A DV may request a list of all accredited ADs, by making a HTTP GET request at an endpoint provided by its HM.

Parameter	0..n	Description
ServiceUUID	1	ServiceUUID is an identifier of a ServiceInstance as listed in the Service catalog. Provided here to refer to the service for which the list is requested.
RequestedAuthnContext	0..1	Optionally, an additional parameter 'RequestedAuthnContext' MAY be included with a LoA equal to or lower than listed in the Service Catalog.

Example RequestADlist

```
GET /listAD.xml?ServiceUUID=a392d917-d965-4cb8-bff4-238694fc3336 HTTP/1.1
Host: hm.example.nl
```

Processing rules for RequestADList

A requesting DV:

- MUST supply the ServiceUUID registered in the Service Catalog for the ServiceInstance for which authentication will be requested as the 'ServiceUUID' parameter.
- MAY optionally request the list of ADs for a LoA equal to or lower than listed in the Service Catalog.

A receiving HM:

- MUST validate a request.

ProvideADlist (2)

A HM MUST respond with a signed list of valid, applicable and accredited ADs for the requested service. This list MUST be a subset of the Network metadata.

The list is a signed SAML EntitiesDescriptor, containing one EntityDescriptor per AD or two in case validity dates are used as in Metadata for participants.

Each EntityDescriptor contains one IDPSSODscriptor with one or more SingleSignOnService elements and one Organization element. The Orgnization element contains a OrganizationName, OrganizationDisplayName and OrganizationURL, as per SAML metadata specification. Other element and attributes as described in Metadata for participants MAY be present.

Example ProvideADlist (SAML metadata)

```
<md:EntitiesDescriptor
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:eme="urn:etoegang:1.11:metadata-extension">

    <ds:Signature>...</ds:Signature>
```

```
    <md:EntityDescriptor entityID="urn:etoegang:AD:...">
        <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:SingleSignOnService Location="https://..." Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact" eme:name="app" />
            <md:SingleSignOnService Location="https://..." Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact" eme:name="web" />
        </md:IDPSSODescriptor>
        <md:Organization>
            <md:OrganizationName xml:lang="nl">AD A</md:OrganizationName>
            <md:OrganizationDisplayName xml:lang="nl">AD A</md:OrganizationDisplayName>
            <md:OrganizationURL xml:lang="nl">https://...</md:OrganizationURL>
        </md:Organization>
    </md:EntityDescriptor>

    <md:EntityDescriptor entityID="urn:etoegang:AD:...">
        <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:SingleSignOnService Location="https://..." Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact" />
        </md:IDPSSODescriptor>
        <md:Organization>
            <md:OrganizationName xml:lang="nl">AD B</md:OrganizationName>
            <md:OrganizationDisplayName xml:lang="nl">AD B</md:OrganizationDisplayName>
            <md:OrganizationURL xml:lang="nl">https://...</md:OrganizationURL>
        </md:Organization>
    </md:EntityDescriptor>

</md:EntitiesDescriptor>
```

Processing rules for ProvideADlist

A responding HM:

- MUST provide a subset of the Network metadata, containing all applicable ADs for the requested service. The subset:
    - MUST contain all valid ADs supporting at least a LevelOfAssurance equal to or greater than the minimum requested level of assurance.
        - The eIDAS Berichtenservice (EB) MUST NOT be included as one of the valid ADs.
    - MUST contain the requested NameIDFormat(s) (=EntityConcernedType).
    - MUST contain values holding an exact copy of the corresponding values in the Network metadata.
    - MUST be sorted alphabetically by OrganizationDisplayName.
    - MUST not contain any other entries.
- MUST sign this metadata using its own certificate as listed in the Network metadata for signing.

A receiving DV:

- MUST validate the signature on the response before processing the response.
- MUST display all ADs using the OrganizationDisplayName in the provided list when presenting a User the list for AD preselection.
- MUST display all ADs in the order of the list provided by the HM.
- MUST use the entityID of the EntityDescriptor and Location attribute of the SignleSignOnService element corresponding with the User's selection to populate the IDPEntry in the Scoping element.
- In case of the eIDAS-berichtenservice (EB).
    - The DV MUST use a separate login-link for the eIDAS-berichtenservice (EB), and MUST NOT present the EB in the eHerkenning list of AD's (see GUC1 Gebruiken eToegang als dienstafnemer).
    - MAY use the ISOName to change the language settings for a user.
- SHOULD ignore other elements and attributes in the list.
- SHOULD take 'validFrom' and 'validUntil' of entries into account.
- SHOULD cache the list received from an HM per service, for the duration of maximum 15 minutes. The DV MUST NOT use a list older than 30 minutes for presentation to a User; in case the list expires the DV MUST forwarded the User to the HM as if no pre-selection is implemented.

Interface specifications AD-BSNk

The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

In order to provide a polymorphic pseudonym and/or identity of the acting user, an interface is necessary beween the AD/MU and BSNk.

This interface facilitates three functions:

1. It implements AUC6 Activeren BSNfor the MU.
2. It implements AUC10 Transformeren so the AD can transform the PI into the EI or the PP into an EP.
3. It registers the status of the authentication means in the BSNk inzageregister. The <ReadableCardInfo> that SHOULD be used is "eHerkenningsmiddel bij <naam aanbieder>"

Interface specifications MR-BSNk

The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

In order to realize step 7 in the AUC3.1 Registreren bevoegdheid eenmanszaken an interface is necessary beween the MR and BSNk. This interface wil implement AUC6 Activeren BSN for the MR. In order to facilitate the transformation of the PI or PP this interface will also implement AUC10 Transformeren. This will allow the MR to transform the PI into the EI or the PP into an EP of the owner of the sole trader for the DV who requested this information.

The correct recipientKeySetVersion used in this transformation MUST be read from the Service catalog by reading the field BSNk-recipientKeySetVersion. If no BSNk-recipientKeySetVersion has been set, the RKSV MUST be derived from the validity.notBefore (YYYYMMDD notation) date of the most recent issued (using validity.notBefore) certificate of the service instance in the Service catalog.

On a technical level this interface is identical (a specified SOAPaction will be used between MR and BSNk) to the Interface Specifications aux MR - BSNk. The MR MUST implement this interface as if it were an AD communicating to the BSNk.

Information security requirements

This chapter describes the requirements that apply to the information security measures that are implemented.

- Digital signature
- DNSSEC
- Encryption
    - SAML encryption — Encryption in combination with SAML is achieved via XML-encryption. This paragraph provides an explanation of encrypted elements as well as elements encrypted to multiple recipients.
- End-to-end encryption — End-to-end encryption is applied in Elektronische Toegangsdiensten to protect privacy of anyone (acting users) or organisations (especially "single person businesses" or "eenmanszaak"). The BSN is one of the main privacy concerns, following from Dutch law, but other personally identifiable information must also be protected. Using end-to-end encryption as described on this page avoids an Herkenningsmakelaar (HM) becoming an unintended hotspot for information on service usage.
- PKIoverheid
- Secure connection
- Secure cookies
- Synchronize system clocks

Digital signature

To guarantee authenticity, integrity and non-repudiation, each message described MUST be provided with a digital signature from the message sender. The message recipient MUST validate all of the digital signatures in the message before processing it.

- The recipient MUST check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
- The recipient MUST NOT process the message if it contains parts that are not signed with a valid digital signature.

The following requirements apply to generating digital signatures:

- The digital signature is embedded in the message content with Enveloped Signature Transform http://www.w3.org/2000/09/xmldsig#enveloped-signature.
- Canonicalization MUST be carried out according to the exclusive c14n method without comments, as identified by 'http://www.w3.org/2001/10/xml-exc-c14n#' (see http://www.w3.org/TR/xml-exc-c14n/)
- Digests MUST be calculated with the SHA256 algorithm.
- The SignatureValue MUST be calculated with the RSA-SHA256 algorithm.
- The sender MUST sign messages with a PKIoverheid certificate (see for requirements PKIoverheid) with a key length of at least 2048 bits. The (extended) key usage of the used certificate MUST allow use for signing.
- In case of signing metadata, the <Signature> element MUST contain only an <X509Data> element with an <X509Certificate> element.
  In all other cases, The signature MAY contain a <KeyInfo> element that contains a <KeyName>. The <KeyName> MUST match the <KeyName> stated in the metadata of the sender for the respective role. The signature MUST NOT contain other elements (such as <X509Data>). If a <KeyInfo> element is not included in the message, the metadata MUST contain at least one (1) valid certificate against which the message can be validated. If the metadata contains more than one certificate, the participant MUST validate the message against each valid certificate. The participant MAY agree with its service consumers to limit the period in which the metadata contains more than one certificate. This enables the high utilization of the system to be controlled.
- The Reference MUST refer to the signed element via an ID attribute in the local document, as per the signature profile of SAML2.0 core (§5.4) and SAML 2.0 Metadata (§3.1).

DNSSEC

Every Deelnemer (Participant) in the network MUST publish DNSSEC records for their domains registered for use within the network. Every Deelnemer SHOULD verify DNSSEC records when communicating with other parties in the context of Elektronische Toegangsdiensten. Dienstverleners (Service Providers) SHOULD publish and verify DNSSEC records.

Encryption

Encryption is used to guarantee confidentiality. In case encryption MAY or MUST be used, one MUST use the block encryption algorithms identified by the following URI in conjunction with the use of XML Encryption

- http://www.w3.org/2001/04/xmlenc#aes256-cbc

For asymmetric encryption, used to encrypt keys, the RSA algorithm in combination with OAEP padding and a SHA-1 digest MUST be used, as described at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#rsa-oaep-mgf1p. These algorithms are identified as

- http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
- http://www.w3.org/2000/09/xmldsig#sha1

SAML encryption

Encryption in combination with SAML is achieved via XML-encryption. This paragraph provides an explanation of encrypted elements as well as elements encrypted to multiple recipients.

Encrypted elements

Any element that will be encrypted has to conform to the following:

- The element MUST be encrypted using applicable encryption algorithms, as defined in Encryption.
- A new, cryptographically sound randomly generated symmetric key MUST be used per encrypted element.
- The @Recipient of the resulting <EncryptedKey> MUST be set to the EntityID of the recipient.
- XML contents in the encrypted element MUST have all namespace definitions.

Multiple recipients

SAML and XML-encryption allow for multiple recipients of the same encrypted element. The construct for this is specified in more detail in errata E43 of SAML 2.0 errata 05. In case of multiple recipients:

- each EncryptedKey MUST have a CarriedKeyName equal to the KeyName used in the KeyInfo of the EncryptedData.
- each EncryptedKey SHOULD have a ReferenceList, refering back to the data encrypted with the symmetric key contained.
- Upon decryption, elements without an EncryptedKey intended for the decrypting recipient MAY be ignored and EncryptedKeys for other recipients of encrypted elements SHOULD be ignored.

EncryptedID

An <EncryptedID> MUST contain a SAML <NameID> after decryption, with the following properties:

- The Format attribute MUST be set to 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'.
- The NameQualifier attribute MUST be populated with the full name of the type of identifying attribute (e.g. 'urn:etoegang:EntityConcernedID:KvKnr').
    - For Intern pseudoniem identifiers, the NameQualifier MUST contain the OIN format of the EntityID (KvK number) of the "Authenticatiedienst".
    - For other Identificerende kenmerken, the NameQualifier MUST contain the identifing attribute's name, in URI format. For instance for a BSN the value is 'urn:etoegang:1.9:EntityConcernedID:BSN' and for a Specific pseudonym the value is 'urn:etoegang:1.9:EntityConcernedID:Pseudo'.
- The attributes SPNameQualifier and SPProvidedID MUST NOT be used.
- In case more than one certificate is listed for encryption for the recipient, the pseudonym MUST be encrypted for each certificate. This will result in multiple EncryptedKeys, see above.

EncryptedAttribute

An <EncryptedAttribute> MUST contain a SAML <Attribute> after decryption, with the following properties:

- The @Name attribute MUST be present.
- One <AttributeValue> per value of the attribute MUST be used.

Examples

Below two examples are given, with encryption and after decryption. the EncryptedID example is for a single recipient, the EncryptedAttribute example is for multiple recipients. The same construct for single / multiple recipient can be used in the other encrypted element types.

Example EncryptedID

```
<saml2:EncryptedID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
       Id="_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04/xmlenc#Element">
       <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
       <ds:KeyInfo>
           <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
               URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
       </ds:KeyInfo>
       <xenc:CipherData>
           <xenc:CipherValue>AZkW3hbBaQkxs...</xenc:CipherValue>
       </xenc:CipherData>
   </xenc:EncryptedData>
   <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
       Recipient="urn:etoegang:...">
       <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
           <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
       </xenc:EncryptionMethod>
```

```
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData>
            <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
        </xenc:ReferenceList>
    </xenc:EncryptedKey>
</saml2:EncryptedID>
```

Example NameID after decryption

```
<saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent" NameQualifier="urn:etoegang:1.9:EntityConcernedID:BSN">999999047</saml2:NameID>
```

Example EncryptedAttribute - multiple recipients

```
 <saml2:EncryptedAttribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <xenc:EncryptedData Id="_3c63798db8a16b54ade207ea0df28ad4" Type="http://www.w3.org/2001/04/xmlenc#Element">
        <xenc:EncryptionMethod xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
        <ds:KeyInfo>
            <ds:KeyName>_dd0d7a0215f94ea81b170a2e65834ce8</ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData>
            <xenc:CipherValue>5efOYLEoY1PD2145...</xenc:CipherValue>
        </xenc:CipherData>
    </xenc:EncryptedData>
    <xenc:EncryptedKey Id="_fd73ad54daf1ca14a4aac30ea850340a" Recipient="urn:etoegang:...">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        </xenc:EncryptionMethod>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData>
            <xenc:CipherValue>H5nzimm7fAZuzdnZ...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
            <xenc:DataReference URI="#_3c63798db8a16b54ade207ea0df28ad4" />
        </xenc:ReferenceList>
        <xenc:CarriedKeyName>_dd0d7a0215f94ea81b170a2e65834ce8</xenc:CarriedKeyName>
    </xenc:EncryptedKey>
    <xenc:EncryptedKey Id="_e152fcf0772b8921f09ec0c1a45f1fa4" Recipient="urn:etoegang:...">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        </xenc:EncryptionMethod>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
            <xenc:CipherValue>xyH8nQscJYAaYwJopGaLPk...</xenc:CipherValue>
        </xenc:CipherData>
        <xenc:ReferenceList>
            <xenc:DataReference URI="#_3c63798db8a16b54ade207ea0df28ad4" />
        </xenc:ReferenceList>
        <xenc:CarriedKeyName>_dd0d7a0215f94ea81b170a2e65834ce8</xenc:CarriedKeyName>
    </xenc:EncryptedKey>
</saml2:EncryptedAttribute>
```

Example Attribute after decryption

```
<saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:attrext="urn:oasis:names:tc:SAML:
attributes:ext" Name="urn:etoegang:attribute:18OrOlder" attrext:OriginalIssuer="urn:etoegang:1.9:attribute-
sourceid:NLWID" attrext:LastModified="2015-03-31T12:00:00Z">
    <saml2:AttributeValue>false</saml2:AttributeValue>
</saml2:Attribute>
```

End-to-end encryption

End-to-end encryption is applied in Elektronische Toegangsdiensten to protect privacy of anyone (acting users) or organisations (especially "single person businesses" or "eenmanszaak"). The BSN is one of the main privacy concerns, following from Dutch law, but other personally identifiable information must also be protected. Using end-to-end encryption as described on this page avoids an Herkenningsmakelaar (HM) becoming an unintended hotspot for information on service usage.

Introduction

Personally Identifiable Information (PII) forms the basis of authentication and authorisation (mandates). PII can lead to identification of the particular person, either through the data itself (identifiers), or by combining data, leading to recognising the person through patterns in that data. Within eTD, PII is dispersed over various registers, operated by various participants. During the authentication and authorisation processes this data must be combined using assertions that are strongly linked together, in order to firmly establish involved identities and appropriate mandates that can be trusted by service providers in order to securely provide requested services.

Usage of this sensitive data implies that both "security" and "privacy" are important. Security refers to confidentiality, integrity (among which authenticity) and availability of the information. Privacy aims that the user is always in control of his/her data, and can trust that only parties for which (s)he gave consent for, have access to that data.

In order to protect PII during this process, several measures are taken, jointly called "end-to-end encryption", that are intended to:

- allows only the intended recipients to see data as needed to perform the required service (principle of "least privilege"); this applies to eTD-participants as well as service providers
- prevent "hotspots" to attack; within eTD this applies especially to the HM, since all information is routed through the HM.

Overview of protection measures

The data that must be protected, is categorised as:

- identifiers (BSN, pseudonyms, KvK-nrs, etc)
- content/attributes (name, address, date of birth, etc)

Both categories contain data that is considered sensitive, but the measures to protect them, while partly overlapping, are also partly different.

Basic measures that apply to both categories, are:

- Sensitive data is encrypted for the intended recipient using XML-based encryption to provide confidentiality
    - for "content" the only valid recipient is the DV (for "identifiers", see below)
      note that for Service Intermediation (dienstbemiddeling) it is important to distinguish between the "dienstbemiddelaar" (DB, Service Broker) and "dienstaanbieder" (DA, service provider); each has its own entry/service in the Service Catalog, and the data must be encrypted for the appropriate party that provides that particular service.
- Assertions are digitally signed to provide proof of integrity/authenticity
- Key management is regulated to provide appropriate availability

For "content" these basic measures are deemed sufficient.

For "identifiers", on top of these basic measures, some additional measures were taken, because:

- some identifiers (especially BSN) are determined as extra sensitive in Dutch law
- identifiers are more easily recognised by hackers, and allow for easy correlation of related data
- identifiers are sometimes relevant to multiple relying parties (recipients; e.g. DV, MR) and must therefore be encrypted separately for each recipient

The additional measures for identifiers are:

- Pseudonymisation:
    - Using separate pseudonyms for the user per "relying party" whenever this is sufficient (i.e. no formal identifier like "BSN" needed)
    - These pseudonyms are persistent per "relying party", so it can recognise "returning users"
    - These pseudonyms are different across "relying parties", so users cannot be traced across "relying parties".
- Encryption of identifiers
    - All identifiers (including the pseudonyms) are encrypted during transfer in each assertion
    - The "encrypted value" is different during each "transfer", so in-between parties (e.g. HM) cannot relate various "transfers" of the same identifier
    - For identifiers and pseudonyms based on the "BSN", and the "eIDAS Uniqueness Identifier", polymorphic encryption is used
        - In the future, polymorphic encryption could also be used for other identifier types

Note that using the BSN for polymorphic encryption, requires "activation" of the BSN at BSNk. BSNk only allows this activation if a minimum authentication of LoA 3 (substantial) is provided.

Impact on interfaces

The measures described above are applied in different ways, depending on the situation. The relevant situations are detemined by aspects like:

- "is the acting person acting for him/herself (no representation), or someone else (representation of person or organisation)",
- "is the BSN required or not",
- "is the BSN known by the eTD-participant or not", and
- "what version of the interfaces are supported by the Service Provider".

Normal "content" is only intended for the Service Provider (and not for any of the eTD-participants). This means that when this data is deemed sensitive, it is always XML-encrypted with the public key of the Service Provider, as provided in the Service Catalog. Therefore only the Service Provider can access this data.

For "identifiers", the sections below apply.

No representation

The situation of "no representation" means that:

- the acting subject ("handelende persoon") acts for him-/herself
- the legal subject ("belanghebbende") is the same person as the acting person

This implies that no specific "mandate" is required, and the MR is not involved. So, next to the Service Provider, only the AD and HM are involved

In principle individuals can also have restrictions regarding authorisations on services for themselves, like when the person is "minor", "deemed not to be capable of taking responsibility", etc. So even when currently, "mandates" are not required for "non-representation", this may change over time.

Depending on the required service (as specified in the Service Catalog), 2 main scenarios, requiring different measures, apply to this:

1. BSN is required by the service, or
2. a pseudonym suffices for this service

BSN required

A service is requested for which the service provider requires a BSN as identifier for the acting person, as specified in the Service Catalog. The service provider must be authorised to receive a BSN for this particular service. This means that the service must be authorised on the "Autorisatielijst BSN".

The main consequences are:

1. The BSN of the acting subject must be activated with BSNk by the AD, during onboarding, resulting in a Polymorphic Identity (PI), which is managed by the AD
2. The AD transforms the PI into an Encrypted Identity (EI, or "Versleutelde Identiteit": VI), encrypted for the Service Provider, which is the only relying party in this scenario
3. The AD adds the EI to the AD-assertion and returns this in its response to the HM
4. The HM adds all relevant "identifiers" and "content" in its response to the Service Provider
5. The DV decrypts the EI to a BSN.

Pseudonym required

A service is requested that requires a pseudonym for the acting person (not a BSN), as specified in the Service Catalog. For this situation, 2 different scenarios are possible, depending if the user has on-boarded at his/her MU/AD with BSN or not.

- In case (s)he did NOT onboard with BSN, the AD must produce a so-called Specific pseudonym (SP), which is usually related to the "means of authentication", and not to the BSN.
- Otherwise, the AD has activated the BSN at BSNk and received a Polymorphic Pseudonym (PP), and could work with this.

Currently, the default pseudonym is the Specific Pseudonym. Only in case of eIDAS Outbound, the Polymorphic Pseudonym is used. In the latter case, this is explicitly specified in the Service Catalog.
When the "Wet Digitale Overheid" (WDO) comes into force, this may need to change. At that time further guidelines must be determined when to use which type of pseudonym.

In case the Specific Pseudonym is required:

1. The AD provides an encrypted Specific pseudonym of the user for the DV to the HM, encrypted to the DV
2. The HM can provide the encrypted pseudonym in its response to the DV, without being able to access the value of the pseudonym nor being able to trace users across DV's
3. The DV can decrypt the pseudonym and use it as an identifier to the account of the user for its business processes.

In case the Polymorphic Pseudonym is required:

- The BSN of the acting subject must be activated with BSNk by the AD, during on-boarding, resulting in a Polymorphic Identity (PI), which is managed by the AD
- The AD transforms the PP into an Encrypted Pseudonym (EP, or "Versleuteld Pseudoniem": VP), encrypted for the Service Provider
- The AD adds the EP to the AD-assertion and returns this in its response to the HM
- The HM adds all relevant "identifiers" in its response to the Service Provider
- The DV decrypts the EP to a PP and uses this as identification of the user.

Representation

Currently only representation of organisations is supported. In the future, also representation of individuals may be supported. This is an overview of the different options:

1. An employee (or other contracted person) performs services for an organisation (supported)
2. Organisation A performs services for organisation B, executed by a person working for organisation A: "Ketenmachtiging" or "chain authorisation" (supported)
3. Organisation performs service for individual consumer (not supported yet; requires co-operation with other schemes)
4. Individual performs service for another individual (not supported yet; requires co-operation with other schemes)

Option 1 and 2 are described further. Option 3 and 4 are out-of-scope, and may be added later.

Employee / contractor for organisation (single authorization)

1. The AD provides to the HM:
    a. an encrypted Internal pseudonym of the user for the MR, as EncryptedID, encrypted to the MR
    b. any identifiers as specified in the ActingSubjectTypesAllowed in the appropriate service in the service catalog, as EncryptedID, encrypted to the DV
2. The HM
    a. forwards this in the request to the MR
    b. is not able to access the value of the EncryptedIDs and is not able to trace recurring users.
3. The MR
    a. decrypts the pseudonym from the HM request.
    b. selects the appropriate user authorization
    c. provides EncryptedID's (encrypted to the DV that delivers the service) containing
        i. the Specific pseudonym of the user to the HM, and
        ii. any identifiers of the represented entity as specified in the EntityConcernedTypesAllowed in the service definition
4. The HM provides the EntityConcernedTypes and the specific pseudonym of the acting user for the DV in its response to the DV.
5. The DV can use the EntityConcernedTypes and the specific pseudonym of the user for its business processes.

Organisation to organisation (chain authorisation)

1. The AD provides to the HM:
    a. an encrypted Internal pseudonym of the user for the MR, as EncryptedID, encrypted to the MR
    b. any identifiers as specified in the ActingSubjectTypesAllowed in the appropriate service in the service catalog, as EncryptedIDs, encrypted to the DV
2. The HM
    a. forwards this in the request to the MR of the user (MR1)
    b. is not able to access the value of the pseudonym and is not able to trace recurring users.
3. MR1
    a. decrypts the pseudonym from the HM request
    b. selects the user authorization for organisation A (Intermediary organisation).
    c. allows the user to choose the ultimate represented party (organisation B)
    d. provides a response to the HM with:
        i. the Specific pseudonym of the user to the HM as EncryptedID, encrypted to the DV
        ii. the standard identifier of the organisation A (intermediary organisation) as EncryptedID, encrypted to MR2 and DV
        iii. an "obligation" with the following data related to the ultimate "represented party"
            1. the "default identifier" (currently KvK-nr), as EncryptedID, encrypted to MR2
            2. the "identity of the expected mandates register".
4. The HM
    a. forwards this information in a request to the MR of the represented party (MR2)
    b. is not able to access the value of the pseudonym and is not able to trace recurring users.
5. MR2
    a. decrypts the EncryptedIDs (encrypted to MR2) for the intermediary organisation (A) and represented organisation (B);
    b. selects the appropriate authorization of intermediary organisation (A) for represented organisation (B);
    c. provides a response to the HM with any identifiers of the "represented entity" as specified in the EntityConcernedTypesAllowed in the service definition as EncryptedIDs, encrypted to the DV.
6. The HM provides in its response to the DV
    a. the EncryptedIDs (encrypted to the DV) of organisation A and B and
    b. the EncryptedIDs (encrypted to the DV) of the acting user
7. The DV decrypts the EncryptedID's of both organisations and the user as it sees fit, and uses them for its business processes.

PKIoverheid

In order to use PKIoverheid properly, message recipients MUST meet the requirements for the receiving party described in the PKIoverheid Programma van Eisen (PKIoverheid Requirements), refer to **https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/.**

The following aspects are important:

- Trust the root certificates which are still valid and not revoked from the website https://cert.pkioverheid.nl/; The following PKI root certificates are NOT allowed:
  - So called "TEST certificaten"
  - Roots which are marked with "Persoon"
- Know and trust all valid domain and TSP certificates under the PKIo hierarchy, refer to https://cert.pkioverheid.nl/, with the exception of the folowing domains:
  - Organisatie Persoon
  - Burger
  - Autonome apparaten
  - Private Personen
- Check the PKIoverheid CRL on https://crl.pkioverheid.nl regularly;
- Participants MUST process and handle changes made on the pages https://cert.pkioverheid.nl/ and https://crl.pkioverheid.nl within 10 business days.

Secure connection

The network wants to promote the use of strong cipher suites with minimum discomfort for end-users. Those roles that are in direct contact with their customers (e.g. a HM with it's DV's and an AD/MR with its users) are allowed to tighten security based on their risk analysis.

All communication between peers in these specifications is based on HTTP. All communication MUST be secured using Transport Layer Security, TLS. As a result, all communication MUST be transported over HTTPS (https://tools.ietf.org/html/rfc2818).

For HTTPS and TLS, any implementation MUST take the recommendations in BCP195 (https://tools.ietf.org/html/rfc7525) and the latest version of the NCSC-security guidelines for TLS-usage (currently https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1/ICT-beveiligingsrichtlijnen+voor+Transport+Layer+Security+v2.1.pdf). The following requirements are applicable for this specification in relation to the NCSC guidelines:

- For back-channel communication, the guidelines categorized as "good" MUST be applied.
- For front-channel communication, the guidelines for "good" MUST be applied and the guidelines for "sufficient" MAY be applied, depending on target audience and support requirements.
- Guidelines categorized as "insufficient" MUST NOT be applied and those categorized as "phase out" SHOULD NOT be used.

As HTTP itself is stateless, implementations are free to choose a method of maintaining state or sessions with a User-agent when applicable. The following applies for any HTTP state/session mechanism:

- HTTP servers MUST ensure session and state information is secured and User-agents are properly instructed with relevant security settings (e.g. proper cookie lifetime, Secure setting for cookies, CORS headers and similar).
- Any HTTP session or state tracking mechanisms MUST be implemented using current best practices to avoid session hijacking and other attacks. For more information, see for instance https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Session_Management_Cheat_Sheet.md.

Secure cookies

If a participant uses cookies to store user preferences and/or session information, the parameters *Secure* and *HttpOnly* SHOULD be used.

For the cookie that is used to store AD selection by HM, refer to Single sign-on and user sessions.

Synchronize system clocks

The network uses Coordinated Universal Time, i.e. UTC. All time stamps in the messages are formatted as **yyyy-mm-ddThh:mm:ssZ**. The T(time) and Z (zulu) are fixed values.

Each participant and service provider MUST synchronize the system with a reliable and precise time source so the system time never deviates more than 2 seconds either way.

Interface Specifications Auxillary Systems

The interface is provided by the BSNk, for more information you can contact the beheerorganisatie BSNk via **servicecentrum@logius.nl.**

Interface specifications aux HM-BSNk - ProvideDVkeys

This interface between a HM and BSNk Key Management (BSNk-Sleutelbeheer) enables a HM to request DV-keys that are required by every Service Provider (Dienstverlener) to get an identity (e.g. BSN) or persistent pseudonym as a result of an authentication request. Further information about the Sleutelbeheer role of BSNk can be found in the BSNk documentation. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.The HM MUST:

- Only initiate the request based on a authentic request of the DV.
- Hand over the key material unaltered to the DV, using measures to ensure integrity and confidentiality.

DV-key format

Information about the technical format of the key file provided to Dienstverleners (Service Providers) can be found in the BSNk documentation. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.

Interface Specifications aux MR - BSNk

The BSNk shall expose web services for MachtigingsRegisters and publish the corresponding WSDL document. Further information can be found in the BSNk documentation. Voor meer informatie kunt u contact opnemen met de beheerorganisatie BSNk via servicecentrum@logius.nl.

BSNk: activate

The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

This interface between a MachtigingsRegister and BSNk is used to activate a user's social security number (BSN) for government related electronic services. The activation requires a BSN and validation data and will result in the provisioning of one or more Polymorphic Pseudonymization structures (e. g. Polymorphic Identity and Polymorphic Pseudonym) by the BSNk.

The interface described in this document is used to implement the use case "AUC6 Activeren BSN" (activate BSN) and MUST be implemented by every MachtigingsRegister.

WSDL

WSDL activate

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  name="BSNK_activate"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">

            <xsd:import namespace="urn:oasis:names:tc:SAML:2.0:assertion" schemaLocation="saml-schema-assertion-
2.0.xsd"/>

            <xsd:element name="ProvidePPRequest" type="bsnk:ProvidePolymorphicRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide PP for a
                        specific user, for future use via ProvideEP queries.
                        The 'BSNk' will generate one or more
                        polymorphic pseudonym(s) for the identified user.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ProvidePP_PPCAOptimizedRequest" type="bsnk:ProvidePolymorphicRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide PP for a
                        specific user, for future use via ProvideEP queries.
                        The 'BSNk' will generate one or more
                        polymorphic pseudonym(s) for the identified user. This
                        request will result in one-or-more polymorphic
                        pseudonyms in a form optimized for usage as a PPCA.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvidePolymorphicRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="RequesterKeySetVersion" type="bsnk:KeyVersionType" />
                            <xsd:choice>
                                <xsd:element name="BSN" type="bsnk:BSNType" />
                                <xsd:element name="EncryptedBSN" type="bsnk:EncryptedBSNType"/>
                                <xsd:element name="EncryptedIdentity" type="bsnk:EncryptedIdentityType" />
                                <xsd:sequence>
                                    <xsd:element name="eIDAS-UniquenessID" type="bsnk:eIDAS-UniquenessIDType"/>
                                    <xsd:element name="EncryptedBSN" type="bsnk:EncryptedBSNType" minOccurs="0"
/>
                                </xsd:sequence>
```

```
                </xsd:choice>
                <xsd:element name="DocumentType" type="bsnk:DocumentTypeType" minOccurs="0" />
                <xsd:element name="DocumentID" type="bsnk:DocumentIDType" minOccurs="0" />
                <xsd:element name="GivenNames" type="bsnk:GivenNamesType" minOccurs="0" />
                <xsd:element name="SurName" type="bsnk:SurNameType" minOccurs="0" />
                <xsd:element name="DateOfBirth" type="bsnk:BirthDateType" minOccurs="0" />
                <xsd:element name="PlaceOfBirth" type="bsnk:PlaceOfBirthType" minOccurs="0" />
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>
<xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
    <xsd:sequence>
        <xsd:element name="Requester" type="bsnk:OINType" />
    </xsd:sequence>
    <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
    <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
</xsd:complexType>
<xsd:simpleType name="KeyVersionType">
    <xsd:annotation>
        <xsd:documentation>Key(set) version type.</xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:positiveInteger"/>
</xsd:simpleType>
<xsd:simpleType name="BSNType">
    <xsd:annotation>
        <xsd:documentation>In case a BSN consists of a number of
           only 8 digits, the BSN shall be padded with a preceding
           '0' (digit zero).
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:length value="9" />
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="EncryptedIdentityType">
    <xsd:annotation>
        <xsd:documentation>Identity encrypted as an EncryptedIdentity
            according to Polymorphic Pseudonimization.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:base64Binary" />
</xsd:simpleType>
<xsd:simpleType name="eIDAS-UniquenessIDType">
    <xsd:annotation>
        <xsd:documentation>To be used only in eIDAS context.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string" />
</xsd:simpleType>
<xsd:complexType name="EncryptedBSNType">
    <xsd:annotation>
        <xsd:documentation>BSN encrypted in the form of a
            SAML2 EncryptedID.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
        <xsd:element ref="saml2:EncryptedID" />
    </xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="OINType">
    <xsd:annotation>
        <xsd:documentation>OIN type.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:length value="20" />
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="DocumentIDType">
    <xsd:annotation>
```

```
            <xsd:documentation>Document ID as appearing on the Identity
                Document referenced
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="15" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="DocumentTypeType">
        <xsd:annotation>
            <xsd:documentation>Type of Identity Document referenced.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="NL-Paspoort" />
            <xsd:enumeration value="NL-Identiteitskaart" />
            <xsd:enumeration value="NL-Rijbewijs" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="GivenNamesType">
        <xsd:annotation>
            <xsd:documentation>Given names as these appear on the
                Identity Document referenced. If given names are not
                fully known than must contain all known initials.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="200" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="SurNameType">
        <xsd:annotation>
            <xsd:documentation>Surname as appears on the
                Identity Document referenced.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="210" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="BirthDateType">
        <xsd:union>
            <xsd:simpleType>
                <xsd:restriction base="xsd:date" />
            </xsd:simpleType>
            <xsd:simpleType >
                <xsd:restriction base="xsd:gYearMonth" />
            </xsd:simpleType>
            <xsd:simpleType >
                <xsd:restriction base="xsd:gYear" />
            </xsd:simpleType>
        </xsd:union>
    </xsd:simpleType>
    <xsd:simpleType name="PlaceOfBirthType">
        <xsd:annotation>
            <xsd:documentation>For Dutch places of birth this value
                must correspond to the exact value as listed in table
                33 of the logic design of the BRP. MUST NOT be used for
                foreign places of birth.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="40" />
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:element name="ProvidePPResponse" type="bsnk:ProvidePolymorphicResponseType">
        <xsd:annotation>
            <xsd:documentation>
                Response to a ProvidePPRequest or
                ProvidePP_PPCAOptimizedRequest.
            </xsd:documentation>
```

```
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="ProvidePP_PPCAOptimizedResponse" type="bsnk:ProvidePolymorphicResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a ProvidePP_PPCAOptimizedRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvidePolymorphicResponseType">
            <xsd:complexContent>
                <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                    <xsd:sequence>
                        <xsd:element name="PolymorphicPseudonym" type="bsnk:PolymorphicPseudonymType"
maxOccurs="unbounded" />
                    </xsd:sequence>
                </xsd:extension>
            </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
            <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
            <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
            <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
        </xsd:complexType>
        <xsd:complexType name="PolymorphicPseudonymType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:base64Binary" />
            </xsd:simpleContent>
        </xsd:complexType>
        <xsd:element name="ProvidePolymorphicFault" type="bsnk:ProvidePolymorphicFaultType">
            <xsd:annotation>
                <xsd:documentation>
                    Fault response to a ProvidePPRequest or
                    ProvidePP_PPCAOptimizedRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ProvidePolymorphicFaultType">
            <xsd:sequence>
                <xsd:element name="FaultReason" type="bsnk:ProvidePolymorphicFaultReasonType" />
                <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType" maxOccurs="unbounded"
/>
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="ProvidePolymorphicFaultReasonType">
            <xsd:union memberTypes="bsnk:FaultReasons bsnk:ProvidePolymorphicFaultReasons" />
        </xsd:simpleType>
        <xsd:simpleType name="FaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotFound">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            zero matches.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="AuthorizationError">
                    <xsd:annotation>
                        <xsd:documentation>Authentication invalid or access denied.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Request invalid.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="TemporarilyUnavailable">
                    <xsd:annotation>
                        <xsd:documentation>Request could temporarily not be
```

```
                            processed. A new request for activation MAY be send
                            at a later moment by the requesting party.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="ProvidePolymorphicFaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotEnoughInfo">
                    <xsd:annotation>
                        <xsd:documentation>Provided information may resolve
                            to a unique match, but not enough assurance
                            (e.g. against typos) can be established.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="NotUnique">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            more than one match.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="DocumentRejected">
                    <xsd:annotation>
                        <xsd:documentation>Document not accepted.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="ProvisioningRefused">
                    <xsd:annotation>
                        <xsd:documentation>Activation refused for other
                            (non-disclosed) reason.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:complexType name="FaultDescriptionType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:string">
                    <xsd:attribute name="lang" type="xsd:language" />
                </xsd:extension>
            </xsd:simpleContent>
        </xsd:complexType>
    </xsd:schema>
</wsdl:types>

<wsdl:message name="BSNK_ProvidePPRequest">
    <wsdl:part name="in" element="bsnk:ProvidePPRequest" />
</wsdl:message>

<wsdl:message name="BSNK_ProvidePP_PPCAOptimizedRequest">
    <wsdl:part name="in" element="bsnk:ProvidePP_PPCAOptimizedRequest" />
</wsdl:message>

<wsdl:message name="BSNK_ProvidePPResponse">
    <wsdl:part name="out" element="bsnk:ProvidePPResponse" />
</wsdl:message>

<wsdl:message name="BSNK_ProvidePP_PPCAOptimizedResponse">
    <wsdl:part name="out" element="bsnk:ProvidePP_PPCAOptimizedResponse" />
</wsdl:message>

<wsdl:message name="BSNK_ProvidePolymorphicFault">
    <wsdl:part name="fault" element="bsnk:ProvidePolymorphicFault" />
</wsdl:message>

<wsdl:portType name="BSNK_Activate_Port">
    <wsdl:operation name="BSNK_ProvidePP">
```

```
            <wsdl:input message="bsnk:BSNK_ProvidePPRequest" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvidePPRequest" />
            <wsdl:output message="bsnk:BSNK_ProvidePPResponse" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvidePPResponse" />
            <wsdl:fault message="bsnk:BSNK_ProvidePolymorphicFault" name="BSNK_ProvidePolymorphic_Fault"/>
        </wsdl:operation>
        <wsdl:operation name="BSNK_ProvidePP_PPCAOptimized">
            <wsdl:input message="bsnk:BSNK_ProvidePP_PPCAOptimizedRequest" wsam:Action="urn:nl-gdi-eid:1.0:
webservices:ProvidePP_PPCAOptimizedRequest" />
            <wsdl:output message="bsnk:BSNK_ProvidePP_PPCAOptimizedResponse" wsam:Action="urn:nl-gdi-eid:1.0:
webservices:ProvidePP_PPCAOptimizedResponse" />
            <wsdl:fault message="bsnk:BSNK_ProvidePolymorphicFault" name="BSNK_ProvidePolymorphic_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNK_Activate_SOAP" type="bsnk:BSNK_Activate_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNK_ProvidePP">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvidePPRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNK_ProvidePolymorphic_Fault">
                <soap:fault name="BSNK_ProvidePolymorphic_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="BSNK_ProvidePP_PPCAOptimized">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvidePP_PPCAOptimizedRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNK_ProvidePolymorphic_Fault">
                <soap:fault name="BSNK_ProvidePolymorphic_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="BSNK_Activate_Service">
        <wsdl:port binding="bsnk:BSNK_Activate_SOAP" name="BSNK_Activate">
            <soap:address location="https://.../TODO/Activate" />
        </wsdl:port>
    </wsdl:service>

</wsdl:definitions>
```

Request

Consists of a registration request message <ProvidePPRequest> in the SOAP body of the request message. SOAP should be implemented according to the Web services requirements.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this Request
<Requester>	1	EntityID (OIN) of the requesting MachtigingsRegister.
<RequesterKeySetVersion>	1	Key set version of the requesting MachtigingsRegister .
<BSN>	0..1	

		Sector ID for Dutch citizens. String of 9 characters, in case a BSN consists of a number of only 8 digits, the BSN shall be padded with a preceding '0' (digit zero). As verification data at least DocumentID and one or more other identity supporting elements (those other than DocumentType) MUST be provided. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<EncryptedBSN>	0..1	An encrypted BSN. This BSN MUST be encrypted using XML-encryption, as per (XML/SAML) Encryption. Either a BSN, EncryptedBSN, EncryptedIdentity or eIDAS-uniquenessID MUST be provided.
<EncryptedIdentity>	0..1	Identity (typically BSN) encrypted as EncryptedIdentity under Polymorphic Pseudonimization. Either a BSN, EncryptedBSN, or EncryptedIdentity MUST be provided.
<EncryptedBSN>	0..1	At this moment an encryptedBSN is for exclusive use by an eIDAS-berichtenservice.
<DocumentType>	0..1	String max 20 chars. Value represents the type of government-issued document that was used. Possible values are "NL-Paspoort", "NL-Identiteitskaart" and "NL-Rijbewijs".
<DocumentID>	0..1	String max 15 chars. Value represents the ID of a government-issued document that was used. MUST be present together with <DocumentType>.
<GivenNames>	0..1	String max 200 chars. Must contain all given names, if given names are not fully known than MUST contain all known Initials. MUST be present together with <*SurName*>. An empty value can be used to specify the current subject has not registered a given name in the BRP.
<SurName>	0..1	String max 210 chars. Surname including prefixes, as stated on the Identity Document. MUST be present together with <*GivenNames*>.
<DateOfBirth>	0..1	Date of birth of the user. In XML-schema a choice between 'date', 'gYear' or 'gYearMonth' format. In case the specific day or month is unknown (also expressed as 1900-*00-00* or 1900-03-*00*), the value MUST be expressed as a gYear or gYearMonth.
<PlaceOfBirth>	0..1	String max 40 chars. NB For Dutch places of birth this value MUST correspond to the exact value as listed in table 33 of the logic design of the BRP (see https://publicaties.rvig.nl/) MUST NOT be used for foreign places of birth.

N.B. Only providing the BSN is not deemed to identify a subject with sufficient assurance, additional information must be provided for verification. In general: the more information is provided in the request, the more chance of a unique match with sufficient assurance.

DocumentType and DocumentID will be deprecated and removed in future revisions of this interface.

Response

Consists of a response message <ProvidePPResponse> in the SOAP body of the response message, containing one or more Polymorphic Pseudonyms. In case a response is received, the request resulted in a unique and valid match and the cryptographic transformation of the specified BSN to a Polymorphic Pseudonym and/or Polymorphic Identity. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) localized <FaultDescription>s.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the Response
@InResponseTo	1	Unique identifier of the Request this is a response to (@RequestID of request)
<PolymorphicPseudonym>	1..n	One or more signed Polymorphic Pseudonymization structure(s) for the User. At least one structure MUST be provided, the exact number depends on the request and requester: ▪ A <ProvicePPRequest> will receive one Signed Polymorphic Identity and one Signed Polymorphic Pseudonym. ▪ A <ProvidePP_PPCAOptimizedRequest> will receive one Signed PIP and one Signed Polymorphic Pseudonym.

For encoding of the Signed Polymorphic Identity / Pseudonym / PIP, see Handreiking Polymorphic Pseudonimization Notation.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
NotEnoughInfo	Request rejected. Provided information may resolve to a unique match, but not enough assurance (e.g. against typos) can be established.
NotUnique	Request rejected. Provided information results in more than one match.
NotFound	Request rejected. Provided information results in zero matches.
DocumentRejected	Request rejected. Document not accepted.
ProvisioningRefused	Request rejected. Activation refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for activation MAY be sent at a later moment by the requesting party.

BSNk: registerStatusEIM

The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

A MachtigingsRegister uses this interface to register the status the collection(s) of authorizations per person at the BSNk Inzageregister, every time when a new authorization is added or the status of the collection is changed. A MachtigingsRegister MUST register the status of every 'collection of authorizations' (with a description) BSNk Inzageregister that makes sense to the involved Person. A MachtigingsRegister MUST NOT register the status of every individual autorisation. As a minimum a MachtigingsRegister MUST make a distinction between autorisations with this Person as Representative and as Representee. At this moment ETD only supports Representee! As a maximum a MachtigingsRegister can register multiple collections of authorizations at the BSNk Inzageregister, for instance with a specific purpose eg "Business authorizations for administrative employees".

The interface described in this document is used to implement the use case AUC6 Activeren BSN and MUST be implemented by every MachtigingsRegister.

WSDL registerStatusEIM

```
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  name="BSNK_registerStatusEIM"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">

            <xsd:element name="RegisterStatusEIMRequest" type="bsnk:RegisterStatusEIMRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to register a EIM status.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="RegisterStatusEIMRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="EncryptedPseudonym" type="bsnk:EncryptedPseudonymType" />
                            <xsd:element name="DeprecatedEP" type="bsnk:EncryptedPseudonymType" minOccurs="0"/>
                            <xsd:element name="MeansNumber" type="bsnk:MeansNumberType" />
                            <xsd:element name="StatusDateTime" type="xsd:dateTime" />
                            <xsd:element name="LevelOfAssurance" type="bsnk:LevelOfAssuranceType" />
                            <xsd:element name="MeansType" type="bsnk:MeansType" />
                            <xsd:element name="Domains" type="bsnk:DomainsType" minOccurs="0"/>
                            <xsd:element name="ReadableCardInfo" type="bsnk:ReadableCardInfoType" minOccurs="0"
/>
                            <xsd:element name="IDP" type="bsnk:OINType" minOccurs="0" />
                            <xsd:element name="Status" type="bsnk:StatusType" />
                            <xsd:element name="RevocationURL" type="bsnk:RevocationURLType" minOccurs="0" />
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
                <xsd:sequence>
                    <xsd:element name="Requester" type="bsnk:OINType" />
                </xsd:sequence>
                <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
                <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
            </xsd:complexType>
            <xsd:simpleType name="MeansNumberType">
                <xsd:restriction base="xsd:string">
                    <xsd:maxLength value="16" />
```

```
<!--                    <xsd:pattern value="[0-9]+"></xsd:pattern> -->
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="LevelOfAssuranceType">
            <xsd:restriction base="xsd:anyURI">
<!--                    <xsd:maxLength value="128" /> -->
                <xsd:enumeration value="http://eidas.europa.eu/LoA/substantial" />
                <xsd:enumeration value="http://eidas.europa.eu/LoA/high" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:complexType name="DomainsType">
            <xsd:sequence>
                <xsd:element name="Domain" type="bsnk:DomainType" minOccurs="1" maxOccurs="2"/>
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="DomainType">
            <xsd:restriction base="xsd:token">
                <xsd:enumeration value="Private" />
                <xsd:enumeration value="Public" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="MeansType">
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="25" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="StatusType">
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="64" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="EncryptedPseudonymType">
            <xsd:annotation>
                <xsd:documentation>Pseudonym encrypted as an EncryptedPseudonym
                    according to Polymorphic Pseudonimization.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:base64Binary" />
        </xsd:simpleType>
        <xsd:simpleType name="ReadableCardInfoType">
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="40" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="RevocationURLType">
            <xsd:restriction base="xsd:anyURI">
                <xsd:maxLength value="1024" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="OINType">
            <xsd:annotation>
                <xsd:documentation>OIN type.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:length value="20" />
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:element name="RegisterStatusEIMResponse" type="bsnk:RegisterStatusEIMResponseType">
            <xsd:annotation>
                <xsd:documentation>
                    Response to a RegisterStatusEIMRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="RegisterStatusEIMResponseType">
            <xsd:complexContent>
                <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
                    <xsd:sequence>
                        <xsd:element name="Status" type="bsnk:StatusType" />
                    </xsd:sequence>
```

```
                </xsd:extension>
            </xsd:complexContent>
        </xsd:complexType>
        <xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
            <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
            <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
            <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
        </xsd:complexType>
        <xsd:element name="RegisterStatusEIMFault" type="bsnk:RegisterStatusEIMFaultType">
            <xsd:annotation>
                <xsd:documentation>
                    Fault response to a RegisterStatusEIMRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="RegisterStatusEIMFaultType">
            <xsd:sequence>
                <xsd:element name="FaultReason" type="bsnk:RegisterStatusEIMFaultReasonType" />
                <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType" maxOccurs="unbounded"
/>
            </xsd:sequence>
        </xsd:complexType>
        <xsd:simpleType name="RegisterStatusEIMFaultReasonType">
            <xsd:union memberTypes="bsnk:FaultReasons bsnk:RegisterStatusEIMFaultReasons" />
        </xsd:simpleType>
        <xsd:simpleType name="FaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotFound">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            zero matches.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="AuthorizationError">
                    <xsd:annotation>
                        <xsd:documentation>Authentication invalid or access denied.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Request invalid.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="TemporarilyUnavailable">
                    <xsd:annotation>
                        <xsd:documentation>Request could temporarily not be
                            processed. A new request for activation MAY be send
                            at a later moment by the requesting party.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:simpleType name="RegisterStatusEIMFaultReasons">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="NotUnique">
                    <xsd:annotation>
                        <xsd:documentation>Provided information results in
                            more than one match.
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="RegistrationRefused">
                    <xsd:annotation>
                        <xsd:documentation>Registration refused for other
                            (non-disclosed) reason.
                        </xsd:documentation>
                    </xsd:annotation>
```

```
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:complexType name="FaultDescriptionType">
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="lang" type="xsd:language" />
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="BSNK_RegisterStatusEIMRequest">
        <wsdl:part name="in" element="bsnk:RegisterStatusEIMRequest" />
    </wsdl:message>

    <wsdl:message name="BSNK_RegisterStatusEIMResponse">
        <wsdl:part name="out" element="bsnk:RegisterStatusEIMResponse" />
    </wsdl:message>

    <wsdl:message name="BSNK_RegisterStatusEIMFault">
        <wsdl:part name="fault" element="bsnk:RegisterStatusEIMFault" />
    </wsdl:message>

    <wsdl:portType name="BSNK_RegisterStatusEIM_Port">
        <wsdl:operation name="BSNK_RegisterStatusEIM">
            <wsdl:input message="bsnk:BSNK_RegisterStatusEIMRequest" wsam:Action="urn:nl-gdi-eid:1.0:
webservices:RegisterStatusEIMRequest" />
            <wsdl:output message="bsnk:BSNK_RegisterStatusEIMResponse" wsam:Action="urn:nl-gdi-eid:1.0:
webservices:RegisterStatusEIMResponse" />
            <wsdl:fault message="bsnk:BSNK_RegisterStatusEIMFault" name="BSNK_RegisterStatusEIM_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNK_RegisterStatusEIM_SOAP" type="bsnk:BSNK_RegisterStatusEIM_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNK_RegisterStatusEIM">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:RegisterStatusEIMRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNK_RegisterStatusEIM_Fault">
                <soap:fault name="BSNK_RegisterStatusEIM_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="BSNK_RegisterStatusEIM_Service">
        <wsdl:port binding="bsnk:BSNK_RegisterStatusEIM_SOAP" name="BSNK_RegisterStatusEIM">
            <soap:address location="https://.../TODO/RegisterStatusEIM" />
        </wsdl:port>
    </wsdl:service>

</wsdl:definitions>
```

Request

Consists of a registration request message <RegisterStatusEIMRequest> in the SOAP body of the request message. SOAP should be implemented accoording to the Web services requirements .

Element/@Attribute	0..n	Description

@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this request
<Requester>	1	EntityID (OIN) of the requesting MachtigingsRegister.
<EncryptedPseudonym>	1	Encrypted Pseudonym of the user to be transformed to a pseudonym for the BSNk Inzageregister
<LevelOfAssurance>	1	Choice http://eidas.europa.eu/LoA/substantial or http://eidas.europa.eu/LoA/high. Specifies the (highest) LoA of any active registered authorization (either as "Representative" or "Representee").
<MeansNumber>	1	For a MachtigingsRegister MeansNumber identifies the 'collection of authorizations' to which the status applies. As a minimum a MachtigingsRegister MUST make a distinction between (a collection with) autorisations with this Person as Representative and as Representee. At this moment ETD only supports Representee! As a maximum a MachtigingsRegister can register multiple collections of authorizations at the BSNk Inzageregister, that makes sense for this specific Person. A MachtigingsRegister MUST NOT register the status of every individual autorisation. MeansNumber MUST be unique per user , but MUST not be usable to identify the user. For privacy reasons this MeansNumber MUST have a low entropy, preferably 01, 02 ...09, so that many users have the same MeansNumber(s).
<StatusDateTime>	1	DateTime of status change, MUST not be after @DateTime of this request. The resolution of this field MUST be between (inclusive) minutes and milliseconds.
<MeansType>	1	String max 25 chars. MeansType represents a – for the user – readable version of the type of authorizations'. For the ETD MachtigingsRegister the type SHOULD always be "Machtiging". Note, other authorization types (not ETD) could be "Wettelijke Vertegenwoordiging" or "Volmacht".
<Domains>	0..1	The domains where the autorisations can be used, optional.
<Domain>	1..n	One element per domain for which the autorisations can be used. Allowed values are 'Public' and 'Private'.
<ReadableCardInfo>	0..1	String max 60 chars. ReadableCardInfo is text that – combined with the MeansType – has just enough information for a user to recognise the specific 'collection of authorizations' in the domain of the MachtigingsRegister. ReadableCardInfo MUST be unique per user, but MUST not be usable to identify the user. F or privacy reasons this ReadableCardInfo MUST have a low entropy so that many users have this same Readable CardInfo. For Autorisations a second part has to be added with the date of the last added Autorisation eg "Last Authorization added at 31-01-2018". Therefor the MR has to register a new status with every new autorisation. For MachtigingsRegister this element is required for every registration to have the most actual "Last Autorisation" (any new will overwrite the old text).
<Status>	1	*MUST contain one of the specified statusses:* ***Activated*** (as long as any authorization in this collection is active in the BSN Domain), ***Suspended*** (if the last active authorization in this collection is suspended), ***Expired*** (if the last active authorization in this collection is expired) or ***Revoked*** (if the last active authorization in this collection is Revoked). This element is required for every registration to have the most actual status. Any new status will overwrite the old status.
<RevocationURL>	0..1	String max 1024 chars. RevocationURL is a valid URL which can be used by mijnoverheid (when providing the user an overview of electronic identification means) to redirect the user to the MachtigingsRegister for managing this collection of autorisations, for instance suspending authorizations. For privacy reasons this RevocationURL can have a random collection-specific unique-ID (not a userid!), but otherwise MUST consist of low entropy data. The URL could use other elements from this registration request message (except En cryptedPseudonym). In the Metadata the RoleDescriptor for MachtigingsRegister already has a generic URL to the MachtigingsRegister authorization management function. That URL will be default unless a RevocationURL is provided. This RevocationURL could be used to direct the user directly to the appropriate collection of authorizations. Or a RevocationURL with a random collection-specific unique-ID could me used to immediately Suspend the collection for a short period of time , possibly even without authenticating the user. Any new will overwrite the old text and empty string can be used to cancel the (working of this) RevocationURL.

Processing rules for Status Registration Request

A requesting MachtigingsRegister

- MUST await a successful response or retry to send the request. Requests MUST be buffered and retried during 7 days.
- SHOULD adhere to a maximum of 1 status update per unit of the resolution of the StatusDateTime, otherwise the MU SHOULD increase the resolution of the StatusDateTime.
- MUST log and investigate failures.

Response

Consists of a response message <RegisterStatusEIMResponse> in the SOAP body of the request message. In case a response is received, the request resulted in new or a unique and valid match of an existing electronic identification means. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) localized <FaultDescription>.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the response
@InResponseTo	1	Unique identifier of the request this is a response to (@RequestID of request)

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
NotUnique	Request rejected. Provided information results in more than one match.
NotFound	Request rejected. Provided information results in zero matches.
RegistrationRefused	Request rejected. Registration refused for other non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for registration MAY be sent at a later moment by the requesting party.

BSNk: transform

The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

In order to realize step 7 in the AUC3.1 Registreren bevoegdheid eenmanszaken an interface is necessary beween the MR and BSNk. This interface wil implement AUC6 Activeren BSN for the MR. In order to facilitate the transformation of the PI this interface will also implement AUC10 Transformeren. This will allow the MR to transform the PI to the VI of the owner of the sole trader for the DV who requested this information.

This interface describes the message exchange between MR and BSNk. It fulfills two functions: obtaining a Polymorphic Pseudonym and Polymorphic Identity for a newly registered user with the MR (activate) and transforming a Polymorphic Pseudonym or Polymorphic Identity to an Encrypted Pseudonym or Encrypted Identity specialized for a Relying Party.

Interface Transform

This interface between an Machtigingenregisterand BSNk transforms a given Polymophic Pseudonym to a Relying Party specific Encrypted Pseudonym or Polymorphic Identity to an Encrypted Identity. An Machtigingenregister uses this interface after authenticating an User.

WSDL transform

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
                  xmlns:bsnk="urn:nl-gdi-eid:1.0:webservices"
                  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
                  name="BSNk_transform"
                  targetNamespace="urn:nl-gdi-eid:1.0:webservices">

    <wsdl:types>
        <xsd:schema targetNamespace="urn:nl-gdi-eid:1.0:webservices"
                    attributeFormDefault="unqualified"
                    elementFormDefault="qualified">
            <xsd:element name="ProvideEPRequest" type="bsnk:ProvideEncryptedRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide an encrypted
                        pseudonym of a user for a specific relying party
                        (service provider).
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ProvideEIRequest" type="bsnk:ProvideEncryptedRequestType">
                <xsd:annotation>
                    <xsd:documentation>Request message to provide an encrypted
                        identity of a user for a specific relying party
                        (service provider).
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideEncryptedRequestType">
                <xsd:complexContent>
                    <xsd:extension base="bsnk:BSNkProvideRequestBasetype">
                        <xsd:sequence>
                            <xsd:element name="RelyingParty" type="bsnk:OINType" />
                            <xsd:element name="RelyingPartyKeySetVersion" type="bsnk:KeyVersionType" />
                            <xsd:element name="PolymorphicPseudonym" type="bsnk:PolymorphicPseudonymType" />
                            <xsd:element name="Role" type="bsnk:RoleType" minOccurs="0" />
                            <xsd:element name="TransactionID" type="bsnk:TransactionIDType" minOccurs="0" />
                        </xsd:sequence>
                    </xsd:extension>
                </xsd:complexContent>
            </xsd:complexType>
            <xsd:complexType name="BSNkProvideRequestBasetype" abstract="true">
                <xsd:sequence>
                    <xsd:element name="Requester" type="bsnk:OINType" />
```

```
    </xsd:sequence>
    <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
    <xsd:attribute name="RequestID" type="xsd:ID" use="required" />
</xsd:complexType>
<xsd:complexType name="PolymorphicPseudonymType">
    <xsd:simpleContent>
        <xsd:extension base="xsd:base64Binary"/>
    </xsd:simpleContent>
</xsd:complexType>
<xsd:simpleType name="KeyVersionType">
    <xsd:annotation>
        <xsd:documentation>Key(set) version type.</xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:positiveInteger"/>
</xsd:simpleType>
<xsd:simpleType name="OINType">
    <xsd:annotation>
        <xsd:documentation>OIN type.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:length value="20" />
    </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="RoleType">
    <xsd:annotation>
        <xsd:documentation>Role type.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:integer"/>
</xsd:simpleType>
<xsd:simpleType name="TransactionIDType">
    <xsd:annotation>
        <xsd:documentation>TransactionID Type.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string">
        <xsd:length value="128" />
    </xsd:restriction>
</xsd:simpleType>

<xsd:element name="ProvideEPResponse" type="bsnk:ProvideEncryptedResponseType">
    <xsd:annotation>
        <xsd:documentation>
            Response to a ProvideEPRequest.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="ProvideEIResponse" type="bsnk:ProvideEncryptedResponseType">
    <xsd:annotation>
        <xsd:documentation>
            Response to a ProvideEIRequest.
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:complexType name="ProvideEncryptedResponseType">
    <xsd:complexContent>
        <xsd:extension base="bsnk:BSNkProvideResponseBasetype">
            <xsd:sequence>
                <xsd:element name="EncryptedPseudonym" type="bsnk:EncryptedPseudonymType" />
            </xsd:sequence>
        </xsd:extension>
    </xsd:complexContent>
</xsd:complexType>
<xsd:complexType name="BSNkProvideResponseBasetype" abstract="true">
    <xsd:attribute name="DateTime" type="xsd:dateTime" use="required" />
    <xsd:attribute name="ResponseID" type="xsd:ID" use="required" />
    <xsd:attribute name="InResponseTo" type="xsd:NCName" use="required" />
</xsd:complexType>
<xsd:simpleType name="EncryptedPseudonymType">
    <xsd:restriction base="xsd:base64Binary" />
```

```
            </xsd:simpleType>
            <xsd:element name="ProvideEncryptedFault" type="bsnk:ProvideEncryptedFaultType">
                <xsd:annotation>
                    <xsd:documentation>
                        Fault response to a ProvideEPRequest of ProvideEIRequest.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ProvideEncryptedFaultType">
                <xsd:sequence>
                    <xsd:element name="FaultReason" type="bsnk:ProvideEncryptedFaultReasonType" />
                    <xsd:element name="FaultDescription" type="bsnk:FaultDescriptionType" maxOccurs="unbounded"
/>
                </xsd:sequence>
            </xsd:complexType>
            <xsd:simpleType name="ProvideEncryptedFaultReasonType">
                <xsd:union memberTypes="bsnk:FaultReasons bsnk:ProvideEncryptedFaultReasons" />
            </xsd:simpleType>
            <xsd:simpleType name="FaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="NotFound">
                        <xsd:annotation>
                            <xsd:documentation>Provided information results in
                                zero matches.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="AuthorizationError">
                        <xsd:annotation>
                            <xsd:documentation>Authentication invalid or access denied.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="SyntaxError">
                        <xsd:annotation>
                            <xsd:documentation>Request invalid.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="TemporarilyUnavailable">
                        <xsd:annotation>
                            <xsd:documentation>Request could temporarily not be
                                processed. A new request for provisioning MAY be
                                send at a later moment by the requesting party.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="ProvideEncryptedFaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="ProvisioningRefused">
                        <xsd:annotation>
                            <xsd:documentation>Transformation refused for other
                                (non-disclosed) reason.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:complexType name="FaultDescriptionType">
                <xsd:simpleContent>
                    <xsd:extension base="xsd:string">
                        <xsd:attribute name="lang" type="xsd:language" />
                    </xsd:extension>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:schema>
    </wsdl:types>

    <wsdl:message name="BSNk_ProvideEPRequest">
```

```
        <wsdl:part name="in" element="bsnk:ProvideEPRequest" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEIRequest">
        <wsdl:part name="in" element="bsnk:ProvideEIRequest" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEPResponse">
        <wsdl:part name="out" element="bsnk:ProvideEPResponse" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEIResponse">
        <wsdl:part name="out" element="bsnk:ProvideEIResponse" />
    </wsdl:message>

    <wsdl:message name="BSNk_ProvideEncryptedFault">
        <wsdl:part name="fault" element="bsnk:ProvideEncryptedFault" />
    </wsdl:message>

    <wsdl:portType name="BSNk_Transform_Port">
        <wsdl:operation name="BSNk_ProvideEP">
            <wsdl:input message="bsnk:BSNk_ProvideEPRequest" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvideEPRequest" />
            <wsdl:output message="bsnk:BSNk_ProvideEPResponse" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvideEPResponse" />
            <wsdl:fault message="bsnk:BSNk_ProvideEncryptedFault" name="BSNk_ProvideEncrypted_Fault"/>
        </wsdl:operation>
        <wsdl:operation name="BSNk_ProvideEI">
            <wsdl:input message="bsnk:BSNk_ProvideEIRequest" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvideEIRequest" />
            <wsdl:output message="bsnk:BSNk_ProvideEIResponse" wsam:Action="urn:nl-gdi-eid:1.0:webservices:
ProvideEIResponse" />
            <wsdl:fault message="bsnk:BSNk_ProvideEncryptedFault" name="BSNk_ProvideEncrypted_Fault"/>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="BSNk_Transform_SOAP" type="bsnk:BSNk_Transform_Port">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="BSNk_ProvideEP">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvideEPRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNk_ProvideEncrypted_Fault">
                <soap:fault name="BSNk_ProvideEncrypted_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
        <wsdl:operation name="BSNk_ProvideEI">
            <soap:operation soapAction="urn:nl-gdi-eid:1.0:webservices:ProvideEIRequest" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
            <wsdl:fault name="BSNk_ProvideEncrypted_Fault">
                <soap:fault name="BSNk_ProvideEncrypted_Fault" use="literal" />
            </wsdl:fault>
        </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="BSNk_Transform_Service">
        <wsdl:port binding="bsnk:BSNk_Transform_SOAP" name="BSNk_Transform">
            <soap:address location="https://.../TODO/Transform" />
        </wsdl:port>
    </wsdl:service>
```

```
</wsdl:definitions>
```

Request

Consists of a transformation request message <ProvideEPRequest> or <ProvideEIRequest> in the SOAP body of the request message. SOAP should be implemented according to the Web services requirements .

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the request.
@RequestID	1	Unique identifier for this request.
<Requester>	1	EntityID (OIN) of the requesting MachtigingsRegister.
<RelyingParty>	1	EntityID (OIN) of the intended relying party.
<RelyingPartyKeySetVersion>	1	Key set version to be used for relying party.
<PolymorphicPseudonym>	1	Polymorphic Pseudonymization structure for the user to be transformed to an encrypted pseudonym or identity. Only one (non-signed) Polymorphic Pseudonym / Identity MUST be present, depending on the request type.
<Role>	0..1	Optional "persoonsrol". Reserved for future use where the same user can act in different roles, e.g. private, volunteer and employee.
<TransactionID>	0..1	Optional "transactie ID". Reserved for future use where privacy prohibits use of a persistent pseudonym. TransactionID can be used to create a transaction-, session- or case- specific pseudonym. Also for guarantees for the 4-eyes principle, TransactionID can be used in combination with the default Role (otherwise a person could break a 4-eyes signature by using two different Roles). Another example is eIDAS that requires a pseudonym per EU country, for which a countryID can be used als TransactionID to make the resulting pseudonym specific and persistent per country.

Rules for processing a Transformation Request

A requesting MachtigingsRegister:

- MUST authenticate a User at the requested Level of Assurance before requesting a transformation.
- MUST check the relying party is listed in the Autorisatielijst BSN as authorized before requesting transformation of a PI.
    - For ETD this requirement is implemented via the (aggregation) of the ServiceCatalog (by the BO ETD).
- MUST only provide a PP for a <ProvideEPRequest> and MUST only provide a PI for a <ProvideEIRequest>.
- SHOULD randomize the PP/PI to be transformed before requesting a transformation, to enhance the privacy of the User.

Response

Consists of a response message <ProvideEPResponse> or <ProvideEIResponse> in the SOAP body of the response message, containing an Encrypted Pseudonym or Encrypted Identity for the requested Relying Party. In case an error occurs a SOAP fault will be used. The SOAP fault will contain error codes as <FaultReason> as described below, with one (or more) (localized) <FaultDescription>s.

Element/@Attribute	0..n	Description
@DateTime	1	Time of issuing of the response.
@ResponseID	1	Unique identifier of the Response
@InResponseTo	1	Unique identifier of the Request this is a response to (@RequestID of request)
<EncryptedPseudonym>	1	Resulting encrypted form Polymorphic Pseudonymization structure resulting from the transformation. One Signed Encrypted Pseudonym or Signed Encrypted Identity structure for the User for the RelyingParty MUST be present, depending on the request type.

For encoding of the (Signed) Encrypted Pseudonym / Identity, see Polymorphic Pseudonymization Notation.

Rules for processing a Transformation Response:

A receiving MachtigingsRegister:

- SHOULD pass the resulting Signed Encrypted Pseudonym or Signed Encrypted Identity structure unaltered to the relying party.

FaultReasons

The following response codes are used to indicate the status of a response.

ResponseCode	Description
ProvisioningRefused	Request rejected. Transformation of a Polymorphic Pseudonym refused for non-disclosed reason.
AuthorizationError	Request rejected. Authentication invalid or access denied. A HTTP 403 status response MAY be given instead of a SOAP-fault with this response.
SyntaxError	Request rejected. Request invalid.
TemporarilyUnavailable	Request could temporarily not be processed. A new request for transformation of a Polymorphic Pseudonym or Polymorphic Identity MAY be sent at a later moment by the requesting party.

Alternative interfaces

For eHerkenning, the use of Interface specifications DV-HM from versions 1.9 and up are allowed.

An HM MAY offer alternative interfaces to DV's, provided they meet the Information security requirements described in this document.

Prior to doing so, the HM MUST submit the specifications for each alternative interface to the Beheerorganisatie for approval.

Attribute elements

Within the interface specifications, a number of generic SAML, XACML and specific Elektronische Toegangsdiensten attributes are defined. These form our "profile".

- Generic attribute elements
  - EntityID — All systems in the network are identified by a unique EntityID, which is specified in the SAML metadata.
  - Level of assurance — Elektronische Toegangsdiensten distinguishes five different levels of assurance.
  - LinkedDeclarationSignatureValue
  - OIN format — The OIN format is used to indicate participants, service providers and specific types of service consumers and intermediaries. OIN stands for Organization Identifying Number.
  - Pseudonyms — A user may be referred to as follows:
    - Encrypted Pseudonym — An Encrypted Pseudonym is a Persistent Pseudonym encrypted under Polymoprohic Pseudonimization for a specific recipient.
    - Internal pseudonym — The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the user, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the same internal pse
    - Persistent Pseudonym — A Persistent Pseudonym is a pseudonym identifier for a natural person specific for the relying party, that is persistent independent of the Attesting Party.
    - Polymorphic Pseudonym — A Polymorphic Pseudonym is a cryptographic structure that can be transformed into a specific Encrypted Pseudonym, without disclosing the relevant subject due to Polymorphic Pseudonimization.
    - Specific pseudonym — The specific pseudonym is unique for each different combination of user, represented service consumer, intermediary and service provider.
  - ServiceID — ServiceID is an identifier of a service that is unique in the context of the service provider.
  - ServiceUUID — ServiceUUID is an identifier of a service that is unique in the context of the network, but not linked to one service provider.
- SAML attribute elements — This section describes the data elements that occur in messages as SAML attribute element.
  - ActingSubjectID — A SAML Attribute element with one or more identities of the user for one or more Relying Parties.
  - AuthorizationRegistryID — A SAML Attribute element with an EntityID from the MR that must be queried in the use case GUC4 Aantonen bevoegdheid.
  - DeprecatedActingSubjectID — A SAML Attribute element with one or more deprecated identities of the user for one or more Relying Parties, used to support migrations of identifiers.
  - EherkenningPreferredLanguage — A URL or POST variable containing the language preference of user.
  - EntityConcernedID (SAML) — A SAML Attribute element with the identifying attribute of the service consumer that is represented by the user (who might be the same).
  - IntendedAudience — A SAML Attribute element with an EntityID from the DV that will be the recipient of the response.
  - Representation — A SAML Attribute element with an indication whether there is an issue of representation
  - ServiceID (SAML) — A SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
  - ServiceUUID (SAML) — A SAML Attribute element with the ServiceUUID of the service for which access is being requested or for which authorization has been determined.
- XACML attribute elements — This chapter describes all of the XACML data elements defined for Elektronische Toegangsdiensten.
  - ActingEntityID — A XACML Attribute element containing the specific pseudonym of the user.
  - ActingSubjectID (XACML)
  - Action-ID — A XACML Attribute element containing the action ID.
  - AssertionConsumerServiceIndex — An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the Herkenningsmakelaar.
  - Assertions
  - DeprecatedActingSubjectID (XACML) — A XACML Attribute element containing the specific pseudonym of the user, for purposes of migrating user identifiers.
  - EncryptedAttribute — An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the Attribute catalog.
  - Intermediates — A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
  - LegalSubjectID
  - LevelOfAssurance — A XACML Attribute element containing the minimum level of assurance that is required by the service provider.
  - LevelOfAssuranceUsed — An XACML Attribute element containing the level of assurance of the registered authorization.
  - ServiceID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceID (SAML).
  - ServiceUUID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceUUID (SAML).

Generic attribute elements

- EntityID
- Level of assurance
- LinkedDeclarationSignatureValue
- OIN format
- Pseudonyms
    - Encrypted Pseudonym
    - Internal pseudonym
    - Persistent Pseudonym
    - Polymorphic Pseudonym
    - Specific pseudonym
- ServiceID
- ServiceUUID

EntityID

All systems in the network are identified by a unique EntityID, which is specified in the SAML metadata.The EntityID has the format **urn:etoegang:<ROLE>:<OIN>:entities:<index>** where <ROLE> can have the values DV, HM, AD, MR or EB, <OIN> represents the OIN of the participant. The <index> is a number between 0 and 8999 that can be selected by the participant or the service provider to define different endpoints. Numbers between 9000 and 9999 are reserved for test systems.

When changes are made to the participant's system (e.g. when moving to a new version of Elektronische Toegangsdiensten) the participant MAY change a system's EntityID.

Although they look similar, EntityID's are not to be confused with ServiceID's. There is an n:n relationship between EntityID's and ServiceID's. One system may offer more than one service, or the other way around: more systems can offer the same service.

Level of assurance

Elektronische Toegangsdiensten distinguishes five different levels of assurance.

LoA	eIDAS	SAML2 AuthnContextClassRef element
1	Non existent	urn:etoegang:core:assurance-class:loa1
2	Low	urn:etoegang:core:assurance-class:loa2
2+	Low	urn:etoegang:core:assurance-class:loa2plus
3	Substantial	urn:etoegang:core:assurance-class:loa3
4	High	urn:etoegang:core:assurance-class:loa4

Other values MUST NOT be used.

Refer to Betrouwbaarheidsniveaus for legal context, and Normenkader betrouwbaarheidsniveaus for level of assurance in the context of the eIDAS regulation (EU 2015/1502).

For the Level of Assurance communicated in assertions in Elektronische Toegangsdiensten technical interfaces, the following rules apply:

- The AD MUST communicate the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied. An AD MUST NOT communicate a level for which it is not certified.
- The MR MUST communicate the Level of Assurance of the registered authorization. A MR MUST NOT communicate a level for which it is not certified.
    - In case of a chain of authorizations, the MR MUST communicatie the minimum of the LoA of all Representation authorizations in the applicable chain (so far).
    - In case of a request for a portal service, a MR MUST communicate the Level of Assurance as the minimum Level of Assurance of all applicable service authorizations chosen by the user.
- The HM MUST communicate the effective Level of Assurance of the combined assertions. The effective Level of assurance is the minimum of the LoA of the Authentication assertion and (if applicable) the LoA of the Representation authorization assertion(s).

The MR communicates two Levels of Assurance in its Assertion. A LevelOfAssurance (requested) and a LevelOfAssuranceUsed (actually obtained). The HM MUST use the LevelOfAssuranceUsed from the MR Assertion as the LoA of the Representation authorization.

LinkedDeclarationSignatureValue

Description	The value of the signature of the referenced Assertion.
Name	urn:etoegang:core:LinkedDeclarationSignatureValue
Type	http://www.w3.org/2001/XMLSchema#base64Binary
Issuer (XACML)	Applicable in case attribute is enclosed in XACML: EntityID of the MR issuing the linked declaration.
Value	(copy of the) Base64 value of the SignatureValue of the Signature by the Issuer of the referenced Assertion.
Comment	Including the SignatureValue links the containing declaration to the referenced Assertion. Neither Assertion can be altered without breaking the Signatures, providing cryptographic assurance of the reference from the containing Assertion to the referenced declaration.

OIN format

The OIN format is used to indicate participants, service providers and specific types of service consumers and intermediaries. OIN stands for Organization Identifying Number.The OIN format is defined in DigiKoppeling. An OIN consists of the following concatenated elements:

- An 8-digit prefix that tells the register where the number is defined
- A number whose value depends on the register

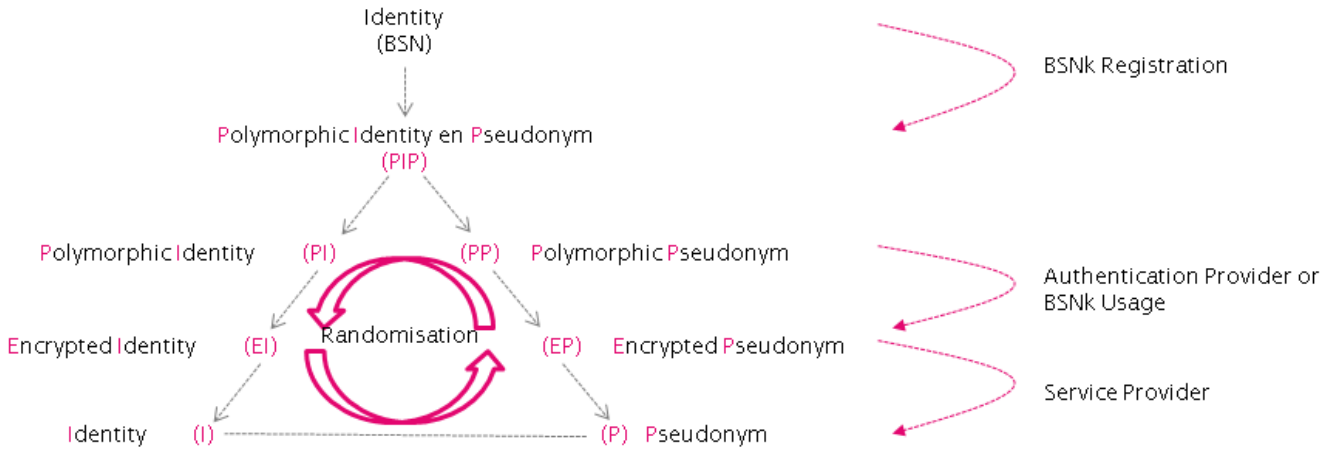
Pseudonyms

A user may be referred to as follows:

- In the event of representation:
    1. inside the network with an Internal pseudonym issued by the AD; and
    2. inside and outside of the network with a Specific pseudonym issued by the MR
- In the event of non-representation:
    1. Inside and outside of the network with a Specific pseudonym issued by the AD

For polymorfe pseudonimisering the following pseudonyms are discerned in the Afsprakenstelsel ETD:

Pseudonyms	Transformation of	Unique to	May be transformed into
Polymorphic Pseudonym	a cryptographic derivative of a root identifying attribute, such as the BSN	a Participant (MU/AD),	Encrypted Pseudonym
Polymorfe Identiteit			Encrypted Identity
Encrypted Pseudonym	Polymorphic Pseudonym	a Relying Party	Persistent Pseudonym
Encrypted Identity			Identity, equal to the root identifying attribute the original PIP was derived from, such as BSN.
Persistent Pseudonym	Encrypted Pseudonym		-



- Encrypted Pseudonym — An Encrypted Pseudonym is a Persistent Pseudonym encrypted under Polymoprohic Pseudonimization for a specific recipient.
- Internal pseudonym — The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the user, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the same internal pse
- Persistent Pseudonym — A Persistent Pseudonym is a pseudonym identifier for a natural person specific for the relying party, that is persistent independent of the Attesting Party.
- Polymorphic Pseudonym — A Polymorphic Pseudonym is a cryptographic structure that can be transformed into a specific Encrypted Pseudonym, without disclosing the relevant subject due to Polymorphic Pseudonimization.
- Specific pseudonym — The specific pseudonym is unique for each different combination of user, represented service consumer, intermediary and service provider.

Encrypted Pseudonym

An Encrypted Pseudonym is a Persistent Pseudonym encrypted under Polymoprohic Pseudonimization for a specific recipient.

An Encrypted Pseudonym is derived from a Polymorphic Pseudonym. Due to the cryptographic nature of an Encrypted Pseudonym, it can be derived from a Polymorphic Pseudonym and randomized without disclosing the actual pseudonym or identity of the subject.

The Attesting Party will include an Encrypted Pseudonym in the Assertion for every relying party (Ontvangende Partij). The Encrypted Pseudonym is specific for the recipient and can be decrypted to a Persistent Pseudonym.

Internal pseudonym

The internal pseudonym is determined by the AD and MUST be unique within the AD its context. Every time the same authentication token is used, it should return the same internal pseudonym. When requested by the user, a new pseudonym MAY always be ignored. An internal pseudonym that has been used MUST NOT be reused. The only exception is when an authentication token is replaced and the AD can determine with sufficient certainty that it is really being replaced. In this case, the same internal pseudonym MAY be used for the new authentication token.

The format of the internal pseudonym MUST have a hexadecimal value of 32 byte. For example, ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

Persistent Pseudonym

A Persistent Pseudonym is a pseudonym identifier for a natural person specific for the relying party, that is persistent independent of the Attesting Party.A Persistent Pseudonym is an identifier for a natural person, that a relying party will obtain after decrypting an Encrypted Pseudonym.

The resulting pseudonym is independent of the entity asserting the pseudonym for the User, thus does not differ between one Attesting Party or another.

The resulting pseudonym is specific to the relying party, thus preserving privacy of the user by preventing linking across relying organisations.

Polymorphic Pseudonym

A Polymorphic Pseudonym is a cryptographic structure that can be transformed into a specific Encrypted Pseudonym, without disclosing the relevant subject due to Polymorphic Pseudonimization.A Polymorphic Pseudonym is derived from the identity of a natural person. The Polymorphic Pseudonym can be transformed into an Encrypted Pseudonym specific for a relying party, without disclosing the original identity.

A Polymorphic Pseudonym is specific for a natural person for usage at a specific Attesting Party. Hereby Polymorphic Pseudonyms support compartmentalization between different Attesting Parties, since it can only be used in the context of that specific Attesting Party.

Specific pseudonym

The specific pseudonym is unique for each different combination of user, represented service consumer, intermediary and service provider.

It can be created in two ways:

1. In the event of representation by an MR
2. In the event of non-representation by an AD

A specific pseudonym is preferably generated once and then stored, but it can also be generated for each request as long as it is always generated in the same way and the same value is generated for each request.

Differences in specific pseudonyms can be used by service providers to determine that the users are different (four-eye principle). This is the reason why an MR MUST have permission to generate a new pseudonym for an existing combination of service provider, user and service consumer (or intermediary in the case of chain authorizations) from the authorization manager or legal representative of the service consumer (or the intermediary). Reasons to generate a new pseudonym can be:

- user has been assigned a new job in the same company and may therefore no longer obtain access with the old pseudonym to files at service providers that are linked to the old role;
- The identity of the user was accidently disclosed to the service provider(s) and a new pseudonym is needed to protect/pseudonymize the identity;
- Migration to a new pseudonym is needed because the service providers merged/split.

The format of the specific pseudonym MUST have a hexadecimal value of 32 byte. For example,
ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890

In the event of representation, this value is followed by an @ and hexadecimal value of 16 byte. For example,
ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890@ABCDEF1234567890ABCDEF1234567890

The 32-byte value MUST be a random value This can be achieved, for example, by calculating an SHA256 hash over the following elements (in this sequence and separated by a separator):

1. The service provider's OIN.
2. A unique (but not necessarily exclusive) identifying attribute for the user in the context of the service consumer. This attribute MAY be determined by the administrator or the creator of the pseudonym, but MAY also be the Internal pseudonym.
3. The identifying attribute for the represented service consumer (only in the event of representation without chain authorization) or for an intermediary (in the event of chain authorization).

Other methods to reach a 32-byte random value are also allowed.

The value of 16 byte MUST be an MD5 hash over the identifying attribute for the represented service consumer (or intermediary in the case of chain authorization).



Other formats of specific pseudonyms may be in use. Users of the specific pseudonym are advised not to use (parts of) the pseudonym for other purposes than to identify the user.

ServiceID

ServiceID is an identifier of a service that is unique in the context of the service provider.

Services are registered in the Service catalog with both a ServiceID and a ServiceUUID.

The ServiceID is an urn in the format **urn:etoegang:DV:<OIN>:services:<index>** where <OIN> represents the OIN of the service provider. When calculating a unique ServiceID, any prefix zero's in the index are ignored.

Registered services MUST have an index of 1 or higher. A portal function is specified (in messages and in the Service catalog) by the reserved index with value '0'. When an index with value '0' is used in a request, then a multivalued ServiceID MAY be returned in the response, representing all ServiceID's for which the subject has a registered authorization.



Although they look similar, EntityID's are not to be confused with ServiceID's. There is an n:n relationship between EntityID's and ServiceID's. One system may offer more than one service, or the other way around: more systems can offer the same service.

ServiceUUID

ServiceUUID is an identifier of a service that is unique in the context of the network, but not linked to one service provider.

Services are registered in the Service catalog under ServiceInstance with both a ServiceUUID and a ServiceID.

A Machtigingenregister (MR) (entitlements registry) MUST register entitlements to the ServiceUUID rather than the ServiceID. This way, service providers can share ServiceUUID's for generic services, such as "Apply for a parking permit". Once a user is entitled for this service, he will be entitled for the same service for all service providers that offer it.



There are also ServiceUUID's registered in the ServiceCatalog under ServiceDefinition, but the interface specifications refer to the ServiceUUID under ServiceInstance.

SAML attribute elements

This section describes the data elements that occur in messages as SAML attribute element.

- ActingSubjectID — A SAML Attribute element with one or more identities of the user for one or more Relying Parties.
- AuthorizationRegistryID — A SAML Attribute element with an EntityID from the MR that must be queried in the use case GUC4 Aantonen bevoegdheid.
- DeprecatedActingSubjectID — A SAML Attribute element with one or more deprecated identities of the user for one or more Relying Parties, used to support migrations of identifiers.
- EherkenningPreferredLanguage — A URL or POST variable containing the language preference of user.
- EntityConcernedID (SAML) — A SAML Attribute element with the identifying attribute of the service consumer that is represented by the user (who might be the same).
- IntendedAudience — A SAML Attribute element with an EntityID from the DV that will be the recipient of the response.
- Representation — A SAML Attribute element with an indication whether there is an issue of representation
- ServiceID (SAML) — A SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
- ServiceUUID (SAML) — A SAML Attribute element with the ServiceUUID of the service for which access is being requested or for which authorization has been determined.

ActingSubjectID

Description	A SAML Attribute element with one or more identities of the user for one or more Relying Parties.
Name	urn:etoegang:core:ActingSubjectID
Type	urn:oasis:names:tc:SAML:2.0:assertion#EncryptedID
AttributeValue	One or more SAML EncryptedID(s), specific per Recipient (specified using the @Recipient of the EncryptedKey).
Comments	The type and value of the contained identifier vary per context and recipient. The NameQualifier of the NameID after decryption holds the used type .

AuthorizationRegistryID

Description	A SAML Attribute element with an EntityID from the MR that must be queried in the use case GUC4 Aantonen bevoegdheid.This EntityID MUST exist in the metadata. See SAML metadata
Name	urn:etoegang:core:AuthorizationRegistryID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See EntityID
Comments	When an AuthorizationRegistryID is returned by an AD, the value of the Representation attribute MUST be TRUE.

DeprecatedActingSubjectID

Description	A SAML Attribute element with one or more deprecated identities of the user for one or more Relying Parties, used to support migrations of identifiers.
Name	urn:etoegang:core:DeprecatedActingSubjectID
Type	urn:oasis:names:tc:SAML:2.0:assertion#EncryptedID
AttributeValue	One or more SAML EncryptedID(s), specific per Recipient (specified using the @Recipient of the EncryptedKey).
Comments	The type and value of the contained identifier vary per context and recipient. The NameQualifier of the NameID after decryption holds the used type.

EherkenningPreferredLanguage

Description	A URL or POST variable containing the language preference of user.
Name	EherkenningPreferredLanguage
Format	Following ISO 639-1:2002

EntityConcernedID (SAML)

Description	A SAML Attribute element with the identifying attribute of the service consumer that is represented by the user (who might be the same).
Name	Any value listed in Identificerende kenmerken
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See Identificerende kenmerken

IntendedAudience

Description	A SAML Attribute element with an EntityID from the DV that will be the recipient of the response.
Name	urn:etoegang:core:IntendedAudience
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See EntityID
Comments	Both AD and MR need the EntityID's of the DV(s) to process requests according to specs as definied in Interface specifications HM-AD and interface specification HM-MR. Since the AD and MR do not have an administration of DV EntityID's, the HM will provide the correct EntityID in the request using this extension. In case of dienstbemiddeling (serviceintermediation) the HM provides the EntityID's of both the both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary). In case of a DV for whom only the OIN is known, the notation 'urn:etoegang:DV:<*OIN*>' is to be used.

Representation

Description	A SAML Attribute element with an indication whether there is an issue of representation
Name	urn:etoegang:core:Representation
Type	http://www.w3.org/2001/XMLSchema#boolean
AttributeValue	true or false

ServiceID (SAML)

Description	A SAML Attribute element with the ServiceID of the service for which access is being requested or for which authorization has been determined.
Name	urn:etoegang:core:ServiceID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See ServiceID

ServiceUUID (SAML)

Description	A SAML Attribute element with the ServiceUUID of the service for which access is being requested or for which authorization has been determined.
Name	urn:etoegang:core:ServiceUUID
Type	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See ServiceUUID

XACML attribute elements

This chapter describes all of the XACML data elements defined for Elektronische Toegangsdiensten.

- ActingEntityID — A XACML Attribute element containing the specific pseudonym of the user.
- ActingSubjectID (XACML)
- Action-ID — A XACML Attribute element containing the action ID.
- AssertionConsumerServiceIndex — An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the Herkenningsmakelaar.
- Assertions
- DeprecatedActingSubjectID (XACML) — A XACML Attribute element containing the specific pseudonym of the user, for purposes of migrating user identifiers.
- EncryptedAttribute — An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the Attribute catalog.
- Intermediates — A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
- LegalSubjectID
- LevelOfAssurance — A XACML Attribute element containing the minimum level of assurance that is required by the service provider.
- LevelOfAssuranceUsed — An XACML Attribute element containing the level of assurance of the registered authorization.
- ServiceID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceID (SAML).
- ServiceUUID (XACML) — An optional XACML Attribute element that matches the SAML attribute described in ServiceUUID (SAML).

ActingEntityID

Description	A XACML Attribute element containing the specific pseudonym of the user.The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:ActingEntityID
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	See Pseudonyms

Warning

This ID is used for backwards compatibility purposes. It will be deprecated in the next release.

ActingSubjectID (XACML)

Description	A XACML Attribute element containing one or more identities of the user for one or more Relying Parties.
@AttributeId	urn:etoegang:core:ActingSubjectID
@Datatype	urn:oasis:names:tc:SAML:2.0:assertion#EncryptedID
@Issuer	EntityID of the asserting MR.
AttributeValue	The type and value of the contained identifier vary per context and recipient. The NameQualifier of the NameID after decryption MUST be urn:etoegang:1.13:EntityConcernedID:Pseudo

Action-ID

Description	A XACML Attribute element containing the action ID.The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:oasis:names:tc:xacml:1.0:action:action-id
@Datatype	http://www.w3.org/2001/XMLSchema#string
AttributeValue	MUST contain the value 'Authenticate'

AssertionConsumerServiceIndex

Description	Elektronische Toegangsdiensten: This attribute element indicates the URL to which the response must be sent.An XACML Attribute element based on the SAML attribute with the same name containing the value that MUST match an index of the AssertionConsumerService in the metadata of the Herkenningsmakelaar.The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:AssertionConsumerServiceIndex
@Datatype	http://www.w3.org/2001/XMLSchema#unsignedShort
@Issuer	EntityID of the Herkenningsmakelaar
AttributeValue	0 to 65535

Assertions

Description	A XACML element that contains an MR <authorization assertion> for checking authorization in GUC9 Token refresh (native apps).
@AttributeId	urn:etoegang:core:Assertions
@Datatype	urn:oasis:names:tc:SAML:2.0:assertion#Assertion
@Issuer	EntityID of the Herkenningsmakelaar
AttributeValue	copy of SAML <assertion> or XACML <authorization assertion> in XML form, copied such that Signature still can be validated.

DeprecatedActingSubjectID (XACML)

Description	A XACML Attribute element containing the specific pseudonym of the user, for purposes of migrating user identifiers.The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:DeprecatedActingSubjectID
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the issuing MR
AttributeValue	The NameQualifier of the NameID after decryption holds the used type, see Specific pseudonym.

EncryptedAttribute

Description	An encrypted additional attribute whereby each encrypted attribute is assigned a unique Encrypted_DATA_ID that is the same as the name of the attribute in the Attribute catalog. The service provider's service certificate that is included in the service catalogue MUST be used for encryption. A level of assurance is also passed for each EncryptedAttribute. A cipher value is included in the encrypted attribute. This cipher value contains the encrypted value of the request attribute that is encrypted with the key of the DV in the service catalogue.

Example	**Example attribute metadata**
	
	`<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
	`Name="urn:etoegang:1.9:attribute:FirstName"`
	`xmlns:ext="urn:oasis:names:tc:SAML:attribute:ext"`
	`ext:LastModified="2014-7-23T7:34:00Z"`
	`ext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:NLWID">`
	`<saml:AttributeValue xsi:type="xs:string">Maurice</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example of a multivalued attribute:
	
	Example multivalued attribute metadata
	
	`<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
	`Name="urn:etoegang:1.9:attribute:Bankaccount"`
	`xmlns:ext="urn:oasis:names:tc:SAML:attribute:ext"`
	`ext:LastModified="2014-7-23T7:34:00Z"`
	`ext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:`
	`0000000012312123100">`
	`<saml:AttributeValue xsi:type="xs:string">NL91INGB0006481668</saml:AttributeValue>`
	`<saml:AttributeValue xsi:type="xs:string">NL91INGB0003712814</saml:AttributeValue>`
	`<saml:AttributeValue xsi:type="xs:string">NL91INGB0006481665</saml:AttributeValue>`
	`</saml:Attribute>`

Intermediates

Description	A multi-value SAML Attribute element containing the identification attributes of intermediaries in a chain authorization.
Name	urn:etoegang:core:Intermediates
Type	multi-value, with values of the type urn:etoegang:1.9:IntermediateEntityID:
AttributeValue	See Identificerende kenmerken. (the multi-value attribute contains only one value).

LegalSubjectID

Description	A XACML Attribute element containing the identifier of the Legal subject in case of Representation. The value(s) contain SAML EncryptedIDs holding an identifier for the Represented entity. The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:LegalSubjectID
@Datatype	urn:oasis:names:tc:SAML:2.0:assertion#EncryptedID
@Issuer	EntityID of the asserting MR.
AttributeValue	The type and value of the contained identifier vary per context and recipient. The NameQualifier of the NameID after decryption holds the used type, see Identificerende kenmerken.

LevelOfAssurance

Description	A XACML Attribute element containing the minimum level of assurance that is required by the service provider.The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:LevelOfAssurance
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the eHerkenningsmakelaar.
AttributeValue	See Level of assurance

LevelOfAssuranceUsed

Description	An XACML Attribute element containing the level of assurance of the registered authorization.If there are several registrations(authorizations) for an assertion and these registrations are established at different levels of assurance (for instance a generic authorization at level eH2 and a specific authorization at level eH3), the highest level of assurance MUST be used. The element MUST NOT contain other attributes (@) than those described here.
@AttributeId	urn:etoegang:core:LevelOfAssuranceUsed
@Datatype	http://www.w3.org/2001/XMLSchema#string
@Issuer	EntityID of the ”machtigingenregister”. See EntityID
AttributeValue	See Level of assurance

ServiceID (XACML)

Description	An optional XACML Attribute element that matches the SAML attribute described in ServiceID (SAML).

ServiceUUID (XACML)

Description	An optional XACML Attribute element that matches the SAML attribute described in ServiceUUID (SAML).

Bindings

Different bindings can be used in SAML to transport messages between parties.

The interfaces Interface specifications HM-AD and Interface specifications HM-MR MUST use Artifact-Artifact binding.

The interface Interface specifications DV-HM MUST use Artifact binding for the response. The Herkenningsmakelaar (HM) MUST offer the Artifact binding and MAY offer alternative bindings to the Dienstverlener (DV) to communicate the Authentication Request. The response will always be delivered over an Artifact-binding (i.e. Artifact-Artifact, Redirect-Artifact or Post-Artifact).

The interface Interface specifications HM-EB MUST use Artifact-Artifact binding.

[HTTP Artifact] [ArtifactResolve] [ArtifactResponse] [SAML SOAP binding] [Alternative bindings to communicate the Authnrequest to the Herkenningsmakelaar] [HTTP Post] [HTTP Redirect]

HTTP Artifact

The SAML V2.0 defined artifact type of type code 0x0004, as described in paragraph §3.6.4 of the SAML Bindings 2.0 document MUST be used. Note that the artifact resolution endpoint is a web service as described under Web services. Furthermore, an artifact MUST be provided only once, as per §3.6.5.2 of SAML Bindings 2.0.

The <Status> element of an ArtifactResponse MUST always include a <StatusCode> element with the code value 'urn:oasis:names:tc:SAML:2.0:status:Success', in accordance with SAML Binding §3.6.6.

In case an Artifact cannot be provided, an error MUST be returned in the Status element of the response child element of the ArtifactResponse. A generic Response (SAML ResponseType) element MAY be used to hold that status.The status reported in the response child element's Status MUST be in accordance with Error handling.

SAML Bindings 2.0 §3.6.4 recommends filling the artifact's SourceID in artifacts by taking the SHA-1 hash of the issuer (= EntityID). In Elektronische Toegangsdiensten all parties MUST apply this recommended method to define and resolve the SourceID in artifacts.

SAML Bindings 2.0 §3.6.3 specifies that artifact can be encoded as either HTTP GET or HTTP POST request and both techniques MUST be supported.

ArtifactResolve

@ID	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	Elektronische Toegangsdiensten: MUST NOT be included.
@Consent	Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the sender. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the sender for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included.
Artifact	SAML: Contains the Artifact that was received as query parameter.

ArtifactResponse

@ID	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	SAML: Unique characteristic of the AuthnRequest for which this Response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.

@IssueInstant	SAML: Time at which the message was created.
@Destination	Elektronische Toegangsdiensten: MUST NOT be included
@Consent	Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn:oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the receiver. The attributes NameQualifier, SPNameQualifier, Format and SPProviderID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the sender for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included.
Status	The <Status> element MUST include a <StatusCode> element with the code value 'urn:oasis:names:tc:SAML:2.0:status:Success', if the response is valid and the artifact can be resolved. Otherwise, an error MUST be returned in accordance with Error handling.
any ##any	MUST contain a Response message if the responder recognizes the artifact as valid, otherwise contains no additional elements. The Response message MAY contain a Signature (even though it's integrity is already guaranteed by the signature on the artifact response)

SAML SOAP binding

For back-channel requests without user interaction, the SAML SOAP binding can be prescribed. The following apply in this case:

- the communication MUST use a mutual authenticated Secure connection. This MUST be established using TLS with certificates as listed in the Network metadata or the DV metadata for HM.
- the SAML v 2.0 SOAP binding as described in paragraph 3.2 of the SAML Bindings 2.0 document MUST be used.
- as SOAPAction, the value 'http://www.oasis-open.org/committees/security' MUST be used.
- The following HTTP headers MUST be set:
  - Cache-Control = "no-cache, no-store"
  - Pragma = "no-cache"

Alternative bindings to communicate the Authnrequest to the Herkenningsmakelaar

HTTP Post

The implementation of a HTTP Post binding MUST meet the following requirements:

- The AuthnRequest MUST be signed, using a digitial signature (<ds:Signature>) as described in Digital signature.
- The message MUST be encoded as a parameter 'SAMLRequest' in a HTML form using base64 encoding to be submitted via HTTP POST.
- A RelayState MAY be used, it MUST be encoded as a parameter 'RelayState'.
- Client-side scripting SHOULD be used to submit the form, but MUST NOT be required; the user MUST be able to submit the form manually.

HTTP Redirect

The implementation of the HTTP Redirect binding MUSTmeet the following requirements:

- The AuthnRequest message MUST NOT contain a <ds:Signature> element.
- The message MUST be compressed using the DEFLATE method and in turn represented in Base-64 encoding.
- The compressed and coded message MUST be added to the URL as a query string parameter and MUST be designated as SAMLRequest.
- If RelayState data is included in the HTTP Redirect message, it must be encoded separately and added to the URL as a query string parameter and MUST be designated as RelayState. If a RelayState is not provided, the whole parameter MUST be absent in the URL.
- A digital signature MUST be calculated over the part of the URL SAMLRequest=value&RelayState=value. This digital signature MUST be generated as described in Digital signature. The digital signature MUST be included as a query string parameter. This parameter is designated as Signature.

Error handling

This chapter describes how errors MUST be handled in the network, in order to inform and serve both users and participants sufficiently.

Status codes

For error handling, conformity regarding the interpretation of the status codes as used in the <Response> element is critical. Only the following top-level status codes MAY be used:

urn:oasis:names:tc:SAML:2.0:status:Requester	This status code is used for errors caused by the initiator of the SAML request. For example, because an assurance level is requested which is not supported by the recipient, or because the request message has expired.
urn:oasis:names:tc:SAML:2.0:status:Responder	This status code is used for errors caused by the recipient of the SAML request. For example, because of technical failure or because the recipient does not support requested (optional) functionality.

Only the following second-level status codes MAY be used:

urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	This status code is used when an user cannot be authenticated for example because invalid credentials have been provided or the cancel button has been used.
urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	This status code is used when a message is correctly formatted by the requester, and understood by the recipient, but that functionality is requested which is not supported by the recipient.
urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	This status code is only used by the BSNk in case a pseudoID is queried but not associated.

Cancelling

During the process of authenticating and authorizing, a user may cancel the process by clicking on the cancel button. Examples:

- A user arrives at a Herkenningsmakelaar (HM), but does not yet have an account
- A user has selected the wrong Authenticatiedienst (AD) and wishes to retry the selection
- A user does not want to authenticate now, and be returned to the Service provider

If a user cancels, the participant MUST direct the user automatically to the latest sender of a SAML request, accompanying a valid SAML response message including valid SAML status codes (**urn:oasis:names:tc:SAML:2.0:status:Responder** with **urn:oasis:names:tc:SAML:2.0:status:AuthnFailed**). A <StatusMessage> element MAY be included, containing for example the value "Authentication cancelled".

If a Herkenningsmakelaar receives a cancellation message (from an Authenticatiedienst or Machtigingenregister (MR)), it MUST ask the user to re-select an Authenticatiedienst or cancel.

If a Dienstverlener (DV) receives a cancellation message (from a Herkenningsmakelaar), it MUST indicate to the user that he is not logged in, and MAY offer the user the option to re-authenticate.

Attributes not supported

A participant can receive a message that matches the Interface specifications, but cannot be processed by the recipient. Examples:

- The request contains an attribute that cannot be provided by the participant

A participant receiving such a message

- MUST show the user a message indicating what went wrong
- MUST show the user information on how to proceed, see **Dialoogbeschrijving.**
- MAY offer the user the option to cancel, in that case the flow continues as stated in Cancelling

Incorrect message (recoverable)

A participant can receive a message that matches the Interface specifications, but cannot be processed by the recipient. Examples:

- The request contains an Level of assurance that cannot be provided by the participant
- The request contains an EntityConcernedType that cannot be provided by the participant

The recipient MUST direct the user to initiator of the SAML request, accompanying a valid SAML response message including valid SAML status codes (**urn:oasis:names:tc:SAML:2.0:status:Responder** with **urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported**). A <StatusMessage> element MUST be included, containing a description of the problem (for example "Level of assurance not supported").

A participant receiving such a response

- MUST show the user a message indicating authentication has failed, including the contents of <StatusMessage>.

- MUST show the user information on how to proceed, see Dialoogbeschrijving
- If the participant is a Herkenningsmakelaar, it MUST ask the user to re-select an Authenticatiedienst or cancel.

Incorrect message (non-recoverable)

A participant can receive an invalid formatted message. Examples:

- Not a valid SAML message
- XML does not match XSD

Alternatively, the message can be valid according to SAML specifications, but it does not match the Interface specifications. Examples:

- Unknown issuer
- Invalid NotValidOnOrAfter
- Invalid signature
- The request contains invalid ServiceID, attributes or EntityConcernedTypes
- The response contains ServiceID, attributes, EntityConcernedTypes or a Level of assurance that does not match the request

Such messages are the result of either a wrong implementation of a participant, or an attempt to hack the system. The user cannot always be sent back to the requester, because the source of the message is unknown and/or cannot be trusted. If the message is a response, it would not make sense to send the user back to the responder.

A participant that receives a message in this category

- MUST investigate the nature of the error.
- MUST show the user a message indicating a non-recoverable error has occured
- MUST show the user information on how to proceed, see Dialoogbeschrijving
- MUST return a SAML response message with status codes (**urn:oasis:names:tc:SAML:2.0:status:Requester** and **urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported**) or an HTTP error in case a binding is used where a synchronuous response is expected and can be returned, like SOAP.
- If the participant is a Herkenningsmakelaar, it MUST ask the user to re-select an Authenticatiedienst or cancel.

Single sign-on and user sessions

Within certain boundaries, single sing-on and user sessions are allowed. This document describes the technical requirements.

For other requirements, see Use cases Single Sign-On.

Sessions at participants

Participants MAY maintain a session for single sign-on if the user so indicated. The following data MAY be maintained in this session:

- an Herkenningsmakelaar (HM) maintains user preferences (selected AD and MR).
- an Authenticatiedienst (AD) maintains the identity of the user. Based on this session, the AD MAY directly issue a new authentication assertion to the service providers making a request in which single sign-on is specified. The requirements for the maximum life span must be followed.
- an Machtigingenregister (MR) maintains user preferences (chosen party to represent).

The maximum life span of a session at the AD is 2 hours unless a new authentication assertion is issued in the meantime whereby the session MAY be extended to a maximum of 2 hours.

Participants MAY provide a user the option to log out.

This option has the same function as logging out from a service provider (see below). Participants and service providers must ensure that cookies are deleted after logging out or after the expiry of an authentication session, and that previously received forms that are resubmitted generate an error.

Shared domain cookies

For cookies in which the choice for an preferred AD is saved, the Identity Provider Discovery Profile is applied as follows:

- The shared domain is '*.sso.eherkenning.nl'
- The name of the cookie MUST be '_saml_idp'
- The cookie MUST have the path prefix '/'.
- The parameters Secure and HttpOnly MUST be used.
- The cookie is persistent.
- The content of the cookie consists of one or more Base-64 encoded URI values, each separated by a single space.
- Each URI value represents the unique identification number for an AD as defined in EntityID. When there is no AD related to the value stored in the cookie, the HM MUST act as if no cookie was set and MUST uncheck the checkbox stating "Bewaar selectie authenticatiedienst".

To ensure that the common domain cookies are available for all HMs, they are sent from the browser of the user to a cookie server that belongs to the respective HM but placed in the shared domain. Redirects and/or a script can be used to include this information in the HTML page that is sent to the user.

If a script is used, cookie handling must be programmed in such a way that, if the cookie server does not respond, the process is continued as if a cookie value did not have to be read or written. If redirects or scripts are used, the HM SHOULD detect when a sent request is not being answered and the same request is being resubmitted. In that case, repeated requests must follow an alternative path without cookies. The objective of doing this is to prevent obstructing the process when cookies do not work.

See also Proces onderhoud cookieserver.

Sessions at service providers

A service provider using SSO is responsible for local session management. During the session, the service provider MUST permanently offer and display a log-out option. A service provider must implement the log-out functionality as follows:

- Session cookies must be deleted and the session must be destroyed
- Submitted forms must be deleted (so that resubmitting the same form from the browser generates an error message)
- The session is then redirected to the HM and a logout message sent according to Interface specifications DV-HM

SubjectConfirmation

The SubjectConfirmation exists in a Subject, and is used in two manners on Subjects:

- To hold a 'bearer' confirmation in a response to an AuthnRequest, to conform to the WebSSO profile.

A <*Subject*> in an <*Assertion*> can contain two different types of <*SubjectConfirmation*> elements. Below is a description for each of these usages. Note that bearer confirmations MAY be applicable to a single Assertion.

SubjectConfirmation for bearer confirmation (WebSSO)

In case a relying party is requesting authentication of a user according to the SAML Web SSO profile, a 'bearer' SubjectConfirmation (see SAML 2.0 Profiles, §3.3 and §4.1.4).

Element/@Attribute	0..n	Description
<*SubjectConfirmation*>	0..1	(Only for the Declaration of Identity or a HM Summary Declaration to the DV) Allows for association of client with assertion to conform to the SAML Web SSO profile.
@Method	1	MUST contain the value 'urn:oasis:names:tc:SAML:2.0:cm:bearer'.
<*SubjectConfirmationData*>	1	
@NotBefore	0	MUST NOT be used.
@NotOnOrAfter	1	Indicates maximum validity of the assertion
@Recipient	1	The assertion consumer Service index of the immediate requester to which an attesting entity can present the assertion
@InResponseTo	1	The ID of the request this assertion is in response to
@Address	0	MUST NOT be used.

Example SubjectConfirmation WebSSO

```
...
    <saml:Subject>
        ...
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_52B816C631C564BACF59E758CBA91717" NotOnOrAfter="2016-
02-05T09:11:48Z" Recipient="https://..."/>
        </saml:SubjectConfirmation>
    </saml:Subject>
...
```

Web services

When web services are used within Elektronische Toegangsdiensten, the web service standards as defined in DigiKoppeling/Forum Standaardisatie "*pas toe of leg uit*" (comply or explain) are adhered to, with an exception for SSL. This results in:

- the web service MUST conform to WS-I Basic Profile 1.1. This implies the use of SOAP 1.1, WSDL 1.1 and XML 1.0 (second edition).
- the web service MUST use WS-Addressing as per WS-I Basic Profile 1.2.
- the web service MUST conform to WS-I Simple SOAP Binding Profile Version 1.0.
- the connection MUST be secured using (mutual authenticated) TLS, with the parameters as defined under Secure connection.

Linking of Assertions

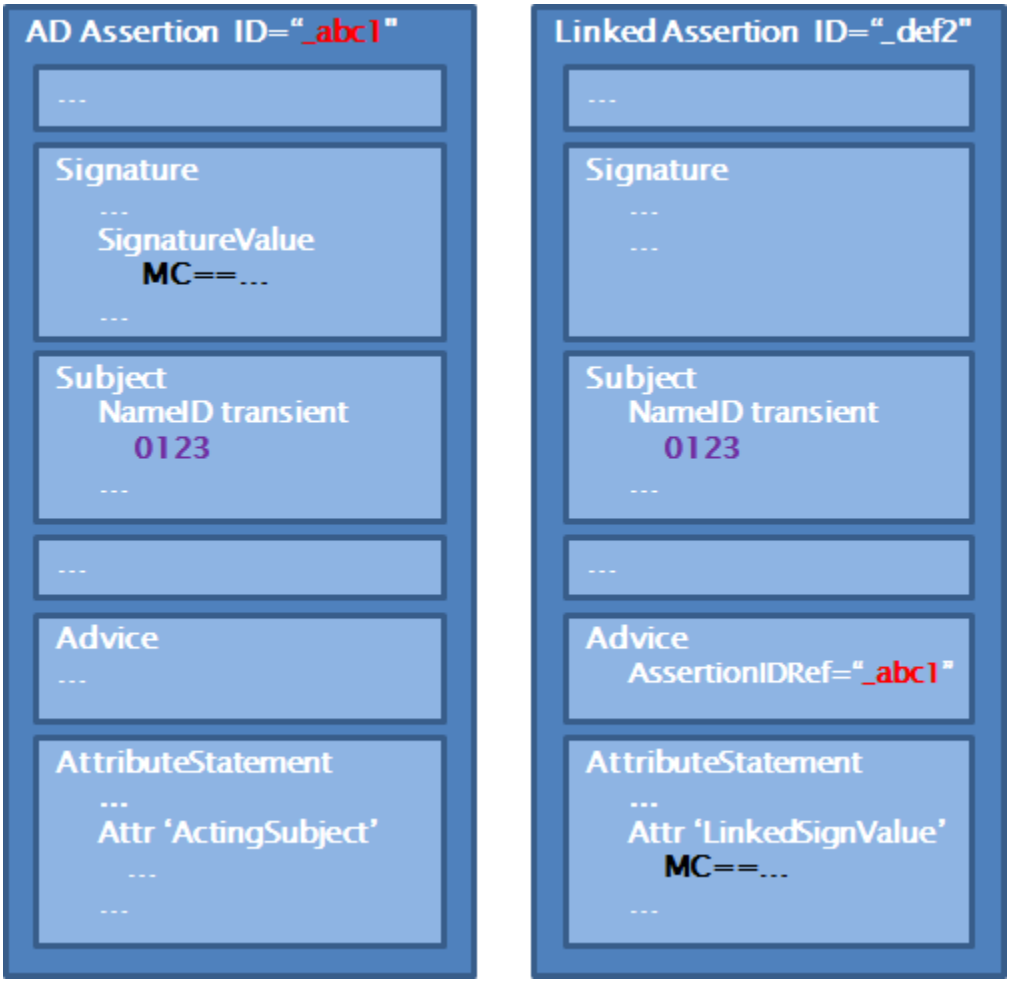
The Afsprakenstelsel Elektronische Toegangsdiensten uses Assertions provided by multiple issuers, from various roles applicable for the particular use case (e.g. with Respresentation). This page explains how these Assertion (declarations) are linked together.

Throughout a Herkenning, various roles may provide some of the information required for the complete result presented to the Dienstverlener (DV). These Assertions are linked based on the relationship between the User and the Dienstafnemer.

The Herkenningsmakelaar will return an Assertion with the combined result of a Herkenning. This Assertion will hold all underlying Assertions under an element <Advice>.

The initial Assertion of a chain is the Assertion by the AD authenticating the User. Subsequent related Assertions are linked to this Assertion.

Each linked Assertions is linked to another using the AssertionIDRef under Advice and bound through inclusion of the SignatureValue of the linked Assertions, using a LinkedDeclarationSignatureValue attribute. By including the SignatureValue in this way, the Assertion is linked cryptographically and secured against modifications.

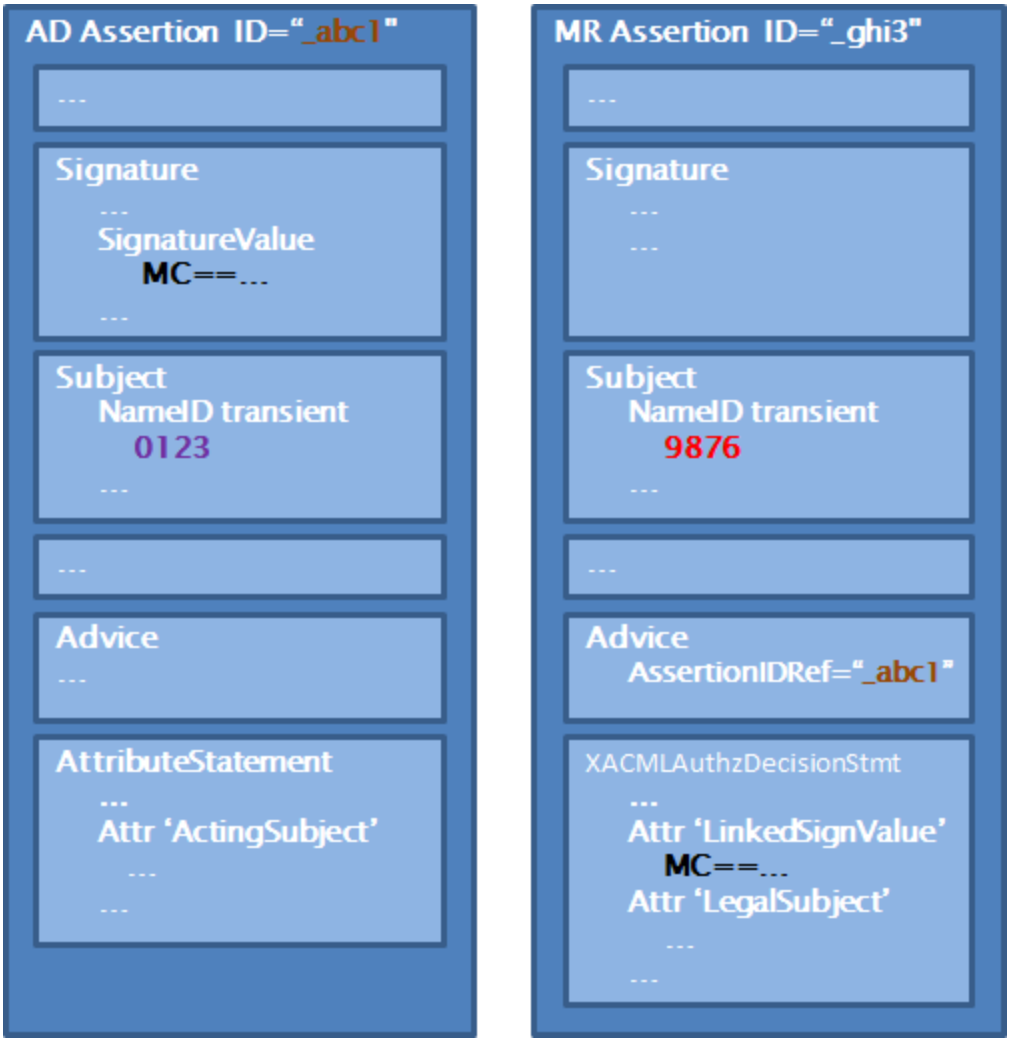


Each underlying Assertion will hold information about the Subject of that Assertion. Assertions part of a single Herkenning stating information about the exact same Subject, will all have a NameID with the same 'transient' ID created by the Authenticatiedienst upon authentication of the User. Assertions part of a single Herkenning stating information about distinct other Subjects – i.e. those about the User and about the entity represented – will have a different transient NameID. Each new Herkenning will result in new transient identifiers for each Subject.

Representation

In case of representation, the various Assertions will by definition not describe the same Subject. Each new authorization in an authorization chain will therefore introduce a different transient Subject to describe the new entity in the authorization chain.

The Assertions are themselves are linked in the same way as described above, using the AssertionIDRef to link them and an attribute LinkedDeclarationSignatureValue to cryptographically bind them.


AD Assertion ID="_abc1"
...
Signature
...
SignatureValue
MC==...
...
Subject
NameID transient
0123
...
...
Advice
...
AttributeStatement
...
Attr 'ActingSubject'
...
...
MR Assertion ID="_ghi3"
...
Signature
...
...
Subject
NameID transient
9876
...
...
Advice
AssertionIDRef="_abc1"
XACMLAuthzDecisionStmt
...
Attr 'LinkedSignValue'
MC==...
Attr 'LegalSubject'
...
...

Polymorphic Pseudonymization Notation

Polymorfe encryptie en pseudonimisering, uses scheme wide keys. To facilitate key management procedures, all scheme-wide keys are versioned using schemeKeySetVersion. For the BSNk documentation you can contact Logius.

This paragraph describes the technical format of polymorphic identities and pseudonyms and related key formats. Polymorphic identities and pseudonyms in the scheme are based on cryptographic properties of elliptic curves.

Usages of Polymorphic Pseudonymization

- Activation
    - Polymorphic Identity or Pseudonym
    - Encrypted Identity or Pseudonym
- Usage (transformation and decryption)
    - Encrypted Identity or Pseudonym
    - Identity or Pseudonym

Format for Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym is a combination of points on an elliptic curve. In order for the Identity or Pseudonym to be properly usable in the scheme, some additional information is needed. This information is necessary for practical management and secure implementation of Identity or Pseudonym in the Scheme and consists of elements like versioning (for key management) and recipient. The syntax for expressing an Identity or Pseudonym with this information is listed below.

Values of the notations below SHALL be represented as (the base64 encoding of) the DER-encoded structure in ASN.1 notation.

Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym consists of 3 points on an elliptic curve. Polymorphic Identity or Pseudonym are provided via the beheerorganisatie BSNk. They are used via the interface spec BSNk: transform. The notation for a complete Polymorphic Identity or Pseudonym is as follows:

Polymorphic Identity or Pseudonym ASN.1 notation

```
PolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

PolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}
```

Herein the schemeVersion indicates the version of the cryptographic scheme and this syntax and SHALL start at 1. The schemeKeySetVersion is a version that SHALL start at 1 and represents the effective set of long term scheme master keys (PP-M, PD-M, etc...). The schemeVersion defines the elliptic curve used in the scheme as well. The creator SHALL contain the entityID (OIN) of the creator, and the recipient SHALL contain the entityID (OIN) of the recipient. The recipientKeySetVersion holds the version number for the set of recipient's keys for Polymorphic Identities and Pseudonyms (PA-Di). Note: In schemeVersion 1 the recipientKeySetVersion for MUs and ADs is a sequence starting at 1. Type defines the identity type the Pseudonym is derived of, e.g. from a BSN or an eIDAS Uniqueness Identifier. This field is not necessary in identity based forms as here the identity type will become clear as part of decryption of the final structure, i.e. the Encrypted Identity. The values currently defined are the ASCII value of 'B' (0x42) for BSN based and 'E' (0x45) when based on a eIDAS uniqueness identifier. ECPoint is identical to ECPoint as defined in BSI TR 03111 and ANSI X9.62 (2005). Here two encodings are specified, compressed and compressed. Both encodings are allowed, with a preference for uncompressed encoding.

A Polymorphic Identity of Polymorphic Pseudonym can be signed for integrity protection:

```
SignedPolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity-signed),
    signedPI SEQUENCE {
        polymorphicIdentity PolymorphicIdentity,
        auditElement OCTET STRING,
```

```
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}

SignedPolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym-signed),
    signedPP SEQUENCE {
        polymorphicPseudonym PolymorphicPseudonym,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}
```

An auditElement holds an audit value consisting of an identifier for the creator, a timestamp and a sequence number from that creator. This auditElement is 16 bytes in big-endian (32-bit origin, 32-bit timestamp and 64-bit sequence-number). The origin identifies the party providing the Polymorphic/Encrypted Identity or Pseudonym and the unique device used. The timestamp and sequence number can be used in case of a compromise or dispute, so that mitigating measure or resolution can be accomplished. Note: the timestamp is 32-bit in seconds since 1 jan 1970 UTC. The auditElement is encrypted under a key only retrievable by the supervisor of the scheme, which is provided to the supervisior by the keymanagement role.

The signatureValue can be used to assert the authenticity of the (polymorphic/encrypted) Identity or Pseudonym. The signature is applied to the byte sequence of the complete DER-encoded signed sequence (e.g. signedPP in a SignedPolymorphicPseudonym). The public key for verification can be retrieved using the creator from the structure covered under the signature and the signingKeyVersion.

```
-- ECPoint is described in ANSI X9.62 (2005), annex E.6.
-- In particular, encoding from point to octet string and
-- from octet string to a point is defined in annex A.5.7
-- and A.5.8 of ANSI X9.62.
ECPoint ::= OCTET STRING

ECDSA-Signature ::= SEQUENCE {
    signatureType      OBJECT IDENTIFIER (ecdsa-with-SHA384),
    signatureValue     EC-Sig-Value
}

-- EC-Sig-Value is identitical to BSI TR 03111 ECDSA-Sig-Value.
-- which is identical to ECDSA-Sig-Value defined in RFC5480 as well.
EC-Sig-Value ::= SEQUENCE {
    r  INTEGER,
    s  INTEGER
}

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4)
    ecdsa-with-SHA2(3) 3 }

id-BSNk-scheme-nl OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1)
nederlandse-overheid(1003) logius-beheer-usve(10) }

id-BSNk-identifiers OBJECT IDENTIFIER ::= { id-BSNk-scheme-nl 1 }

id-BSNk-polymorphics OBJECT IDENTIFIER ::= { id-BSNk-identifiers 1 }

id-BSNk-polymorphic-identity OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 1 }

id-BSNk-polymorphic-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 2 }

id-BSNk-polymorphic-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 3 }

id-BSNk-polymorphic-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 4 }
```

PIP – PPCA optimized

For privacy enhanced implementation, Polymorphic Identities and Pseudonyms can be implemented on a smartcard. This is called a PP-card application, or PPCA. A Polymorphic Identity and a Polymorphic Pseudonym can be combined to 5 points on an elliptic curve rather than six, for optimization in a smartcard implementation. The PPCA-optimized PIP version of Polymorphic Identities or Pseudonyms are provided in Interface spec BSNk: activate.

The combined notation for an Polymorphic Identity and Pseudonym is as follows:

Polymorphic Identity and Pseudonym (PIP) ASN.1 notation

```
PIP ::= SEQUENCE {
    notationIdentifier  OBJECT IDENTIFIER (id-BSNk-polymorphic-pip),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (5)) OF ECPoint
}
```

The first, second and fourth ECPoint in a PIP correspond to those of a PI. Similarly, the first, third and fifth correspond to those of a PP. In this fashion one can extract a PI and PP from a PIP.

There also exists a signed version of a PIP:

```
SignedPIP::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pip-signed),
    signedPIP SEQUENCE {
        pip PIP,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}
```

Which follows the same concepts as described for a Polymorphic Identity or Polymorphic Pseudonym.

```
id-BSNk-polymorphic-pip OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 5 }

id-BSNk-polymorphic-pip-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 6 }

-- the following OID is reserved for usage in the specifications of the protocol for PP on smartcard
(polymorphic card application)
id-PCA OBJECT IDENTIFIER ::= { id-BSNk-scheme-nl 9 }
```

Encrypted Identity or Pseudonym

An Encrypted Identity or Pseudonym consists of 3 points on an elliptic curve. The notation for a complete Encrypted Identity and an Encrypted Pseudonym is as follows:

Encrypted pseudoID ASN.1 notation

```
EncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

EncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    diversifier IA5String OPTIONAL,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}
```

```
SignedEncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity-signed),
    signedEI SEQUENCE {
        encryptedIdentity EncryptedIdentity,
        auditElement OCTET STRING
    },
    signatureValue EC-Schnorr-Signature
}

SignedEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym-signed),
    signedEP SEQUENCE {
        encryptedPseudonym EncryptedPseudonym,
        auditElement OCTET STRING
    },
    signatureValue EC-Schnorr-Signature
}

DirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym),
    schemeVersion INTEGER,
    schemeKeySetVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

SignedDirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym-signed),
    signedDEP SEQUENCE {
        directEncryptedPseudonym DirectEncryptedPseudonym,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}
```

The fields correspond to the same fields in a Polymorphic Identity or Pseudonym. The recipientKeySetVersion holds the version number for the set of recipient's keys for Identities and Pseudonyms (PD-Di, PC-Di and PI-Di). Note: In schemeVersion 1 the recipientKeySetVersion for DVs is a value of 8 decimal digits corresponding with the issue date (notBefore) of the certificate, in the format YYYYMMDD, used to request the PEM file at the party generating the keys within the scheme.

A DirectEncryptedPseudonym is – with the exception of the diversifier – identical to an EncryptedPseudonym, although an additonal key and processing step are needed for decryption. The signed form uses a ECDSA instead of a Schnorr signature. This form is (currently) only applicable for reporting from BSNk_registration to CIF.

```
EC-Schnorr-Signature ::= SEQUENCE {
        signatureType      OBJECT IDENTIFIER (ecschnorr-plain-SHA384),
        signatureValue     EC-Sig-Value
}

bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}

id-ecc OBJECT IDENTIFIER ::= { bsi-de algorithms(1) 1 }

ecschnorr-plain-signatures OBJECT IDENTIFIER ::= { id-ecc signatures(4) 3 }

ecschnorr-plain-SHA384 OBJECT IDENTIFIER ::= { ecschnorr-plain-signatures 3 }
```

The auditElement is similar to the auditElement of a Polymorphic Identity or Pseudonym. The signature is a Schnorr signature for efficiency.

```
id-BSNk-encrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 2 }
```

```
id-BSNk-encrypted-identity OBJECT IDENTIFIER ::= { id-BSNk-encrypted 1 }

id-BSNk-encrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 2 }

id-BSNk-encrypted-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 3 }

id-BSNk-encrypted-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 4 }

id-BSNk-encrypted-direct-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 5 }

id-BSNk-encrypted-direct-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 6 }
```

Identity or Pseudonym

Finally, an Encrypted Identity or Pseudonym can be decrypted into a Identity or Pseudonym respectively, consisting of (the X coordinate of) 1 point on an elliptic curve. The Identity or Pseudonym is not directly used in any of the interfaces, but is the RECOMMENDED representation of a Identity or Pseudonym for a relying party to use after decryption of a Encrypted Identity or Pseudonym.

Decrypted pseudoID ASN.1 notation

```
Identity ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-identifier),
    schemeVersion          INTEGER,
    schemeKeySetVersion    INTEGER,
    recipient              IA5String,
    type                   INTEGER,
    identityValue          IA5String
}

Pseudonym ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-pseudonym),
    schemeVersion          INTEGER,
    schemeKeySetVersion    INTEGER,
    recipient              IA5String,
    recipientKeySetVersion INTEGER,
    diversifier            IA5String,
    type                   INTEGER,
    pseudonymValue         IA5String
}
```

In case of an Identity, the identity can be extracted from the X coordinate of the EllipticCurvePoint of the Identity. In schemeVersion 1, the X coordinate, after conversion from a number to a bytearray, contains an encoded identity padded using OAEP as defined in Section 7.1 of RFC8017 (PKCS#1 v2.2). Here the following parameters are chosen:

- The place of n (RSA modulus) is taken by the order of curve q; length in bytes of q is denoted by k as in PKCS #1, i.e. equal to 40 for the Brainpool320r1 curve used in version 1 of the scheme.
- Hash function is SHA384 truncated to first 10 bytes, i.e. hLen = 10.
- Message length mLen = to k – 2hLen – 2 (PKCS #1 only requires), i.e. equal to 18.
- MGF1 as defined in PKCS #1 is used as Mask Generation Function.
- Optional Label is empty string.

The decoded identity (18 bytes) consists of a prefix of three bytes and the identity (e.g. BSN). The prefix consists of a version, a type and a length of the identifier. All not used bytes are zero. That is, 15 bytes is the longest size supported for an identifier in version 1.

In case of a Pseudonym, the identifying, persistent pseudonym of a user is the EllipticCurvePoint of the Pseudonym. The RECOMMENDED representation of a Pseudonym used in a DV registration, consists of the recipientKeySetVersion (decimal string of length 8) of the closing key with the uncompressed EllipticCurvePoint appended. If two such representations are equal the pseudonyms correspond to the same person. However, we can only deduce that two pseudonyms do not correspond to the same person if the pseudonymValue differ while all other values are equal. We note that the recipientKeySetVersion of the closing key can be different from the recipientKeySetVersions of the EI and EP decryption key.

For each decrypted pseudonym the DV shall archive the additional fields decrypted from the Encrypted Pseudonym.

```
id-BSNk-decrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 3 }

id-BSNk-decrypted-identifier OBJECT IDENTIFIER ::= { id-BSNk-decrypted 1 }

id-BSNk-decrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-decrypted 2 }
```

Key formats

Polymorphic pseudonimization uses various keys. These keys have been versioned, see the syntax above.

Keys for relying parties are provided using the notation described in DV-key format.

Several of the scheme-wide keys are public, and can be used to use the polymorphism or verify signatures. These keys are defined in Metadata and under the role PPSteutelSet in RoleDescriptors non-Participants. For these public keys the brainpool P320r1 curve is used, which is a named curve defined as

```
-- Brainpool curves and the TeleTrust namespace are defined in BSI TR-03111
ecStdCurvesAndGeneration OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) teletrust(36) algorithm(3)
    signature-algorithm(3) ecSign(2) ecStdCurvesAndGeneration(8)
}

ellipticCurve OBJECT IDENTIFIER ::= { ecStdCurvesAndGeneration 1 }

versionOne OBJECT IDENTIFIER ::= { ellipticCurve 1 }

brainpoolP320r1 OBJECT IDENTIFIER ::= { versionOne 9 }
```

Interface specifications and the interpretation of LOAs

The ETD framework uses the LOA quite loosely to define a level at which a login means or authorisation MUST be in order for a user to login. Because these LOA levels are defined in various locations around the framework, this page will give an overview of all of them and how they interact with each other.

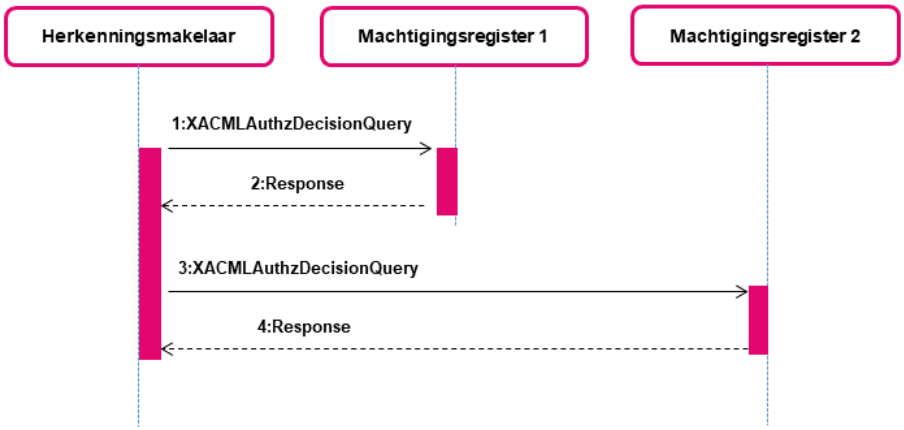
Locations of LOA:

Location in AS	Field/location	Rationale
Service catalog	(AuthnContextClassRef)	This is the maximum LOA as defined by the DV. Means and authorisations need to have this LOA or higher to login.
Interface specifications DV-HM	(Request/RequestedAuthnContext /AuthnContextClassRef)	This allows a DV to override its own minimum LOA downward. Therefore can only be lower or equal than the one in the service catalog. Also known as the minimum-minimumLOA. (Minimal LOA for minimal functionality)
Interface specifications DV-HM	(Response/AuthnContextClassRef)	This is the LOA which is communicated back to the DV
Interface specifications HM-AD	(Request/RequestedAuthnContext)	This allows a DV to override its own minimum LOA downward. Therefore can only be lower than the one in the service catalog. Also known as the minimum-minimumLOA. (Minimal LOA for minimal functionality) This LOA is passed on by the HM.
Interface specifications HM-AD	(Response/AuthnStatement)	This communicates the level at which the user has authenticated himself. This level needs to be higher or equal to the level as stated in the service catalog or the request.
Interface specifications HM-MR	(Request /LevelOfAssurance)	This allows a DV to override its own minimum LOA downward. Therefore can only be lower than the one in the service catalog. Also known as the minimum-minimumLOA. (Minimal LOA for minimal functionality) This LOA is passed on by the HM.
Interface specifications HM-MR	(Response/LevelOfAssuranceUsed)	This communicates the level at which the authorisation was registered. This level needs to be higher or equal to the level as stated in the service catalog or the request.

Schematically the attributes are passed like this:

DV->HM	HM->AD	HM->MR	AD->HM	MR->HM	HM->DV
(Request/RequestedAuthnContext /AuthnContextClassRef)	(Request/RequestedAuthnContext)	(Request /LevelOfAssurance)	X	X	X
X	X	X	(Response/AuthnStatement)	(Response/LevelOfAssuranceUsed)	(Response/AuthnContextClassRef)

Interface specifications HM-MR chain authorization



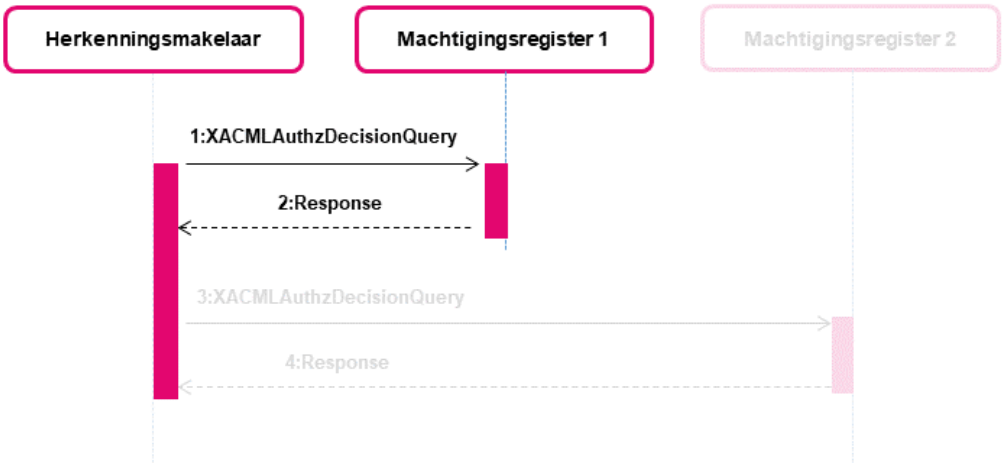
This page describes the messages for the backchannel interface between an Herkenningsmakelaar (HM) (broker) and a Machtigingenregister (MR) (authorization information provider).

Elektronische Toegangsdiensten only supports chains with one intermediary:

- User_G (user) > Intermediary_A > ServiceConsumer_B.

The Intermediary_A registers a mandate for User_G at MR1 and the ServiceConsumer_B registers a mandate for Intermediary_A at MR2. MR2 has no user-interaction, therefore the User_A has to select ServiceConsumer_B (including appropriate MR2) at MR1 in order to proceed with chain authorization flow. MR1 can use discovery-services (of all MR2) during mandate registration of Intermediary_A or during user authorization flow.

MR1 receives a HM-MR request



After receiving the AD-response, the HM forwards User_G via a HM-MR request to MR1. At that point the MR1 will decide together with the User_G if the request will be a standard or 'authorisation-chain' request. In the case of a chain authorisation the the rules for processing will be slightly different than described in Interface specifications HM-MR. Below only the differences to default HM-MR process rules are described per 'subsection'.

Rules for processing request

Subsection	Differences to default HM-MR process rules
A receiving MR MUST provide an Assertion:	• MR1 will create a XACMLAuthzDecision Statement in the Authorisation assertion containing: • a <Obligations> element that MUST contain the EntityID of MR2 in urn:etoegang:core:RequireConfirmationFromNextMR attribute

	• a <Request><Subject> element that MUST contain an LegalSubjectID with and EncryptedID only for MR2 (not for the ServiceProvider, MR2 wil add the appropriate ECTA's for ServiceConsumer_B)
	• a <Request><Resource> element that:
	  • MUST contain an IntermediateEntityID generated of the type urn:etoegang:1.9:IntermediateEntityID:KvKnr. Other intermediary entity Id's MUST NOT be included.
	  • MUST contain the ServiceID and ServiceUUID for which the User_G MUST has a mandate from Intermediary_A and for which Intermediary_A SHOULD have a mandate from ServiceConsumer_B at MR2. MR1 can use MR2 discovery service to determine appropriate ServiceUUID. For Portal Request see "ServiceUUID and Portal Request" infobox below.
	  • MUST ignore requested attributes (MR2 wil provide ServiceConsumer_B attributes and eHerkenning does not have attributes for Intermediary other than CompanyName)

Rules for processing response

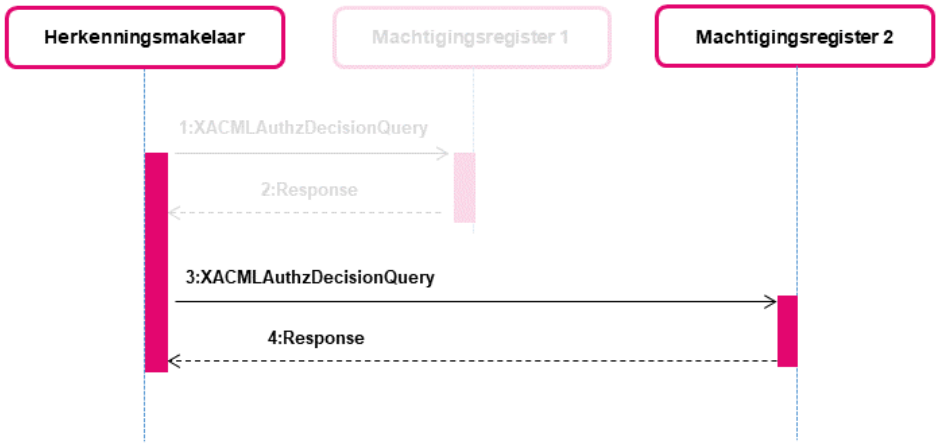
Subsection	Differences to default HM-MR process rules
A receiving HM:	• Determines 'Authorisation Chain' flow IF the MR1-assertion specifies MR2 in the urn:etoegang:core: RequireConfirmationFromNextMR element in <XACMLAuthzDecision Statement><Obligations> • Determines the appropriate AD-assertion based on the AssertionIDRef in the <Advice> element of the MR1-Assertion. This AssertionIDRef references the AD-Assertion this MR1-Assertion is directly linked to.

Examples

Example of Response with Obligations

```
<xacml-context:Response xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
        <xacml-context:Result>
                <xacml-context:Decision>Permit</xacml-context:Decision>
                        <xacml-context:Status>
                                <xacml-context:StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok" />
                        </xacml-context:Status>
                        <xacml-policy:Obligations>
                                <xacml-policy:Obligation ObligationId="urn:etoegang:core:
RequireConfirmationFromNextMR" FulfillOn="Permit">
                                <xacml-policy:AttributeAssignment DataType="http://www.w3.org/2001
/XMLSchema#string"
                                 AttributeId="urn:etoegang:core:AuthorizationRegistryID">urn:nl:eherkenning:MR:
99999900000001:entities:0017
                                </xacml-policy:AttributeAssignment>
                        </xacml-policy:Obligation>
                </xacml-policy:Obligations>
        </xacml-context:Result>
</xacml-context:Response>
```

HM requests MR2 via SOAP interface



This query and response resemble the XACMLAuthzDecisionQuery and Response as described in Interface specifications HM-MR, but differs on the following aspects.

Rules for processing request

Subsection	Differences to default HM-MR process rules

A requesting HM:	• MUST get MR2 EntityID from MR1-assertion from <Obligations> element
	• Create a SOAP-message with an XACMLAuthzDecisionQuery in the message body and send this message via a SOAP backchannel to MR2
	• XACMLAuthzDecisionQuery MUST provide
	  • a verbatim copy of both the MR1-Assertion and AD-Assertion in <Extensions><Assertion> element:
	  • MR1-Assertion is copied from MR1-response
	  • AD-Assertion is copied from (the original) AD-response as referenced to by the AssertionIDRef in the <Advice> element of the above MR1-Assertion
	  • a LegalSubjectID in <Request>**<Subject>** containing the appropriate EntityConcernedID of the ServiceConsumer_B (default is KvKnr) as an EncryptedID@MR2 (not as an EncryptedID@DV!)
	  • an IntermediairyEntityID in <Request>**<Subject>** containing exactly one value with Intermediary KvK-nr (urn:etoegang:1.9:IntermediateEntityID:KvKnr)
	  • ServiceID and ServiceUUID in <Request><Resource> which MUST be copied from <Request><Resource> in MR1-assertion

Rules for processing request

Subsection	Differences to default HM-MR process rules

A receiving MR MUST provide an Assertion:	• MR2 recognizes this as a claim confirmation request based on the presence of the urn:etoegang:1.9:IntermediateEntityID:KvKnr attribute in the MR1 assertion (in<Request><Resource> element of the XACMLAuthzDecision Statement).
	• MR2 MUST use ServiceUUID(s) from MR1.assertion (instead of HM-request) to determine response.ServiceID's for which the Intermediate has a valid mandate.
	• MUST provide and <Advice> element containing an AssertionIDRef referencing to the MR1-assertion (not AD-Assertion!), see Linking of Assertions.
	• MUST provide an <XACMLAuthzDecision>
	  • containing in <Subject>
	  • a <LinkedDeclarationSignatureValue> with Signature value of the MR1-Assertion referenced to via AssertionIDRef in <Advice> element mentioned above.
	  • NO <ActingSubjectID> (or <ActingEntityID> in case of backward compatibility), because MR1 should add ActingSubjectID not MR2
	  • a <LegalSubjectID> with the appropriate ECTA's and identifiers (see infobox on HM-MR page) for ServiceConsumer_B based on the requested ECTA-set as described in the ServiceCatalog for the original ServiceUUID/ServiceID that is requested by the DV and added as Attribute in the AD-assertion (which is included in the HM-MR2 request).
	  • containing in <Resource>
	  • IF Intermediate.CompanyName (of Intermediate_A) is not available THEN 'Deny' and start Error Handling
	  • IF available SP-certificate THEN an extra EncryptedAttribute@SP with the Intermediate.CompanyName (of Intermediate_A as known by the ServiceConsumer_B) as a value of urn:etoegang:1.13:attribute-Intermediate:CompanyName
	  • IF NOT available SP-certificate THEN continue without Intermediate.CompanyName
	  • IF any attributes of ServiceConsumer B are requested, MR2 MUST assume UserConsent
	  • the ServiceID and ServiceUUID with value(s) identical to MR1 assertion for which Intermediary_A the MUST have a mandate from ServiceConsumer_B, otherwise Deny

ServiceUUID and Portal Request

A ServiceUUID (value) in the specifications always represents a ServiceInstanceUUID, which is a DV-specific ServiceInstance of a ServiceDefinition. A ServiceDefinition is identified using a ServiceUUID which is can be referred to as a ServiceDefinitionUUID. Mandates are registered on a ServiceDefinition (not a DV-specific ServiceInstance). Therefor MR1 and MR2 have to check on valid mandates by looking up the ServiceDefinition belonging to the requested ServiceInstance.

MR2 is not allowed to extent or reduce the ServiceInstance-list in MR1 assertion. Even more, MR2 will Deny the request if Intermediairy_A does not have a valid mandate for all of the services in this list. To prevent such a deny, MR1 should be very carefull composing the ServiceInstance-list and only add ServiceInstance's in the response for which the Intermediary has a mandate (from ServiceConsumer_B) at MR2. MR1 can use DiscoveryService for this purpose.

Intermediate.CompanyName

is the name of the Intermediate Company that MR2 uses when ServiceConsumer_B is registering or managing mandates for this intermediate. The Intermediate CompanyName is either the registered official name or trade name (KvK: statutaire naam of handelsnaam). CompanyName has a value of urn:etoegang:1.13:attribute-Intermediate:CompanyName. MR2 always has to return the I ntermediate CompanyName. Except when the ServiceProvider does not have an encryption certifiate in the ServiceCatalog for this service. Because attributes always need to be encrypted.

Discovery Interface MR-MR chain authorisations

This page describes the messages for the interface specification between a Machtigingenregister (MR) (authorization information provider) and a Machtigingenregister (MR) (authorization information provider) in order to provide the chain authorisation functionality. In order to maintain the same level of security as is usual in other SOAP services like the one the BSNk provides, the security demands including SOAP-signing and encryption of the message is added in the supplementary page MR-MR webservice Security.

During SOAP signing the body of both request and response MUST be signed with a WS-Security header containing an XMLSignature based on the PKIo certificate. The WS-Security signature MUST include the KeyInfo in the signature, as a BinarySecurityToken, as per WS-Security X.509 Certificate Token Profile 1.0, §3.3.2. The certificate referenced MUST be listed in the Metadata for participants in a KeyDescriptor of the Participant marked for the use "signing" (or without use, the default includes signing).

The content requirements for signing and encryption are added in the supplementary page MR-MR webservice Security.

Elektronische Toegangsdiensten only supports chains with one intermediary:

- User G (user) > Intermediary A > Service consumer B.

The authorization that the user may act on behalf of Intermediary A is registered as authorization with the first MR. The information that there is an authorization from Service consumer B for Intermediary, and in which MR it is stored, MUST also be known by the first MR (or retrieved at the time of authentication).

ChainInformationQuery

This is a SOAP service to be implemented by the MR. Schematically it looks like this:

Name	Required	Description
ID	YES	Unique message attribute, like the SAML ID field
RequestingEntityId	YES	The entityID of the MR requesting this information. The EntityID MUST match the entityID of the MR in the Network metadata
IntermediarySubjectID_Type	YES	ECTA type to use to identify the intermediary company. MUST be set to EntityConcernedID:KvKnr. Only one LegalSubjectID_Type element MUST be included
IntermediarySubjectID	YES	Contains the value of the ECTA of the intermediary
LegalSubjectID_Type	YES	ECTA type to use to identify the Service consumer company.
LegalSubjectID	YES	Contains the value of the ECTA of the Service consumer which is to be represented Only one LegalSubjectID element MUST be included
LegalSubjectIDService Restriction_Type	NO	MUST be set to vestigingsnummer if this function is used. No other restructions are currently used
LegalSubjectIDService Restriction	CONDITIONAL	If the tag **LegalSubjectID**ServiceRestriction is used, this tag is required. It contains the value of the **LegalSubjectID**ServiceRestriction_Type
Service_Type	YES	Can be set to either **OIN** or **ServiceUUID**. If OIN is used all services belonging to the OIN are requested. The ServiceUUID option can be used to request a specific service.
Service	YES	In case Service_Type is **OIN**: ▪ An OIN must be selected from the Service catalog. ▪ All services which are registed under this OIN will be part of the discovery request In case Service_Type is **ServiceUUID** ▪ A serviceUUID MUST be selected from a service definition in the Service catalog. ▪ Only the selected service is part of the discovery request
LOAmin	NO	Specifies the minimum LOA level to be considered by the responding MR

Processing rules for creating the request:

- The sender MUST sign and encrypt the request with the keys of the MR in the Network metadata
- The MR MAY only inquire if a chain authorisation exists if one of the organisations is its customer

Processing rules for validating the request:

- The recipient MUST verify the request with the keys of the MR in the Network metadata. The keys must be retrieved from the MR stated in the RequestingEntityId.

Response

Name			Required	Description
ID			YES	Unique message attribute, like the SAML ID field
InResponseTo			YES	This is the same value as send in the ID in the ChainInformationQuery
Signature			YES	A signature that scopes all the elements the Response message, see Digital signature
DateTime			YES	Issue datetime of the response
IntermediarySubjectID_Type			YES	ECTA type to use to identify the intermediary company. MUST be set to EntityConcernedID:KvKnr.
IntermediarySubjectID			YES	Contains the value of the ECTA of the intermediary
LegalSubjectID_Type			YES	ECTA type to use to identify the Service consumer company. MUST return the same LegalSubjectId_Type as included in the request.
LegalSubjectID			YES	Contains the value of the ECTA of the Service consumer which is to be represented MUST return the same LegalSubjectId as included in the request.
LegalSubjectIDServiceRestriction_Type			NO	MUST be set to vestigingsnummer if this function is used. No other restructions are currently used
LegalSubjectIDServiceRestriction			CONDITIONAL	If the tag **LegalSubjectID**ServiceRestriction is used, this tag is required. It contains the value of the **LegalSubjectID**ServiceRestriction_Type
ServiceList			YES	A list of services for which the Intermediary is authorized (see processing rules).
	Service		OPTIONAL, one or more	Specifies the services for which the chainauthz is applicable. If no services are applicable, this element is not used
		ServiceDefinitionUUID	YES	The serviceUUID of the service as specified in the ServiceDefinition of the service catalog.
		LOA	YES	The LOA which is registed at the authorisation which allows usage of this service

Processing rules for creating response

In case Service_Type in the request is **OIN**:

- All services which are registed under this OIN will be part of the discovery request
- The ServiceList MUST return serviceUUID's which are registerd to the requested OIN, if the Intermediary is authorized for these services. If there are no applicable services to return, the ServiceList will remain empty.

In case Service_Type is in the request **ServiceUUID**

- Only the selected service is part of the discovery request
- The ServiceList MUST return the same serviceUUID, if the Intermediary is authorized for these services. Otherwise the ServiceList will remain empty

WSDL example

```
<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:etoegang="urn:etoegang:webservices"
 xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 name="ChainInformationQuery"
 targetNamespace="urn:etoegang:webservices">
    <wsdl:types>
        <xsd:schema targetNamespace="urn:etoegang:webservices"
 attributeFormDefault="unqualified"
 elementFormDefault="qualified">
            <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR
/xmldsig-core/xmldsig-core-schema.xsd"/>
            <xsd:element name="ChainInformationQueryRequest" type="etoegang:ChainInformationQueryRequestType">
                <xsd:annotation>
                    <xsd:documentation>Sends an information request
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>

            <xsd:complexType name="ChainInformationQueryRequestType">
                                <xsd:sequence>
                                        <xsd:element name="RequestingEntityId" type="etoegang:EntityIDType"
minOccurs="1" />
                                        <xsd:element name="IntermediarySubjectID_Type" type="etoegang:ECTA"
minOccurs="1" />
                                        <xsd:element name="IntermediarySubjectID" type="etoegang:ECTAValueType"
minOccurs="1" />
                                        <xsd:element name="LegalSubjectID_Type" type="etoegang:ECTA" minOccurs="
1" />
                                        <xsd:element name="LegalSubjectID" type="etoegang:ECTAValueType"
minOccurs="1" />
                                        <xsd:element name="LegalSubjectIDServiceRestriction_Type" type="
etoegang:ServiceRestrictionTypeType" minOccurs="0" />
                                        <xsd:element name="LegalSubjectIDServiceRestriction" type="etoegang:
ServiceRestrictionType" minOccurs="0" />
                                        <xsd:element name="Service_Type" type="etoegang:ServiceTypeType"
minOccurs="1" />
                                        <xsd:element name="Service" type="etoegang:ServiceType" minOccurs="1" />
                                        <xsd:element name="LOAmin" type="etoegang:LOA" minOccurs="1"
/>
                                </xsd:sequence>
                                <xsd:attribute name="ID" type="xsd:ID" use="required"/>
            </xsd:complexType>
             <xsd:simpleType name="EntityIDType">
                <xsd:annotation>
                    <xsd:documentation>EntityID type.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:maxLength value="100" />
                </xsd:restriction>
            </xsd:simpleType>

            <xsd:simpleType name="ECTA">
                <xsd:annotation>
                    <xsd:documentation>ECTA type.
                    </xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:maxLength value="100" />
                </xsd:restriction>
            </xsd:simpleType>

            <xsd:simpleType name="ECTAValueType">
                <xsd:annotation>
                    <xsd:documentation>ECTAValueType.
```

```
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="200" />
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:simpleType name="ServiceRestrictionTypeType">
            <xsd:annotation>
                <xsd:documentation>ServiceRestrictionTypeType.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="vestigingsnummer"/>
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:simpleType name="ServiceRestrictionType">
            <xsd:annotation>
                <xsd:documentation>ServiceRestrictionType.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="50" />
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:simpleType name="ServiceTypeType">
            <xsd:annotation>
                <xsd:documentation>ServiceTypeType.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="OIN"/>
              <xsd:enumeration value="ServiceUUID"/>
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:simpleType name="ServiceType">
            <xsd:annotation>
                <xsd:documentation>ServiceType.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="50" />
            </xsd:restriction>
        </xsd:simpleType>

        <xsd:simpleType name="LOA">
            <xsd:annotation>
                <xsd:documentation>LOA.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:restriction base="xsd:string">
                <xsd:maxLength value="42" />

            </xsd:restriction>
        </xsd:simpleType>


        <xsd:element name="ChainInformationQueryResponse" type="etoegang:ChainInformationQueryResponseType">
            <xsd:annotation>
                <xsd:documentation>
Response to a ChainInformationQueryRequest.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:complexType name="ChainInformationQueryResponseType">
            <xsd:sequence>
                                <xsd:element ref="ds:Signature" minOccurs="1" />
                <xsd:element name="InResponseTo" type="xsd:ID" minOccurs="1" maxOccurs="1"
```

```
/>
                    <xsd:element name="DateTime" type="xsd:dateTime" minOccurs="1" maxOccurs="1" />
                    <xsd:element name="IntermediarySubjectID_Type" type="etoegang:ECTA" minOccurs="1" />
                    <xsd:element name="IntermediarySubjectID" type="etoegang:ECTAValueType" minOccurs="1" />
                    <xsd:element name="LegalSubjectID_Type" type="etoegang:ECTA" minOccurs="1" />
                    <xsd:element name="LegalSubjectID" type="etoegang:ECTAValueType" minOccurs="1" />
                    <xsd:element name="LegalSubjectIDServiceRestriction_Type" type="etoegang:
ServiceRestrictionTypeType" minOccurs="0" />
                    <xsd:element name="LegalSubjectIDServiceRestriction" type="etoegang:ServiceRestrictionType"
minOccurs="0" />
                    <xsd:element name="ServiceList" type="etoegang:ServiceListType" minOccurs="1" maxOccurs="1"
/>
                </xsd:sequence>
                        <xsd:attribute name="ID" type="xsd:ID" use="required"/>

            </xsd:complexType>
            <xsd:complexType name="EtoegangProvideResponseBasetype" abstract="true">
            </xsd:complexType>
            <xsd:complexType name="ServiceListType">
                <xsd:sequence>
                    <xsd:element name="Service" type="etoegang:ComplexServiceType" maxOccurs="unbounded"
minOccurs="0" />
                </xsd:sequence>
            </xsd:complexType>

            <xsd:complexType name="ComplexServiceType">
                 <xsd:sequence>
                    <xsd:element name="ServiceUUID" type="etoegang:ServiceType" maxOccurs="1" minOccurs="1" />
                    <xsd:element name="LOA" type="etoegang:LOA" maxOccurs="1" minOccurs="1" />
                </xsd:sequence>
            </xsd:complexType>

            <xsd:element name="ChainInformationQueryFault" type="etoegang:ChainInformationQueryFaultType">
                <xsd:annotation>
                    <xsd:documentation>
 Fault response to a ChainInformationQuery.
                    </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:complexType name="ChainInformationQueryFaultType">
                <xsd:sequence>
                    <xsd:element name="FaultReason" type="etoegang:ChainInformationQueryFaultReasonType" />
                    <xsd:element name="FaultDescription" type="etoegang:FaultDescriptionType" maxOccurs="
unbounded" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:simpleType name="ChainInformationQueryFaultReasonType">
                <xsd:union memberTypes="etoegang:FaultReasons etoegang:ChainInformationQueryFaultReasons" />
            </xsd:simpleType>
            <xsd:simpleType name="FaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="AuthorizationError">
                        <xsd:annotation>
                            <xsd:documentation>Authentication invalid or access denied.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                    <xsd:enumeration value="SyntaxError">
                        <xsd:annotation>
                            <xsd:documentation>Request invalid.
                            </xsd:documentation>
                        </xsd:annotation>
                    </xsd:enumeration>
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:simpleType name="ChainInformationQueryFaultReasons">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="AuthorizationError">
                        <xsd:annotation>
                            <xsd:documentation>Service is only accessable by other MR's
                            </xsd:documentation>
```

```
                    </xsd:annotation>
                </xsd:enumeration>
                <xsd:enumeration value="SyntaxError">
                    <xsd:annotation>
                        <xsd:documentation>Invalid syntax used
                        </xsd:documentation>
                    </xsd:annotation>
                </xsd:enumeration>
            </xsd:restriction>
        </xsd:simpleType>
        <xsd:complexType name="FaultDescriptionType">
            <xsd:simpleContent>
                <xsd:extension base="xsd:string">
                    <xsd:attribute name="lang" type="xsd:language" />
                </xsd:extension>
            </xsd:simpleContent>
        </xsd:complexType>

    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="ETOEGANG_ChainInformationQueryRequest">
    <wsdl:part name="in" element="etoegang:ChainInformationQueryRequest" />
  </wsdl:message>
  <wsdl:message name="ETOEGANG_ChainInformationQueryResponse">
    <wsdl:part name="out" element="etoegang:ChainInformationQueryResponse" />
  </wsdl:message>
    <wsdl:message name="ETOEGANG_ChainInformationQueryFault">
    <wsdl:part name="ETOEGANG_ChainInformationQueryFault" element="etoegang:ChainInformationQueryFault"  />
  </wsdl:message>
  <wsdl:portType name="ETOEGANG_ChainInformationQuery_Port">
   <wsdl:operation name="ETOEGANG_ChainInformationQuery">
    <wsdl:input message="etoegang:ETOEGANG_ChainInformationQueryRequest" wsam:Action="urn:etoegang:
webservices:ChainInformationQueryRequest" />
     <wsdl:output message="etoegang:ETOEGANG_ChainInformationQueryResponse" wsam:Action="urn:etoegang:
webservices:ChainInformationQueryResponse" />
      <wsdl:fault message="etoegang:ETOEGANG_ChainInformationQueryFault" name="
ETOEGANG_ChainInformationQueryFault"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="ETOEGANG_ChainInformationQuery_SOAP" type="etoegang:ETOEGANG_ChainInformationQuery_Port"
>
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="ETOEGANG_ChainInformationQuery">
      <soap:operation soapAction="urn:etoegang:webservices:ChainInformationQueryRequest" />
      <wsdl:input>
        <soap:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal" />
      </wsdl:output>
      <wsdl:fault name="ETOEGANG_ChainInformationQueryFault">
        <soap:fault name="ETOEGANG_ChainInformationQueryFault" use="literal" />
      </wsdl:fault>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="ETOEGANG_ChainInformationQuery_Service">
    <wsdl:port binding="etoegang:ETOEGANG_ChainInformationQuery_SOAP" name="ETOEGANG_ChainInformationQuery">
      <soap:address location="https://.../TODO/ChainInformationQuery" />
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

MR-MR webservice Security

Signing requirements (from Digital signature)

To guarantee authenticity, integrity and non-repudiation, each message described MUST be provided with a digital signature from the message sender. The message recipient MUST validate all of the digital signatures in the message before processing it.

- The recipient MUST check that the message is signed with a valid digital signature that envelopes the whole message with Enveloped Signature Transform.
- The recipient MUST NOT process the message if it contains parts that are not signed with a valid digital signature.

The following requirements apply to generating digital signatures:

- The digital signature is embedded in the message content with Enveloped Signature Transform http://www.w3.org/2000/09/xmldsig#enveloped-signature.
- Canonicalization MUST be carried out according to the exclusive c14n method without comments, as identified by 'http://www.w3.org/2001/10/xml-exc-c14n#' (see http://www.w3.org/TR/xml-exc-c14n/)
- Digests MUST be calculated with the SHA256 algorithm.
- The SignatureValue MUST be calculated with the RSA-SHA256 algorithm.
- The sender MUST sign messages with a PKIoverheid certificate (see for requirements PKIoverheid) with a key length of at least 2048 bits. The (extended) key usage of the used certificate MUST allow use for signing.
- In case of signing metadata, the <Signature> element MUST contain only an <X509Data> element with an <X509Certificate> element.
  In all other cases, The signature MAY contain a <KeyInfo> element that contains a <KeyName>. The <KeyName> MUST match the <KeyName> stated in the metadata of the sender for the respective role. The signature MUST NOT contain other elements (such as <X509Data>). If a <KeyInfo> element is not included in the message, the metadata MUST contain at least one (1) valid certificate against which the message can be validated. If the metadata contains more than one certificate, the participant MUST validate the message against each valid certificate. The participant MAY agree with its service consumers to limit the period in which the metadata contains more than one certificate. This enables the high utilization of the system to be controlled.
- The Reference MUST refer to the signed element via an ID attribute in the local document, as per the signature profile of SAML2.0 core (§5.4) and SAML 2.0 Metadata (§3.1).

Encryption Requirements (from Secure connection)

The network wants to promote the use of strong cipher suites with minimum discomfort for end-users. Those roles that are in direct contact with their customers (e.g. a HM with it's DV's and an AD/MR with its users) are allowed to tighten security based on their risk analysis.

All communication between peers in these specifications is based on HTTP. All communication MUST be secured using Transport Layer Security, TLS. As a result, all communication MUST be transported over HTTPS (https://tools.ietf.org/html/rfc2818).

For HTTPS and TLS, any implementation MUST take the recommendations in BCP195 (https://tools.ietf.org/html/rfc7525) and the latest version of the NCSC-security guidelines for TLS-usage (currently https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1/ICT-beveiligingsrichtlijnen+voor+Transport+Layer+Security+v2.1.pdf). The following requirements are applicable for this specification in relation to the NCSC guidelines:

- For back-channel communication, the guidelines categorized as "good" MUST be applied.
- For front-channel communication, the guidelines for "good" MUST be applied and the guidelines for "sufficient" MAY be applied, depending on target audience and support requirements.
- Guidelines categorized as "insufficient" MUST NOT be applied and those categorized as "phase out" SHOULD NOT be used.

As HTTP itself is stateless, implementations are free to choose a method of maintaining state or sessions with a User-agent when applicable. The following applies for any HTTP state/session mechanism:

- HTTP servers MUST ensure session and state information is secured and User-agents are properly instructed with relevant security settings (e.g. proper cookie lifetime, Secure setting for cookies, CORS headers and similar).
- Any HTTP session or state tracking mechanisms MUST be implemented using current best practices to avoid session hijacking and other attacks. For more information, see for instance https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Session_Management_Cheat_Sheet.md.

Multiple certificates

SAML and XML-encryption allow for multiple ‘recipients’ of the same encrypted element. The (SAML) construct for this is specified in more detail in errata E43 of SAML 2.0 errata 05.
This feature MAY be used to help facilitate a certificate change at the Service Provider, by (temporarily) allowing both the old and/or the new certificate to be used. The following additional requirements than apply.

- each EncryptedKey MUST have a CarriedKeyName equal to the KeyName used in the KeyInfo of the EncryptedData.
- each EncryptedKey SHOULD have a ReferenceList, referring back to the data encrypted with the symmetric key contained.

Attribuutverstrekking

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Een AD, MR of EB kan als attribuutverstrekker optreden. Zij mogen alleen attributen aanbieden die in de Attribuutcatalogus beschreven worden.

Een deelnemer moet voor elk door te geven attribuut of identificerend kenmerk**,** dat nog niet in de Attribuutcatalogus staat, opnieuw toetreden /zijn bestaande toetreding aanpassen. Zie Proces toetreden.

Gebruiken van attribuutverstrekking

De attribuutcatalogus is in eerste instantie bedoeld voor deelnemers. Zij communiceren richting hun dienstverleners welke attributen zij leveren. De attribuutcatalogus beschrijft verder welke attributen een attribuutverstrekker aanvullend MAG kunnen leveren. Attributen waarvan de naam met urn: etoegang:*x.y*:attribute: (met *x.y* een versie van het AS) begint, mogen enkel door Authenticatiediensten worden geleverd. Attributen waarvan de naam met urn:etoegang:*x.y*:attribute-represented: begint, mogen enkel door Machtigingenregisters worden geleverd. Aangezien de eIDAS-berichtenservice (EB) zowel als AD als MR optreedt, mag de EB beide leveren.

Attributen worden door een dienstverlener gevraagd aan de Herkenningsmakelaar (d.m.v. een AttributeConsumingServiceIndex verwijzend naar RequestedAttribute(s) in de DV metadata for HM) die de vraag vervolgens doorzet naar een AD of een MR (als extensie in de vraag in RequestedAttributes). De attributen worden aan de dienstverlener verstrekt in een <AttributeStatement> XML element. Attributen worden versleuteld opgestuurd door de deelnemers die de betreffende attributen verstrekken.

De verdere specificaties voor attribuutverstrekking zijn beschreven in Interface specifications.

Identificerende kenmerken

Dit hoofdstuk beschrijft de identificerende kenmerken binnen Elektronische Toegangsdiensten.

Deze attributen zijn niet opgenomen in de Attribuutcatalogus.

Identificerende kenmerken van dienstafnemers

Een speciale categorie attributen zijn de identificerende kenmerken van de verschillende soorten dienstafnemers of intermediairs.

Geleverde identificerende kenmerken van dienstafnemers hebben een attribuutnaam die begint met "urn:etoegang:<versie>:EntityConcernedID:".

Geleverde identificerende kenmerken van intermediairs hebben een attribuutnaam die begint met "urn:etoegang:<versie>:IntermediateEntityID:".

De volgende paragrafen beschrijven de typen identificerende kenmerken van dienstafnemers en intermediairs.

- Indien 'Vertegenwoordiging' het teken ✅ bevat, dan mag dit type identificerend kenmerk worden gebruikt voor dienstafnemers.
- Indien 'Vertegenwoordiging' het teken ❌ bevat, dan mag dit type identificerend kenmerk NIET worden gebruikt voor dienstafnemers.
- Indien 'Ketenmachtigen' het teken ✅ bevat, dan mag dit type identificerend kenmerk worden gebruikt voor dienstafnemers ~~of intermediairs~~ in een keten van machtigingen.
- Indien 'Ketenmachtigen' het teken ❌ bevat, dan mag dit type identificeren kenmerk NIET worden gebruikt voor dienstafnemers.

NB: Ketenmachtigingen maken voor intermediairs gebruik van het KvK nummer.

EncryptedID

Alle identificerende kenmerken binnen Elektronische Toegangsdiensten worden geleverd als SAML EncryptedID. Het type identificerend kenmerk wordt als NameQualifier van dit EncryptedID gecommuniceerd.

Voor identifiers die per ontvangende partij verschillen, zoals urn:etoegang:1.12:EntityConcernedID:PseudoID, kan uit het 'Recipient' attribuut van de EncryptedKey worden afgeleid voor wie deze bestemd en bruikbaar is.

EntityConcernedID:eIDASLegalIdentifier

Attribuutnaam	urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier
Omschrijving	Een identificerend kenmerk dat wordt gebruikt om een Niet Natuurlijk Persoon bij Herkenning via eIDAS te identificeren binnen Elektronische Toegangsdiensten
Formaat	String, lengte varieert per lidstaat van oorsprong.
Ketenmachtigingen	✗
Vertegenwoordiging	✓

EntityConcernedID:KvKnr

Attribuutnaam	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:IntermediateEntityID:KvKnr
Omschrijving	Het KvK nummer van de vertegenwoordigde dienstafnemer/intermediair of vergelijkbaar nummer
Formaat	Het KvK nummer bestaat uit 8 cijfers, bijvoorbeeld 12345678
Ketenmachtigingen	✅
Vertegenwoordiging	✅

EntityConcernedID:PROBASnr

Attribuutnaam	urn:etoegang:1.13:EntityConcernedID:PROBASnr
Omschrijving	Door de Belastingdienst uitgereikt nummer aan organisaties die niet staan ingeschreven in het Handelsregister. Het PROBASnr staat ingeschreven in het PROBAS-register welke in beheer is bij Ministerie van Buitenlands Zaken.
Formaat	Het PROBASnr bestaat uit 9 cijfers. Voorbeeld: 123456789.
Ketenmachtigingen	✅
Vertegenwoordiging	✅

EntityConcernedID:Pseudo

Attribuutnaam	urn:etoegang:1.9:EntityConcernedID:Pseudo
Omschrijving	Een specifiek pseudoniem dat wordt gebruikt om een consument te identificeren binnen eHerkenning.
Formaat	32 byte hex
Ketenmachtigingen	
Vertegenwoordiging	

EntityConcernedID:RSIN

Attribuutnaam	urn:etoegang:1.9:EntityConcernedID:RSIN
Omschrijving	Het Rechtspersonen en Samenwerkingsverbanden Identificatienummer van de vertegenwoordigde dienstafnemer/intermediair
Formaat	Het RSIN bestaat uit 9 cijfers. Voorbeeld: 123456789.
Ketenmachtigingen	✅
Vertegenwoordiging	✅

ServiceRestriction:SubdossierNr

Attribuutnaam	urn:etoegang:1.9:ServiceRestriction:SubdossierNr
Omschrijving	Het vestigingsnummer (oude formaat) van de vertegenwoordigde dienstafnemer
Formaat	Het vestigingsnummer bestaat uit 4 cijfers, bijvoorbeeld 0001
Ketenmachtigingen	Nee voor intermediair, Ja voor dienstafnemer
Vertegenwoordiging	✅

⚠ Een beperking tot een vestiging betekent dat de vertegenwoordiger alleen bevoegd is om de desbetreffende vestiging te vertegenwoordigen.

Indien een dienstverlener een beperking op subdossier- of vestigingsnummer accepteert

- MOET deze ook transacties accepteren zonder deze beperking
- MOET deze een aangeleverde beperking respecteren. Het negeren ervan kan dit als gevolg hebben dat er geen rechtsgeldige rechtshandeling tot stand is gekomen
- MAG dit subdossier- of vestigingsnummer niet gebruikt worden als bepaling van de locatie, maar alleen om de grenzen van de vertegenwoordigingsbevoegdheid vast te stellen

⚠ ServiceRestriction:SubdossierNr zelf dient niet te worden opgenomen in de dienstencatalogus (als EntityTypeConcernedAllowed), indien een DV deze nog gebruikt. Om aan te geven dat een DV deze beperking accepteert, dient ServiceRestriction:Vestigingsnr in de dienstencatalogus te worden opgenomen. Een MR MOET het SubdossierNr meeleveren naast het Vestigingsnr, zolang de KvK deze nog levert.

ⓘ Kamer van Koophandel heeft aangekondigd te stoppen met het leveren van dit attribuut. Doorgifte van dit attribuut is op lange termijn niet gegarandeerd.

ServiceRestriction:Vestigingsnr

Attribuutnaam	urn:etoegang:1.9:ServiceRestriction:Vestigingsnr
Omschrijving	Het vestigingsnummer (nieuwe formaat) van de vertegenwoordigde dienstafnemer
Formaat	Het vestigingsnummer bestaat uit 12 cijfers, bijvoorbeeld 123456789012
Ketenmachtigingen	Nee voor intermediair, Ja voor dienstafnemer
Vertegenwoordiging	✅

⚠ Een beperking tot een vestiging betekent dat de vertegenwoordiger alleen bevoegd is om de desbetreffende vestiging te vertegenwoordigen.

Indien een dienstverlener een beperking op subdossier- of vestigingsnummer accepteert

- MOET deze ook transacties accepteren zonder deze beperking
- MOET deze een aangeleverde beperking respecteren. Het negeren ervan kan dit als gevolg hebben dat er geen rechtsgeldige rechtshandeling tot stand is gekomen
- MAG dit subdossier- of vestigingsnummer niet gebruikt worden als bepaling van de locatie, maar alleen om de grenzen van de vertegenwoordigingsbevoegdheid vast te stellen

urn:etoegang:1.12:EntityConcernedID:BSN

NameQualifier	urn:etoegang:1.12:EntityConcernedID:BSN
Omschrijving	Een **urn:etoegang:1.12:EntityConcernedID:BSN** wordt gebruikt om een Natuurlijk persoon of éénmanszaak te identificeren binnen Elektronische Toegangsdiensten. Dit **urn:etoegang:1.12:EntityConcernedID:BSN** is een BSN die om privacy-redenen specifiek per Dienstverlener polymorf is versleuteld.
Formaat	Base64 representatie van een versleutelde identiteit, als drie punten op een elliptische kromme, specifiek voor de Dienstverlener (DER-encoded structure in ASN.1 notatie, een (Signed)EncryptedIdentity, zie Handreiking Polymorphic Pseudonimization Notation). Na decryptie levert dit een 9 cijferig BSN op.
Ketenmachtigingen	✅
Vertegenwoordiging	✅
Overig	• MAG gebruikt worden om een gebruiker te identificeren middels een ASTA of ECTA

urn:etoegang:1.12:EntityConcernedID:PseudoID

NameQualifier	urn:etoegang:1.12:EntityConcernedID:PseudoID
Omschrijving	Een **urn:etoegang:1.12:EntityConcernedID:PseudoID** wordt gebruikt om een Natuurlijk persoon te identificeren binnen Elektronische Toegangsdiensten, voor gebruik binnen eHerkenning. Het PseudoID is een Dienstverlener specifiek persistent pseudoniem dat om privacy-redenen ook nog eens specifiek per Dienstverlener is versleuteld. Dit persistente pseudoniem is identiek voor de gebruiker onafhankelijk van welke Verklarende Partij de gebruiker gebruik maakt.
Formaat	Base64 representatie van versleutelde identiteit, als drie punten op een elliptische kromme, specifiek voor de Dienstverlener (DER-encoded structure in ASN.1 notatie, een (Signed)EncryptedPseudonym, zie Handreiking Polymorphic Pseudonimization Notation.
Ketenmachtigingen	✗
Vertegenwoordiging	✗
Overig	• MAG gebruikt worden om een gebruiker te identificeren middels een ASTA of ECTA

urn:etoegang:1.13:EntityConcernedID:Pseudo

Attribuutnaam	urn:etoegang:1.13:EntityConcernedID:Pseudo
Omschrijving	Een Specifiek Peudoniem dat wordt gebruikt om een vertegenwoordiger (igv vertegenwoordiging) te identificeren binnen eHerkenning.
Formaat	32 byte hex gevolgd door een @ en een 16 byte hex ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890@ABCDEF1234567890ABCDEF1234567890 (zie Specific pseudonym)
Ketenmachtigingen	✅
Vertegenwoordiging	✅

Attribuutcatalogus

Een aantal attributen MOET kunnen worden geleverd. Dit zijn verplicht te verstrekken attributen. De attribuutcatalogus beschrijft welke attributen een attribuutverstrekker kan leveren.

Attributen waarvan de naam met urn:etoegang:*x.y*:attribute: (met *x.y* een versie van het AS) begint, mogen enkel door Authenticatiediensten worden geleverd. Attributen waarvan de naam met urn:etoegang:*x.y*:attribute-represented: begint, mogen enkel door Machtigingdiensten worden geleverd. Aangezien de eIDAS-berichtenservice (EB) voor eIDAS-inbound zowel als AD als MR optreedt, mag de EB beide leveren.

> Voor eIDAS-outbound, levert de BRP de minimale vereiste attributenset en heeft de EB de rol van Dienstbemiddelaar.

Elke deelnemer MAG alleen de attributen verstrekken die gespecificeerd zijn in de attribuutcatalogus. De attribuutcatalogus bestaat uit een ondertekend <AttributeCatalogue> element. Signing gebeurt met dezelfde *private key* waarmee ook de metadata ondertekend wordt. Zie Digital signature.

Een deelnemer MOET op een gemeenschappelijk overeengekomen tijdstip de attribuutcatalogus verwerken. Dit hoeft niet op basis van de XML representatie van de attribuutcatalogus te gebeuren, zolang men de kenmerken van de attributen in acht neemt.

XML formaat

Data element		0..n	Invulling
@Version		1	Elektronische Toegangsdiensten: Versie van de attribuutcatalogus in het formaat: urn:etoegang:<scheme version>:<omgeving>:attribute-catalogue:<sequence number>. Bijvoorbeeld: urn:etoegang:1.11:attribute-catalogue:P:1
@IssueInstant		1	Elektronische Toegangsdiensten: Tijd waarop de attribuutcatalogus is aangemaakt
Signature		1	Elektronische Toegangsdiensten: MOET de elektronische handtekening van de partij die de attribuutcatalogus heeft aangemaakt, over het hele bericht bevatten
Attribute		1..n	Elektronische Toegangsdiensten: Eén of meerdere elementen die een attribuut specificeren met de kenmerken uit Attribuutcatalogus.
	Name	1	Elektronische Toegangsdiensten: Naam van het attribuut.
	Type	1	Elektronische Toegangsdiensten: Type van het attribuut. Bijvoorbeeld “http://www.w3.org/2001/XMLSchema#string”
	FriendlyName	1..n	Elektronische Toegangsdiensten: Een korte omschrijving van het attribuut zodat de betekenis van het attribuut eenduidig geïnterpreteerd wordt, één voorkomen per taal.
	@lang	1	taal van FriendlyName, om in gebruikersinterfaces te tonen.
	Description	1..n	Elektronische Toegangsdiensten: Een gedetailleerde omschrijving van het attribuut zodat de betekenis van het attribuut eenduidig geïnterpreteerd wordt, één voorkomen per taal.
	@lang	1	taal van Description, om in (toelichtingen bij) gebruikersinterfaces te tonen.
	PermissibleSource	1..n	Elektronische Toegangsdiensten: Referentie aan bronnen welke het attribuut op mogen leveren.

> De beheerorganisatie publiceert de laatste versie van de attribuutcatalogus op https://extranet.eherkenning.nl/1.11/attribuutcatalogus.xml.

Schema AttribuutCatalogus

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:eac="urn:etoegang:1.9:attribute-catalogue"
    targetNamespace="urn:etoegang:1.9:attribute-catalogue"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd">

    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />
```

```
    <xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
        schemaLocation="http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd" />

    <xs:element name="Attribute" type="eac:AttributeType" />
    <xs:complexType name="AttributeType">
        <xs:sequence>
            <xs:element name="Name" type="xs:anyURI" />
            <xs:element name="Type" type="xs:anyURI" />
            <xs:element name="FriendlyName" type="md:localizedNameType" maxOccurs="unbounded" />
            <xs:element name="Description" type="md:localizedNameType" maxOccurs="unbounded" />
            <xs:element name="PermissibleSource" type="xs:anyURI" maxOccurs="unbounded" />
        </xs:sequence>
    </xs:complexType>

    <xs:element name="AttributeCatalogue" type="eac:AttributeCatalogueType" />
    <xs:complexType name="AttributeCatalogueType" >
        <xs:sequence>
            <xs:element ref="ds:Signature" />
            <xs:element ref="eac:Attribute" maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="IssueInstant" type="xs:dateTime" use="required" />
        <xs:attribute name="Version" type="xs:anyURI" use="required" />
    </xs:complexType>

</xs:schema>
```

Toegestane bronnen

Bij elke wijziging moet het attribuut met dezelfde betrouwbaarheid opnieuw gevalideerd worden

URN	Omschrijving	Eisen aan het verificatieproces van het attribuut
urn:etoegang:1.11:attribute-sourceid:ID	Geregistreerd door deelnemer vanaf een geldig identiteitsbewijs volgens het Normenkader betrouwbaarheidsniveaus	Tijdens een registratieproces op betrouwbaarheidsniveau 3 of 4 overgenomen (of afgeleid van) het ID, of overgenomen van een kopie ID en gecontroleerd bij een tweede bron
urn:etoegang:1.11:attribute-sourceid:IDCopy	Geregistreerd door deelnemer vanaf een kopie van een geldig identiteitsbewijs volgens het Normenkader betrouwbaarheidsniveaus	Tijdens een registratieproces op betrouwbaarheidsniveau 2 overgenomen (of afgeleid van) een kopie ID
urn:etoegang:1.9:attribute-sourceid:NLGBA	Verkregen door deelnemer vanaf de Basisregistratie Persoonsgegevens	Opgehaald uit de Basisregistratie Persoonsgegevens (op basis van een Tijdens een registratieproces op betrouwbaarheidsniveau 3 of 4 van een WID overgenomen BSN)
urn:etoegang:1.11:attribute-sourceid:NLKvK	Verkregen van het Handelsregister van de Kamer van Koophandel	Conform eisen geldend voor de betrouwbaarheid van vaststellen identiteit Dienstafnemer
urn:etoegang:1.11:attribute-sourcei	Verkregen door de eIDAS-node verkregen vanuit een andere lidstaat. Als PermissibleSource in de attributencatalogus wordt 'urn:etoegang:1.11:attribute-sourceid:eIDAS' opgenomen. Bij levering van het attribuut wordt het land van oorsprong wordt als postfix toegevoegd (ISO-3166-1 alpha-2, tweeletterig; aangevuld met 'eIDAS'),	Geen. Het attribuut is niet gecontroleerd door de deelnemer, maar verkregen van een andere EU-lidstaat.

d:eIDAS*:XX*	bijvoorbeeld 'urn:etoegang:1.11:attribute-sourceid:eIDAS:*DE*' voor attributen verkregen via eIDAS vanuit Duitsland	
urn:etoegang:1.9:attribute-sourceid:SelfDeclared	Zelfverklaard, zonder controle door de deelnemer	Geen. Het attribuut is niet gecontroleerd door de deelnemer, maar door de Gebruiker zelf opgegeven.
EntityID	Het EntityID van de deelnemer die de controle heeft uitgevoerd	De deelnemer heeft een proces ingericht waarmee het attribuut onlosmakelijk geassocieerd is met de gebruiker. Bijvoorbeeld door de Gebruiker tijdens het proces A UC2 Verkrijgen authenticatiemiddel een e-mail- of postadres op te laten geven en daar een OTP naar toe te sturen. Als de Gebruiker zich met zijn middel kan authenticeren en deze OTP kan opgeven, is dat voldoende bewijs dat hij toegang heeft tot het opgegeven adres.
urn:etoegang:1.13:attribute-sourceid:NLPROBAS	Verkregen uit PROBAS	Conform eisen geldend voor de betrouwbaarheid van vaststellen identiteit Dienstafnemer

Attribuutcatalogus generiek

URN	Omschrijving	Formaat	Toegestane bron	Verplicht of optioneel?
urn:etoegang:1.9:attribute:PostalCode	Postcode van de gebruiker. *eIDAS: PostCode.*	String max 12	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.9:attribute:HouseNumber	Huisnummer van de gebruiker.	Integer	SelfDeclared	Optioneel
urn:etoegang:1.9:attribute:HouseNumberSuffix	Huisnummer toevoeging van de gebruiker.	String max 5	SelfDeclared	Optioneel
urn:etoegang:1.11:attribute:POBox	Postbusnummer van de gebruiker. *eIDAS: POBOX.*	String, max 20	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:Thoroughfare	Straat van de gebruiker. *eIDAS: Thoroughfare*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:LocatorDesignator	Huisnummer, of andere unieke identificatie van een adres op een "straat" (*thoroughfare*) van de gebruiker. *eIDAS: LocatorDesignator*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:LocatorName	Naam van een gebouw of deel ervan als specialisatie van het adres van de gebruiker. *eIDAS: LocatorName*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:AddressArea	Wijk of deel van een gemeente van de gebruiker. *eIDAS: CvaddressArea*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:PostName	Plaatsnaam in het adres van de gebruiker. *eIDAS: PostName*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:AdminunitSecondline	Provincie of staat binnen het adres van de gebruiker. *eIDAS: AdminunitSecondline*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute:AdminunitFirstline	Tweeletterige landcode van het adres conform ISO3166-1 (alpha-2), of de volledige naam van het land van de gebruiker. *eIDAS: AdminunitFirstline*	String max 100	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:PostalCode	Postcode van de vertegenwoordigde. *eIDAS: PostCode*	String max 12	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:HouseNumber	Huisnummer van de vertegenwoordigde.	Integer	SelfDeclared	Optioneel
urn:etoegang:1.11:attribute-represented:HouseNumberSuffix	Huisnummer toevoeging van de vertegenwoordigde.	String max 5	SelfDeclared	Optioneel
urn:etoegang:1.11:attribute-represented:POBox	Postbusnummer van de vertegenwoordigde. *eIDAS: POBOX*	String, max 20	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:Thoroughfare	Straat van de vertegenwoordigde. *eIDAS: Thoroughfare*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:LocatorDesignator	Huisnummer, of andere unieke identificatie van een adres op een "straat" (*thoroughfare*) van de vertegenwoordigde. *eIDAS: LocatorDesignator*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:LocatorName	Naam van een gebouw of deel ervan als specialisatie van het adres van de vertegenwoordigde. *eIDAS: LocatorName*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:AddressArea	Wijk of deel van een gemeente van de vertegenwoordigde. *eIDAS: CvaddressArea*	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:PostName	Plaatsnaam in het adres van de vertegenwoordigde. *eIDAS: PostName*	String max 200	SelfDeclared, eIDAS	Optioneel
	Provincie of staat binnen het adres van de vertegenwoordigde.	String	SelfDeclare	Optioneel

urn:etoegang:1.11:attribute-represented:AdminunitSecondline	*eIDAS: AdminunitSecondline*	max 200	d, eIDAS	
urn:etoegang:1.11:attribute-represented:AdminunitFirstline	Drieletterige landcode van het adres conform ISO3166-1 (alpha-3), of de volledige naam van het land van de vertegenwoordigde. *eIDAS: AdminunitFirstline*	String max 100	SelfDeclared, eIDAS	Optioneel

Attribuutcatalogus natuurlijke personen

Voor eIDAS-outbound, levert de BRP de minimale vereisten attributenset van de handelende natuurlijke persoon. Deze worden niet geleverd door AD van het Afsprakenstelsel.

URN	Omschrijving	Formaat	Bron	Verplicht of optioneel?
urn:etoegang:1.9:attribute:FirstName	Beschikbare voorna(a)m(en) van de gebruiker (beschikbaarheid is afhankelijk van de bron)	String max 200	ID, IDCopy, eIDAS	Verplicht
urn:etoegang:1.9:attribute:Initials	Initialen van de voorna(a)m(en) van de gebruiker	String max 35	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:FamilyNameInfix	Voorvoegsel behorend bij Achternaam, conform Voorvoegseltabel GBA (Tabel 36). Zie Logisch Ontwerp GBA-V (element 02.30, blz. 236) voor uitleg over de toepassing van de tabel op een achternaam.	String max 10	ID, IDCopy, eIDAS	Verplicht (indien van toepassing bij bijbehorende achternaam)
urn:etoegang:1.9:attribute:FamilyName	Achternaam (geslachtsnaam) van de gebruiker	String max 200	ID, IDCopy, eIDAS	Verplicht
urn:etoegang:1.11:attribute:BirthName	Naam van de gebruiker bij geboorte	String max 200	eIDAS	-
urn:etoegang:1.11:attribute:non-transliterated:FirstName	Voornaam van de gebruiker in ander alfabet	String max 200	eIDAS	-
urn:etoegang:1.11:attribute:non-transliterated:FamilyName	Achternaam van de gebruiker in ander alfabet	String max 200	eIDAS	-
urn:etoegang:1.11:attribute:non-transliterated:FirstNameAtBirth	Voornaam van de gebruiker bij geboorte in ander alfabet	String max 200	eIDAS	-
urn:etoegang:1.11:attribute:non-transliterated:FamilyNameAtBirth	Achternaam van de gebruiker bij geboorte in ander alfabet	String max 200	eIDAS	-
urn:etoegang:1.9:attribute:DateOfBirth	Geboortedatum van de gebruiker *Volgens de BRP zijn de volgende afwijkende datumformaten toegestaan: jjjj-mm-dd, jjjj-mm-00, jjjj-00-00, 0000-00-00*	String 10 jjjj-mm-dd	ID, IDCopy, eIDAS	Verplicht
urn:etoegang:1.9:attribute:18OrOlder	Is gebruiker ouder dan 18	true/false	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:16OrOlder	Is gebruiker ouder dan 16	true/false	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:12OrOlder	Is gebruiker ouder dan 12	true/false	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:65OrOlder	Is gebruiker ouder dan 65	true/false	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:PlaceOfBirth	Geboorteplaats van de gebruiker	String max 40	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:Gender	Geslacht van de gebruiker	"M", "F", "U"	ID, IDCopy, eIDAS	Optioneel
urn:etoegang:1.9:attribute:Email	E-mailadres van de gebruiker	URI, max 320; mailto:<localname>@<domain name> (RFC6068)	SelfDeclared	Optioneel
urn:etoegang:1.9:attribute:Mobile	Mobiele nummer van de gebruiker	URI, max 19; tel:+<CountryCode><phonenumber> (RFC3966)	SelfDeclared	Optioneel

Attributencatalogus niet-natuurlijke personen

URN	Omschrijving	Formaat	Bron	Verplicht of optioneel?
urn:etoegang:1.11:attribute-represented:CompanyName	Huidige naam van de organisatie, waaronder deze geregistreerd staat (NL: in het handelsregister).	String max 200	KvK, eIDAS PROBAS	Verplicht
urn:etoegang:1.13:attribute-intermediate:CompanyName	Huidige naam van de organisatie van de intermediair, waaronder deze geregistreerd staat (NL: in het handelsregister).	String max 200	KvK	Optioneel
urn:etoegang:1.11:attribute-represented:non-transliterated: CompanyName	Huidige naam van de organisatie in ander alfabet (bijvoorbeeld Grieks), waaronder deze geregistreerd staat.	String max 200	eIDAS	- (wordt gevuld door AD in andere lidstaat)
urn:etoegang:1.11:attribute-represented:VATRegistrationNumber	BTW-nummer. NL: Dit attribuut is een afgeleide van het RSIN en wordt daartoe aan de hand van het RSIN gevalideerd.	String max 200	KvK, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:TaxReferenceNumber	Fiscaal referentienummer. NL: Dit attribuut is een afgeleide van het RSIN en wordt daartoe aan de hand van het RSIN gevalideerd.	String max 200	KvK, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:ChamberOfCommerce	De identificatiecode bedoeld in artikel 3, lid 1, van Richtlijn 2009/101/EG van het Europees Parlement en de Europese Raad. NB: Voor Nederlandse organisaties wordt EntityConcernedID:KvKnr gebruikt ipv ChamberOfCommerce.	String max 200	eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:KvKnr	Het KvK nummer van de vertegenwoordigde dienstafnemer.	String max 200	KvK	Verplicht
urn:etoegang:1.11:attribute-represented:LEI	De identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) nr. 1247/2012 van de Europese Commissie. NL: Gevuld met LEI (Legal Entity Identifier) zoals verkregen van KvK.	String max 200	KvK, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:EORI	Het registratie- en identificatienummer van marktdeelnemer bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Europese Commissie. NL: Gevuld met het Economic Operator Registration and Identification nummer zoals uitgegeven door Douane, obv RSIN zoals verkregen van KvK.	String max 200	KvK, eIDAS	Optioneel
urn:etoegang:1.11:attribute-represented:SEED	Het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Europese Raad. Gevuld met System for Exchange of Excise Data | accijnsnummer, zoals uitgegeven door Douane.	String max 200	SelfDeclared, eIDAS	Optioneel
urn:etoegang: 1.11:attribute-represented:SIC	De Standard Industrial Classification: Een viercijferige code om de bedrijfsvoering van de rechtspersoon te classificeren.	String max 200; optioneel meervoudig	KvK, eIDAS	Optioneel
urn:etoegang:1.13:attribute-represented:Subsidy	Dit attribuut geeft aan of een bedrijf recht heeft op subsidie en op welke grond. (Attribuut is case-insensitive)	String, mogelijke waardes: BELASTINGDIENST	EntityID van de MR	Optioneel

Handreiking Polymorphic Pseudonimization Notation



The specifications on this page are a copy of the one provided in the "Uniforme Set van Eisen" (USvE) version 1.0. Please note that the Afsprakenstelsel Elektronische Toegangsdiensten adheres to these USvE specifications, and a copy is included here for information only. The copy may have been modified to reflect Afsprakenstelsel Elektronische Toegangsdiensten terminology and references.

Polymorphic Pseudonymization uses a number of cryptographic structures. These crypto-structures are denoted in the Interface Specifications as follows:

Pseudonym (Dutch)	Notation	Pseudonym (English)	Notation	Explanation
Polymorf Pseudoniem	PP@MU	Polymorphic Pseudonym	PP@MU	PP denotes the pseudonym is a Polymorphic Pseudonym. The abbrevation following the '@' symbol denotes the relying party the Polymorphic Pseudonym is unique to.
Polymorfe Identiteit	PI@MU	Polymorphic Identity	PI@MU	PI denotes the pseudonym is a Polymorphic Identity. The abbrevation following the '@' symbol denotes the relying party the Polymorphic Pseudonym is unique to.
Versleuteld Pseudoniem	VP@DV	Encrypted Pseudonym	EP@DV	VP in Dutch or EP in English denotes the pseudonym is an Encrypted Pseudonym. The abbrevation following the '@' symbol denotes the relying party the Encrypted Pseudonym is unique to.
Versleutelde Identiteit	VI@DV	Encrypted Identity	EI@DV	VI in Dutch or EI in English denotes the pseudonym is an Encrypted Identity. The abbrevation following the '@' symbol denotes the relying party the Encryped Pseudonym is unique to.
persistent Pseudoniem	P@DV	persistent Pseudonym	P@DV	P denotes the pseudonym is a persistent Pseudonym. The abbrevation following the '@' symbol denotes the relying party the persistent Pseudonym is unique to.
Identiteit	-	Identity	-	The Identity in polymorphic pseudonymization refers to the identity obtained after decryption of an Encrypted Pseudonym by a receiving party. This Identity equals the root identifying attribute used to generate the PIP that Polymorph Pseudonyms are based on, for example the BSN. Instead of referring to the decrypted Encrypted Pseudonym as Identity, the root identifying attribute is used instead.
Sleutelmateriaal		DV-keys		The Dienstverlener (DV) specific keymaterial necessary to decrypt Encrypted Pseudonyms.
		PolymorphicSchemePublicKeySet		Polymorphic Pseudonymization scheme general public keys.

This paragraph describes the technical format of polymorphic identities and pseudonyms and related key formats. Polymorphic identities and pseudonyms in the scheme are based on cryptographic properties of elliptic curves.

Usages of Polymorphic Pseudonymization

- Activation
  - Polymorphic Identity or Pseudonym
  - Encrypted Identity or Pseudonym
- Usage (transformation and decryption)
  - Encrypted Identity or Pseudonym
  - Identity or Pseudonym

Format for Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym is a combination of points on an elliptic curve. In order for the Identity or Pseudonym to be properly usable in the scheme, some additional information is needed. This information is necessary for practical management and secure implementation of Identity or Pseudonym in the Scheme and consists of elements like versioning (for key management) and recipient. The syntax for expressing an Identity or Pseudonym with this information is listed below.

Values of the notations below SHALL be represented as (the base64 encoding of) the DER-encoded structure in ASN.1 notation.

Polymorphic Identity or Pseudonym

A Polymorphic Identity or Pseudonym consists of 3 points on an elliptic curve. Polymorphic Identity or Pseudonym are provided via the Interface spec BSNk: activate. They are used via the interface Interface spec BSNk: transform. The notation for a complete Polymorphic Identity or Pseudonym is as follows:

Polymorphic Identity or Pseudonym ASN.1 notation

```
PolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity),
    schemeVersion INTEGER,
```

```
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

PolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}
```

Herein the schemeVersion indicates the version of the cryptographic scheme and this syntax and SHALL start at 1. The schemeKeyVersion is a version that SHALL start at 1 and represents the effective set of long term scheme master keys (PP-M, PD-M, etc...). The schemeKeyVersion defines the elliptic curve used in the scheme as well. The creator SHALL contain the entityID (OIN) of the creator, and the recipient SHALL contain the entityID (OIN) of the recipient. The recipientKeySetVersion holds the version number for the set of recipient's keys for Polymorphic Identities and Pseudonyms (PA-Di). Note: In schemeVersion 1 the recipientKeySetVersion for MUs and ADs is a sequence starting at 1. Type defines the identity type the Pseudonym is derived of, e. g. from a BSN or an eIDAS Uniqueness Identifier. This field is not necessary in identity based forms as here the identity type will become clear as part of decryption of the final structure, i.e. the Encrypted Identity. The values currently defined are the ASCII value of 'B' (0x42) for BSN based and 'E' (0x45) when based on a eIDAS uniqueness identifier. ECPoint is identical to ECPoint as defined in BSI TR 03111 and ANSI X9.62 (2005). Here two encodings are specified, compressed and compressed. Both encodings are allowed, with a preference for uncompressed encoding.

A Polymorphic Identity of Polymorphic Pseudonym can be signed for integrity protection:

```
SignedPolymorphicIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-identity-signed),
    signedPI SEQUENCE {
        polymorphicIdentity PolymorphicIdentity,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}

SignedPolymorphicPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pseudonym-signed),
    signedPP SEQUENCE {
        polymorphicPseudonym PolymorphicPseudonym,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    },
    signatureValue ECDSA-Signature
}
```

An auditElement holds an audit value consisting of an identifier for the creator, a timestamp and a sequence number from that creator. This auditElement is 16 bytes (32-bit creator, 32-bit timestamp and 64-bit sequence-number). The creator identifies the party providing the Polymorphic/Encrypted Identity or Pseudonym and the unique device used. The timestamp and sequence number can be used in case of a compromise or dispute, so that mitigating measure or resolution can be accomplished. Note: the timestamp is 32-bit in seconds since 1 jan 1970 UTC. The auditElement is encrypted under a key only retrievable by the supervisor of the scheme, which is provided to the supervisior by the keymanagement role.

The signatureValue can be used to assert the authenticity of the (polymorphic/encrypted) Identity or Pseudonym. The signature is applied to the byte sequence of the complete DER-encoded signed sequence (e.g. signedPP in a SignedPolymorphicPseudonym). The public key for verification can be retrieved using the creator from the structure covered under the signature and the signingKeyVersion.

```
-- ECPoint is described in ANSI X9.62 (2005), annex E.6.
-- In particular, encoding from point to octet string and
-- from octet string to a point is defined in annex A.5.7
-- and A.5.8 of ANSI X9.62.
ECPoint ::= OCTET STRING

ECDSA-Signature ::= SEQUENCE {
    signatureType      OBJECT IDENTIFIER (ecdsa-with-SHA384),
    signatureValue     EC-Sig-Value
}
```

```
-- EC-Sig-Value is identitical to BSI TR 03111 ECDSA-Sig-Value.
-- which is identical to ECDSA-Sig-Value defined in RFC5480 as well.
EC-Sig-Value ::= SEQUENCE {
    r  INTEGER,
    s  INTEGER
}

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4)
    ecdsa-with-SHA2(3) 3 }

id-BSNk-scheme-nl OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16) nl(528) nederlandse-organisatie(1)
nederlandse-overheid(1003) ..... TODO }

id-BSNk-identifiers OBJECT IDENTIFIER ::= { id-BSNk-scheme-nl 1 }

id-BSNk-polymorphics OBJECT IDENTIFIER ::= { id-BSNk-identifiers 1 }

id-BSNk-polymorphic-identity OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 1 }

id-BSNk-polymorphic-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 2 }

id-BSNk-polymorphic-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 3 }

id-BSNk-polymorphic-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 4 }
```

PIP – PPCA optimized

For privacy enhanced implementation, Polymorphic Identities and Pseudonyms can be implemented on a smartcard. This is called a PP-card application, or PPCA. A Polymorphic Identity and a Polymorphic Pseudonym can be combined to 5 points on an elliptic curve rather than six, for optimization in a smartcard implementation. The PPCA-optimized PIP version of Polymorphic Identities or Pseudonyms are provided in Interface spec BSNk: activate.

The combined notation for an Polymorphic Identity and Pseudonym is as follows:

Polymorphic Identity and Pseudonym (PIP) ASN.1 notation

```
PIP ::= SEQUENCE {
    notationIdentifier  OBJECT IDENTIFIER (id-BSNk-polymorphic-pip),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (5)) OF ECPoint
}
```

The first, second and fourth ECPoint in a PIP correspond to those of a PI. Similarly, the first, third and fifth correspond to those of a PP. In this fashion one can extract a PI and PP from a PIP.

There also exists a signed version of a PIP:

```
SignedPIP::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-polymorphic-pip-signed),
    signedPIP SEQUENCE {
        pip PIP,
        auditElement OCTET STRING,
        signingKeyVersion INTEGER
    }
    signatureValue ECDSA-Signature
}
```

Which follows the same concepts as described for a Polymorphic Identity or Polymorphic Pseudonym.

```
id-BSNk-polymorphic-pip OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 5 }

id-BSNk-polymorphic-pip-signed OBJECT IDENTIFIER ::= { id-BSNk-polymorphics 6 }
```

Encrypted Identity or Pseudonym

An Encrypted Identity or Pseudonym consists of 3 points on an elliptic curve. The notation for a complete Encrypted Identity and an Encrypted Pseudonym is as follows:

Encrypted pseudoID ASN.1 notation

```
EncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

EncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    diversifier IA5String OPTIONAL,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

SignedEncryptedIdentity ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-identity-signed),
    signedEI SEQUENCE {
        encryptedIdentity EncryptedIdentity,
        auditElement OCTET STRING
    }
    signatureValue EC-Schnorr-Signature
}

SignedEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-pseudonym-signed),
    signedEP SEQUENCE {
        encryptedPseudonym EncryptedPseudonym,
        auditElement OCTET STRING
    }
    signatureValue EC-Schnorr-Signature
}

DirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym),
    schemeVersion INTEGER,
    schemeKeyVersion INTEGER,
    creator IA5String,
    recipient IA5String,
    recipientKeySetVersion INTEGER,
    type INTEGER,
    points SEQUENCE (SIZE (3)) OF ECPoint
}

SignedDirectEncryptedPseudonym ::= SEQUENCE {
    notationIdentifier OBJECT IDENTIFIER (id-BSNk-encrypted-direct-pseudonym-signed),
    signedDEP SEQUENCE {
        directEncryptedPseudonym DirectEncryptedPseudonym,
        auditElement OCTET STRING
```

```
    }
    signatureValue EC-Schnorr-Signature
}
```

The fields correspond to the same fields in a Polymorphic Identity or Pseudonym. The recipientKeySetVersion holds the version number for the set of recipient's keys for Identities and Pseudonyms (PD-Di, PC-Di and PI-Di). Note: In schemeVersion 1 the recipientKeySetVersion for DVs is a value of 8 decimal digits corresponding with the issue date (notBefore) of the certificate, in the format YYYYMMDD, used to request the PEM file at the party generating the keys within the scheme.

A DirectEncryptedPseudonym is identitical to an EncryptedPseudonym, although an additonal processing step is needed before decryption. This form is only applicable for reporting from BSNk_registration to CIF.

```
EC-Schnorr-Signature ::= SEQUENCE {
        signatureType      OBJECT IDENTIFIER (ecschnorr-plain-SHA384),
        signatureValue     EC-Sig-Value
}

bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}

id-ecc OBJECT IDENTIFIER ::= { bsi-de algorithms(1) 1 }

ecschnorr-plain-signatures OBJECT IDENTIFIER ::= { id-ecc signatures(4) 3 }

ecschnorr-plain-SHA384 OBJECT IDENTIFIER ::= { ecschnorr-plain-signatures 3 }
```

The auditElement is similar to the auditElement of a Polymorphic Identity or Pseudonym. The signature is a Schnorr signature for efficiency.

```
id-BSNk-encrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 2 }

id-BSNk-encrypted-identity OBJECT IDENTIFIER ::= { id-BSNk-encrypted 1 }

id-BSNk-encrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 2 }

id-BSNk-encrypted-identity-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 3 }

id-BSNk-encrypted-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 4 }

id-BSNk-encrypted-direct-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-encrypted 5 }

id-BSNk-encrypted-direct-pseudonym-signed OBJECT IDENTIFIER ::= { id-BSNk-encrypted 6 }
```

Identity or Pseudonym

Finally, an Encrypted Identity or Pseudonym can be decrypted into a Identity or Pseudonym respectively, consisting of (the X coordinate of) 1 point on an elliptic curve. The Identity or Pseudonym is not directly used in any of the interfaces, but is the RECOMMENDED representation of a Identity or Pseudonym for a relying party to use after decryption of a Encrypted Identity or Pseudonym.

Decrypted pseudoID ASN.1 notation

```
Identity ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-identifier),
    schemeVersion          INTEGER,
    schemeKeyVersion       INTEGER,
    recipient              IA5String,
    type                   INTEGER,
    identityValue          IA5String
}

Pseudonym ::= SEQUENCE {
    notationIdentifier     OBJECT IDENTIFIER (id-BSNk-decrypted-pseudonym),
    schemeVersion          INTEGER,
    schemeKeyVersion       INTEGER,
    recipient              IA5String,
    recipientKeySetVersion INTEGER,
```

```
    diversifier             IA5String,
    type                    INTEGER,
    pseudonymValue          IA5String
}
```

In case of an Identity, the identity can be extracted from the X coordinate of the EllipticCurvePoint of the Identity. In schemeVersion 1, the X coordinate, after conversion from a number to a bytearray, contains an encoded identity padded using OAEP as defined in Section 7.1 of RFC8017 (PKCS#1 v2.2). Here the following parameters are chosen:

- The place of n (RSA modulus) is taken by the order of curve q; length in bytes of q is denoted by k as in PKCS #1, i.e. equal to 40 for the Brainpool320r1 curve used in version 1 of the scheme.
- Hash function is SHA384 truncated to first 10 bytes, i.e. hLen = 10.
- Message length mLen = to k – 2hLen – 2 (PKCS #1 only requires), i.e. equal to 18.
- MGF1 as defined in PKCS #1 is used as Mask Generation Function.
- Optional Label is empty string.

The decoded identity (18 bytes) consists of a prefix of three bytes and the identity (e.g. BSN). The prefix consists of a version, a type and a length of the identifier. All not used bytes are zero. That is, 15 bytes is the longest size supported for an identifier in version 1.

In case of a Pseudonym, the identifying, persistent pseudonym of a user is the EllipticCurvePoint of the Pseudonym. The RECOMMENDED representation of a Pseudonym used in a DV registration, consists of the recipientKeySetVersion (decimal string of length 8) of the closing key with the uncompressed EllipticCurvePoint appended. If two such representations are equal the pseudonyms correspond to the same person. However, we can only deduce that two pseudonyms do not correspond to the same person if the pseudonymValue differ while all other values are equal. We note that the recipientKeySetVersion of the closing key can be different from the recipientKeySetVersions of the EI and EP decryption key.For each decrypted pseudonym the DV shall archive the additional fields decrypted from the Encrypted Pseudonym.

```
id-BSNk-decrypted OBJECT IDENTIFIER ::= { id-BSNk-identifiers 3 }

id-BSNk-decrypted-identifier OBJECT IDENTIFIER ::= { id-BSNk-decrypted 1 }

id-BSNk-decrypted-pseudonym OBJECT IDENTIFIER ::= { id-BSNk-decrypted 2 }
```

Key formats

Polymorphic pseudonimization uses various keys. These keys have been versioned, see the syntax above.

Keys for relying parties are provided using the notation described in DV-key format.

Several of the scheme-wide keys are public, and can be used to use the polymorphism or verify signatures. These keys are defined in Metadata and under the role PPSteutelSet in RoleDescriptors non-Participants. For these public keys the brainpool P320r1 curve is used, which is a named curve defined as

```
-- Brainpool curves and the TeleTrust namespace are defined in BSI TR-03111
ecStdCurvesAndGeneration OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) teletrust(36) algorithm(3)
    signature-algorithm(3) ecSign(2) ecStdCurvesAndGeneration(8)
}

ellipticCurve OBJECT IDENTIFIER ::= { ecStdCurvesAndGeneration 1 }

versionOne OBJECT IDENTIFIER ::= { ellipticCurve 1 }

brainpoolP320r1 OBJECT IDENTIFIER ::= { versionOne 9 }
```

SAML metadata

This chapter describes the metadata the participants must supply, how the Beheerorganisatie publishes the aggregated metadata, and how it is to be interpreted by the participants.

Participants must use SAML metadata in the network to describe the URLs and certificates that are used for the different interfaces. Participants supply metadata and the Beheerorganisatie validates, aggregates and publishes it according to Proces netwerkmetadata.

Moreover, service providers adapting to the standard DV-HM interface specifications, MUST exchange SAML metadata with their supporting HM systems based on specifications describes in this chapter.

- DV metadata for HM — For each service, a Dienstverlener (DV) MUST supply metadata to the HM as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element.
- HM metadata for DV — A Herkenningsmakelaar (HM) MUST supply metadata to the service provider as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element.
- Metadata for participants — A participant MUST supply metadata to the Beheerorganisatie (BO) for every system that implements the role of HM, AD, MR, EB or KR in the network. A participant MUST NOT supply metadata for a role or functionality it has not been assigned.
- Network metadata — The Beheerorganisatie checks the participants' metadata for conformity, deletes the signatures and aggregates the metadata into one file.
- Authorization List BSN format — The Beheerorganisatie BSNk provides the Autorisatielijst BSN containing the OIN's of all organisations authorized to use BSN. Every OIN also accompanied by a name to improve problem solving activities. The Beheerorganisatie BSNk publishes the Autorisatielijst BSN in a location specified in their metadata. The file is available in XML format. Further information about the Autorisatielijst can be found in the BSNk documentation (contact Logius for more information).
- Key provisioning list format — The Beheerorganisatie BSNk provides the Sleutelverstrekkingslijst containing the OIN's of all Service Providers (Dienstverlener) for whom DV-key material has been provided to their Broker (Toegangsdienst). The Sleutelverstrekkingslijst is mainly for transparency reasons (like Certificate Transparency, IETF RFC6962). The Beheerorganisatie BSNk publishes the Sleutelverstrekkingslijst in a fixed location. The file is available in XML format. Further information about the Key Provisioning list forma

DV metadata for HM

For each service, a Dienstverlener (DV) MUST supply metadata to the HM as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element.Signing metadata MUST meet the requirements for signing and encrypting, see Digital signature. For eIDAS-outbound the EB and BRP MUST act in the same way as a Dienstverlener.

Metadata:

This section describes the layout of the metadata. Elements not listed in this table MUST NOT be included in the metadata.

Element/@Attribute	0..n	Description
EntityDesciptor	1	SAML: Required element to start Metadata
@EntityId	1	SAML: MUST contain the EntityID;
@Version	0..1	Elektronische toegangsdiensten: MAY contain an additional version attribute containing the version of the interface specifications on which the entity communicates;
Signature	1	SAML: MUST be included to verify the integrity of the message.
SPSSODescriptor	1	SAML: the SPSSODescriptor implements profiles specific to service providers
@AuthnRequestsSigned	1	Elektronische toegangsdiensten: Must be set to true
@WantsAssertionsSigned	1	Elektronische toegangsdiensten: Must be set to true
@ProtocolSupportEnumeration	1	SAML: Denotes the protocols which can be used. Currently scoped to SAML2.
KeyDescriptor	1..n	SAML: An SPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing" and one or more KeyDescriptor elements with the use XML attribute with the value "encryption". Alternatively, at least one KeyDescriptor without a use XML attribute MAY be included, indicating the default that the key is for both signing and encryption. Every KeyDescriptor element marked for "signing" MUST contain a KeyName element and a valid PKIoverheid certificate with which the service provider its SAML messages and/or direct TLS connections can be authenticated. KeyDescriptors marked for "signing" are also the keys that will be used to specify the attesting Entity through Holder-of-Key-Subjectconfirmation in case of DienstBemiddeling. KeyDescriptors marked for "signing' MUST be valid and comply with the requirements in Secure connection. Every KeyDescriptor element marked for "encryption" MUST contain a KeyName element and a valid PKIoverheid certificate to be used to encrypt IDs and attributes for the DV. Note: HMs must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.
ArtifactResolutionService	1..n	Elektronische toegangsdiensten: The ArtifactResolutionService MUST be implemented at least once per service.
@Binding	1	SAML: The binding parameter denotes the type of binding used. In theArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML artifact resolution endpoint
@Index	1	SAML: The index of the binding, MUST be unique for all ArtifactResolutionService elements
AssertionConsumerService	1..n	SAML: The most common AssertionConsumerService is the HTTP-Artifact service binding. This binding is used by the web interface specifications. See Interface specifications for more information. A Service of a Dienstverlener (Service Provider) MAY be offered using only an endpoint with SOAP binding in the AssertionConsumerService of the SPSSODescriptor. In such a case, the Service MUST only be consumed via Dienstbemiddeling (service intermediation). A Service with both a HTTP (Artifact, GET or POST) and SOAP binding, is accessible directly and using Dienstbemiddeling
@Binding	1	SAML: The binding parameter denotes the type of binding used. This is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML endpoint
@Index	1	SAML: The index of the binding, MUST be unique for all AssertionConsumerService elements.
@isDefault	0..1	If several AssertionConsumerService entries are included, one of these entries MUST be flagged as default by setting the isDefault XML attribute with value "true".

AttributeConsumingService	1..n	A service provider MUST include at least one service AttributeConsumingService element in which the service provider indicates which attributes are requested by default. A Service provider MAY include additional AttributeConsumingService elements containing different sets of attributes it wants to receive for the respective additional services. Multiple AttributeConsumingService elements MAY be present and can be mapped to the same ServiceID. This allows DVs to request authentication for a single service with varying attributes depending on the context. The union of all attributes that may be queried for a ServiceID MUST be declared in the Service Catalog.
@Index	1	The index of the binding, has to be unique for each AttributeConsumingService.
@isDefault	0..1	In case multiple AttributeConsumingServices are defined, the 'isDefault' XML attribute on that AttributeConsumingService element MUST be used to indicate the default service.
ServiceName	1..n	SAML: Name of the service
@lang	0..1	SAML: Localized name of the service, must be in ISO 31661 alpha2 format
RequestedAttribute	1..n	Each AttributeConsumingService MUST contain exactly one attribute with the same name as ServiceID. This ServiceID MUST reference the entry for the Service of the requesting Dienstverlener (Service Provider) in the Service catalog. In case of Dienstbemiddeling (service intermediation) this ServiceID MUST reference the entry for the Service of the Dienstbemiddelaar (service intermediary). The AttributeConsumingService MAY contain one or more RequestedAttributes that are in the Attribuutcatalogus.
@Name	1	The name of the requested attribute. MUST correspond with attributes from Attribuutcatalogus.
@isRequired	0..1	For each requested attribute that is included, the service provider MAY use isRequired to indicate whether the attribute is required for the DV application to work properly. If isRequired is not defined, the default value 'false' is implied.

The XML schema for the DV Metadata is that of the SAML 2.0 Metadata specification (see https://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd). The optional version attribute is identical to the version attribute as defined in the Metadata for participants, to be used on the EntityDescriptor.

Processing Rules for the HM

- The HM MUST validate the metadata provided by the DV.
- The HM MUST validate the Required attributes based on the Attribuutcatalogus.
- The HM MUST validate the metadata based on the SAML specification
- The HM MAY validate the URL Location parameters in the AssertionConsumerService and ArtifactResolutionService.
- After successfull validation the HM MUST use the DV metadata. The HM MUST NOT use self generated metadata when DV metadata is available
- After successfull validation the HM MUST use the supplied DV metadata as input to create a derivative for the Dienstverlener (DV). The HM MAY use additional information as log as it does not overwrite the DV metadata.
- After successfull validation the HM MUST add the PKIoverheid certificate's in the KeyDescriptor element(s) marked for "encryption" into the ServiceCertificate of the corresponding ServiceInstance in the Service catalog . Note: In the case of DV's employing versions 1.9 or lower, the HM MAY add a valid PKIoverheid certificate of it's own (containing the OIN of the HM) for decryption purposes.
- The HM MAY archive this metadata for future use.

Example DV Metadata

```
<md:EntityDescriptor entityID="urn:etoegang:DV:...">
    <ds:Signature>...</ds:Signature>
    <md:SPSSODescriptor ...>
        ...
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Example DV SPSSODescriptor

```
...
<md:SPSSODescriptor AuthnRequestsSigned="true"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

```
    <md:KeyDescriptor>...</md:KeyDescriptor>

    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="0" />
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://..." index="1" isDefault="true"/>
    <md:AssertionConsumerService Binding="urn:etoegang:1.11:binding:native-app" Location="my-app://..." index="
2"/>

    <md:AttributeConsumingService isDefault="true" index="1">
        <md:ServiceName xml:lang="nl">Voorbeeld Dienst 1</md:ServiceName>
        <md:RequestedAttribute Name="urn:etoegang:DV:00000003123456780000:services:0001"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:FirstName"/>
        <md:RequestedAttribute isRequired="true"
            Name="urn:etoegang:attribute:18OrOlder"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:PlaceOfBirth"/>
    </md:AttributeConsumingService>
    <md:AttributeConsumingService isDefault="false" index="2">
        <md:ServiceName xml:lang="nl">Voorbeeld Dienst 50</md:ServiceName>
        <md:RequestedAttribute Name="urn:etoegang:DV:00000003123456780000:services:0050"/>
        <md:RequestedAttribute isRequired="false"
            Name="urn:etoegang:attribute:Gender"/>
        <md:RequestedAttribute isRequired="true"
            Name="urn:etoegang:attribute:DateOfBirth"/>
    </md:AttributeConsumingService>
</md:SPSSODescriptor>
...
```

Example DV KeyDescriptor

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor use="encryption">
        <ds:KeyInfo>
              <ds:KeyName>
acfe784b 391916f1 0aedf8e7 9c503658 c71b437e
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>...
```

HM metadata for DV

A Herkenningsmakelaar (HM) MUST supply metadata to the service provider as a valid SAML file according to urn:oasis:names:tc:SAML:2.0:metadata with one signed EntityDescriptor element.Signing metadata MUST meet the requirements for signing SAML messages described Information security requirements.

Each EntityDescriptor element MUST contain the entityID and an additional version attribute and MUST NOT contain other SAML attributes. The version attribute contains the version of the interface specifications on which the entity communicates.

An IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes.

For eIDAS-outbound the EB and BRP act as a Dienstverlener, so the HM must also provide the same information to them.

Metadata:

This section describes the layout of the metadata. Elements not listed in this table MUST NOT be included in the metadata.

Element/@Attribute	0..n	Description
IDPSSODescriptor	1	Elektronische Toegangsdiensten: A Herkenningsmakelaar MUST include only one IDPSSODescriptor and MUST NOT include any other elements. An IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes.
KeyDescriptor	1..n	SAML: An IDPSSODescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing" and one or more KeyDescriptor elements with the use XML attribute with the value "encryption". Every KeyDescriptor element marked for "signing" MUST contain a KeyName element and a valid PKIoverheid certificate with which the service provider its SAML messages and/or direct TLS connections can be authenticated. KeyDescriptors marked for "signing" are also the keys that will be used to specify the attesting Entity through Holder-of-Key-Subjectconfirmation in case of DienstBemiddeling. KeyDescriptors marked for "signing" MAY contain certificates other than PKIoverheid for authenticating direct TLS connections, as long as such certificates are valid and comply with the requirements in Secure connection. Every KeyDescriptor element marked for "encryption" MUST contain a KeyName element and a valid PKIoverheid certificate to be used to encrypt IDs and attributes for the DV. Note: HMs must process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.
ArtifactResolutionService	1..n	Elektronische toegangsdiensten: The ArtifactResolutionService MUST be implemented at least once per service.
@Binding	1	SAML: The binding parameter denotes the type of binding used. In theArtifactResolutionService this is the SAML-SOAP binding only. The value of this attribute is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML endpoint
@Index	1	SAML: The index of the binding, MUST be unique for all ArtifactResolutionService elements
SingleLogoutService	0..n	Elektronische Toegangsdiensten: MAY be implemented more than once. Describes the endpoint used to log the user out of its current session.
@Binding	1	SAML: The binding parameter denotes the type of binding used. This is an urn relating to: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML endpoint
SingleSignOnService	1..n	Elektronische Toegangsdiensten: MUST contain at least one SingleSignOnService element for which the Binding attribute has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact If the HM offers support for native apps through the OAuth2 protocol, the IDPSSODescriptor from the HM MUST contain one SingleSignonService element with a Binding attribute which has the value 'urn:etoegang:1.11:bindings:native-app', representing the endpoint supporting native apps using the OAuth2 protocol.
@Binding	1	SAML: The binding parameter denotes the type of binding used. This is an urn relating to:http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
@Location	1	SAML: The URL of the SAML endpoint

Processing rules for the DV

- The HM metadata MUST be validated by the DV
- The DV MUST check if the endpoints in the location parameters are available.
- The DV MAY skip validation of SingleSignOnService elements if they are not used
- The DV MUST use the HM metadata if validation succeeds.

Example Herkenningsmakelaar

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="
true">
...
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="0" />
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://...."
/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://...."
/>
    <md:SingleSignOnService Binding="urn:etoegang:1.11:binding:native-app" Location="https://...." />
 </md:IDPSSODescriptor>
...
```

Example

```
...
<md:KeyDescriptor use="signing">
        <ds:KeyInfo>
              <ds:KeyName>
2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
              </ds:KeyName>
              <ds:X509Data>
                  <ds:X509Certificate>
...
                   </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
</md:KeyDescriptor>
...
```

Metadata for participants

A participant MUST supply metadata to the Beheerorganisatie (BO) for every system that implements the role of HM, AD, MR, EB or KR in the network. A participant MUST NOT supply metadata for a role or functionality it has not been assigned.

This requirement is for metadata for the production network. This requirement does not apply to metadata for the test network, because it must also be possible to test the systems of parties that have not yet joined.

A participant that has several roles in the network MUST supply metadata for each role separately.

EntityDescriptor

The participant MUST publish SAML metadata for the Beheerorganisatie complying to the specifications defined for the namespace urn:oasis:names:tc:SAML:2.0:metadata, with one signed EntitiesDescriptor element. Signing metadata MUST meet the requirements for signing, see Digital signature.

The EntitiesDescriptor element MUST contain an attribute Name with a value formatted as urn:etoegang:<scheme version>:<omgeving>:<sequence number>, whereby <scheme version> indicates the version of the framework, <omgeving> the respective environment (P or T), and <sequence number> is a sequence number that distinguishes the different versions of metadata.

The EntitiesDescriptor MAY contain an Extensions element that contains a PublicationInfo element with the URL and creation date of the metadata file.

The EntitiesDescriptor element contains one or more EntityDescriptor elements.

Each EntityDescriptor element MUST contain the EntityID and an additional version attribute, MAY contain a SAML validUntil, EH validFrom, name and ISOname attributes and MUST NOT contain other SAML attributes. The version attribute contains the version of the interface specifications on which the entity communicates. The additional attributes are described below.

The EntityDescriptor MUST contain one or more elements of the type ContactPerson containing an administrative non-personal name, email address, and telephone number that can be contacted by participants or the Beheerorganisatie in the event of an incident. The field 'company' is optional for Contactperson but may be filled in. In case the Contactperson is employed by a different company, the field 'company' of the contactperson MUST be filled in. "The metadata MUST NOT contain personally identifiable information in the sense of the GDPR/AVG.

The metadata MUST contain data about one's own organization by including one element of the type Organization, which describes the name (OrganizationName), the readable name for users (OrganizationDisplayName), and the website (OrganizationURL).

The same role MAY be filled by several systems. Metadata is supplied for each of the systems. The metadata MUST contain a different EntityID in which the Organization element is the same.

urn:etoegang:1.13:metadata-extension

ValidFrom	1	Electronische toegangsdiensten: For communicating a time specific change on an Entity, a participant can use SAML attribute validUntil and Elektronische Toegangsdiensten specific attribute validFrom (see schema below) on the EntityDescriptor. This can for instance be used to facilitate the transition to a new version, replacing certificates, etc...
Version	1	Electronische toegangsdiensten: Denotes the ETD version of an endpoint.
Name	1	Electronische toegangsdiensten: MUST be included if there is more than one SingleSignOnService element defined
ISOName	1	Electronische toegangsdiensten: MAY be implemented to denote the countrycode (formatted according ISO 3166-1 alpha-2 for an endpoint. MAY be used by other configuration elements.

Example Participant EntitiesDescriptor

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
    ID="[reference for dsig]"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:eme="urn:etoegang:1.13:metadata-extension"
    Name="urn:etoegang:1.13:metadata:P:23">

    <ds:Signature>...</ds:Signature>
    <md:Extensions>
        <mdrpi:PublicationInfo publisher="https://.../productie_metadata.xml" creationInstant="2019-04-07T10:39:
03Z"/>
    </md:Extensions>

    <md:EntityDescriptor
        entityID="urn:etoegang:HM:9999990000010000:entities:0001"
        eme:version="1.9"
        eme:validFrom="2019-04-01T0:04:00Z">
```

```
        ...
        <md:Organization>
            ...
        </md:Organization>
        ...
        <md:ContactPerson>
            ...
        </md:ContactPerson>
    </md:EntityDescriptor>

</md:EntitiesDescriptor>
```

Versions

When a system can send messages based on different versions of the framework, metadata MUST be supplied for each version. So, if an entity can communicate on several versions of the interface, both are included in the EntitiesDescriptor as separate EntityDescriptor. These EntityDescriptor elements MAY have the same or different EntityIDs.

An HM MUST include separate EntityDescriptor elements in the metadata for the different logical systems that support the individual versions of the Elektronische Toegangsdiensten interfaces. So, an HM that can communicate on several versions of the interface will include both versions in the metadata as separate EntityDescriptor in the EntitiesDescriptor. These EntityDescriptors MAY have the same or different values for their EntityID attributes.

An AD/KR/MR MUST inspect the values of version in the metadata to determine which EntityDescriptor is to be used to communicate with an HM. Only communication details from the applicable version MUST be used for processing requests and for authentication and securing of communication.

ValidFrom and ValidUntil

For communicating a time specific change on an Entity, a participant can use SAML attribute validUntil and Elektronische Toegangsdiensten specific attribute validFrom (see schema below) on the EntityDescriptor. This can for instance be used to facilitate the transition to a new version, replacing certificates, etc...

An HM MAY have one valid EntityDescriptor per supported version at any given time. If validFrom and/or validUntil are present, an AD/KR/MR MUST only accept requests from an HM using the communication details from a valid EntityDescriptor.

An AD/KR/MR has only one valid EntityDescriptor at a given point in time. An AD/KR/MR MAY provide exactly two different EntityDescriptor elements, one of these EntityDescriptor elements MUST contain a validUntil, the other EntityDescriptor element MUST contain a validFrom. The dateTime value of both fields MUST be the same. These two EntityDescriptors MAY have the same or different EntityIDs. An HM MUST use the validFrom and validUntil in the metadata, if present, to determine which EntityDescriptor is valid for communication with an AD/KR/MR.

Different EntityDescriptor elements for the same role MUST always be contained in a single EntitiesDescriptor element.

See example Example 2 ED - versions and validity.1.13.xml

Level of assurance

An AD or MR MUST include the Level of assurance at which recognition requests can be processed in the EntityDescriptor, in the form of an extension of the EntityDescriptor element as described in the document SAML V2.0 Identity Assurance Profiles.

Example LoA

```
...
    <md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

        <mdattr:EntityAttributes>
            <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oasis:names:
tc:SAML:attribute:assurance-certification">
                <saml:AttributeValue>urn:etoegang:assurance-class:loa3</saml:AttributeValue>
            </saml:Attribute>
        </mdattr:EntityAttributes>

    </md:Extensions>
...
```

Discovery endpoint

An MR MUST include an endpoint which can be used by other MR's for the discovery service as specified on Discovery Interface MR-MR chain authorisations This endpoint is defined as an attribute in the following manner:

Attribute name	Value
Name	urn:etoegang:service:discovery:V1
NameFormat	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
AttributeValue	<URL VALUE OF ENDPOINT>

Example discovery endpoint

```
<md:EntityDescriptor eme:version="1.13" entityID="urn:etoegang:MR:...:entities:...."> 
    <md:Extensions>
        <mdattr:EntityAttributes>
            ...
            <saml:Attribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                    Name="urn:etoegang:service:discovery:V1">
                <saml:AttributeValue>https://example.mr.nl/discoveryEndpoint</saml:AttributeValue>
            </saml:Attribute>
                        ...
        </mdattr:EntityAttributes>
    </md:Extensions>
    ...
</md:EntityDescriptor>
```

RoleDescriptors

AD IDPSSODescriptor

An AD MUST include one IDPSSODescriptor element. The descriptor MUST contain at least one SingleSignOnService element, one SingleLogoutService and at least one ArtifactResolutionService element. The descriptor MUST NOT include any other elements. The first SingleSignOnService MUST indicate it supports the SAML Artifact Binding with the attributes Binding and Location. In case multiple SingleSignOnService elements are present, each MUST have an eme:name attribute, allowing Users to select an applicable endpoint. A SingleSignOnService and SingleLogoutService elements MUST indicate it supports the SAML Artifact binding with the attributes Binding and Location, and MUST NOT contain any other attributes.

AD Example Descriptor

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="
true">
    ...
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="1" />
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://...."
/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://...." eme:name="AD1SAMLendpoint1"/>
    ...
</md:IDPSSODescriptor>
...
```

MR IDPSSODescriptor

A MR MUST include one IDPSSODescriptor element. The descriptor MUST contain at least one SingleSignOnService elements and at least one ArtifactResolutionService element. The descriptor MUST NOT include any other elements. The first SingleSignOnService and SingleLogoutService elements MUST indicate it supports the SAML Artifact binding with the attributes Binding and Location, and MUST NOT contain any other attributes. In case a MR supports chain authorizations, another SingleSignOnService element MUST be present, with the indication it supports the SAML SOAP binding with the attributes Binding and Location, and MUST NOT contain any other attributes. The SingleLogoutService MUST NOT be defined as part of the MR IDPSSODescriptor element.

MR Example Descriptor

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="
```

```
true">
    ...
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="1" />
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://...." eme:name="AD1SAMLendpoint1"/>
    ...
</md:IDPSSODescriptor>
...
```

EB IDPSSODescriptor

The eIDAS-berichtenservice (EB) MUST provide an IDPSSODescriptor in its metadata, identical to one an AD/MR would supply.

HM SPSSODescriptors

An HM MUST include only one IDPSSODescriptor and only one SPSSODescriptor and MUST NOT include any other elements. The IDPSSODescriptor from the HM MAY contain several SingleSignOnService and SingleLogoutService elements and MUST contain at least one SingleSignOnService and one SingleLogoutService element for which the Binding attribute has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact. The SPSSODescriptor from the HM MUST contain two AssertionConsumerService elements with a Binding attribute which has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact, and with indices 1 and 2 for responses from ADs and MRs, MUST contain at least one ArtifactResolutionService element with the SOAP binding and MAY NOT contain any other elements.

If the HM offers support for eIDAS, the the SPSSODescriptor from the HM MUST contain one (extra) AssertionConsumerService element with a Binding attribute which has the value urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact, and with index 5.

Example HM descriptor

```
...
<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="
true">
    ...
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="1" />
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://...."
/>
    ...
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://...."
/>
        ...
</md:IDPSSODescriptor>
<md:SPSSODescriptor AuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
>
    ...
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://..."
index="1" />
    ...
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://..." index="1"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="
https://..." index="2"/>
 </md:SPSSODescriptor>
...
```

BSNk

BSNk fulfills two roles within the Netwerk (voor Elektronische Toegangsdiensten):

- The role of Sleutelbeheerder (SB).
- The role of cryptographic service provider.

The BSNk is a special participant as the Beheerorganisatie (BO) uses the metadata published (and as specified) by the BSNk (Link will follow)

Example metadata BSNk

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
```

```
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:
2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor>
            <ds:KeyInfo>
                <!--  PIP/PP/PI public signing key U for BSNk-activate in test network -->
                <ds:KeyName>urn:nl-gdi-eid:pp-key:test:1:U:1</ds:KeyName>
                <ds:KeyValue>
                    <ds11:ECKeyValue>
                        <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                        <ds11:PublicKey>Mwo=...</ds11:PublicKey>
                    </ds11:ECKeyValue>
                </ds:KeyValue>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:BSN</md:NameIDFormat>
        <md:SingleSignOnService Location="https://bsnk.exmaple.nl/kr/activate" Binding="http://schemas.xmlsoap.
org/soap/http" />
        <md:NameIDMappingService Location="https://bsnk.exmaple.nl/kr/tranform" Binding="http://schemas.xmlsoap.
org/soap/http" />
    </md:IDPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld BSNk</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld BSNk</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://bsnk.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:SurName>BSNk koppelregister</md:SurName>
        <md:EmailAddress>koppelregister@bsnk.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

The BSNk as Key Management Authority MUST publish its details as an SPSSODescriptor. The AssertionConsumerEndpoint element MUST contain the endpoint for obtaining Dienstverlener keys (AUC10 Verstrekken sleutelmateriaal Dienstverleners).

The EntityDescriptor of the Sleutelbeheerder MUST contain an AdditionalMetadataLocation element, containing the location where the Autorisatielijst BSN can be obtained.

Example SleutelBeheer EntityDescriptor

```
<md:EntityDescriptor entityID="urn:nl-gdi-eid:entity:99999999012345670000"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">

    <md:SPSSODescriptor WantAssertionsSigned="true" AuthnRequestsSigned="true" protocolSupportEnumeration="urn:
oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
```

```
        <md:NameIDFormat>urn:nl-gdi-eid:1.0:id:Pseudonym</md:NameIDFormat>
        <md:AssertionConsumerService Location="https://bsnk.example.nl/keymgmt/dv/key-request" index="1"
isDefault="true" Binding="http://schemas.xmlsoap.org/soap/http" />
    </md:SPSSODescriptor>
    <md:Organization>
        <md:OrganizationName xml:lang="nl">Voorbeeld BSNk</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="nl">Voorbeeld BSNk</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="nl">https://bsnk.example.nl/</md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="technical">
        <md:SurName>BSNk sleutelbeheer</md:SurName>
        <md:EmailAddress>sleutelbeheer@bsnk.example.nl</md:EmailAddress>
        <md:TelephoneNumber>+31-10-1234567</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

WantAuthnRequestsSigned

An IDPSSODescriptor element MUST contain the WantAuthnRequestsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes. An SPSSODescriptor element MUST contain the AuthnRequestsSigned XML attribute with value "true" and a WantAssertionsSigned XML attribute with value "true" and MUST NOT contain any other optional attributes.

NameIDFormat

An IDPSSODescriptor element MUST contain one or more NameIDFormat XML attribute(s), containing the Identificerende kenmerken (EntityConcernedTypes) the participant supports. A SPSSODescriptor of a Participant (as used by HM) MUST NOT contain a NameIDFormat.

The following NameIDFormats should be included per role, if certified for the applicable domain (and conditions):

Role	Application domain	Additional condition	include NameIDFormat
HM	*Citizen domain	eHerkenning branding	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.12:EntityConcernedID:BSN
	Consumer domain	eHerkenning branding	urn:etoegang:1.9:EntityConcernedID:Pseudo urn:etoegang:1.12:EntityConcernedID:PseudoID
	Business domain	eHerkenning branding	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr
AD	Consumer domain	eHerkenning branding	urn:etoegang:1.9:EntityConcernedID:Pseudo urn:etoegang:1.12:EntityConcernedID:PseudoID
	Business domain	eHerkenning branding	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr
MR	Business domain	eHerkenning branding; KvKnr supported	urn:etoegang:1.9:EntityConcernedID:KvKnr
		eHerkenning branding; RSIN nummer supported	urn:etoegang:1.9:EntityConcernedID:RSIN
		eHerkenning branding; PROBASnr supported	urn:etoegang:1.13:EntityConcernedID:PROBASnr
		eHerkenning branding; KvKnr + chain authorization supported	urn:etoegang:1.9:IntermediateEntityID:KvKnr
		eHerkenning branding; RSIN nummer chain authorization supported	urn:etoegang:1.9:IntermediateEntityID:RSIN
EB	*Citizen domain	eHerkenning branding	urn:etoegang:1.12:EntityConcernedID:BSN urn:etoegang:1.12:EntityConcernedID:PseudoID
	Consumer domain	eHerkenning branding	urn:etoegang:1.9:EntityConcernedID:Pseudo
	Business domain	eHerkenning branding	urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier

*Citizen domein: only voor EU Citizens

Example NameIDFormat

```
...
<md:IDPSSODescriptor>
    ...
```

```
        <md:NameIDFormat>urn:etoegang:1.9:EntityConcernedID:KvKnr</md:NameIDFormat>
        <md:NameIDFormat>urn:etoegang:1.9:EntityConcernedID:Pseudo</md:NameIDFormat>
    ...
</md:IDPSSODescriptor>
...
```

KeyDescriptor

An IDPSSODescriptor, SPSSODescriptor or AttributeAuthorityDescriptor element MUST contain one or more KeyDescriptor elements with the use XML attribute with value "signing". The IDPSSODescriptor of a MR or the AttributeAuthorityDescriptor of a KR MUST contain at least one or more KeyDescriptor with the use XML attribute with value "encryption". Alternatively, at least one KeyDescriptor without a use XML attribute MAY be included, indicating the default that the key is for both signing and encryption. Every KeyDescriptor element marked for "signing" MUST contain a KeyName element and a valid PKIoverheid certificate with which the participant's SAML messages and/or direct TLS connections can be authenticated. KeyDescriptors marked for "signing" MAY contain valid certificates for authenticating direct TLS connections that are not PKIoverheid, as long as they comply with the requirements in Secure connection. Every KeyDescriptor element marked for "encryption" MUST contain a KeyName element and a valid PKIoverheid certificate for encrypting IDs and attributes for that participant.

In case a role is a source or recipient for Polymorphic Pseudonyms (or Polymorphic Identities), this roles has one or more PP-scheme specific keys. These keys are versioned, to allow for key-management.

A role MAY have one or more versions of PP-KeySet in use. In case no version is specified, the default value "1" is to be used as keyset version. In case multiple KeySetVersions are listed, one MUST be marked as"default".

Additional KeyDescriptor elements without specificied "use" attribute MAY be included, to describe (derived) keys used in the Polymorphic Pseudonymzation algorithm. These KeyDescriptor MUST contain a KeyInfo element, with a KeyName element using 'urn:nl-gdi-eid:1.0:pp-key:<Environment>:<SchemeKeySetVersion>:<KeyName>:<KeyVersion>' to describe the key. In case of public keys, these MUST be included as KeyValue element using a ECKeyValue and a NamedCurve with PublicKey (NOTE: ECKeyValue is specified in XML-signature 1.1). In case of derived keys, other elements MUST NOT be included.

> **Note**
>
> Service providers and participants MUST process all of the described KeyDescriptor elements. KeyName in the signatures and protocol messages indicates which certificate in the metadata is used for the signature.

Example KeyDescriptor

```
...
<md:KeyDescriptor>
    <ds:KeyInfo>
        <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:test:1:AA_D99999999012345670000:1</ds:KeyName>
    </ds:KeyInfo>
</md:KeyDescriptor>
<md:KeyDescriptor>
    <ds:KeyInfo>
        <!-- PIP/PP/PI public signing key for BSNk-activate in test network -->
        <ds:KeyName>urn:nl-gdi-eid:1.0:pp-key:test:1:U:1</ds:KeyName>
            <ds:KeyValue>
            <ds11:ECKeyValue>
                <!-- brainpool P320r1 curve -->
                <ds11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.9"/>
                <ds11:PublicKey>
                   MQo=...
                </ds11:PublicKey>
            </ds11:ECKeyValue>
        </ds:KeyValue>
    </ds:KeyInfo>
</md:KeyDescriptor>
...
```

To request an identifier from the preceding version 1.11 of the Afsprakenstelsel for migration purposes, the MR MAY request a DeprecatedActingSubjectID. To receive encrypted pseudonyms based on earlier OINs or recipientkeysetversions, the MR MAY include a DeprecatedRelyingPartyID with a DeprecatedEntityID and DeprecatedRecipientKeysetVersion. To indicate whether to receive an internal pseudonym or persistent pseudonym, the MR MUST supply a UserTypeRequested in the metadata: InternalPseudonym for the internal pseudonym, PseudoID for the Encrypted Pseudonym.

See examples: Example 3 - example metadata extension.xml and XML schema metadata extension.1.13.xsd

Network metadata

The Beheerorganisatie checks the participants' metadata for conformity, deletes the signatures and aggregates the metadata into one file.The aggregated metadata consists of a signed EntitiesDecriptor element with an cacheDuration XML attribute with value "P7D" and an Name XML attribute with a value formatted as **urn:etoegang:*VERSIEAS*:metadata:*OMGEVING*:*VOLGNUMMER***, whereby *VERSIEAS* indicates the version of the framework, *OMGEVING* the respective environment (P or A), and *VOLGNUMMER* is a sequence number that distinguishes the different versions of metadata. The signature MUST meet the requirements described in Information security requirements.

The EntitiesDescriptor element contains 5 EntitiesDescriptor elements with the names Authenticatiediensten, Machtigingenregisters, Koppelregisters, Inters telseldiensten and Herkenningsmakelaars (prefixed with 'urn:etoegang:role:') that contain the metadata from the participants in the different roles. Under the role "Interstelseldiensten" the eIDAS-berichtenservice is listed, HMs MUST treat this as if it were both an AD and MR. That is, in message validation it can regard it as an AD/MR depending on context. However for services classified as 'eIDAS-inbound' it MUST NOT list it as an AD for AD-selection by the user (instead, the DV must list this as a separate authentication option, not the HM). Furthermore, it MUST send requests as per Interface specifications HM-EB.

The EntitiesDescriptor element can also contain an additional Dienstverleners (service providers) element that contains fictitious service providers. Each Herkenningsmakelaar MUST process the named service providers. These service providers are named in the service catalogue and can be used by the Beheerorganisatie and for testing.

The EntitiesDescriptor element also contains an Extensions element that contains a PublicationInfo element with the URL and creation date of the metadata file, which MUST be filled by the Beheerorganisatie.

The Beheerorganisatie publishes the metadata in a fixed location. In order to maintain the privacy of the contacts' details in the metadata, the location is a non-indexed URL with server-side SSL that can only be shared with the participants.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntitiesDescriptor
    ID="[reference for dsig]"
    Name="urn:etoegang:1.13:metadata:P:36"
    cacheDuration="P7D"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <ds:Signature>...</ds:Signature>

    <md:Extensions>
            <mdrpi:PublicationInfo publisher="https://.../productie_metadata.xml" creationInstant="2019-05-
07T10:39:03Z"/>
        </md:Extensions>

    <md:EntitiesDescriptor Name="urn:etoegang:role:Authenticatiediensten">
        ...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="urn:etoegang:role:Machtigingenregisters">
        ...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="urn:etoegang:role:Koppelregisters">
        ...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="urn:etoegang:role:Herkenningsmakelaars">
        ...
    </md:EntitiesDescriptor>
    <md:EntitiesDescriptor Name="urn:etoegang:role:Interstelseldiensten">
       ...
    </md:EntitiesDescriptor>
</md:EntitiesDescriptor>
```

A participant MUST process the metadata periodically at a time that is predefined by the Beheerorganisatie. Data about the URL and the periodicity are described in Proces netwerkmetadata.

A participant MUST use an automated process to process the metadata that finishes in 15 minutes. A participant MUST be able to start this automated process (e.g., manually) between the predefined periods in agreement with the Beheerorganisatie to accommodate a rollback or other changes.

Authorization List BSN format

The Beheerorganisatie BSNk provides the Autorisatielijst BSN containing the OIN's of all organisations authorized to use BSN. Every OIN also accompanied by a name to improve problem solving activities. The Beheerorganisatie BSNk publishes the Autorisatielijst BSN in a location specified in their metadata. The file is available in XML format. Further information about the Autorisatielijst can be found in the BSNk documentation (contact Logius for more information).

Key provisioning list format

The Beheerorganisatie BSNk provides the Sleutelverstrekkingslijst containing the OIN's of all Service Providers (Dienstverlener) for whom DV-key material has been provided to their Broker (Toegangsdienst). The Sleutelverstrekkingslijst is mainly for transparency reasons (like Certificate Transparency, IETF RFC6962). The Beheerorganisatie BSNk publishes the Sleutelverstrekkingslijst in a fixed location. The file is available in XML format. Further information about the Key Provisioning list format can be found in the BSNk documentation (Contact Logius for more information).

Service catalog

This chapter describes the format and publication of the Dienstencatalogus (DC) (service catalog).

The Service catalog holds the information of services offered by Dienstverleners (service providers). A DV can own one or more Service Definitions and one or more Service Instances:

- A Service Definition has the elements to describe the functionality of the Service.
- A Service Instance has the technical details for an implementation of the Service as operated by the Dienstverlener (DV).

In case of Dienstbemiddeling (Service Intermediation): The Service Instance of the Dienstbemiddelaar (DB) (Service Intermediary) references the Service Instance of the Dienstaanbieder (DA) (service supplier) by ServiceUUID, using the IntermediatedService.

Format

The service catalog MUST have the following format:

- IssueInstant (time at which the service catalog was created)
- Version (version of the service catalog in the format urn:etoegang:<scheme version>:service-catalogue:<omgeving>:<sequence number>. Example: urn:etoegang:1.11:service-catalogue:T:1
- Signature (signature from the Beheerorganisatie (BO), Herkenningsmakelaar (HM) or Dienstverlener (DV) for authenticity, integrity and non-repudiation).
- Per Dienstverlener:
    - IsPublic (attribute that indicates whether the service provider is in public)
    - ServiceProviderID (The service provider's OIN (government ID number)
    - OrganizationDisplayName (the name of the service provider as it MUST be displayed by participants, max 64 characters).
    - Per ServiceDefinition:
        - IsPublic (attribute that indicates whether the service is using eHerkenning in public)
        - ServiceUUID (a universally unique identifier that is used for registering entitlements. It is possible the same UUID is shared between multiple service providers, in that case they will use the same entitlement)
        - ServiceName (name of the service determined by the service provider, max 64 characters).
        - ServiceDescription (short description of the service determined by the service provider, max 1024 characters. MRs MAY use this text to help administrators determine the authorizations).
        - ServiceDescriptionURL (a URL of max 512 characters where a detailed description of the service can be found, determined by the service provider. MRs MAY include this link to help administrators determine the authorizations).
        - AuthnContextClassRef (assurance level that is required for the service, determined by the service provider)
        - HerkenningsmakelaarId (the OIN of the Herkenningsmakelaar (HM) that provides the service catalog entry for this service definition)
        - EntityConcernedTypesAllowed (multivalue entry with the different types of service consumers that are granted access to the service). In case multiple EntityConcernedTypes are defined, they are assigned to Identifier sets (for more information on identifier sets, see below).
        - ActingSubjectTypesAllowed (multivalue entry with the different types of acting subjects that are granted access to the service). In case multiple ActingSubjectTypes are defined, they are assigned to Identifier sets
            - Allowed ActingSubjectTypes are:
                - urn:etoegang:1.12:EntityConcernedID:PseudoID
                - urn:etoegang:1.12:EntityConcernedID:BSN
                - urn:etoegang:1.13:EntityConcernedID:Pseudo (is always included by default and MUST NOT be specified in the ActingSubjectTypesAllowed identifier set)

                
                If the AD cannot deliver the ASTA, the AD will throw an error, see Interface specifications HM-AD

        - EntityConcernedTypesAllowed and ActingSubjectTypesAllowed are split in their own lists and MUST be processed accordingly.

            - The AD MUST process the ActingSubjectTypesAllowed list AND the EntityConcernedID:Pseudo
            - the MR and EB (in case of inbound authentication requests) MUST process the EntityConcernedTypesAllowed list

        - Both EntityConcernedTypesAllowed and ActingSubjectTypesAllowed are grouped in separate Identifier Sets. An identifier set is a cluster of identifier Types with the same set number.
            - Identifier Set MUST adhere to the following rule:
                - Identifiers MAY be used in multiple identifier sets

                
                An SP may request multiple EntityConcernedTypes in an identifier set. The SP may also indicate to honor restrictions. When an Attribute with a ServiceRestriction is included in the AttributeStatement, users can access the service under the restrictions as specified for that type of restriction. Currently, the only restrictions supported are ServiceRestriction:Vestigingsnr and ServiceRestriction:SubdossierNr (deprecated). The ServiceRestriction:Vestigingsnr CAN be indicated in the Service catalog, in such case both the ServiceRestriction:Vestigingsnr and ServiceRestriction:SubdossierNr will be returned, if applicable.

                - Identifier sets either only contain ASTA's or ECTA's

> The ASTA's MUST NOT be requested by DV's, ONLY the EB and BRP MAY request ASTA's

- ServiceRestrictionsAllowed (multivalue entry with the different types of service restrictions the service provider can honor).
- RequestedAttribute (multivalue entry with all the attributes that may be requested for this service)
  - PurposeStatement (a statement by the service provider why this attribute is requested, 1024 characters).
  - isRequired: For each requested attribute that is included, the service provider MAY use isRequired to indicate whether the attribute is required for the DV application to work properly. If isRequired is not defined, the default value 'false' is implied.

- Per ServiceInstance:
  - IsPublic (attribute that indicates whether the service provider is in public)
  - ServiceID (an identifier of a service instance that is unique in the context of the service provider)

    > If the DV provides a portal function, it MUST be specified in the service catalog with a reserved index number 0.

  - BsnkStructureVersion - Optional: This element is required when the ECTA or ASTA has a BSN or PseudoID, otherwise it MUST NOT be used. Value must be a valid BsnkStructureVersion (see BSNk confluence "1" or "2"). If no version is used, or if the BsnkStructureVersion is invalid, version 1 MUST be used.
  - BsnkRecipientKeySetVersion - Optional: This element is required when the ECTA set or ASTA set contains a BSN or PseudoID, otherwise it MUST NOT be used. Value must be identical to the RKSV as noted on the BSNk keys the ServiceProvider is using voor decrypting the BSN or PseudoID.

    > The old way of getting the recipientKeySetVersion (by retrieving this from the most recent certificate) MUST NOT be used after 1-1-2021.

  - ServiceUUID (a universally unique identifier to allow identifying and referencing this instance)
  - InstanceOfService (a reference to a ServiceUUID of a Service definition being implemented. An InstanceOfService MUST be present).
  - IntermediatedService (a reference to a ServiceUUID of a Service instance in case Dienstbemiddeling (Note: Service Intermediation only available for eIDAS outbound) applies. An intermediating service MUST NOT reference a service instance that applies Dienstbemiddeling. The intermediated Service MAY have the same InstanceOfService and therefore only require one mandate).
  - ServiceURL (optional URL of max 512 characters where the service can be found).
  - PrivacyPolicyURL (a URL of max 512 characters where the privacy policy for this service can be found). Optional for Dienstbemiddeling services.
  - HerkenningsmakelaarId (the OIN of the Herkenningsmakelaar (HM) that provides the service catalog entry for this service instance)
  - AdditionalHerkenningsmakelaarId (multivalue entry with the OINs for the other HMs that provide this service)
  - SSOSupport (a boolean that indicates if the service supports SingleSignOn)
  - ServiceCertificate (Service provider's PKI certificate with a public key that can be used to encrypt requested attributes and IDs). This certificate MUST be a valid PKIoverheid certificate. Note that multiple certificates may be provided for cases like changing certificates. (Additonally: Signing certificates must NOT be used here but should be placed in the DV metadata for HM).
  - ServiceIntermediation (indication if intermediation of the service (Dienstbemiddeling) requires approval of the Service Provider, see AUC7 Proces verlenen toestemming dienstbemiddeling)
    - @intermediationAllowed (attribute indicating approval is required; possible values "noIntermediation" (default), "generalAvailable", "serviceProviderOnly", "requiresApproval")
    - ServiceIntermediationAllowed (optional, holds one or more OINs of any Dienstbemiddelaar allowed to intermediate a service if @intermediationAllowed has the value "requiresApproval").
  - Classifiers (optional, multivalued entry that allows for one or more classifications of a ServiceInstance)
    - Classifier (value indicating a particular classification applied for this SerivceInstance)
      The following classifiers are defined:

Classifier	Description	Usage restrictions
PublicDomain	The ServiceInstance is operated by the Dienstverlener (Service Provider) to implement a service under a responsibility in the public domain.	The Dienstverlener MUST operate under "Artikel 1:1 Algemene Wet Bestuursrecht". Although a service in the public domain will typically request an urn:etoegang:1.12 or EntityConcernedID:RSIN, this is not mandatory. Other identifiers may be used by services classified as PublicDomain as well. Service requesting aforementioned identifiers typically do operate as a PublicDomain service. In case the ServiceInstance is classified as 'eIDAS-outbound' as well, the actual DV in another member state operates under an equivalent legislation and are requested as such via the eIDAS interoperability framework (eIDAS: SPType 'public').
eIDAS-inbound	The service is an eTD-service that is receptive to	Services that want to accept authentication and authorization through eIDAS MUST be classified as 'eIDAS-inbound'. Currently the eIDAS-

	users from other eIDAS-member states.	berichtenservice only accepts messages in the public domain. Therefore a service must use BOTH classifiers 'eIDAS-inbound' AND 'PublicDomain' combined to connect effectively to eIDAS.
eIDAS-outbound	The service is a proxy for services in other member states under the eIDAS regulation.	The eIDAS-berichtenservice has proxy-services listed in the Service Catalog for services in other eIDAS-member states that may be accessed through eIDAS. These proxy services MUST be classified as 'eIDAS-outbound'.

The elements OrganizationDisplayName, ServiceName, ServiceDescription, ServiceDescriptionURL, PurposeStatement, ServiceURL and PrivacyPolicyURL MAY be included for different languages.

Note: At this moment the use of ASTA-sets and Service Intermediarion is limited to the EB for eIDAS Outgoing.

Any ServiceProvider interested in ServiceIntermediation or ASTA-sets should contact their HM for the proper procedure.

Any changes in ServiceIntermediation elements in the ServiceCatalog will not be propagated automatically.

Rules for processing Service Catalog

- All ServiceUUIDs MUST be both global and temporal unique. The Beheerorganisatie MUST verify all UUIDs that are used are defined only once. Significant changes to a Service SHOULD result in a new distinct ServiceUUID. ServiceDefinitions with the same ServiceUUID are exempt from global uniqueness, these are shared services and MUST be identical (identical but excluding @IsPublic and HerkenningsmakelaarId).
- Herkenningsmakelaar passes on the ServiceUUID of the ServiceInstance matching the requested combination of Dienstverlener-AttributeConsumingServiceIndex, or whatever other mechanic used in the bilateral DV-HM interface, in further authentication and attribute requests.
- A receiving AD/MR/BSNk inspects the Service Catalogue to determine the exact authorization demands and relying parties for the requested ServiceInstance based upon the ServiceUUID. The following logic applies:
  - The ServiceUUID of the referenced ServiceDefinition is always used to determine the mandate/authorization demands.
  - The requested ServiceInstance always determine the relying entity (or entities) for the authorization request.
  - In case of service intermediation: a service instance references a service instance (rather than a service definition) via the IntermediatedService element.
  - In case of service intermediation: the service instance pointed to is considered the true relying party; the requesting party is merely an acceptable attesting entity (only to be included in subjectconfirmation HoK).
- Participants MUST check the validity of the Service Certificate when using any attributes in the certficate.
- In case of service intermediation; the approval verification MUST be based on the ServiceIntermediation element belonging to the referenced service instance. The following rules apply:

@intermediationAllowed	Processing rule
noIntermediation	Participants MUST NOT allow service intermediation for the Service (default)
generalAvailable	Participants MUST allow service intermediation by any dienstverlener listed in the Service Catalog as service intermediary for the Service
serviceProviderOnly	Participants MUST only allow the Service Provider itself to perform service intermediation (*Dienstbemiddelaar* = *Dienstaanbieder*)
requiresApproval	Participants MUST allow only those Service Intermediaries that have their OIN listed under ServiceIntermediationAllowed to perform service intermediation for the Service

Make sure to look at the rule relating to the use of BSN and minimal level of assurance mentioned in Betrouwbaarheidsniveaus

The XML schema of the Service Catalog below is currently not correct. Use it only as example.
A new initiative was started to automatically validate various XML-schemas, which always uses up-to-date XML-schemas.

XML schema Service Catalog

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Schema for AS_1.14 Release
    $Date: 2020-09-07
    $Author:rahulkumar.gupta@kpn.com
-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
```

```
    xmlns:esc="urn:etoegang:1.13:service-catalog"
    targetNamespace="urn:etoegang:1.13:service-catalog"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR/xmldsig-core
/xmldsig-core-schema.xsd"/>
    <xs:import namespace="urn:oasis:names:tc:SAML:2.0:assertion" schemaLocation="http://docs.oasis-open.org
/security/saml/v2.0/saml-schema-assertion-2.0.xsd"/>
    <xs:import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="http://docs.oasis-open.org
/security/saml/v2.0/saml-schema-metadata-2.0.xsd"/>

    <!--Elements-->
    <xs:element name="ServiceDefinition" type="esc:ServiceDefinitionType" />
    <xs:complexType name="ServiceDefinitionType">
        <xs:sequence>
            <xs:element ref="esc:ServiceUUID" />
            <xs:element ref="esc:ServiceName" maxOccurs="unbounded"/>
            <xs:element ref="esc:ServiceDescription" maxOccurs="unbounded"/>
            <xs:element ref="esc:ServiceDescriptionURL" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="saml2:AuthnContextClassRef"/>
            <xs:element ref="esc:HerkenningsmakelaarId"/>
            <xs:element ref="esc:EntityConcernedTypesAllowed" minOccurs="1" maxOccurs="unbounded"/>
            <xs:element ref="esc:ActingSubjectTypesAllowed" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:ServiceRestrictionsAllowed" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:RequestedAttribute" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute ref="esc:IsPublic" use="required"/>
    </xs:complexType>
    <xs:element name="ServiceInstance" type="esc:ServiceInstanceType" />
    <xs:complexType name="ServiceInstanceType">
        <xs:sequence>
            <xs:element ref="esc:ServiceID" minOccurs="1"/>
            <xs:element ref="esc:ServiceUUID" />
            <xs:element ref="esc:InstanceOfService" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="esc:IntermediatedService" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="esc:ServiceURL" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:PrivacyPolicyURL" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:HerkenningsmakelaarId"/>
            <xs:element ref="esc:AdditionalHerkenningsmakelaarId" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="SSOSupport" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
            <xs:element ref="esc:EntityConcernedTypesAllowed" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:ServiceCertificate" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element ref="esc:ServiceIntermediation" minOccurs="0" />
            <xs:element ref="esc:Classifiers" minOccurs="0" />
            <xs:element ref="esc:BsnkStructureVersion" minOccurs="0"/>
            <xs:element ref="esc:BsnkRecipientKeySetVersion" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute ref="esc:IsPublic" use="required"/>
    </xs:complexType>

    <xs:element name="ServiceCatalogue">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ds:Signature"/>
                <xs:element ref="esc:ServiceProvider" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute ref="esc:IssueInstant" use="required"/>
            <xs:attribute ref="esc:Version" use="required"/>
            <xs:attribute name="ID" type="xs:string"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="EntityConcernedTypesAllowed">
        <xs:complexType>
            <xs:simpleContent>
                <xs:extension base="xs:anyURI">
                    <xs:attribute name="setNumber" type="xs:nonNegativeInteger" use="optional"/>
                </xs:extension>
            </xs:simpleContent>
        </xs:complexType>
    </xs:element>
```

```
  <xs:element name="ActingSubjectTypesAllowed">
  <xs:complexType>
    <xs:simpleContent>
     <xs:extension base="xs:anyURI">
                 <xs:attribute name="setNumber" type="xs:nonNegativeInteger" use="optional"/>
     </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
  <xs:element name="ServiceRestrictionsAllowed">
      <xs:complexType>
          <xs:simpleContent>
              <xs:extension base="xs:anyURI"/>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="ServiceDescription">
      <xs:complexType>
          <xs:simpleContent>
              <xs:restriction base="md:localizedNameType">
                  <xs:maxLength value="1024"/>
              </xs:restriction>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="ServiceDescriptionURL">
      <xs:complexType>
          <xs:simpleContent>
              <xs:restriction base="md:localizedURIType">
                  <xs:maxLength value="512"/>
              </xs:restriction>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="ServiceURL">
      <xs:complexType>
          <xs:simpleContent>
              <xs:restriction base="md:localizedURIType">
                  <xs:maxLength value="512"/>
              </xs:restriction>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="PrivacyPolicyURL">
      <xs:complexType>
          <xs:simpleContent>
              <xs:restriction base="md:localizedURIType">
                  <xs:maxLength value="512"/>
              </xs:restriction>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="ServiceID" type="xs:anyURI"/>
  <xs:element name="ServiceUUID" type="xs:string"/>
<xs:element name="BsnkStructureVersion" type="xs:string"/>
<xs:element name="BsnkRecipientKeySetVersion" type="xs:string"/>
  <xs:element name="ServiceName">
      <xs:complexType>
          <xs:simpleContent>
              <xs:restriction base="md:localizedNameType">
                  <xs:maxLength value="64"/>
              </xs:restriction>
          </xs:simpleContent>
      </xs:complexType>
  </xs:element>
  <xs:element name="ServiceProvider">
      <xs:complexType>
          <xs:sequence>
              <xs:element ref="esc:ServiceProviderID"/>
              <xs:element ref="esc:OrganizationDisplayName" maxOccurs="unbounded"/>
              <xs:element ref="esc:ServiceDefinition" minOccurs="0" maxOccurs="unbounded"/>
```

```
                <xs:element ref="esc:ServiceInstance" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute ref="esc:IsPublic" use="required"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="ServiceProviderID" type="esc:OINType"/>
    <xs:element name="RequestedAttribute" type="esc:RequestedAttributeType" />
    <xs:complexType name="RequestedAttributeType">
        <xs:complexContent>
            <xs:extension base="md:RequestedAttributeType">
                <xs:sequence>
                    <xs:element ref="esc:PurposeStatement" maxOccurs="unbounded"/>
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:element name="PurposeStatement" type="esc:PurposeStatementType"/>
    <xs:complexType name="PurposeStatementType">
        <xs:simpleContent>
            <xs:restriction base="md:localizedNameType">
                <xs:maxLength value="1024" />
            </xs:restriction>
        </xs:simpleContent>
    </xs:complexType>
    <xs:element name="ServiceCertificate">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="md:KeyDescriptor"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="HerkenningsmakelaarId" type="esc:OINType"/>
    <xs:element name="AdditionalHerkenningsmakelaarId" type="esc:OINType"/>
    <xs:element name="OrganizationDisplayName">
        <xs:complexType>
            <xs:simpleContent>
                <xs:restriction base="md:localizedNameType">
                    <xs:maxLength value="64"/>
                </xs:restriction>
            </xs:simpleContent>
        </xs:complexType>
    </xs:element>
    <xs:element name="InstanceOfService" type="xs:string"/>
    <xs:element name="IntermediatedService" type="xs:string"/>
    <xs:element name="ServiceIntermediation">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="esc:ServiceIntermediationAllowed" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="intermediationAllowed" type="esc:IntermediationAllowedType" default="
noIntermediation"/>
        </xs:complexType>
    </xs:element>
    <xs:simpleType name="IntermediationAllowedType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="noIntermediation"/>
            <xs:enumeration value="generalAvailable"/>
            <xs:enumeration value="serviceProviderOnly"/>
            <xs:enumeration value="requiresApproval"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:element name="ServiceIntermediationAllowed" type="esc:OINType"/>
    <xs:simpleType name="OINType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-9]{20}"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:element name="Classifiers" type="esc:ClassifiersType" />
    <xs:complexType name="ClassifiersType">
        <xs:sequence>
            <xs:element name="Classifier" type="xs:string" maxOccurs="unbounded"/>
```

```
        </xs:sequence>
    </xs:complexType>

    <!--Attributes-->
    <xs:attribute name="IssueInstant" type="xs:dateTime"/>
    <xs:attribute name="IsPublic" type="xs:boolean"/>
    <xs:attribute name="Version" type="xs:anyURI"/>

</xs:schema>
```

Example Service Catalog with one service

```
<?xml version="1.0" encoding="UTF-8"?>
<esc:ServiceCatalogue xmlns:esc="urn:etoegang:1.11:service-catalog" xmlns:md="urn:oasis:names:tc:SAML:2.0:
metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" esc:
IssueInstant="2015-12-28T10:19:57Z" esc:Version="urn:etoegang:1.11:service-catalogue:P:506" ID="_dc">

  <ds:Signature>...</ds:Signature>

  <esc:ServiceProvider esc:IsPublic="true">
    <esc:ServiceProviderID>99999999000000000099</esc:ServiceProviderID>
    <esc:OrganizationDisplayName xml:lang="nl">Voorbeeld DV</esc:OrganizationDisplayName>
    <esc:OrganizationDisplayName xml:lang="en">Example SP</esc:OrganizationDisplayName>

    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>6bae98e3-5ef9-4576-98c8-5aba4b8e672d</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (attributen LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (attributes LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:Pseudo</esc:
EntityConcernedTypesAllowed>
      <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" isRequired="false">
        <esc:PurposeStatement xml:lang="nl">Om voornaam te kunnen testen...</esc:PurposeStatement>
        <esc:PurposeStatement xml:lang="en">For testing Firstname...</esc:PurposeStatement>
      </esc:RequestedAttribute>
      <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:Initials" isRequired="false">
        <esc:PurposeStatement xml:lang="nl">Om initialen te kunnen testen...</esc:PurposeStatement>
        <esc:PurposeStatement xml:lang="en">For testing initials</esc:PurposeStatement>
      </esc:RequestedAttribute>
      <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FamilyName" isRequired="true">
        <esc:PurposeStatement xml:lang="nl">Om achternaam te kunnen testen...</esc:PurposeStatement>
        <esc:PurposeStatement xml:lang="en">For testing family name...</esc:PurposeStatement>
      </esc:RequestedAttribute>
      <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:DateOfBirth" isRequired="true">
        <esc:PurposeStatement xml:lang="nl">Om geboortedatum te kunnen testen...</esc:PurposeStatement>
        <esc:PurposeStatement xml:lang="en">For testing birthdate...</esc:PurposeStatement>
      </esc:RequestedAttribute>
    </esc:ServiceDefinition>

    <esc:ServiceInstance esc:IsPublic="true">
      <esc:ServiceID>urn:etoegang:DV:99999999000000000099:services:9999</esc:ServiceID>
      <esc:ServiceUUID>9adfede3-eda5-4385-b938-9ccb954b2ad5</esc:ServiceUUID>
      <esc:InstanceOfService>6bae98e3-5ef9-4576-98c8-5aba4b8e672d</esc:InstanceOfService>
      <esc:ServiceURL xml:lang="nl">http://example.nl</esc:ServiceURL>
      <esc:ServiceURL xml:lang="en">http://example.com</esc:ServiceURL>
      <esc:PrivacyPolicyURL xml:lang="nl">http://example.etoegang.nl/privacy.html</esc:PrivacyPolicyURL>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:SSOSupport>false</esc:SSOSupport>
      <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
```

```
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
    </esc:ServiceInstance>

  </esc:ServiceProvider>

</esc:ServiceCatalogue>
```

Example Service with service intermediation

```
...
   <esc:ServiceProvider esc:IsPublic="true">
    <esc:ServiceProviderID>99999999000000000098</esc:ServiceProviderID>
    <esc:OrganizationDisplayName xml:lang="nl">Voorbeeld DV</esc:OrganizationDisplayName>
    <esc:OrganizationDisplayName xml:lang="en">Example SP</esc:OrganizationDisplayName>

    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed>urn:etoegang:1.12:EntityConcernedID:BSN</esc:EntityConcernedTypesAllowed>
    </esc:ServiceDefinition>

    <esc:ServiceInstance esc:IsPublic="true">
      <esc:ServiceID>urn:etoegang:DV:99999999000000000098:services:9998</esc:ServiceID>
      <esc:ServiceUUID>94148585-90e3-467e-be43-5f5270326215</esc:ServiceUUID>
      <esc:InstanceOfService>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:InstanceOfService>
      <esc:ServiceURL xml:lang="nl">http://example.nl</esc:ServiceURL>
      <esc:PrivacyPolicyURL xml:lang="nl">http://example.etoegang.nl/privacy.html</esc:PrivacyPolicyURL>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:SSOSupport>false</esc:SSOSupport>
      <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
      <esc:ServiceIntermediation intermediationAllowed="requiresApproval">
          <esc:ServiceIntermediationAllowed>99999999000000000098</esc:ServiceIntermediationAllowed>
          <esc:ServiceIntermediationAllowed>99999999000000000097</esc:ServiceIntermediationAllowed>
      </esc:ServiceIntermediation>
    </esc:ServiceInstance>

  </esc:ServiceProvider>

  <esc:ServiceProvider esc:IsPublic="true">
    <esc:ServiceProviderID>99999999000000000097</esc:ServiceProviderID>
    <esc:OrganizationDisplayName xml:lang="nl">Voorbeeld Dienstbemiddelaar</esc:OrganizationDisplayName>
    <esc:OrganizationDisplayName xml:lang="en">Example Service Intemediary</esc:OrganizationDisplayName>

    <esc:ServiceInstance esc:IsPublic="true">
      <esc:ServiceID>urn:etoegang:DV:99999999000000000097:services:9997</esc:ServiceID>
      <esc:ServiceUUID>71dccfdd-2d4f-44e5-b03d-01c6580fad80</esc:ServiceUUID>
      <esc:IntermediatedService>94148585-90e3-467e-be43-5f5270326215</esc:IntermediatedService>
      <esc:ServiceURL xml:lang="en">http://example.com</esc:ServiceURL>
      <esc:PrivacyPolicyURL xml:lang="en">http://example.etoegang.nl/privacy_en.html</esc:PrivacyPolicyURL>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:SSOSupport>false</esc:SSOSupport>
```

```
      <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>...</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
    </esc:ServiceInstance>
  </esc:ServiceProvider>
...
```

Example Service with one EntityConcernedType

```
...
    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.12:EntityConcernedID:PseudoID</esc:
EntityConcernedTypesAllowed>
    </esc:ServiceDefinition>
...
```

Example Service with two EntityConcernedTypes simultaniously

```
...
    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:RSIN</esc:
EntityConcernedTypesAllowed>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
    </esc:ServiceDefinition>
...
```

Example Service with twoEntityConcernedTypes as alternatives

```
...
    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:RSIN</esc:
EntityConcernedTypesAllowed>
```

```
      <esc:EntityConcernedTypesAllowed setNumber="2">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
    </esc:ServiceDefinition>
...
```

Example Service with multiple Identifier sets

```
...
    <esc:ServiceDefinition esc:IsPublic="true">
      <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
      <esc:ServiceName xml:lang="nl">Voorbeelddienst</esc:ServiceName>
      <esc:ServiceName xml:lang="en">Example Service</esc:ServiceName>
      <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3)</esc:ServiceDescription>
      <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
      <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
      <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:RSIN</esc:
EntityConcernedTypesAllowed>
      <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
      <esc:EntityConcernedTypesAllowed setNumber="2">urn:etoegang:1.12:EntityConcernedID:BSN</esc:
EntityConcernedTypesAllowed>
      <esc:EntityConcernedTypesAllowed setNumber="2">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
    </esc:ServiceDefinition>
...
```

Example Service Accessible for EU-citizens via eIDAS

```
...
    <esc:ServiceProvider esc:IsPublic="true">
        <esc:ServiceProviderID>99999999000000000099</esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl">Voorbeeld DV</esc:OrganizationDisplayName>
        <esc:OrganizationDisplayName xml:lang="en">Example SP</esc:OrganizationDisplayName>

        <esc:ServiceDefinition esc:IsPublic="true">
            <esc:ServiceUUID>c230649d-647d-4289-80c7-b0297e3e6a29</esc:ServiceUUID>
            <esc:ServiceName xml:lang="nl">Voorbeelddienst EU-ready</esc:ServiceName>
            <esc:ServiceName xml:lang="en">Example Service EU-ready</esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl">Voorbeelddienst (BSN LoA3) die open staat voor EU-burgers via
eIDAS</esc:ServiceDescription>
            <esc:ServiceDescription xml:lang="en">Example Service (BSN LoA3) available for EU-citizens eIDAS<
/esc:ServiceDescription>
            <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:ServiceDescriptionURL>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed>urn:etoegang:1.12:EntityConcernedID:BSN</esc:
EntityConcernedTypesAllowed>
        </esc:ServiceDefinition>

        <esc:ServiceInstance esc:IsPublic="true">
            <esc:ServiceID>urn:etoegang:DV:99999999000000000099:services:9994</esc:ServiceID>
            <esc:ServiceUUID>fabce53f-7ba6-44d7-aa75-789ec56431ad</esc:ServiceUUID>
            <esc:InstanceOfService>c230649d-647d-4289-80c7-b0297e3e6a29</esc:InstanceOfService>
            <esc:ServiceURL xml:lang="nl">http://example.nl</esc:ServiceURL>
            <esc:ServiceURL xml:lang="en">http://example.com</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">http://example.etoegang.nl/privacy.html</esc:PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
                            <ds:X509Certificate>...</ds:X509Certificate>
                        </ds:X509Data>
```

```
                    </ds:KeyInfo>
                </md:KeyDescriptor>
            </esc:ServiceCertificate>
            <esc:Classifiers>
                <esc:Classifier>PublicDomain</esc:Classifier>
                <esc:Classifier>eIDAS-inbound</esc:Classifier>
            </esc:Classifiers>
            <esc:BsnkStructureVersion>2</esc:BsnkStructureVersion>
            <esc:BsnkRecipientKeySetVersion>20201231</esc:BsnkRecipientKeySetVersion>
        </esc:ServiceInstance>

        <esc:ServiceInstance esc:IsPublic="true">
            <esc:ServiceID>urn:etoegang:DV:99999999000000000099:services:9993</esc:ServiceID>
            <esc:ServiceUUID>128d0878-2bc7-4400-9068-8427c5abeb47</esc:ServiceUUID>
            <esc:InstanceOfService>c230649d-647d-4289-80c7-b0297e3e6a29</esc:InstanceOfService>
            <esc:ServiceURL xml:lang="nl">http://app.example.nl</esc:ServiceURL>
            <esc:ServiceURL xml:lang="en">http://app.example.com</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">http://example.etoegang.nl/app/privacy.html</esc:
PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
                            <ds:X509Certificate>...</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </md:KeyDescriptor>
            </esc:ServiceCertificate>
            <esc:Classifiers>
                <esc:Classifier>PublicDomain</esc:Classifier>
                <esc:Classifier>eIDAS-inbound</esc:Classifier>
            </esc:Classifiers>
            <esc:BsnkStructureVersion>2</esc:BsnkStructureVersion>
            <esc:BsnkRecipientKeySetVersion>20201231</esc:BsnkRecipientKeySetVersion>
        </esc:ServiceInstance>
    </esc:ServiceProvider>
...
```

Example: Service Intermediation for eIDAS-UIT - EB intermediates BRP

```
...
    <esc:ServiceProvider>
        <esc:ServiceProviderID>99999999000000000098</esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl">BRP</esc:OrganizationDisplayName>
        <esc:OrganizationDisplayName xml:lang="en">BRP</esc:OrganizationDisplayName>
        <esc:ServiceDefinition>
            <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
            <esc:ServiceName xml:lang="nl">Verstrekken BRP-attributen</esc:ServiceName>
            <esc:ServiceName xml:lang="en">Verstrekken BRP-attributen</esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl">Verstrekken BRP-attributen tbv EU inlog </esc:
ServiceDescription>
            <esc:ServiceDescription xml:lang="en">Verstrekken BRP-attributen tbv EU inlog </esc:
ServiceDescription>
            <esc:ServiceDescriptionURL xml:lang="nl">http://eb-toelichting.rvo.nl</esc:ServiceDescriptionURL>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
            <esc:ActingSubjectTypesAllowed setNumber="1">urn:etoegang:1.12:EntityConcernedID:BSN</esc:
ActingSubjectTypesAllowed>
        </esc:ServiceDefinition>

        <esc:ServiceInstance>
            <esc:ServiceID>urn:etoegang:DV:99999999000000000098:services:9998</esc:ServiceID>
            <esc:ServiceUUID>94148585-90e3-467e-be43-5f5270326215</esc:ServiceUUID>
            <esc:InstanceOfService>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:InstanceOfService>
```

```
            <esc:ServiceURL xml:lang="nl">http://attrdienst.brp.nl</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">http://statement.brp.nl/privacy.html</esc:PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
                            <ds:X509Certificate>...</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </md:KeyDescriptor>
            </esc:ServiceCertificate>
            <esc:ServiceIntermediation intermediationAllowed="requiresApproval">
                <esc:ServiceIntermediationAllowed>99999999000000000097</esc:ServiceIntermediationAllowed>
            </esc:ServiceIntermediation>
            <esc:Classifiers>
                <esc:Classifier>eIDAS-outbound</esc:Classifier>
            </esc:Classifiers>
            <esc:BsnkStructureVersion>2</esc:BsnkStructureVersion>
            <esc:BsnkRecipientKeySetVersion>20201231</esc:BsnkRecipientKeySetVersion>
        </esc:ServiceInstance>
    </esc:ServiceProvider>

    <esc:ServiceProvider>
        <esc:ServiceProviderID>99999999000000000097</esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl">NL EU-knooppunt</esc:OrganizationDisplayName>
        <esc:OrganizationDisplayName xml:lang="en">NL EU-knooppunt</esc:OrganizationDisplayName>
        <esc:ServiceDefinition>
            <esc:ServiceUUID>hj67b0d3-eb48-4836-a9a4-fde50e32ac89</esc:ServiceUUID>
            <esc:ServiceName xml:lang="nl">Duitsland-overheid</esc:ServiceName>
            <esc:ServiceName xml:lang="en">Germany Public service</esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl">Duitsland-overheid (BSN LoA3)</esc:ServiceDescription>
            <esc:ServiceDescription xml:lang="en">Germany Public service(BSN LoA3)</esc:ServiceDescription>
            <esc:ServiceDescriptionURL xml:lang="nl">http://eb-toelichting.rvo.nl</esc:ServiceDescriptionURL>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:KvK</esc:
EntityConcernedTypesAllowed>
            <esc:ActingSubjectTypesAllowed setNumber="1">urn:etoegang:1.12:EntityConcernedID:PseudoID</esc:
ActingSubjectTypesAllowed>
        </esc:ServiceDefinition>

        <esc:ServiceInstance>
            <esc:ServiceID>urn:etoegang:DV:99999999000000000097:services:9997</esc:ServiceID>
            <esc:ServiceUUID>71dccfdd-2d4f-44e5-b03d-01c6580fad80</esc:ServiceUUID>
            <esc:InstanceOfService>hj67b0d3-eb48-4836-a9a4-fde50e32ac89</esc:InstanceOfService>
            <esc:IntermediatedService>94148585-90e3-467e-be43-5f5270326215</esc:IntermediatedService>
            <esc:ServiceURL xml:lang="en">http://example.com</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="en">http://example.etoegang.nl/privacy_en.html</esc:
PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
                            <ds:X509Certificate>...</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </md:KeyDescriptor>
            </esc:ServiceCertificate>
            <esc:Classifiers>
                <esc:Classifier>eIDAS-outbound</esc:Classifier>
            </esc:Classifiers>
            <esc:BsnkStructureVersion>2</esc:BsnkStructureVersion>
            <esc:BsnkRecipientKeySetVersion>20201231</esc:BsnkRecipientKeySetVersion>
        </esc:ServiceInstance>
    </esc:ServiceProvider>
```

```
...
```

Example: Service Intermediation: Intermediate Service and Intermediairy Service have the same InstanceOfService (and therefore only require one mandate)

```
...
    <esc:ServiceProvider>
        <esc:ServiceProviderID>99999999000000000098</esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl">Naam DienstAanbieder</esc:OrganizationDisplayName>
        <esc:OrganizationDisplayName xml:lang="en">Name Intermediated ServiceProvider</esc:
OrganizationDisplayName>

        <esc:ServiceDefinition>
            <esc:ServiceUUID>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:ServiceUUID>
            <esc:ServiceName xml:lang="nl">Naam Bemiddelde Dienst</esc:ServiceName>
            <esc:ServiceName xml:lang="en">Name Intermediated Service</esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl">Beschrijving Bemiddelde Dienst</esc:ServiceDescription>
            <esc:ServiceDescription xml:lang="en">Description Intermedated Service</esc:ServiceDescription>
            <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl/</esc:ServiceDescriptionURL>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed setNumber="1">urn:etoegang:1.9:EntityConcernedID:KvKnr</esc:
EntityConcernedTypesAllowed>
        </esc:ServiceDefinition>

        <esc:ServiceInstance>
            <esc:ServiceID>urn:etoegang:DV:99999999000000000098:services:9998</esc:ServiceID>
            <esc:ServiceUUID>94148585-90e3-467e-be43-5f5270326215</esc:ServiceUUID>
            <esc:InstanceOfService>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:InstanceOfService>
            <esc:ServiceURL xml:lang="nl">http://example.nl/</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">http://example.etoegang.nl/privacy.html</esc:PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
                            <ds:X509Certificate>...</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                </md:KeyDescriptor>
            </esc:ServiceCertificate>
            <esc:ServiceIntermediation intermediationAllowed="requiresApproval">
                <esc:ServiceIntermediationAllowed>99999999000000000097</esc:ServiceIntermediationAllowed>
            </esc:ServiceIntermediation>
        </esc:ServiceInstance>
    </esc:ServiceProvider>

    <esc:ServiceProvider>
        <esc:ServiceProviderID>99999999000000000097</esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl">DV Naam</esc:OrganizationDisplayName>
        <esc:OrganizationDisplayName xml:lang="en">SP Name</esc:OrganizationDisplayName>
        <esc:ServiceInstance>
            <esc:ServiceID>urn:etoegang:DV:99999999000000000097:services:9997</esc:ServiceID>
            <esc:ServiceUUID>71dccfdd-2d4f-44e5-b03d-01c6580fad80</esc:ServiceUUID>
            <esc:InstanceOfService>cf48b0d3-ea45-4436-a6c4-fde50e19ef70</esc:InstanceOfService>
            <esc:IntermediatedService>94148585-90e3-467e-be43-5f5270326215</esc:IntermediatedService>
            <esc:ServiceURL xml:lang="en">http://example.com</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="en">http://example.etoegang.nl/privacy_en.html</esc:
PrivacyPolicyURL>
            <esc:HerkenningsmakelaarId>99999999000000000010</esc:HerkenningsmakelaarId>
            <esc:SSOSupport>false</esc:SSOSupport>
            <esc:ServiceCertificate>
                <md:KeyDescriptor use="encryption">
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                        <ds:X509Data>
```

```
                        <ds:X509Certificate>...</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </md:KeyDescriptor>
        </esc:ServiceCertificate>
    </esc:ServiceInstance>
</esc:ServiceProvider>
...
```

The use of BsnkRecipientKeySetVersion for BSNk-tranformation service is added tot AUC10.2 (see AUC10.2 MachtigingsRegister of Authenticatiedienst gebruikt BSNk transformatie functie)

The use of BsnkStructureVersion to select the appropriate BSNk-tranformation service is added tot AUC10.2 (see AUC10.2 MachtigingsRegister of Authenticatiedienst gebruikt BSNk transformatie functie)

Publication

The Beheerorganisatie publishes the service catalog at a predetermined location. Before it is published, the service catalog is sorted by HerkenningsmakelaarId and then by the ServiceID.

A participant MUST process the service catalog according to Proces doorvoeren nieuwe dienstencatalogus.

Testing

This document describes the tests that (aspiring) participants should perform.To ensure that new releases and the application process of participants go smoothly, it is required that new functionality or systems are tested thoroughly before taken into production. It is the responsibilty of the (aspiring) participants to demonstrate interoperability and to create trust and confidence with the other participants related to their implementation. This document distinguishes Simulator test cases and Chain test cases. The simulator tests are executed utilizing the Elektronische Toegangsdiensten simulator, an instrument for initiating requests and validating responses. Focus on these tests is conformity with the Afsprakenstelsel. Chain tests are executed in a separate network of systems, each in its own DTAP A-environment. During the chain tests, the focus is interoperability of all participants' systems.

The (aspiring) participant contacts the Beheerorganisatie when ready for executing chain test and for readiness of production go-live. The (aspiring) participant must proof their readiness to the BO by means of a demonstration of the functionality and a presentation of the testproces and results. Based on the outcome of this proof, it is determined whether or not technical issues are remaining which should be solved before joining. Based on the outcome of these tests, it is determined whether or not technical issues are remaining which should be solved before joining.

It is the sole responsibility of the (future) participant that the functionality is working correctly as described in the agreed specifications and that it is interoper able with another participants system. For each technical release implementation the participants will make an agreement of the scope of testing: which usecases have to be shown and the criteria to pass. That agreement is part of the implementation plan, therefore public, and guarantees uniformity and a level playing field.

The participant is free to choose how to proof that the agreed specifications are implemented correctly. The participant can use a provided simulator, or his own, but must be able to provide proof in a way that a third party (Beheerorganisatie) can be convinced.

Interoperability is difficult to proof for the first participant because there is not another party available to demonstrate it. The participants can make agreements with each other to tackle this issue to shorten the time to market.

Continue here

- Requirements for testing
    - Acquire test means — In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other.
    - Announce chain test — To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.
    - Exchange metadata — Within the network, all Herkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.
    - Process service catalog — All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a aggregated service catalog. See Proces doorvoeren nieuwe dienstencatalogus.
- Network monitoring

Requirements for testing

In order to test your systems, be sure the following requirements are met.

- Acquire test means — In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other.
- Announce chain test — To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.
- Exchange metadata — Within the network, all Herkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.
- Process service catalog — All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a aggregated service catalog. See Proces doorvoeren nieuwe dienstencatalogus.

Acquire test means

In order to facilitate chain testing, it is necessary that all participants in the network must have authentication means and corresponding authorizations of each other. An applicant is therefore entitled to request such information from other parties. The applicant should also supply means and authorizations to the other participants when requested.

An HM is not required to test all provided levels of assurace for each AD/MR, and therefore needs only one test mean for each AD/MR.

Announce chain test

To be able to get support from other participants in a timely manner, it is necessary that all participants are aware when a chain test will take place.It is therefore required to announce a chain test. Refer to Onderhoud for more details.

Exchange metadata

Within the network, all Herkenningsmakelaars, Authenticatiediensten and Machtigingenregisters should exchange each others metadata, so the systems can verify the origin of a request and subsequently process it.
The beheerorganisatie has a process in place to aggregate metadata and publish one file which contains all relevant metadata. For the test environment, this also contains the metadata for all simulated entities, including the simulated Dienstverlener.



Refer to Proces netwerkmetadata for the process of metadata aggregation.

Process service catalog

All systems in the network must be aware of the properties of each service, in order to process authentication requests in a correct way. For this purpose, the beheerorganisatie maintains a aggregated service catalog. See Proces doorvoeren nieuwe dienstencatalogus.For the test network, there is a separate service catalog, which holds all services which are offered by the simulated Dienstverlener.

Network monitoring

The Beheerorganisatie does not actively monitor the network's status.

It is possible to monitor the networkstatus by executing automatic tests periodically. For this purpose, participants might purchase or develop their own tooling. Whenever the participants wish to monitor the network themselves actively, they MUST use the monitoring OIN (99999900000002) which is mentioned in the service catalog.

Informatiebeveiliging en privacy

Dit hoofdstuk bevat de normenkaders en het beleid aangaande borging van veiligheid, privacy en continuïteit van Elektronische Toegangsdiensten.

Het bevat de volgende onderdelen:

- Beleid voor informatiebeveiliging — Dit document bevat het beleid voor informatiebeveiliging dat onderdeel is van het Afsprakenstelsel Elektronische Toegangsdiensten.
- Privacybeleid — Om Herkenningsdiensten te kunnen leveren worden persoonsgegevens verwerkt. De verwerking van persoonsgegevens is alleen rechtmatig als wordt voldaan aan de voorwaarden die de Algemene verordening gegevensbescherming (AVG) of andere toepasselijke specifieke privacy wet- en regelgeving hieraan stelt.
- Gemeenschappelijk normenkader informatiebeveiliging — ISO 27001:2013 beheersdoelstellingen en beheersmaatregelen binnen de scope van eToegangsdiensten, - activiteiten, -objecten en -informatie
- Normenkader betrouwbaarheidsniveaus — Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast.
- Attributenbeleid

Beleid voor informatiebeveiliging

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Dit document bevat het beleid voor informatiebeveiliging dat onderdeel is van het Afsprakenstelsel Elektronische Toegangsdiensten.

Het is voorzien dat het Afsprakenstelsel een groeiende maatschappelijke rol vervult in het burgerdomein, bedrijvendomein en consumentendomein als leverancier van vertrouwen tussen gebruikers en aanbieders van online diensten. De diensten die binnen de kaders van het stelsel worden geleverd zijn vertrouwensdiensten en daarmee een essentieel onderdeel van de strategie voor informatiebeveiliging van Gebruikers en Dienstverleners. Het verwerven en behouden van vertrouwen van de Dienstverleners en Gebruikers is daarom een belangrijke randvoorwaarde voor het succes van het Stelsel. Het Afsprakenstelsel bevat de strategische, tactische en operationele eisen waaraan partijen moeten voldoen om Herkenningsdiensten te mogen leveren als onderdeel van het stelsel (zie Algemeen). Het beleid voor informatiebeveiliging is een instrument voor de borging van dit vertrouwen.

Doelstelling

Het beleid voor informatiebeveiliging bevat beleidskaders die tot doel hebben de veilige en betrouwbare werking van het Stelsel te waarborgen.

Beleidsdoelstellingen:

- De Gebruikers en Dienstverleners ervaren een ongestoorde en veilige werking van de stelseldiensten die zij afnemen.
- Deelnemers, Beheerorganisatie van het stelsel en de beheerder van het BSNk integreren informatiebeveiliging in hun bedrijfsvoering en informeren de Toezichthouder.
- De Eigenaar (merkeigenaar en politiek verantwoordelijke) van het Stelsel is in staat gesteld om op transparante wijze verantwoording af te leggen over het behalen van de doelstelling van dit beleid.
- De Toezichthouder is in staat gesteld om effectief en onafhankelijk het publieke belang van het Stelsel te bewaken op de naleving van stelselafspraken inzake informatiebeveiliging van het Stelsel.

Dit beleid is van toepassing voor alle partijen die deelnemen in het Stelsel en vastgesteld door het Tactisch Beraad van het Stelsel.

Organisatie van verantwoordelijkheid voor informatiebeveiliging

Het Stelsel kent verschillende rolhouders die elke een eigen verantwoordelijkheid hebben voor de informatiebeveiliging van het Stelsel.

Eigenaarsrol

De Eigenaar van het Stelsel is politiek verantwoordelijk voor de veilige en betrouwbare werking van het Stelsel. De Eigenaar formuleert daartoe een interne controlestrategie voor het Stelsel en handelt daarnaar. De Eigenaar is 'Merkeigenaar' van het Stelsel en verantwoordelijk voor de merkbescherming. De houder van de rol Eigenaar van het Stelsel is de Minister van Binnenlandse Zaken.

Beheerdersrol

De Beheerorganisatie (BO) van het Stelsel voert zijn taken uit in opdracht van de Eigenaar. De Beheerorganisatie is verantwoordelijk voor de informatiebeveiliging van zijn eigen activiteiten en coördineert de informatiebeveiliging op het niveau van het Stelsel.

BSNk

BSNk heeft als rol een bijzondere positie in het Stelsel. Het ministerie van BZK is opdrachtgever van het BSNk. De Beheerder van het BSNk is geen deelnemer maar moet wel voldoen aan het Afsprakenstelsel, net als een Deelnemer of de Beheerorganisatie van het Stelsel. De Beheerder van het BSNk is daarmee ook verantwoordelijk voor de informatiebeveiliging van zijn eigen activiteiten. In dit document wordt waar beheerder van het BSNk is bedoeld gesproken over BSNk.

Deelnemersrol

De Deelnemer in het Stelsel is een private partij of publieke partij die is toegetreden tot het Stelsel. De Deelnemer is verantwoordelijk voor de informatiebeveiliging van zijn eigen stelselactiviteiten en infrastructuur. De Deelnemers zijn verantwoordelijk voor de naleving van de Stelselafspraken inzake informatiebeveiliging en tevens voor de controle op de naleving van de stelselvoorwaarden voor de afname van stelseldiensten door Gebruikers en Dienstverleners.

Dienstverlenersrol

De Dienstverlener (DV) in het Stelsel is een private partij of publieke partij die Stelseldiensten afneemt van de Deelnemer in het Stelsel. De Dienstverlener is zelf verantwoordelijk voor de informatiebeveiliging van de online dienst die met behulp van het Stelsel aanbiedt. De Dienstverlener is tevens verantwoordelijk voor de naleving van de voorwaarden voor afname van stelseldiensten.

Gebruikersrol

Gebruikers zijn individuele personen en bedrijven. Gebruikers nemen authenticatiediensten en diensten voor machtigingen af van Deelnemers in het stelsel. Gebruikers zijn verantwoordelijk voor de informatiebeveiliging van de eigen gebruikersomgeving.

Toezichthouderrol

Als Eigenaar van het publiek-private afsprakenstelsel voor elektronische toegangsdiensten, is de Minister van Binnenlandse Zaken tevens Toezichthouder. Om de rollen van Eigenaar en Toezichthouder zo veel als mogelijk te scheiden, is een Commissie van Deskundigen (CvD) ingesteld door de Ministerraad.

De Toezichthouder houdt toezicht op de naleving van stelselafspraken door de Eigenaar, Beheerder, Deelnemers en BSNk.

De Commissie van Deskundigen adviseert over te nemen stappen in het kader van toezicht. Hiermee krijgt de minister een onafhankelijk advies over toetredingen en te ondernemen acties in het kader van handhaving en optreden bij incidenten.

De rol van de Stelselgovernance

De ontwikkeling en het onderhoud van het Stelsel is door de Eigenaarsrol belegd bij de Stelselgovernance. De governance omvat het Strategisch Beraad, het Tactisch Beraad en het Operationeel Beraad, in deze raden zijn de Deelnemers en de Dienstverleners vertegenwoordigd, de Beheerorganisatie van het Stelsel vervult de secretarisrol. Besluiten over wijzigingen van Stelselafspraken worden binnen het mandaat van het Strategisch Beraad door het Tactisch Beraad genomen op advies van het Operationeel beraad. Het Tactisch Beraad vervult daarmee het dagelijks bestuur van het Stelsel en is onder meer verantwoordelijk voor de afweging van beveiligingsrisico's en maatregelen.

Generieke beleidsuitgangspunten voor informatiebeveiliging

Het Stelsel kent de volgende generieke beleidsuitgangspunten voor informatiebeveiliging:

Afweging van beveiligingsrisico’s van het Stelsel

1. Het Stelsel MOET over een Stelselrisicoanalyse beschikken. De Beheerorganisatie van het Stelsel MOET zorgdragen voor het tot stand komen van de analyse en het onderhoud daar van. De stelselrisicoanalyse MOET gemaakt worden met een representatieve vertegenwoordiging van Deelnemers, Dienstenaanbieders en de Beheerders van de voorzieningen voor de metadata, dienstencatalogus en BSNk.
2. Het Tactisch Beraad van het stelsel MOET verantwoordelijkheid nemen voor het al dan niet accepteren van de (rest)risico's en de besluiten over het nemen van maatregelen.
3. Besluiten over beveiligingsmaatregelen MOETEN op een risicoafweging zijn gebaseerd.
4. Beveiligingsmaatregelen MOETEN voorschrijvend opgenomen worden in het Afsprakenstelsel als uniformiteit noodzakelijk is voor de veilige en betrouwbare werking van het Stelsel.
5. Herijking van de Stelselrisicoanalyse MOET jaarlijks plaatsvinden. De besluitvorming daarover MOET het wijzigingsproces van het Afsprakenstelsel volgen.
6. Elke Deelnemer en Beheerorganisatie in het stelsel heeft een verantwoordelijke aangewezen voor informatiebeveiliging die met mandaat als aanspreekpunt van de organisatie optreedt.
7. De Beheerorganisatie van het Stelsel is verantwoordelijk voor de samenhangende coördinatie van de beleidsmatige en operationele afweging van beveiligingsrisico's

Stelselnormenkader voor informatiebeveiliging

1. Het Stelsel MOET over een Gemeenschappelijk normenkader informatiebeveiliging beschikken dat zijn basis heeft in de stelselrisicoanalyse.
2. Het Gemeenschappelijk normenkader informatiebeveiliging MOET door de Beheerorganisatie van het Stelsel worden opgesteld en onderhouden in samenwerking met een representatieve vertegenwoordiging van de Deelnemers en de Dienstverleners.
3. De herijking van de het Gemeenschappelijk normenkader informatiebeveiliging en daaruit volgende beveiligingsmaatregelen MOET jaarlijks plaatsvinden. De besluitvorming daarover MOET het wijzigingenproces van het Afsprakenstelsel volgen.
4. Deelnemers MOGEN NIET bij interconnectie om aanvullende zekerheden omtrent de beveiliging van een andere deelnemer vragen bij het gezamenlijk vormgeven van dienstverlening in het kader van het netwerk.
5. Het Stelsel MOET beschikken over een gemeenschappelijke informatie-classificatie voor stelselinformatie die in het Stelsel door de Deelnemers, de Beheerorganisatie van het Stelsel en de Beheerorganisatie van het BSNk wordt verwerkt en opgeslagen.

Naleving en Toezicht

1. Deelnemers, Beheerorganisatie en BSNk MOETEN beschikken over een managementsysteem voor informatiebeveiliging. Zij MOETEN dit managementsysteem laten certificeren of beschikken over een verklaring met minimaal gelijke kwaliteit over de conformiteit van het managementsysteem met de vereisten. Het certificaat of verklaring moet zijn afgegeven door een onafhankelijke en ter zake deskundige partij.
2. De Deelnemers, Beheerorganisatie en BSNk MOETEN aantonen dat zij de stelselafspraken inzake informatiebeveiliging nakomen. Het bewijsmateriaal daarvoor waaronder relevante archieven, loggings, auditrapporten en correctieve actieplannen MOETEN zij inzichtelijk maken voor de Toezichthouder op het Stelsel en op diens verzoek op elk moment voor inzage ter beschikking stellen.

   > Als de wettelijke verankering van het Stelsel en het Toezicht daarop een feit is wordt dit beleidsuitgangspunt door de betreffende wet en de AWB vervangen.

3. De Beheerorganisatie van het Stelsel MOET zorgdragen voor de uitvoering van de controlestrategie van Eigenaar van het stelsel. Dit betekent onder andere dat de Beheerorganisatie van het Stelsel de operationele controles die hij uitvoert MOET archiveren. Het adequaat vastleggen van controles is nodig voor de verantwoording van de Eigenaar over de informatiebeveiliging van het Stelsel én is van belang voor de effectiviteit van het toezicht door de Toezichthouder.

Specifieke beleidsuitgangspunten voor informatiebeveiliging

Op een aantal specifieke onderwerpen kent het Stelsel nadere afspraken :

Afspraken Stelselrisicoanalyse en Gemeenschappelijk Normenkader

De Beheerorganisatie van het Stelsel onderhoudt het Gemeenschappelijk normenkader informatiebeveiliging en de stelselrisicoanalyse:

1. Het Gemeenschappelijk normenkader informatiebeveiliging MOET beveiligingseisen bevatten die voor elke rol in het netwerk van toepassing zijn.
2. Het Gemeenschappelijk normenkader informatiebeveiliging MOET naast de generieke eisen ook specifieke eisen die verschillen per rol in het netwerk bevatten.
3. Het Gemeenschappelijk normenkader Informatiebeveiliging MOET -indien noodzakelijk - onderscheid maken naar toepasselijkheid voor de verschillende betrouwbaarheidsniveaus van de diensten die Deelnemers aanbieden.
4. De Beheerorganisatie van het Stelsel MOET het versiebeheer van de stelselrisicoanalyse en het Gemeenschappelijk normenkader informatiebeveiliging voeren.

Afspraken implementatie Gemeenschappelijk normenkader informatiebeveiliging, certificatie en assurance

1. Deelnemers, Beheerorganisatie en BSNk MOETEN in bezit zijn van een geldige certificaat conform de standaard ISO 27001 of een Third Party Mededeling (jaarlijks) inzake de conformiteit aan de genoemde ISO standaard.
2. In de Verklaring van Toepasselijkheid behorende bij de certificatie dan wel Third Party Mededeling MOETEN minimaal de normen uit het Gemeenschappelijk normenkader informatiebeveiliging zijn opgenomen.
3. Daar waar het Afsprakenstelsel geen maatregelen voorschrijft MOETEN de Deelnemers, Beheerorganisatie en BSNk op basis van risicoanalyse zelf de beheersmaatregelen voor hun activiteiten en infrastructuur definiëren.
4. De stelselrisicoanalyse MOET aantoonbaar onderdeel zijn van in de risicoanalyses van Deelnemers, Beheerorganisatie en BSNk die zij in het kader van hun managementsysteem opstellen.
5. De potentiële deelnemer MOET bij toetreding(en) tot het Stelsel (rollen, functionaliteiten en betrouwbaarheidsniveaus) de verplichting op zich nemen om binnen 6 maanden bij een initiële toetredingen zijn activiteiten voor het Stelsel te laten voorzien van certificatie of een TPM. De potentiële deelnemer MOET daarvoor op het moment van toetreden worden gebonden aan de op dat moment geldende versie van het Gemeenschappelijk Normenkader Informatiebeveiliging en de Stelselrisicoanalyse.
6. Bestaande deelnemers MOETEN bij toetredingen tot nieuwe functionaliteiten, rollen, betrouwbaarheidsniveaus en bijstellingen van het normenkader een redelijke termijn krijgen om de geldende elementen van het Gemeenschappelijk Normenkader Informatiebeveiliging te implementeren en in hun certificatie of TMP in te passen.

Afspraken Gemeenschappelijke Classificatie van Stelselinformatie

Stelselgegevens hebben betekenis op het niveau van het Stelsel. De bescherming van die gegevens door individuele deelnemers en beheerorganisaties moet daarom een gelijk niveau hebben. De Gemeenschappelijke Classificatie van Stelselgegevens (tabel 1) geeft richting aan het nemen van beveiligingsmaatregelen.

In tabel 1 is de classificatie van informatie binnen het Stelsel beschreven. De tabel legt met voorbeelden uit hoe de classificatie moet worden begrepen. Tabel 2 geeft een lijst van voorbeelden van geclassificeerde stelselgegevens en dient als referentie voor de classificatie van overige bestaande en nieuwe Stelselinformatie.

Tabel 1: Classificatie van informatie binnen het Stelsel

Classificatie	Openbaar	Intern	Vertrouwelijk
Uitleg	Alle informatie over het Stelsel bedoeld voor (potentiële) klanten of breder publiek.	• Informatie die door alle direct betrokkenen in het Stelsel wordt uitgewisseld. • De informatie is niet bedoeld voor anderen maar als onverhoopt deze informatie met derden wordt gedeeld treedt er geen substantiële financiële schade of imago schade op.	• Informatie die extra bescherming nodig heeft. • Openbaring aan niet bevoegden brengt het risico van substantiële schade toe aan het Stelsel; financieel, imago gerelateerd of anderszins.
Voorbeeld	• De Stelsel-documentatie • Informatie over de aanbieders van diensten op de website van het Stelsel • Factsheets etc.	• Agenda's en vergaderverslagen • Mails (tenzij expliciet is aangegeven dat deze vertrouwelijk zijn) • Dienstencatalogus • Metadata	• Contractgegevens • Testgegevens • Klantenregistratie AD en MD • Logbestanden
Referentie	• Vertrouwelijkheid is n.v.t. • N.B.: er worden wel eisen gesteld aan juistheid en beschikbaarheid van deze informatie	• Vertrouwelijkheid is laag • AVG • Maatregelniveau: • Baseline • AV23 Risicoklasse 1	• Vertrouwelijkheid is Midden/Hoog • AVG • Maatregelniveau: • Baseline + Specifiek • AV23 Risicoklasse 2

Tabel 2: Referentietabel met voorbeelden van geclassificeerde gegevens

	Referentietabel met gegevens binnen het Stelsel (niet uitputtend)	Classificatie
1	Logbestanden van berichten-/transactieverkeer	Vertrouwelijk - AV23 Risicoklasse 2
2	Contractgegevens	Vertrouwelijk
3	Registraties AD en MD	Vertrouwelijk - AV23 Risicoklasse 2
4	Metadata	Intern[1]
5	Dienstencatalogus	Intern[1]
6	Testgegevens	Vertrouwelijk
7	Auditrapporten	Vertrouwelijk
8	Informatie betreffende de toetreding van deelnemers exclusief het advies aan het Tactisch Beraad	Vertrouwelijk
9	Berichten(verkeer)	Vertrouwelijk
10	SNO rapportages van individuele deelnemers	Vertrouwelijk
11	Generieke managementrapportages	Intern
12	Vergaderverslagen Operationeel Beraad, Tactisch Beraad etc.	Intern
13	Beveiligingsincidenten-registratie	Vertrouwelijk

14	Generieke beveiligingsrapportage (trends)	Intern
15	Documentatie van het Afsprakenstelsel	Openbaar
16	Informatie op de website van het Stelsel	Openbaar
17	RFC's	Intern/Vertrouwelijk[2]
18	Rapporten van security-audits of penetratietesten	Vertrouwelijk

Voetnoten

1. Betreft slechts het aspect vertrouwelijkheid. Er zal wel sprake zijn van extra maatregelen i.v.m. eisen aan de integriteit van de gegevens.
2. Per RFC dient de mate van vertrouwelijkheid te worden vastgesteld en de consequenties voor de behandeling van de RFC in de wijzigingsprocedure. Tenzij anders gespecificeerd, geldt dat de samenvatting Openbaar is, reviewcommentaar Intern, en de RFC tekst Intern zolang deze niet van positief advies is voorzien door het OB.

Afspraken archivering, logging en opvraging

1. Het Stelsel MOET over een Beleid beschikken voor het vastleggen en bewaren van gegevens die in het stelsel worden verwerkt. De doelen van vastleggingen, archivering van berichten, loggings- en bewijsstukken zijn:
    a. Behandelen van geschillen
    b. Audit trail
    c. Bescherming tegen misbruik van digitale identiteiten van gebruikers door derden en na voorvallen van misbruik door derden het faciliteren van het ongedaan maken van transacties.
2. Deelnemers, Beheerorganisatie en BSNk MOETEN zelf verantwoordelijkheid nemen voor de naleving van wettelijke privacy regelgeving.
3. Deelnemers, Beheerorganisatie en BSNk MOETEN alle gearchiveerde stelselgegevens beveiligen tegen toegang door onbevoegden. Dit uitgangspunt omvat alle stelselgegevens.
4. Deelnemers, Beheerorganisatie en BSNk MOETEN een verzoek waarbij gearchiveerde gegevens worden opgevraagd honoreren in de volgende gevallen:
    a. Wanneer er beroep is ingesteld tegen een bestuursrechtelijk besluit dat de publieke Dienstverlener heeft genomen op basis van gegevens die zijn verkregen middels een stelseldienst en de Dienstverlener deze bewijsstukken nodig heeft in het kader van de beroepsprocedure moeten de gegevens worden verstrekt aan zowel betreffende Dienstverlener als gebruiker of machtigingsverlener die het beroep heeft ingesteld.
    b. Op vordering van een bevoegde opsporingsinstantie, een inlichtingen- of veiligheidsdienst of een bevoegde Toezichthouder moeten de gegevens aan betreffende instantie worden verstrekt.
    c. Op verzoek van de Beheerorganisatie. Bijv. omdat elders in de keten informatie verloren is gegaan en met als doel dat de ontbrekende informatie wordt hersteld.
5. Een partij MOET een verzoek voor het vrijgeven van gearchiveerde informatie in beginsel indienen bij de betreffende Deelnemer. Een Dienstverlener MOET een dergelijk verzoek in beginsel indienen bij zijn makelaar. In geval van geschillen, of bij onvoldoende medewerking MAG een partij een verzoek indienen bij de Beheerorganisatie van het Stelsel, die vervolgens de coördinatie op zich MOET nemen.
6. De Deelnemers, Beheerorganisatie en BSNk MOETEN logging kunnen inzetten voor foutopsporing.
7. Deelnemers, Beheerorganisatie en BSNk MOETEN met behulp van logging over elke periode vragen over transacties kunnen beantwoorden waarin een van de volgende criteria, of een combinatie ervan, zijn opgenomen:
    a. Identificerend kenmerk Deelnemer
    b. Identificerend kenmerk/pseudoniem Gebruiker
    c. Identificerend kenmerk dienstbemiddelaar partij (indien van toepassing)
    d. Identificerend kenmerk van dienstverlener
    e. Dienst en dienstenset uit dienstencatalogus
    f. Betrouwbaarheidsniveaus

Indien deelnemers vanwege aanpassingen in de voorgeschreven architectuur niet of niet meer in staat zijn om een of meerdere van deze gegevens op te leveren dan zijn ze ontslagen van de verplichting om die specifieke gegevens op te kunnen leveren.

Meer lezen over bewaartermijnen

Doelomschrijving Authenticatiedienst als verantwoordelijke

Doelomschrijving Middelenuitgever

Doelomschrijving Machtigingenregister

Technische specificaties en procedures voor uitgifte van authenticatiemiddelen

Specificaties voor het beheer van bevoegdheden

Gemeenschappelijk normenkader informatiebeveiliging

Afspraken voor de integriteit van medewerkers

Bij integriteit en betrouwbaarheid gaat het zowel om het handelen in overeenstemming met algemeen aanvaarde maatschappelijke normen en waarden, (wettelijke) richtlijnen en procedures als het nakomen van afspraken en toezeggingen aan klanten, medewerkers, leveranciers en andere belanghebbenden.

1. Deelnemers, Beheerorganisatie en BSNk MOETEN het risico verminderen dat medewerkers worden aangenomen die door hun gedrag de integriteit en betrouwbaarheid van het Stelsel in gevaar brengen.
2. Screening van medewerkers of kandidaat medewerkers MOET betrekking hebben op al het vaste en tijdelijke personeel dat werkzaamheden uitvoert binnen de scope van het Stelsel.

Beleid voor penetratietesten

Het Stelsel MOET periodiek en door een onafhankelijke ter zake deskundige partij laten toetsen of de technische beveiligingsmaatregelen die zijn genomen door Deelnemers, Beheerorganisatie daadwerkelijk effectief en adequaat zijn. Een dergelijke controle is nuttig om zwakke plekken in het systeem te ontdekken en om te controleren hoe doeltreffend de beheersmaatregelen zijn bij het voorkómen van onbevoegde toegang als gevolg van deze zwakke plekken.

Uitgangspunten

Tenminste tweemaal per jaar worden er pentesten uitgevoerd. Deze zullen verdeeld worden in **centraal** (gecoördineerd door de beheerorganisatie) en **dec entraal** (onder directe verantwoordelijkheid van individuele deelnemers).

Centraal

De beheerorganisatie zal tenminste éénmaal per jaar een centrale pentest organiseren. Indien gewenst kan het thema ervan worden bepaald in overleg met de Security officers van de deelnemers tijdens het Security officers overleg.

- Black-box test MOET plaatsvinden op alle endpoints van alle in het netwerk aanwezige systemen.
- Black-box test MOET plaatsvinden op alle aangeboden diensten van de Beheerorganisatie, waaronder Mantis, Confluence en de dienstencatalogus- en metadata-aggregator.
- Deze test MAG NIET plaats vinden tijdens een koppelvlak release en daarmee een release hinderen.

Decentraal

Georganiseerd door deelnemers zelf.

- Deelnemer MOET tenminste éénmaal per jaar een eigen pentest uitvoeren, in elk geval direct volgend op de livegang van een nieuwe koppelvlakrelease.
- Deze pentest MOET tenminste Grey-box, maar MAG White-box worden uitgevoerd.
- Het implementatieplan van een nieuwe release MAG de opdracht tot een pentest bevatten.
- Deelnemer MOET alle endpoints van in het netwerk beschikbare systemen onderwerpen aan een pentest
- Deelnemer MOET ook eventuele uitgebrachte apps (t.b.v. authenticatie e.d.) die een rol in het Netwerk vervullen laten pentesten.
- Deelnemer ZOU bij deze pentest ook gerelateerde systemen, zoals self-service portalen, mee MOETEN nemen

Randvoorwaarden voor penetratietesten

De penetratietest MOET worden uitgevoerd door een partij die:

- Onafhankelijk is van de organisatie waar de pentesten plaatsvinden
- Aantoonbaar deskundig is op het gebied van standaarden die voor het Stelsel relevant zijn, zoals SAML, XACML en Signing.

Rapportage van penetratietesten

Het rapport van de Decentrale en Centrale penetratietest MOET ter inzage worden aangeboden aan de toezichthouder. Uit het rapport van de Centrale penetratietest worden de bevindingen door de Beheerorganisatie gedeeld met de betreffende geauditte partij. Voor bevindingen die geclassificeerd zijn als Hoog dient op basis van een risico analyse een Corrective Action Plan (CAP) gemaakt te worden door de deelnemer en beheerorganisatie, waarin beschreven staat wanneer de bevinding wordt opgelost. Deze dient aangeboden te worden aan de toezichthouder.

De beheerorganisatie rapporteert over de Centrale penetratietest aan het Tactisch Beraad, waarbij individuele bevindingen zijn geanonimiseerd.

Privacybeleid

Om Herkenningsdiensten te kunnen leveren worden persoonsgegevens verwerkt. De verwerking van persoonsgegevens is alleen rechtmatig als wordt voldaan aan de voorwaarden die de Algemene verordening gegevensbescherming (AVG) of andere toepasselijke specifieke privacy wet- en regelgeving hieraan stelt.De naleving van de AVG is een wettelijke plicht. Niet naleving van de privacy wet- en regelgeving en onrechtmatig gebruik van persoonsgegevens kan verschillende gevolgen hebben. Bijvoorbeeld:

- een boete van de Autoriteit Persoonsgegevens;
- imagoschade;
- bestuurlijke aansprakelijkheid;
- schadevergoeding op grond van onrechtmatige daad.

Een ieder van de te onderscheiden rollen in het netwerk elektronische toegangsdiensten heeft een eigen verantwoordelijkheid om bij de verwerking van persoonsgegevens de privacy wet- en regelgeving na te leven. Vanuit de optiek van het afsprakenstelsel is van belang dat voor een ieder die gebruikt maakt van elektronische toegangsdiensten duidelijk is:

1. wie welke verantwoordelijkheid heeft bij de verwerking van persoonsgegevens voor elektronische toegangsdiensten;
2. waar betrokkenen voor vragen over de verwerking van hun persoonsgegeven binnen het afsprakenstelsel terecht kunnen, en
3. dat de naleving van de privacy wet- en regelgeving door de verschillende partijen binnen het afsprakenstelsel ook daadwerkelijk plaats vindt en dit ook kan worden aangetoond.

Dit privacybeleid is opgesteld om ervoor te zorgen dat er sprake is van een aantoonbare rechtmatige verwerking van persoonsgegevens door de deelnemers binnen het afsprakenstelsel. Het doel van dit privacybeleid is drieledig:

1. Inzicht bieden in de verschillende verantwoordelijkheden die binnen het stelsel worden onderscheiden.
2. Een methodiek aanreiken voor de wijze waarop deelnemers binnen het afsprakenstelsel kunnen vastleggen hoe zij voldoen aan de voorwaarden die de privacywet- en regelgeving aan een rechtmatige verwerking van persoonsgegevens stelt.
3. Handvatten aanreiken die door partijen kunnen worden gebruikt om te waarborgen dat zij compliant zijn met de privacy wet- en regelgeving en om dat periodiek te kunnen aantonen.

Leeswijzer

- Beleidsuitgangspunten voor de naleving van de AVG — Het afsprakenstelsel kent de volgende generieke beleidsuitgangspunten voor de naleving van de AVG. Deze beleidsuitgangspunten volgen mede uit de AVG.
- Verantwoordelijkheden partijen afsprakenstelsel elektronische toegangsdiensten — In dit hoofdstuk wordt voor de verschillende in netwerk van het afsprakenstelsel elektronische toegangdiensten te onderscheiden partijen aangegeven wat hun rol is bij de verwerking van persoonsgegevens.
- Invulling voorwaarden voor rechtmatige verwerking — In dit hoofdstuk wordt, per beginsel zoals beschreven in de AVG, concreet aangegeven wat de deelnemers als verantwoordelijke voor de verwerking van persoonsgegevens dienen vast te leggen en te regelen om aan deze beginselen te voldoen.
- Controle op de naleving en privacy managementcyclus — Voor de controle van de naleving van de AVG wordt een aantal instrumenten gehanteerd

Beleidsuitgangspunten voor de naleving van de AVG

Het afsprakenstelsel kent de volgende generieke beleidsuitgangspunten voor de naleving van de AVG. Deze beleidsuitgangspunten volgen mede uit de AVG.

1. Deelnemers, Beheerorganisatie en BSNk, hierna genoemd partijen, zijn zelf verantwoordelijk voor het daadwerkelijk voldoen aan de AVG ongeacht hetgeen in dit beleid is aangegeven.
2. Partijen MOETEN processen ingericht hebben waarmee zij aantonen en waarborgen dat zij voldoen aan de bepalingen van de AVG. De processen hebben minimaal betrekking op:
    a. Inventarisatie en vastlegging van de verwerking van persoonsgegevens met daarbij aangegeven de doelbinding, de rechtmatigheidsgrondslag en de noodzaak voor de verwerking gezien het doel.
    b. Jaarlijkse uitvoering van een Privacy Self Assessment
    c. Het aantoonbaar opvolging geven aan de aanbevelingen die volgen uit een Privacy Impact Analyse.
    d. Waarborgen van de meldplicht datalekken in relatie tot het incidentmanagementproces van het stelsel,
    e. Waarborgen van de bepalingen uit de AVG zoals de informatieplicht en informatieverstrekking aan derden, rechten van betrokkenen en bewaartermijnen.
    f. Waarborgen dat de beveiliging van de verwerking en opslag van beveiliging van persoonsgegevens integraal onderdeel is van het management van de informatiebeveiliging van de organisatie conform het Beleid voor Informatiebeveiliging van het stelsel.
    g. Waarborgen van de juistheid van persoonsgegevens.
3. Partijen MOETEN een medewerker aanwijzen die contactpersoon is inzake de naleving van dit Privacybeleid.
4. Dit Privacybeleid maakt onderdeel uit van het Afsprakenstelsel en daarom MOETEN partijen aan de Toezichthouder van het stelsel de naleving ervan aantonen.

Verantwoordelijkheden partijen afsprakenstelsel elektronische toegangsdiensten

In dit hoofdstuk wordt voor de verschillende in netwerk van het afsprakenstelsel elektronische toegangdiensten te onderscheiden partijen aangegeven wat hun rol is bij de verwerking van persoonsgegevens.

Alle deelnemers van het afsprakenstelsel elektronische toegangsdiensten zijn 'verantwoordelijke' in de zin van de AVG voor de verwerking van de persoonsgegevens voor de rol waarvoor zij zijn toegetreden. Dit houdt in dat Deelnemers ook zelf verantwoordelijk zijn voor de implementatie en de naleving van de voorwaarden die de AVG aan een rechtmatige verwerking van persoonsgegevens stelt.

Naast de rol van 'verantwoordelijke' in de zin van de AVG, geldt specifiek voor de Authenticatiedienst dat zij ook 'bewerker' in de zin van de AVG is voor de verwerking van het BSN nummer. De Authenticatiedienst verwerkt het BSN nummer op basis van een bewerkersovereenkomst met de minister van BZK /BSNk.

De minister van BZK is de verantwoordelijke in de zin van de AVG voor deze verwerking van het BSN nummer door BSNk. De wettelijke basis voor verwerking van het BSN door BSNk is belegd in de wet Elektronisch Berichtenverkeer Belastingdienst en de daarbij behorende Ministeriële Regeling Voorziening GDI[1]. De Authenticatiedienst is verplicht de verwerkingen van persoonsgegevens in zijn hoedanigheid als 'verantwoordelijke' en 'bewerker' in de zin van de AVG strikt gescheiden te houden en zijn organisatie is hier op ingericht.

Voetnoten

1. De formele wettelijke basis voor de verwerking van het BSN door BSNk is artikel X van de Wet elektronisch bestuurlijk verkeer met de belastingdienst. Zie ook https://www.eerstekamer.nl/behandeling/20151028/publicatie_wet/document3/f=/vjyicpz4satc.pdf en artikel 4 van de Regeling Voorziening GDI https://zoek.officielebekendmakingen.nl/stcrt-2015-37158.html

Invulling voorwaarden voor rechtmatige verwerking

In dit hoofdstuk wordt, per beginsel zoals beschreven in de AVG, concreet aangegeven wat de deelnemers als verantwoordelijke voor de verwerking van persoonsgegevens dienen vast te leggen en te regelen om aan deze beginselen te voldoen.

Afbakening set van persoonsgegevens en doel van de verwerking

Om duidelijkheid te bieden over welke set van persoonsgegevens voor welke doeleinden mogen worden verwerkt voor het aanbieden van elektronische toegangsdiensten binnen het Afsprakenstelsel elektronische toegangsdiensten is hieronder een afbakening opgenomen die door de deelnemer kan worden vastgelegd.

Met deze afbakening van toegestane doeleinden en de set van persoonsgegevens die voor die doeleinden mogen worden verwerkt, wordt meer specifiek invulling gegeven aan het in de PIA (Mazars, Privacy Impact Assessement Introductieplateau, versie 1.0 d.d. 31 juli 2015) onderkende risico "function creep".

Hieronder is een afbakening van de toegestane concrete doelomschrijvingen en de hiervoor benodigde set van persoonsgegevens in het kader van het aanbieden van elektronische toegangsdiensten opgenomen. Deze doelomschrijving, inclusief de daarbij behorende rechtmatigheidsgrondslag(en) en set van persoonsgegevens zullen door de Deelnemers worden vastgelegd. Daarnaast is een concrete doelomschrijving voor de doeleinden 'Geschilbeslechting' en 'Klanttevredenheidsonderzoek' opgenomen.

Zowel de afbakening van de doelomschrijvingen als de set van persoonsgegevens moeten worden beschouwd als een voorzet. Het is uiteindelijk altijd aan de Deelnemer om te bepalen of hij van deze set van persoonsgegevens of doelomschrijving wenst af te wijken. Als een Deelnemer meer persoonsgegevens wil verwerken zal hij hiervoor wel de noodzaak moeten kunnen onderbouwen.

Authenticatiedienst als verwerker van het BSN

In het geval de Authenticatiedienst zijn diensten ook in het BSN domein aanbiedt - dat wil zeggen dat private authenticatiemiddelen worden ingezet voor het afnemen van elektronische diensten bij (overheids)organisaties die gerechtigd zijn het BSN te verwerken - wordt een verwerkersovereenkomst voor de verwerking van het BSN afgesloten. De Authenticatiedienst is in dit geval voor de verwerking van het BSN nummer een 'verwerker' in de zin van de AVG. De verwerkersovereenkomst wordt afgesloten tussen de minister van BZK als verantwoordelijke voor het BSNk en de Authenticatiedienst.

In deze verwerkersovereenkomst is onder meer opgenomen met welke doel het BSN door de Authenticatiedienst mag worden verwerkt en welke passende technische en organisatorische beveiligingsmaatregelen de authenticatiedienst ten aanzien van deze verwerking moet nemen.

De wettelijke basis voor de verwerking van het BSN door de minister van BZK in dit kader wordt voorzien in het "Besluit verwerking persoonsgegevens GDI"[1] ter uitvoering bij artikel X van de Wet elektronisch berichtenverkeer Belastingdienst.

De rechtmatigheidsgrondslag voor de verwerking van het BSN door de Authenticatiedienst als vewerker is de uitvoering van de verwerkersovereenkomst die hiervoor wordt afgesloten met de minister van BZK.

De rechtmatigheidsgrondslag voor de doorverstrekking van de persoonsgegevens door Authenticatiedienst aan het BSNk, in het geval de betrokkene bij registratie aangeeft het authenticatiemiddel ook in het publiek domein te willen gebruiken - te weten: voorletters, geslachtsnaam, geboortedatum en geboorteplaats, het pseudoID - geschiedt op basis van toestemming. Deze toestemming wordt al bij de registratie door de Authenticatiedienst aan de betrokkene gevraagd en vastgelegd[1].

Voetnoot

1. Het betreft het "Besluit houdende regels betreffende de verwerking van persoonsgegevens in de voorzieningen voor de generieke digitale infrastructuur DigiD, DigiD Machtigen, MijnOverheid en BSN-Koppelregister (Besluit verwerking persoonsgegevens GDI)".

Doelomschrijving Authenticatiedienst als verantwoordelijke

De persoonsgegevens worden verwerkt met als doel de authenticatie van betrokkene voor het afnemen van een elektronische toegangsdienst zoals vastgelegd in de dienstencatalogus van het Afsprakenstelsel elektronische toegangsdiensten op basis van het door betrokkene gebruikte authenticatiemiddel.

Gegevensset:

- voor identificatie benodigde gegevens, zoals NAW, geboortedatum, geboorteplaats, telefoonnummer(s), e-mailadres, bankrekeningnummer
- voor authenicatie benodigde gegevens, zoals NAW, geboortedatum, geboorteplaats, telefoonnummer(s), e-mailadres, bankrekeningnummer
- voor uitvoering van de overeenkomst benodigde gegevens, zoals registratiegegevens, registratietijdstip, pseudoniemen, transactiegegevens, loggingberichten



De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

Bewaartermijnen:

- Alle benodigde gegevens t.b.v. identificatie bij uitgifte middel en/of registratie machtiging: 7 jaar (na verlopen/intrekking middel/machtiging) tbv fraudeonderzoek en beslechting van geschillen (N.B.: hierbij wordt geen onderscheid gemaakt in het niveau van het middel of machtiging, immers het doel is hetzelfde);
- Gegevens betreffende authenticatie: 7 jaar tbv fraudeonderzoek.

Doelomschrijving Herkenningsmakelaar

De persoonsgegevens worden verwerkt met als doel het berichtenverkeer van en naar de dienstverleners die gebruik maken van het afspraken elektronische toegangsdiensten te ontkoppelen van de interne berichten binnen het netwerk en het routeren van deze berichten naar alle binnen het afsprakenstelsel elektronische toegangsdiensten erkende authenticatiediensten en machtigingenregisters.

Gegevensset:

- voor communicatie met de dienstverlener benodigde gegevens, zoals NAW, geboortedatum, geboorteplaats, telefoonnummer(s), e-mailadres
- voor uitvoering van de overeenkomst benodigde gegevens, zoals registratiegegevens, registratietijdstip, transactiegegevens, loggingberichten



De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

Doelomschrijving klanttevredenheidsonderzoek

De persoonsgegevens worden verwerkt met als doel een klanttevredenheidsonderzoek over de werking van de elektronische toegangsdienst.

Gegevensset

- E-mailadres
- Type elektronische toegangsdienst



De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

Doelomschrijving Machtigingenregister

De persoonsgegevens worden verwerkt met als doel het registreren, beheren, controleren van machtigen en andere bevoegdheden en het afleggen van verklaringen over bevoegdheden en het op verzoek van betrokkene verstrekken van machtigingsverklaringen.

Gegevensset:

- voor controle van de vertegenwoordigingsbevoegdheid benodigde gegevens, zoals KvK nummer, statutaire en handelsnaam van de onderneming; NAW, geboortedatum, geboorteplaats, telefoonnummer(s), e-mailadres, bankrekeningnummer van machtigingsverlener en van gemachtigde
- voor uitvoering van de overeenkomst benodigde gegevens, zoals registratiegegevens, registratietijdstip, pseudoniemen, bevoegdheidsregistratieID, bevoegdheidsgegevens (dienst, duur, omvang bevoegdheid), transactiegegevens, loggingberichten

De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

Bewaartermijnen:

- Alle benodigde gegevens t.b.v. identificatie bij uitgifte middel en/of registratie machtiging: 7 jaar (na verlopen/intrekking middel/machtiging) tbv fraudeonderzoek en beslechting van geschillen (N.B.: hierbij wordt geen onderscheid gemaakt in het niveau van het middel of machtiging, immers het doel is hetzelfde);
- Gegevens betreffende authenticatie: 7 jaar tbv fraudeonderzoek.

Doelomschrijving Middelenuitgever

De persoonsgegevens worden verwerkt met als doel de uitgifte van Authenticatiemiddelen conform de eisen van het gespecificeerde Betrouwbaarheidsniveau.

Gegevensset:

- voor uitgeven van het middel benodigde gegevens, zoals NAW, geboortedatum, geboorteplaats, telefoonnummer(s), e-mailadres, bankrekeningnummer en audio- en beeldmateriaal van de gebruiker;
- voor uitvoering van de overeenkomst benodigde gegevens, zoals registratiegegevens, audio- en beeldmateriaal van de gebruiker, registratietijdstip, pseudoniemen, transactiegegevens, loggingberichten.



De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

Bewaartermijnen:

- Alle benodigde gegevens t.b.v. identificatie bij uitgifte middel en/of registratie machtiging: 7 jaar (na verlopen/intrekking middel/machtiging) tbv fraudeonderzoek en beslechting van geschillen (N.B.: hierbij wordt geen onderscheid gemaakt in het niveau van het middel of machtiging, immers het doel is hetzelfde);
- Gegevens betreffende authenticatie: 7 jaar tbv fraudeonderzoek.

Transparantie

Als uitvloeisel van het Transparantiebeginsel is een deelnemer gehouden om de volgend maatregelen te nemen:

- Melding van verwerkingen van persoonsgegevens bij de Autoriteit Persoonsgegevens vervalt; hiervoor in de plaats stelt de AVG een registratieplicht voor verantwoordelijke en verwerker om zelf verwerkingen te registreren.
- Informatieverstrekking over de verwerking van persoonsgegevens.

De onderliggende procedures die door de deelnemers zullen moeten worden ingericht om aantoonbaar en controleerbaar invulling te kunnen geven aan het zorgvuldigheidsbeginsel zijn:

1. Naleving van de procedure derdeverstrekking.
2. Naleving van de informatieplicht over de verwerking van persoonsgegevens (procedure informatieverstrekking).

De navolgende informatie dient tenminste vanuit de deelnemer aan de betrokkene te worden verstrekt.

1. De identiteit van de verantwoordelijke
2. De doeleinden van de verwerkingen van persoonsgegevens
3. Welke categorieën persoonsgegevens hiervoor worden verwerkt
4. Aan welke derde(n) met welk doel de persoonsgegevens worden verstrekt
5. De rechten die tegen de verwerking van persoonsgegevens kunnen worden ingeroepen. Hier zal door de deelnemer ook moeten worden aangegeven op welke wijze deze rechten kunnen worden uitgeoefend. Dit betekent dat hier ook een procedure voor zal moeten worden ingericht. Zie hiervoor ook Verantwoordelijkheden partijen afsprakenstelsel elektronische toegangsdiensten. De de volgende elementen zullen duidelijk in deze procedure moeten worden vastgelegd:
    a. De wijze waarop een betrokkene een verzoek tot uitoefening van zijn recht kan indienen.
    b. Wie aanspreekpunt is voor de afhandeling van het verzoek.
    c. De wijze waarop de naleving van de wettelijke termijn van vier weken wordt gewaarborgd.

Deze informatie kan bijvoorbeeld worden verstrekt via een privacystatement op de website van de Deelnemer.

Zorgvuldigheid

Het zorgvuldigheidsbeginsel vloeit voort uit het beginsel van Doelbinding en houdt in dat een deelnemer maatregelen dient te nemen.

Het verdient aanbeveling de beveiliging van persoonsgegevens onderdeel te laten uitmaken van het informatiebeveiligingsbeleid.

De onderliggende procedures die door de deelnemers zullen moeten worden ingericht om aantoonbaar en controleerbaar aan het invulling te kunnen geven aan het zorgvuldigheidsbeginsel zijn:

1. Procedure naleving beveiligingsplicht. Indien er een wijziging in de verwerking van persoonsgegevens is, zal op basis van een risico analyse c.q. impactbepaling van deze wijzigingen voor de beveiliging van de persoonsgegevens worden uitgevoerd en zo nodig aanpassing van de beveiligingsmaatregelen. Indien van toepassing ook de overeengekomen beveiligingsmaatregelen in de vewerkersovereenkomst aanpassen.
2. Inpassing van de meldplicht datalekken in het informatiebeveiligingsbeleid en/of incidentmanagementproces dat in dit kader is ingericht.
3. Procedure kwaliteit. Op basis van deze procedure wordt ondervangen dat te veel ontvangen gegevens niet worden verwerkt, geen bovenmatigheid, alsmede een periodieke controle wordt ingevoerd op juistheid en actualiteit van de persoonsgegevens.
4. Procedure bewaartermijnen. Op basis van deze procedure wordt gecontroleerd op de duur van de opslag en de vernietiging van de gegevens op het moment dat de bewaartermijn is bereikt.

Doelbinding

Als uitvloeisel van het beginsel van doelbinding is een deelnemer gehouden om maatregelen te nemen.

De deelnemers moeten om aantoonbaar en controleerbaar aan het doelbindingsbeginsel invulling geven.

Controle op de naleving en privacy managementcyclus

Voor de controle van de naleving van de AVG wordt een aantal instrumenten gehanteerd:

Privacy Self Assessment

De Privacy Self Assessment wordt jaarlijks door de deelnemers zelf uitgevoerd. De uitkomsten van deze PSA worden door de deelnemers aan de Toezichthouder verstrekt. De Toezichthouder controleert of de PSA door de Deelnemer is gehouden.

Privacy Impact Analyse

De Privacy Impact Analyse wordt een onderdeel van de Stelselrisicoanalyse van het afsprakenstelsel. Om hieraan invulling te geven wordt in de Stelselrisicoanalyse een overzicht opgenomen met de geïdentificeerde risico's uit de PIA. Dit zorgt ervoor dat deze privacyrisico's worden meegenomen tijdens het normale proces van herijken van de Stelselrisicoanalyse die tenminste jaarlijks, of bij een belangrijke stelselwijziging - zoals nieuwe functionaliteit of doelgroep plaatsvindt.

Privacy managementcyclus

De controle van de deelnemers op de naleving van de privacy wet- en regelgeving vindt enerzijds plaats via de ISO27001-certificatie op basis waarvan aantoonbaar moet zijn dat wordt voldaan aan de privacy wet- en regelgeving. Anderzijds wordt de controle op de naleving gewaarborgd door middel van de naleving van het privacybeleid op basis waarvan de deelnemers vastleggen welke verwerkingen van persoonsgegevens plaatsvinden, alsmede hierover ook jaarlijks zelf een Privacy Self Assessment uitvoeren waarover zij rapporteren aan de Toezichthouder. Het toezicht op de naleving van de privacy wet- en regelgeving en de verantwoording over de uitvoering hiervan door de deelnemers ligt hiermee bij de Toezichthouder.

Gemeenschappelijk normenkader informatiebeveiliging

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Legenda

Afkorting	Betekenis
v	Vanuit het afsprakenstelsel is er geen nadere specificatie van de norm gegeven. Deelnemers, BSNk en de Beheerorganisatie baseren de keuze van maatregelen op hun uitgevoerde risicoanalyse. In deze risicoanalyse moeten de gegeven risico's op stelselniveau wel worden meegewogen. De norm c.q. beheersmaatregel maakt geen verplicht onderdeel uit van de VvT van de deelnemers en Beheerorganisatie.
S	Vanuit het afsprakenstelsel zijn er nadere specificaties voor de norm gegeven. Er wordt verwezen naar een document of er wordt om speciale aandacht gevraagd. De norm c.q. beheersmaatregel maakt onderdeel uit van de VvT van de Deelnemers, BSNk en Beheerorganisatie.
Sv	De norm is vanuit stelseloptiek relevant, maar er is geen nadere specificatie van de norm gegeven. Dit betekent dat de norm onderdeel uit maakt van de VvT van het ISMS van de Deelnemers, BSNk en Beheerorganisatie of dat er argumenten zijn waarom deze norm vanuit de rol of dienstverlening in het kader van het stelsel niet van toepassing is voor de Deelnemers, BSNk of de Beheerorganisatie. Deze argumenten dienen in relatie tot de VvT controleerbaar te worden vastgelegd en onderdeel gemaakt van het auditdossier.

ISO 27001:2013 beheersdoelstellingen en beheersmaatregelen binnen de scope van eToegangsdiensten, - activiteiten, -objecten en -informatie

Norm	Titel	Doelstellingen en beheersmaatregelen	Deelnemer	BSNk	BO	Opmerkingen	Toelichting en referenties
A.5	**Informatiebeveiligingsbeleid**						
A.5.1	Aansturing door de directie van de informatiebeveiliging	Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.					
A.5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Sv	Sv	Sv	Iedere deelnemer, BSNk en de BO stelt een eigen beleidsdocument voor informatiebeveiliging op waarin rekening wordt gehouden met het beleidsdocument voor informatiebeveiliging dat voor het Netwerk c.q. het stelsel van Elektronische Toegangsdiensten is opgesteld.	De beheerorganisatie beheert het Beleid voor informatiebeveiliging namens het Stelsel.
A.5.1.2	Beoordelen van het informatiebeveiligingsbeleid	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Sv	Sv	Sv	Deelnemers, BSNk en de BO beoordelen regelmatig de werking van het informatiebeveiligingsbeleid en leveren hierover input t.b.v. de beoordeling op stelselniveau.	Beleid voor informatiebeveiliging wordt periodiek beoordeeld met input van de Toezichthouder, de deelnemers, BSNk en de BO.
A.6	**Organiseren van informatiebeveiliging**						
A.6.1	Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.					-
A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Sv	Sv	S		Beheerorganisatie coördineert t.b.v. het stelsel. Concreet door toewijzing van de rollen van security officer, riskmanager en incidentmanager.
A.6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Sv	v	v	Voor MU al standaard bij PKI. Zo mogelijk moet functiescheiding worden toegepast. Waar dit voor kleine organisaties niet mogelijk is moeten compenserende maatregelen worden genomen (bijv. audit trails).	Zwaarte van de maatregelen moet in relatie staan tot de geleverde betrouwbaarheidsniveaus van de dienst. Deelnemers, BSNk en BO richten dit naar eigen inzicht in.
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	v	v	S	Stelseltaak voor BO	De BO onderhoudt op stelselniveau contact met relevante overheidsinstanties.
A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	v	v	S	Stelseltaak voor BO	De BO onderhoudt contact met speciale groepen of fora zoals bij Europese ontwikkelingen (eIDAS) en het NCSC specifiek voor informatiebeveiliging.
A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.

		project.					
A.6.2	Mobiele apparatuur en telewerken	Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.				Mogelijk ontstaat vanuit bestaande normenkaders (hogere betrouwbaarheidsniveaus) een beperking op de mogelijkheid om werkzaamheden via mobiele apparatuur uit te voeren.	Indien draagbare computers en communicatievoorzieningen ten behoeve van het verlenen van stelseldiensten of stelselbeheer worden toegestaan MOETEN passende maatregelen te worden genomen.
A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7	**Veilig personeel**						
A.7.1	Voorafgaand aan het dienstverband	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.					
A.7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	S	S	S	Uit de risicoanalyse (bijv. via "misbruik-scenario's") kan blijken dat per rol en evt. per betrouwbaarheidsniveau onderscheid moet worden gemaakt in het niveau van screening.	1. De wijze en diepgang van de screening moet zijn gerelateerd aan de bevoegdheden en taakstelling van de betreffende medewerker. Zo mag worden verwacht dat de screening voor een systeembeheerder met speciale bevoegdheden ten aanzien van systeemprogrammatuur strenger zal zijn dan voor een ondersteunende stafmedewerker. 2. Basis niveau van screening: Het basisniveau van screening voor alle personeel, moet bestaan uit: a. Het controleren van de juistheid van de identiteit (WID-document); b. Controleren van de juistheid van gegevens in het curriculum vitae en met name van opleidingsgegevens; c. Controleren van relevante referenties. 3. Screening van vast personeel t.b.v. het Stelsel: a. Medewerkers die met activiteiten voor EID zijn belast moeten een Verklaring Omtrent Gedrag (VOG) aanvragen c.q. overleggen in relatie tot de omgang van gegevens waarbij integriteit en vertrouwelijkheid van belang zijn. b. De (originele of digitale kopie) VOG moet worden opgenomen in het personeelsdossier of digitale registratie. c. In het geval een zwaardere screening aantoonbaar al reeds heeft plaatsgevonden mag de

							deelnemer of beheerorganisatie besluiten om de VOG achterwege te laten. Zwaarder dan een VOG zijn bijvoorbeeld: veiligheidsonderzoek door de AIVD (A, B of C onderzoek) of de MIVD, antecedentenonderzoek door een erkend onderzoeksbureau. 4. Screening van tijdelijk personeel: a. Deze screeningprocedure voor intern personeel is ook van toepassing op van externe leveranciers ingehuurd personeel. b. De eisen die aan ingehuurd personeel worden gesteld worden moeten van het zelfde niveau zijn als de eisen aan het vaste personeel; In het contract met de leverancier moet zijn opgenomen: i. welke verantwoordelijkheden deze heeft ten aanzien van het screeningproces en; ii. de verplichting daarover om direct de opdrachtgever te informeren als de screening van een in te zetten of ingezette medewerker niet (volledig) heeft plaatsgevonden of tot een negatief resultaat heeft geleid. 5. De organisatie (deelnemer, BSNk, BO) moet een functionaris aanwijzen die verantwoordelijk is voor het laten uitvoeren van het screeningproces. In veel gevallen ligt deze verantwoordelijkheid bij een securityofficer of een risk manager. 6. De werkgever moet de medewerker verzoeken om een VOG aan te vragen. a. In de aanvraag moet de werkgever aangeven wat de aard van

							het werk is dat de medewerker gaat uitvoeren. b. De werkgever heeft expliciet beleid geformuleerd dat er zorg voor moet dragen dat gedurende het dienstverband van de medewerker de integriteit en betrouwbaarheid aantoonbaar geborgd is. 7. Het screeningsproces moet worden doorlopen voor elk personeelslid (vast of ingehuurd): a. Bij indiensttreding. b. Ingeval van een bestaand dienstverband als de screening nog niet heeft plaatsgevonden of is verlopen. c. Bij verandering van functie of werkgebied van een medewerker als de nieuwe werkzaamheden meer omvatten of in hoge mate afwijken van de vroegere werkzaamheden.
A.7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Sv	Sv	Sv	Bijv. in de vorm van een ondertekend arbeidscontract of vergelijkbaar alternatief.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.2	Tijdens het dienstverband	Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.					
A.7.2.1	Directieverantwoordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Sv	Sv	Sv	Management dient personeel dat een taak /activiteit verricht ten behoeve van een rol in het stelsel, o.m. op de hoogte te stellen van de relevante eisen uit het afsprakenstelsel en bijbehorende procedures	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.2.3	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Sv	Sv	Sv	Voor deelnemers, BSNk en Beheerorganisatie is de maatregel bedoeld voor werknemers die inbreuk op de beveiliging hebben gepleegd. Iedere organisatie binnen het stelsel bepaalt zelf of daartoe een formeel disciplinair proces moet worden vastgesteld.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.3	Beëindiging en wijziging van dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.					Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.8	**Beheer van bedrijfsmiddelen**						
A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.					
A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Sv	Sv	Sv	Het stelsel beschikt niet over gemeenschappelijke bedrijfsmiddelen.	Vooralsnog zijn er geen gemeenschappelijke bedrijfsmiddelen onderkend. Indien dit wel het geval zou worden, is de Beheerorganisatie verantwoordelijk voor het bijhouden van de inventarisatie.
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het	v	v	v		idem

		inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.					
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	v	v	v		idem
A.8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	v	v	v		idem
A.8.2	Informatieclassificatie	Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.					
A.8.2.1	Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	S	S	S	Deelnemers, BSNk en BO moeten een eigen classificatie van hun informatie hebben gebaseerd op de richtlijnen voor classificatie van informatie uit het Informatiebeveiligingsbeleid, de stelselrisicoanalyse en hun eigen risicoanalyse.	Zie Afspraken Gemeenschappelijke Classificatie van Stelselinformatie
A.8.2.2	Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Sv	Sv	S		idem
A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	v	v	v	Het stelsel Elektronische Toegangsdiensten beschikt niet over gemeenschappelijke bedrijfsmiddelen.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.8.3	Behandelen van media	Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.					
A.8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Sv	Sv	Sv	-	Alleen specifiek: Deelnemers, BSNk en BO moeten ten minste een procedure inrichten voor voor zorgvuldig beheer van verwijderbare media die drager zijn van persoonsgegevens en metagegevens.
A.8.3.2	Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Sv	Sv	Sv	Media waar archiveringsgegevens zijn opgeslagen. Media waar persoonsgegevens zijn opgeslagen. Media waar metadata is opgeslagen.	De BO is verantwoordelijk voor het verwijderen van media binnen de eigen organisatiecontext en op het niveau van het stelsel. Deelnemers en BSNk zijn verantwoordelijk voor het verwijderen media binnen de eigen organisatie context.
A.8.3.3	Media fysiek overdragen	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Sv	Sv	Sv	idem	idem
A.9	**Toegangsbeveiliging**						
A.9.1	Bedrijfseisen voor toegangsbeveiliging	Toegang tot informatie en informatieverwerkende faciliteiten beperken.					
A.9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	S Sv	S Sv	S Sv	Specificatie (S) bedoeld voor de registratie van externe gebruikers i.c. bedrijven /klanten van deelnemers. Voor interne gebruikers (medewerkers van deelnemers) bepaalt de deelnemers zelf de invulling (Sv).	Toegangsbeveiligingsbeleid moet in overeenstemming met: 1. de classificatie van informatie voor stelselinformatie en 2. de betrouwbaarheidsniveaus van stelseldiensten t.b.v. gebruikers van stelseldiensten. Zie voor 1) Beleid voor informatiebeveiliging Zie voor 2) Normenkader betrouwbaarheidsniveaus
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	S Sv	S Sv	S Sv	idem	Zie Normenkader betrouwbaarheidsniveaus
A.9.2	Beheer van toegangsrechten van gebruikers	Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.				Op stelselniveau gaat het om de registratie van gebruikers van stelselsystemen: Confluence, Mantis, Metadata, Dienstencatalogus, Managementinformatie, Simulator.	
A.9.2.1	Registratie en uitschrijving van gebruikers	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	S Sv	S Sv	S Sv	Specificatie (S) bedoeld voor de registratie van externe gebruikers i.c. bedrijven /klanten van deelnemers. Voor interne gebruikers (medewerkers van deelnemers) bepaalt de deelnemers zelf de invulling (Sv).	Met name voor MU, MR: Procesbeschrijvingen en registratie moeten voldoen aan de beschrijving van de betrouwbaarheidsniveaus voor het verkrijgen van authenticatiemiddelen en registraties van machtigingen.
A.9.2.2	Gebruikers toegang verlenen	Een formele gebruiker-toegangsverleningsprocedure moet	Sv		Sv		

		worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken					
A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Sv	Sv	Sv		
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	Sv	Sv	Sv		
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Sv	Sv	Sv		
A.9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Sv	Sv	Sv		
A.9.3	Gebruikersverantwoordelijkheden	Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.					
A.9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Sv	Sv	Sv		Gebruikers worden geacht een goede beveiligingspraktijk te hanteren bij het selecteren en gebruik van wachtwoorden. Zie Gebruiksvoorwaarden Elektronische Toegangsdiensten
A.9.4	Toegangsbeveiliging van systeem en toepassing	Onbevoegde toegang tot systemen en toepassingen voorkomen.					
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Sv	Sv	Sv		
A.9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Sv	Sv	Sv		
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Sv	Sv	Sv		Specifiek voor MU: Voor authenticatiemiddelen in het stelsel Zie Normenkader betrouwbaarheidsniveaus
A.9.4.4	Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.10	**Cryptografie**						
A.10.1	Cryptografische beheersmaatregelen	Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.					
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	S	S	S		Conform Information security requirements
A.10.1.2	Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Sv	Sv	Sv		Conform Information security requirements
A.11	**Fysieke beveiliging en beveiliging van de omgeving**						**Deelnemers en BO vullen dit naar eigen inzicht in.**
A.11.1	Beveiligde gebieden	Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.					
A.11.1.1	Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	v	v	v		
A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	v	v	v		
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	v	v	v		
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	v	v	v		

A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	v	v	v		
A.11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	v	v	v		
A.11.2	Apparatuur	Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.					
A.11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	v	v	v		
A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	v	v	v		
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	v	v	v		
A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	v	v	v		
A.11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	v	v	v		
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	v	v	v		
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	Sv	Sv	Sv	Belangrijk hierbij is dat wanneer apparatuur wordt verwijderd/hergebruikt of anderszins er gecontroleerd moet worden dat gevoelige gegevens (bijv. persoonsgegevens, metagegevens, routeringstabellen, etc.) onleesbaar worden gemaakt.	
A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Sv	Sv	Sv		
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Sv	Sv	Sv		
A.12	**Beveiliging bedrijfsvoering**						
A.12.1	Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.					
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Sv	Sv	S		Specifiek voor BO: De BO beheert de procedures, instructies, e.d. die betrekking hebben op het Stelsel.
A.12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	S	S	S		Specifiek voor BO: Alle wijzigingen op het Stelsel worden behandeld conform Proces change en release
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	S	S	S	Maatregel moet gezien worden in het kader van de Service Level afspraken.	Conform Service level
A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	S	S	S	BO is verantwoordelijk voor de coördinatie van de (keten)testen bij wijzigingen en van nieuwe toetreders in het netwerk met behulp van de simulatie-/testtool.	Conform Operationeel handboek en Service level. Het Stelsel hanteert een O, TA en P omgeving en een pre-productie omgeving. Voor de beschikbaarheid en inrichting van het testnetwerk zijn eisen gesteld.
A.12.2	Bescherming tegen malware	Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.					
A.12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Sv	Sv	Sv	Iedere organisatie neemt adequate maatregelen tegen virussen en malware. Bij 'doorbraken' dient onderzocht te worden wat de impact op het netwerk c.q. stelsel is.	
A.12.3	Back-up	Beschermen tegen het verlies van gegevens.					
A.12.3.1	Back-up van informatie	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Sv	Sv	Sv	Back-up strategie moet minimaal de SLA ondersteunen. Additioneel afspraken over:	

						• "dienst" zoals benoemd in SLA: inclusief gegevens die met de dienst beheerd worden, • maximaal dataverlies • afspraken m.b.t. classificatie van gegevens hebben tevens betrekking op de back-up	
A.12.4	Verslaglegging en monitoren	Gebeurtenissen vastleggen en bewijs verzamelen.					
A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	S	S	S	Deze maatregel omvat het loggen van transacties, incidenten, foutmeldingen e.d.	Conform Beleid voor informatiebeveiliging en 1. Elke Deelnemer en BSNk moet het volledige HTTP bericht van binnenkomende communicatie als gevolg van Elektronische Toegangsdiensten loggen. Elke Deelnemer en BSNk moet alle uitgaande SAML berichten loggen. 2. Een Deelnemer en BSNk moet op basis van logging inzicht kunnen geven in het totaal aantal geslaagde transacties (succesvolle responses op verstuurde requests) en het totaal aantal foutieve transacties (requests zonder response of met een foutmelding als response) in een periode. 3. Elke Deelnemer en BSNk moet alle door haar ondertekende en alle door haar ontvangen ondertekende berichten minimaal 7 jaar archiveren. Na deze periode moeten ten minste de in deze berichten voorkomende persoonsgegevens vernietigd worden tenzij noodzaak kan worden aangetoond om deze langer te bewaren 4. Authenticatiediensten moeten bij de gearchiveerde berichten een referentie naar het gebruikte middel opslaan, zodat de audit trail naar de gebruiker sluitend wordt. 5. Machtigingenregisters moeten bij de gearchiveerde berichten een referentie naar de geregistreerde bevoegdheid waarop de verklaring van bevoegdheid berust opslaan, zodat de audit trail naar de machtigingsverlener sluitend wordt. 6. Authenticatiediensten en Machtigingenregisters moeten bewijsstukken die zijn gebruikt bij uitgifte/registratie van middelen of machtigingen 7 jaar archiveren zodat de audittrail naar gebruiker of machtingsverlener sluitend wordt, tenzij beargumenteerd wordt waarom dit niet wordt gearchiveerd
A.12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Sv	Sv	Sv	Dient aan te sluiten op de vereiste historie voor b.v. fraudeonderzoek (geen relatie met archivering), b.v. passend bij 6 maanden periode voor terugzoeken transacties en handelingen op kritieke systemen	Elke deelnemer en BSNk moet logging beveiligd opslaan en moet deze alleen toegankelijk maken voor bevoegde personen. Een deelnemer mag logging niet verwijderen binnen de verplichte bewaartermijn.
A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht

		logbestanden moeten worden beschermd en regelmatig worden beoordeeld.					in, maar moet wel in VvT.
A.12.4.4	Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	S	S	v	Noodzakelijk voor goede berichtenafhandeling, er dient een eenduidige tijdsbron te worden gedefinieerd en gebruikt	Conform Interface specifications. Afspraken omtrent tijdsynchronisatie zijn opgenomen in Synchronize system clocks.
A.12.5	Beheersing van operationele software	De integriteit van operationele systemen waarborgen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in
A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software en moeten procedures worden geïmplementeerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.12.6	Beheer van technische kwetsbaarheden	Benutting van technische kwetsbaarheden voorkomen.					
A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Sv	Sv	S	Er wordt een hoog niveau van beveiliging verwacht. Specifiek wordt van de deelnemer verwacht dat deze zelf de ontwikkelde informatiesystemen test op alle bekende technische kwetsbaarheden in de broncode (test/audittools) en werking van het informatiesysteem (penetratietesten). Daarnaast dient conform de afspraken in het afsprakenstelsel periodiek, op initiatief van de beheerorganisatie, een penetratietest te worden uitgevoerd op het netwerk en de specifieke systemen van een deelnemer en het BSNk.	1. De deelnemers, BSNk en de beheerorganisatie moeten ten minste tweemaal per jaar een penetratietest laten uitvoeren. 2. In het geval dat de beheerorganisatie penetratietesten organiseert ten behoeve van het stelsel dan moeten deelnemers en BSNk hier aan meewerken.
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.12.7	Overwegingen betreffende audits van informatiesystemen	De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.					
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Sv	Sv	S		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT. BO beheert de auditeisen i.e. normenkaders.
A.13	**Communicatiebeveiliging**						
A.13.1	Beheer van netwerkbeveiliging	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen				Beveiligen van verbindingen en ondertekenen van berichten MOET gebeuren conform de specificaties in de koppelvlakbeschrijvingen	
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	S	S	S	Netwerkverkeer tussen deelnemers onderling, tussen deelnemers en dienstverleners en tussen deelnemers en dienstafnemers.	Conform Interface specifications
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	S	S	S	Beheerorganisatie is verantwoordelijk voor doorvertaling maatregelen naar onderlinge afspraken in het afsprakenstelsel. Let ook op doorvertaling naar onderaannemers van de deelnemers.	Conform Interface specifications en BSNk mag uitsluitend pakketten die van trusted IP-adressen komen (white listing) accepteren.
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.13.2	Informatietransport	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.					
A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	S	S	S		Conform Information security requirements. Beleid, procedures en afspraken met betrekking tot de uitwisseling van informatie en programmatuur tussen Deelnemers, BSNk en BO is vastgelegd in het Afsprakenstelsel.
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	S	S	S		Betreft uitwisseling van informatie en programmatuur tussen deelnemers, BSNk en BO.
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	S	S	S		Conform Interface specifications
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Sv	Sv	Sv	Uit risico-analyse zal moeten blijken dat toegang tot bepaalde gegevens extra aandacht voor of eisen ten aanzien van de geheimhoudingsplicht zal vereisen.	Het betreft tenminste die gegevens die persoons- en bedrijfsgevoelige elementen bevatten zoals: • bij MU: registaties van personen en middelen, • bij AD: persistent pseudoniem, authenticatiecredentials

							• bij MR: registraties van personen, bedrijven en machtigingen • bij BSNk: BSN en persistent pseudoniem • bij BO: commerciële informatie deelnemers, metagegevens. Geheimhoudingsovereenkomsten (non-disclosure agreements) worden geacht de eisen ten aanzien van deze gegevens te reflecteren of te omvatten. Het is niet noodzakelijk om betreffende gegevens expliciet in de geheimhoudingsverklaring op te nemen.
A.14	**Acquisitie, ontwikkeling en onderhoud van informatiesystemen**						
A.14.1	Beveiligingseisen voor informatiesystemen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.					
A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT.
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoerings diensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Sv	Sv	S		BO is verantwoordelijk voor het beheer van de openbaar beschikbare informatie van het Stelsel. Van belang is bijv dat informatie over het stelsel juist is en consistent is met de informatie die deelnemers openbaar maken.
A.14.1.3	Transacties van toepassingsdiensten beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	S	S	S	Implementatie conform de relevante koppelvlakspecificaties.	Conform Interface specifications, waarbij te allen tijde een of meerdere versies geïmplementeerd dienen te zijn die door het afsprakenstelsel zijn toegestaan.
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.					
A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in, maar moet wel in VvT.
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	S	S	S		Conform Proces change en release.
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Sv	Sv	Sv	Van belang voor betrouwbaarheid netwerk. Specifiek wordt van Deelnemers, BSNk en Beheerorganisatie een zorgvuldig proces verwacht ten aanzien van wijzigingen in relatie tot de andere partijen en adequaat patch- en updatebeleid.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	S	S	S		Conform Proces change en release. Restricties kunnen volgen uit de besluiten van het Tactisch Beraad.
A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.7	Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Sv	Sv	Sv	Bij uitbesteding van ontwikkelwerkzaamheden aan een onderaannemer, dienen de stelselspecifieke eisen ten aanzien van het te ontwikkelen product doorvertaald te worden naar de onderaannemer.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Sv	Sv	Sv	Bij uitbesteding van ontwikkelwerkzaamheden aan een onderaannemer, dienen de stelselspecifieke eisen ten aanzien van het te ontwikkelen product doorvertaald te worden naar de onderaannemer.	Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	S	S	S	Bij wijzigingen, onderhoud en verstoringen dienen stelselspecifieke afspraken gevolgd te worden.	Conform Operationeel handboek

A.14.3	Testgegevens	Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.					
A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Sv	Sv	S		Conform Testing.
A.15	**Leveranciersrelaties**						
A.15.1	Informatiebeveiliging in leveranciersrelaties	De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.					
A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	v	v	v		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Sv	Sv	Sv	Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke (beveiligings)eisen doorvertaald te worden, de opdrachtgever (deelnemer, BSNk,BO) blijft verantwoordelijk.	Iedere overeenkomst met een derde moet een paragraaf/onderdeel te bevatten met eisen ten aanzien van informatiebeveiliging. Deze eisen moeten zijn gebaseerd op een risicoanalyse.
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	Sv	Sv	Sv	Bij uitbesteding (deel) van de rol/activiteiten aan een onderaannemer, dienen de stelselspecifieke (beveiligings)eisen doorvertaald te worden, de opdrachtgever (deelnemer, BSNk,BO) blijft verantwoordelijk.	Iedere overeenkomst met een derde moet een paragraaf/onderdeel te bevatten met eisen ten aanzien van informatiebeveiliging m.b.t. de toeleveringsketen. Deze eisen moeten zijn gebaseerd op een risicoanalyse.
A.15.2	Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.					
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Sv	Sv	Sv		Deelnemers, BSNk en BO vullen dit naar eigen inzicht in.
A.16	**Beheer van informatiebeveiligingsincidenten**						
A.16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.					
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	S	S	S	Er dient per deelnemer en voor BSNk een contactpersoon te zijn voor coördinatie van beveiligingsincidenten. De centrale coördinatie wordt gedaan door de beheerorganisatie.	Conform Proces incidentmanagement.
A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	S	S	S	-	Conform Proces incidentmanagement.
A.16.1.6	Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	S	S	S	Iedere organisatie dient de beveiligingsincidentregistraties en -rapportages te evalueren op trends en verbeterpunten	Periodiek moeten trend-analyses van incidenten worden gemaakt en besproken in het security officers overleg bestaande uit de de security officers van deelnemers, BSNk en BO. Indien mogelijk en beschikbaar deelt de BO de analyses van het NCSC met de deelnemers.
A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	S	S	S	Bij aanleiding tot onderzoek (intern het stelsel of op verzoek van opsporingsinstanties) dient relevante informatie voor een transactie door de keten van de deelnemers heen verzameld te kunnen worden.	Conform Beleid voor informatiebeveiliging.

A.17	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
A.17.1	Informatiebeveiligingscontinuïteit	Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.					
A.17.1.1	Informatiebeveiligingscontinuïteit	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Sv	Sv	S	Alle Rollen (inclusief BSNk) en BO: Bedrijfscontinuïteit is van belang voor het imago van het netwerk. In te vullen n.a.v. risicoanalyse voor het halen van de service levels. Ook aandacht besteden aan maatregelen voor herstel van de dienstverlening na een calamiteit.	Deelnemers, BSNk en de BO moeten maatregelen nemen op basis van een risicobeoordeling en de SLA. Hierbij moet rekening worden gehouden met processen die zijn uitbesteed processen. Op stelselniveau moet de bedrijfscontinuïteit worden gemonitord door de BO.
A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Sv	Sv	S	Stelseltaak voor BO	Conform Service level
A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Sv	Sv	S	Stelseltaak voor BO	Conform Service level
A.17.2	Redundante componenten	Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.					
A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Sv	Sv	Sv	-	Conform Service level. De BO moet de mate van redundantie van rollen in het Stelsel monitoren.
A.18.	**Naleving**						
A.18.1	Naleving van wettelijke en contractuele eisen	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.					
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Sv	Sv	Sv	-	Conform Juridisch kader. Deelnemers, BSNk en BO moeten zelf een overzicht vast te stellen van toepasselijke wetgeving en contractuele eisen.
A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Sv	Sv	Sv		Deelnemers, BSNk en BO dienen dit zelf in te vullen. De Eigenaar van het stelsel moet de verantwoordelijkheid nemen voor borging van de IPR betreffende stelselbrede rechten zoals het merkenrecht.
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Sv	Sv	Sv	Beschermingsniveau afhankelijk van classificatie.	Conform Juridisch kader en Operationeel handboek
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Sv	Sv	Sv	Er behoort door de Deelnemers, BSNk en de BO een beleid voor bescherming van persoonsgegevens te worden ontwikkeld en ingevoerd. Dit beleid behoort te worden gecommuniceerd naar alle personen die betrokken zijn bij het verwerken van persoonsgegevens.	Conform Privacybeleid en Normenkader betrouwbaarheidsniveaus. En specifiek betreft dit het omgaan met persoonsgegevens i.c. het gebruik van pseudoniemen binnen het netwerk.
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	S	S	S	-	Conform Juridisch kader en Interface specifications.
A.18.2	Informatiebeveiligingsbeoordelingen	Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.					
A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	S	S	S	Voor de deelnemers, het BSNk en de Beheerorganisatie gaat het om het laten uitvoeren van (interne en externe) audits en reviews. Onderdeel van de ISO 27001 certificering is het periodiek/jaarlijks uitvoeren van een controleaudit door de certificerende organisatie.	1. De beheersmaatregelen uit dit document moeten door deelnemers (afhankelijk van hun rol(len) in het stelsel) in hun individuele VvT worden opgenomen. a. Verplichte maatregelen uit het Gemeenschappelijk normenkader informatiebeveiliging mogen niet ontbreken

								in de VvT. Voor dit type maatregel zijn er op stelselniveau reeds uitwerkingen vastgesteld zoals koppelvlakspecificaties, operationeel handboek en procedure- en procesbeschrijvingen. b. Overige gemeenschappelijke maatregelen zijn maatregelen die de deelnemer of beheerorganisatie vanuit zijn rol zou moeten nemen. De deelnemer mag de beheersmaatregel 'niet van toepassing' verklaren maar in dat geval moet deze uitsluiting met argumenten zijn omkleed in de VvT. 2. Deelnemers moeten binnen 3 maanden na vaststelling van de bijstelling van het Gemeenschappelijk normenkader informatiebeveiliging deze hebben geïmplementeerd tenzij het Tactisch Beraad anders besluit. 3. Deelnemers die voor het eerst willen toetreden en de genoemde certificaten of TPM's nog niet kunnen overleggen moeten om te worden toegelaten: • zelf verklaren dat zij aan de materiële eisen van ISO 27001 (inclusief het Gemeenschappelijk Normenkader) voldoen, alsmede aan de gestelde eisen voor de dienstverlening van de betrouwbaarheidsniveaus die geleverd gaan worden. • voorbereidingen in gang hebben gezet voor de ISO 27001 certificatie en /of een TPM van het managementsysteem voor informatiebeveiliging, zoals bedoeld in ISO 27001, alsook de specifieke eisen die zijn gesteld aan de betrouwbaarheidsniveaus van de te leveren diensten. • een risicoanalyse overleggen die op de Elektronische Toegangsdiensten betrekking heeft (en de Stelselrisicoanalyse als input heeft) met daarin aangegeven de reeds

							genomen, nog te nemen maatregelen en de restrisico's. • een GAP-analyse overleggen waarin ten opzichte van het Gemeenschappelijk normenkader informatiebeveiliging is aangegeven welke maatregelen reeds zijn geïmplementeerd en welke maatregelen nog moeten worden geïmplementeerd. 4. De Beheerorganisatie moet per deelnemer bijhouden welke versie van het normenkader van toepassing was bij de audits in het kader van certificering of TPM.
A.18.2.2	Naleving van beveiligingsbeleid en -normen	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Sv	Sv	S	Opstellen en uitvoeren van een controleplan op basis waarvan procedures regelmatig worden gecontroleerd op naleving.	De Deelnemers, BSNk en BO moeten de naleving van informatiebeveiliging kunnen aantonen. De Toezichthouder op het stelsel toetst de naleving van Stelselafspraken door Deelnemers, BSNk en BO.
A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Sv	Sv	S	Opstellen en uitvoeren van een controleplan op basis waarvan informatiesystemen regelmatig worden gecontroleerd op de implementatie van beveiligingsstandaards.	Conform Operationeel handboek. De beheersmaatregel op stelselniveau betreft het (laten) uitvoeren van security assessments zoals pentesten en code reviews.

Normenkader betrouwbaarheidsniveaus

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

Beschrijft de wijze waarop authenticatiemiddelen en machtigingen geclassificeerd worden op betrouwbaarheidsniveau en de normen die daarbij worden toegepast.

eIDAS

Dit normenkader volgt in Technische specificaties en procedures voor uitgifte van authenticatiemiddelen de paragraaf-indeling van de Europese eIDAS uitvoeringsverordening EU 2015/1502. De reden is dat deze structuur het vergemakkelijkt om aan te tonen dat het afsprakenstelsel voldoet aan de in Europees verband gestelde normering. De Uitvoeringsverordening bevat het Europese framework van eisen voor de aanbieders van authenticatiediensten en de betrouwbaarheid van de ingezette authenticatiemiddelen en bijbehorend authenticatiemechanisme. Onderdeel van het Europese framework zijn ook eisen voor onderwerpen zoals privacy, aansprakelijkheid of gebruiksvoorwaarden etc. die in andere delen van het afsprakenstelsel Elektronische Toegangsdiensten zijn uitgewerkt zoals het hoofdstuk Juridica en het Operationeel handboek. Het uitgangspunt van het afsprakenstelsel is om eisen slechts op één plaats vast te leggen. Daar waar dat van met het oog op de oorspronkelijke eIDAS eis belang is, wordt in dit Normenkader Betrouwbaarheidsniveaus dus naar andere delen van het afsprakenstelsel verwezen.

Het eIDAS framework heeft een tweetal specifieke subparagrafen opgenomen die betrekking hebben op uitgifte van authenticatiemiddelen aan rechtspersonen. Nieuw is daarom ten opzichte van de vorige versie van dit normenkader dat een deel van de eisen voor Machtigingenregisters die betrekking hebben op de identificatie van rechtspersonen en registreren van bevoegdheden van het hoofdstuk machtigingen zijn verplaatst naar het Technische specificaties en procedures voor uitgifte van authenticatiemiddelen. Het resterende hoofdstuk voor eisen aan Machtigingenregister heet nu Specificaties voor het beheer van bevoegdheden.

Mapping Levels of Assurance (LoA)

Het eIDAS framework gebruikt andere terminologie voor de aanduiding van betrouwbaarheidsniveaus dan het afsprakentelsel.

Hieronder wordt daarom aangegeven hoe betrouwbaarheidsniveaus zich tot elkaar verhouden.

ETD LoA	eIDAS
1	Non existent
2	Low
2+	Low
3	Substantial
4	High

Leeswijzer

De eisen in dit normenkader zijn 'gestapeld'. Dat betekent dat eisen op een lager betrouwbaarheidsniveau van toepassing zijn op hogere betrouwbaarheidsniveaus tenzij anders is aangegeven.

Technische specificaties en procedures voor uitgifte van authenticatiemiddelen, paragraaf 2.1.1 en 2.1.2 hebben betrekking op de registratie en identificatie van *natuurlijke personen*. De paragrafen 2.1.3 en 2.1.4 hebben betrekking op het registratie en identificatie van *rechtspersonen* en beroepsbeoefenaren. Daar waar in het kader van registratie van de rechtspersoon een vertegenwoordiger van die rechtspersoon als individu moet worden geïdentificeerd wordt verwezen naar de eisen voor identificatie van natuurlijke personen.

De overige paragrafen behandelen de (technische) kwaliteiten van authenticatiemiddelen, het uitgifteproces, eisen aan beveiliging, organisatie en compliance.

Specificaties voor het beheer van bevoegdheden bevat de specificaties voor het beheer van bevoegdheden (machtigingen) van natuurlijke personen die namens een rechtspersoon optreden.

Eisen voor geldigheid van verklaringen voor Dienstverleners bevat de specificaties voor de geldigheid van verklaringen die aan Dienstverleners worden verstrekt.

Technische specificaties en procedures voor uitgifte van authenticatiemiddelen

EH1 vervalt per 1-7-2021

Met ingang van 1 juli 2021 komt het gebruik van het betrouwbaarheidsniveau eH1 te vervallen en moeten de middelen en machtigingen minimaal voldoen aan de normen van het betrouwbaarheidsniveau eH2.

2.1 Inschrijving

2.1.1 Aanvraag en registratie

LoA	Vereiste elementen	
LOA 1	1. De Deelnemers MOETEN de Gebruiksvoorwaarden Elektronische Toegangsdiensten die vastgelegd zijn in Afsprakenstelsel onderdeel maken van de voorwaarden die zij hun klanten opleggen. 2. Deelnemers MOETEN de gebruikers bekend maken met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De Deelnemer MOET de Gebruiker met gebruiksvoorwaarden binden aan: a. de verplichting tot het melden van verlies, misbruik en een vermoeden van misbruik van zijn authenticatiemiddel bij de Deelnemer en; b. binden aan een verplichting om gelijktijdig een verzoek te doen tot revocatie of schorsing van zijn authenticatiemiddel. 4. De Deelnemer MOET de levensduur van het authenticatiemiddel, de procedure voor intrekking en indien van toepassing de procedure voor schorsing en vernieuwing aan de Gebruiker bekend maken. 5. Gebruiksvoorwaarden van Deelnemers moeten aan de Gebruikers ter beschikking worden gesteld 6. De identiteitsverklaring(en) die de Aanvrager aanlevert MOETEN leiden tot een unieke identificatie van de Aanvrager. De aangeleverde gegevens MOET(EN) bestaan uit meervoudige verklaringen die: a. betrekking hebben op de Aanvrager en; b. niet noodzakelijkerwijs uitsluitend bij de Aanvrager bekend zijn. c. de Identiteitsverklaring van de Aanvrager MAG alleen op LoA1 zelf-verklaard (self-asserted) zijn.	
LOA 2	Hetzelfde als LoA1 met toevoeging van: 1. Elke van de volgende kenmerken MOET worden opgevat als te gebruiken voor de meervoudige identiteitsverklaringen zoals bij LoA1 punt 6 is bedoeld: a. Naam (VERPLICHT), in combinatie met: b. Adres of; c. Geboortedatum of; d. Geboorteplaats 2. De aangeleverde identiteitsverklaring MOET zijn gebaseerd op een van de onderstaande officiële bronnen voor identificatiedoeleinden: a. Voor middelen die bedoeld zijn voor gebruik in het burgerdomein: i. Een geldig WID dat voorzien is van een BSN b. Voor overige middelen: i. een geldig Nederlands paspoort of ander nationaal paspoort dat door de Nederlandse Staat wordt erkend. ii. een geldig identiteitskaart uit een Europese Economische Ruimte (EER)-land iii. een geldig Nederlands vreemdelingendocument mits voorzien van een pasfoto. iv. een geldig rijbewijs uit een EER-land mits voorzien van pasfoto v. een geldig gekwalificeerd certificaat	

LOA 3	Hetzelfde als LoA 2 met toevoeging van: 1. Elke van de volgende kenmerken MOET worden opgevat als te gebruiken voor de meervoudige identiteitsverklaringen zoals bij LoA1 punt 6 is bedoeld: a. Naam (VERPLICHT), in combinatie met: b. Adres c. Geboortedatum (VERPLICHT voor middelen die geactiveerd moeten worden bij het BSNk, bijvoorbeeld t.b.v. eIDAS-uitgaand) d. Geboorteplaats e. BSN (VERPLICHT voor middelen die geactiveerd moeten worden bij het BSNk) 2. Tijdens de registratie online aangeleverde verklaringen MOGEN zijn ondertekend met een niet-gekwalificeerd certificaat. 3. De identiteitsverklaring van de Gebruiker MOET worden geverifieerd aan het originele fysieke WID document. 4. Indien BSN wordt gebruikt, MOET de deelnemer het BSN van de Gebruiker verifiëren in zijn originele fysieke WID document.	Ad 3 en 4 Voor LoA3 zijn alternatieve invullingen toegestaan zoals beschreven is in de paragraaf 2.1.2 'Eisen Identificatie op Afstand' en paragraaf 2.1.2 bij LoA3.
LOA 4	Hetzelfde als LoA 3 met toevoeging van: 1. Online aangeleverde verklaringen MOETEN zijn ondertekend met een gekwalificeerd certificaat.	

2.1.2 Bewijs en verificatie van Identiteit (natuurlijk persoon)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	De Deelnemer moet het e-mailadres valideren als deze contactgegevens gebruikt worden als onderdeel van het registratieproces (versturen van activatiecodes, links of (one-time) passwords).	
LOA 2	LoA 1 met toevoeging van: 1. De Deelnemer moet het e-mailadres en telefoonnummer valideren als deze contactgegevens gebruikt worden als onderdeel van het registratieproces (versturen van activatiecodes, links of (one-time) passwords). 2. Voor validatie van de aangeleverde identiteitsverklaringen MOET geaccepteerd worden dat een van de onderstaande bronnen een invulling zijn van een officiële neutrale en betrouwbare bron; a. De Nederlandse Basisadministratie Personen (BRP, voorheen bekend als GBA) b. De HRM-database met persoonsgegevens van medewerkers van een onderneming of rechtspersoon, indien aan voorwaarden i, ii, iii en iv wordt voldaan: i. De bruikbaarheid van het middel is beperkt tot die onderneming of rechtspersoon in Nederland. ii. Het middel en de machtigingen zijn bij dezelfde deelnemer uitgegeven. iii. Het BSN van de gebruiker mag niet worden geregistreerd. iv. Het middel MOET een zodanige werking hebben dat gebruik daarvan in het BSN-domein en consumentendomein onmogelijk is gemaakt. 3. Slechts voor LoA 2 is het overleggen van een kopie van een identiteitsdocument geaccepteerd. a. Verificatie van de echtheidskenmerken MOET voor zover mogelijk worden uitgevoerd door daartoe opgeleid personeel; b. Verificatie MOET worden uitgevoerd in het register voor gestolen of vermiste identiteitsbewijzen. 1. Identificatie MAG eveneens plaatsvinden:	Ad 2 In Nederland is de Basisregistratie Personen (BRP) als de formele en gezaghebbende bron voor identiteitscontrole. Validatie van identificerende gegevens waarbij de HRM database van een werkgever of een werkgeversverklaring als bron wordt gebruikt MOETEN slechts betekenis hebben binnen de bedrijvencontext. Dergelijke validaties zijn vanwege de mogelijkheden tot opzettelijk misbruik door de aanvrager ongeschikt voor uitgifte van middelen die in het BSN-domein en consumentendomein gebruikt kunnen worden. Deelnemers MOGEN NIET dit risico met gebruiksvoorwaarden afdekken. In het geval de bankoverschrijving als een toegevoegde verificatie wordt gebruikt: De bankrekening MOET een privérekening zijn bij een bank waar de aanvrager dezelfde persoon is als de enige bankrekeninghouder en; waarvoor de financiële instelling voor het openen van de bankrekening de rekeninghouder zich conform wettelijke vereisten heeft moeten laten identificeren, op basis van een geldig identiteitsbewijs. Ad 4 Kern van deze norm is dat identificatie bij registratie of uitgifte altijd op het juiste LoA heeft plaats gevonden. Voor een gekwalificeerd certificaat heeft een identificatie op LoA4 plaats gevonden. Ten behoeve van de uitgifte van middelen voor gebruik in het burgerdomein moet altijd een verificatie van het BSN plaatsvinden aan het originele WID van de Aanvrager. Voor LoA3: Validatie van het BSN moet middels een registratie in het BSNk plaatsvinden. Ad 5c M.b.t. vereisten voor validatie van elektronische handtekening die niet op PKI zijn gebaseerd: • Een gelijke kwaliteit (equal quality) van validatie kan uitsluitend worden bereikt met een handgeschreven handtekeningen of op PKI-technologie gebaseerde handtekeningen.

	a. Met een middel op LoA 2 en hoger dat door een Deelnemer in het stelsel is uitgegeven. i. Restrictie: Met een middel van een specifiek LoA MAG NIET zonder aanvullende validaties een Stelseldienst (middel of machtiging) met een hoger LoA worden verstrekt. b. Restrictie: Op basis van een middel dat niet voor gebruik in het burgerdomein is uitgegeven MAG NIET zonder aanvullende validaties een middel voor gebruik in het burgerdomein worden verstrekt. c. Op basis van een gekwalificeerd certificaat dat wordt gebruikt als elektronische handtekening zoals bedoeld in de Verordening (EU) nr. 910/2014. 2. Vereisten voor validatie van middelen (authenticatiemiddelen uitgegeven binnen het Stelsel) en elektronische handtekeningen: a. Deelnemers aan het stelsel MOETEN er op toezien dat het pseudoniem van de gebruiker wordt verstrekt middels het gebruik van het middel of; b. De identificerende gegevens behorende bij het uitgereikte middel worden bij de uitgever van het middel geverifieerd. c. De Deelnemer MOET op PKI gebaseerde elektronische handtekeningen valideren d.m. v. de certificatenketen en op basis van actuele informatie over statusintrekkingen. d. Niet op PKI gebaseerde handtekeningen MOETEN gevalideerd worden met een validatiemethode van gelijke kwaliteit.	
LOA 3	LoA2 met toevoeging van: 1. Identificatie MAG eveneens plaatsvinden met een middel op LoA 3 en hoger dat door een Deelnemer in het stelsel is uitgegeven. i. Restrictie: Met een middel van een specifiek LoA MAG NIET zonder aanvullende validaties een Stelseldienst (middel of machtiging) met een hoger LoA worden verstrekt. ii. Restrictie: Op basis van een middel dat niet voor gebruik in het burgerdomein is uitgegeven MAG NIET zonder aanvullende validaties een middel voor gebruik in het burgerdomein worden verstrekt. 2. De Deelnemer MOET het fysieke adres valideren als de uitgifte van het middel face-to-face (in person) plaatsvindt op het door de aanvrager opgegeven adres voor uitgifte. 3. De Deelnemer MOET registreren welke contactgegevens zijn gevalideerd als onderdeel van het uitgifteproces en welke gegevens slechts zijn opgeslagen als comfortinformatie als onderdeel van de algemene bedrijfsvoering. 4. Fysieke identificatie: een fysieke ontmoeting MOET plaatsvinden tijdens de registratie of tijdens het middelenuitgifteproces. Identificatie op afstand**:** dit is als alternatief voor de fysieke ontmoeting tijdens de registratie of tijdens het middelenuitgifteproces toegestaan. Dit MOET conform de beschreven normelementen in paragraaf Eisen Identificatie op Afstand.. 5. De echtheid van identiteitsbewijzen MOET geverifieerd worden door het origineel van het identiteitsbewijs te controleren op specifiek voor dat identiteitsbewijs unieke en bekende kenmerken waardoor dat document als authentiek kan worden aangemerkt. a. Voor validatie van de verklaringen is het tonen van een fysiek en geldig identiteitsdocument vereist.	Ad 1 Kern van deze norm is dat identificatie bij registratie of uitgifte altijd op het juiste LoA heeft plaats gevonden. Voor een gekwalificeerd certificaat heeft een identificatie op LoA4 plaats gevonden. Ten behoeve van de uitgifte van middelen voor gebruik in het burgerdomein moet altijd een verificatie van het BSN plaatsvinden aan het originele WID van de Aanvrager. Validatie van het BSN moet middels een registratie bij BSNk plaatsvinden. Ad 2 Validatie van het fysieke adres mag worden opgevat als: • de deelnemer controleert of het adres voor afgifte gelijk is aan het adres dat is opgegeven door de aanvrager voordat het middel wordt verzonden per aangetekende post. Deze werkwijze is slechts toegestaan in combinatie met een fysieke ontmoeting tijdens het registratieproces. Of; • de deelnemer controleert of het adres voor afgifte gelijk is aan het adres voor afgifte van het middel en hij identificeert de ontvanger bij uitgifte van het middel als zijnde de aanvrager. Identificatie kan in dit geval ook plaatsvinden door een besteldienst die in opdracht van de deelnemer het middel in persoon overhandigt aan de aanvrager. Deze werkwijze minimaal bedoeld voor situaties waarbij identificatie van de aanvrager in het aanvraagproces niet heeft plaatsgevonden. Ad 4 Voorbeelden van geaccepteerde face-to-face controles zijn • Controle van identiteit door daarvoor opgeleide PostNL-medewerker die het middel komt afleveren • Identificatie door een daarvoor opgeleide balie medewerker van de Authenticatiedienst. • Identificatie door de Dienstafnemer conform de wettelijke verplichting van werkgevers tot identificatie van personeel. • Nota bene 1: Voor middelen die op basis van identificatie door de werkgever worden uitgegeven moet het technisch onmogelijk zijn dat deze middelen in het BSN domein en consumentendomein gebruikt kunnen worden. • Nota bene 2 Mogelijke zelfverklaring moeten worden uitgesloten. Niet acceptabel is dat wettelijke vertegenwoordigers en machtigingenbeheerders over zichzelf een identiteitsverklaring afgeven. • De Dienstafnemer verklaart over de identiteit van de Gebruiker door de Dienstafnemer op grond van de plicht van werkgevers om medewerkers bij in diensttreden te identificeren. Mogelijke zelfverklaring moeten worden uitgesloten. Niet acceptabel is dat een wettelijke vertegenwoordiger en de machtigingenbeheerder

	b. Minimaal een of meer fysieke kenmerken van de Gebruiker moeten worden geverifieerd aan het identiteitsbewijs. c. Verificatie van echtheidskenmerken MOET van worden uitgevoerd door daartoe opgeleid personeel en; d. Additioneel voor de uitgifte van middelen die bedoeld zijn voor het gebruik in het Burgerdomein: e. Indien het BSN wordt gebruikt, dan MOET de Deelnemer in het aanvraagproces ervoor zorgdragen dat het BSN van de Aanvrager in het originele fysieke WID van de Aanvrager is geverifieerd. Indien het WID geen BSN bevat MAG een gewaarmerkt uittreksel bevolkingsregister, niet ouder dan 6 maanden, van de Gebruiker toegepast worden, waarop is vermeld: BSN, naam, geboorteplaats en geboortedatum. Na uitgifte gelden de eisen in 6 en 7. 6. Indien een Gebruiker i. reeds een eHerkenningsmiddel bezit EN ii. het BSN van de Gebruiker is nog niet bekend bij de Authenticatiedienst EN iii. waarbij voor de validatie van de aangeleverde identiteitsverklaringen NIET MAG worden gesteund op de HRM-database, dan kan het BSN worden geregistreerd middels authenticatie met het eTD-identificatiemiddel van de Gebruiker, of een formulier met de handgeschreven handtekening of ondertekening met een gekwalificeerde certificaat van de Gebruiker. In beide gevallen dient een document zoals gespecificeerd onder onderstaande sub i, of sub ii te worden aangeleverd: i. een kopie WID met zichtbaar BSN van de Gebruiker. ii.een gewaarmerkt uittreksel bevolkingsregister, niet ouder dan 6 maanden, van de Gebruiker, waarop is vermeld: BSN, naam, geboorteplaats en geboortedatum. 7. Indien een Gebruiker i. reeds een eHerkenningsmiddel bezit EN ii. het BSN van de Gebruiker is nog niet bekend bij de Authenticatiedienst EN iii. voor de validatie van de aangeleverde identiteitsverklaringen is gesteund op de HRM-database, dan MAG NIET het BSN worden geregistreerd en gelden de vereisten zoals opgenomen in paragraaf 2.1.2 Bewijs en verificatie van Identiteit (natuurlijk persoon).	over zichzelf een identiteitsverklaring afgeven. Indirecte vormen van face-to-face identificatie zijn niet zonder meer acceptabel: • Identificatie op basis van een eerder uitgegeven persoonsgebonden op hetzelfde of hoger niveau waarbij indertijd face-to-face controle heeft plaatsgevonden • Identificatie op basis van een banktransactie. De verificatie op basis van het resultaat van een geslaagde bankoverschrijving is slechts toegestaan als een additionele verificatie. Het is namelijk niet controleerbaar dat de aanvrager een andere persoon gemachtigd heeft voor zijn bankrekening of zijn inloggegevens heeft gedeeld met een andere persoon. Ad 5e ii Voor het toevoegen van het BSN aan een bestaand middel mag voor de validatie van de aangeleverde identiteitsverklaringen niet zijn gesteund op de HRM-database.
LOA 4	LoA3 met toevoeging van: 1. Met gebruik van een middel op LoA4 of gekwalificeerd certificaat kan eveneens een nieuw middel worden aangevraagd. In dit geval MOET geverifieerd worden: a. dat de aanvrager daadwerkelijk in bezit is van het middel; b. dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er daadwerkelijk een identificatie op locatie heeft plaatsgevonden bij aanvraag of uitgifte van het middel, of c. dat bij gebruik van een middel dat buiten het stelsel is uitgegeven er een identificatie op afstand heeft plaatsgevonden die MOET voldoen aan de eisen van het afsprakenstelsel eTD of ETSI TS 119 461 bij aanvraag of uitgifte van het middel.	

Eisen Identificatie op Afstand

LoA	Vereiste elementen	Toelichting en good practice
LOA 3	Op LoA3 wordt Identificatie op Afstand toegestaan, waarbij – naast de geldende vereisten inzake de identiteitsvaststelling - in elk geval moet worden voldaan aan de eisen die zijn vermeld op pagina: Eisen Identificatie op Afstand	

2.1.3 Bewijs en verificatie van identiteit (rechtspersoon)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	• Controledoelstelling: Het machtigingenregister MOET erop toezien dat de vertegenwoordigers van de Dienstafnemer deugdelijk worden geïdentificeerd. • Controledoelstelling: Het machtigingenregister MOET erop toezien dat de Dienstafnemer of de gemachtigde Rechtspersoon deugdelijk wordt geïdentificeerd. • Controledoelstelling: Het machtigingenregister moet erop toezien dat de door de Dienstverlener aangeleverde informatie als feitelijk juist is geverifieerd. • Controledoelstelling: Het machtigingenregister MOET erop toezien dat de bevoegdheden van de vertegenwoordigers van de Dienstafnemer deugdelijk worden geverifieerd. 1. De eerste identificatie van de vertegenwoordigers van de Dienstafnemer MOET conform de vereisten voor identificatie bij uitgifte van LoA1 authenticatiemiddelen (zie paragraaf 2.1.1 en 2.1.2) worden uitgevoerd, OF conform de aangeven alternatieven in punt 4. Dit geldt in het bijzonder voor onder staande vertegenwoordigers: a. De wettelijke vertegenwoordiger(s) van de Dienstafnemer. b. De machtigingenbeheerder die door de wettelijke vertegenwoordiger geautoriseerd is en de machtigingen met betrekking tot de Dienstafnemer administreert. c. De Gevolmachtigde die door de wettelijke vertegenwoordiger geautoriseerd is namens deze te handelen. 2. Het machtigingenregister MOET de Dienstafnemer of de gemachtigde Rechtspersoon registreren. 3. Het machtigingenregister MOET de feitelijke juistheid van de door de aanvrager aangeleverde informatie verifiëren in het Handelsregister van de Kamer van Koophandel alvorens de aanvraag formeel geaccepteerd mag worden. Het volgende MOET ten minste juist zijn: a. Bedrijfsnaam en wettelijke naam van de Dienstafnemer b. Ten minste één vestigingsadres c. Identificatienummers (KvK nummer en RSIN)	Ad 3 Interpretatie: De gegevens die de aanvrager aandraagt moeten zijn vergeleken met de geregistreerde gegevens in het handelsregister. Van de brongegevens in het handelsregister wordt aangenomen dat zij correct zijn. Indien de deelnemer bij de controle in het handelsregister onjuistheden in de gegevens ontdekt of vermoedt bestaat er geen terug meldplicht, tenzij om een andere reden al een terug meld verplichting van toepassing was op de deelnemer. De geregistreerde vestigingsadressen in het handelsregister zijn niet altijd gelijk aan een correspondentieadres. Waar vestigingsadres en correspondentieadres samenvallen, vervalt de eis voor het verifiëren van het correspondentieadres. In het geval van rechtspersonen zonder vestigingsadres moet in elk geval het correspondentieadres gecontroleerd worden. Ad 3b en d Het vestigings- en/of correspondentieadres wordt gebruikt voor schriftelijke communicatie met de organisatie. Voor uitgifte van het token, zie paragraaf 2.2.2 Uitgifte, uitreiking en activering. Ad 3c: KvK nummer en RSIN MOETEN beide bruikbaar zijn in de Machtigingenregisters om machtigingen te registeren. Niet van toepassing op organisaties die niet beschikken over een KvK-nummer en/of RSIN. In het geval van eenmanszaken wordt ten behoeve van de belastingdienst het BSN van de wettelijke vertegenwoordiger als identificatienummer toegevoegd. Deze situatie is van toepassing vanaf niveau eH3 en wordt beschreven in paragraaf 2.1.4. Ad5 Interpretatie: Indien de dienst niet aan professionals wordt geleverd is deze norm niet van toepassing. Bedoeld worden registers zoals het BIG voor zorgprofessionals, BAR voor advocaten en KNB register voor notarissen. Advies: De opsomming is gebaseerd op de lijst van geregistreerde professionals die willen handelen vanuit of namens hun beroep te vinden in het PKI overheid Programma van eisen deel 3a bij 3.2.5-1.: a. Aangewezen door een Staatssecretaris. Niet voor alle professionals bestaat al een dergelijk register. Ad 4.c Het ANBI Register is uitsluitend digitaal bereikbaar via de beveiligde website van de Belastingdienst "opzoeken ANBI". Ad 4.c.iii het RSIN wordt in het ANBI register van de Belastingdienst vermeld in de kolom RSIN. In de situatie dat een ander nummer dan het RSIN staat vermeld kan dit alternatief niet toegepast worden. Ad 4.c.iiii Het correspondentieadres is te achterhalen via de weblink van de instelling op de ANBI pagina en de daar vermelde contactgegevens.

d. Correspondentieadres

4. Toegestane alternatieven voor verificatie:
   a. Alternatief 1: Online verificatie in het Handelsregister van de Kamer van Koophandel of voor acceptatie van de aanvraag.
   b. Alternatief 2 (alleen voor eTD2, eTD2+): Verificatie gebaseerd op een origineel uittreksel van het Handelsregister van de Kamer van Koophandel. Op het moment dat de aanvraag geaccepteerd wordt MAG dit uit treksel niet ouder zijn dan 14 dagen (7 dagen is de wettelijk toepasselijke periode voor het aanleveren van wijzigingen in het Handelsregister van de Kamer van Koophandel).
   c. Alternatief 3:
      Verificatie gebaseerd op controle van het ANBI register. De gegevens van de organisatie die aangeleverd
      worden door de gebruiker MOETEN wor den gecontroleerd bij het ANBI register. Het volgende MOET ten minste juist zijn:
      i. Naam van de instelling
      ii. Vestigingsplaats
      iii. RSIN
      iv. Correspondentieadres
   d. Alternatief 4 (diplomatieke missies en internationale organisaties): Verificatie gebaseerd op controle in PROBAS. De gegevens van de organisatie
      die aangeleverd worden door de vertegenwoordiger MOETEN worden gecontroleerd in PROBAS. Het volgende MOET ten minste juist zijn:
      i. Voornamen vertegenwoordiger;
      ii. Achternaam vertegenwoordiger;
      iii. Geboortedatum vertegenwoordiger;
      iv. Geboorteplaats vertegenwoordiger (Optioneel);
      v. Bevoegdheid vertegenwoordiger;
      vi. Naam organisatie;
      vii. PROBAS-nummer van de organisatie;
      viii. Vestigings- of correspondentieadres van de organisatie.

5. Het machtigingenregister MOET de aangeleverde identiteitskenmerken verifiëren in het relevante beroepsregister in het geval de aanvrager (beroepsmatig) zich wil registreren als Dienstafnemer. Aanvaardbare bewijsbronnen voor beroepsregistratie in Nederland zijn (limitatief):
   a. Accountants Administratieconsulent;
   b. Advocaat; - Octrooigemachtigde;
   c. Registerloods;
   d. Arts (bijvoorbeeld huisartsen en medisch-specialisten zoals chirurgen en psychiaters);
   e. Tandarts; Apotheker; Verloskundige; Fysiotherapeut;
   f. Verpleegkundige;- Psychotherapeut;
   g. Gezondheidszorgpsycholoog;
   h. Notaris; Kandidaat notaris; Toegevoegd notaris;
   i. Gerechtsdeurwaarder; Waarnemend gerechtsdeurwaarder; Toegevoegd kandidaat gerechtsdeurwaarder
   j. Octrooigemachtigde;
   k. Registeraccountant;
   l. Dierenarts;
   m. Zeevarende;
   n. (Hoofd) Bewaarder; Gemandateerd bewaarder;
   o. Technisch medewerker schepen; Inspecteur Scheepsregistratie

	p. Belastingdeurwaarder; Rijksdeurwaarder.	
LOA 2	Zelfde als LoA1 met toevoeging van: 1. Toegestaan als alternatief voor de verificatie van bedrijfsgegevens: Verificatie gebaseerd op een origineel uittreksel van het Handelsregister van de Kamer van Koophandel. Op het moment dat de aanvraag geaccepteerd wordt MAG dit uit treksel niet ouder zijn dan 14 dagen (7 dagen is de wettelijk toepasselijke periode voor het aanleveren van wijzigingen in het Handelsregister van de Kamer van Koophandel). 2. De aanvrager die een aanvraag indient voor een machtiging voor betrouwbaarheidsniveaus LoA2 MOET een wettelijke vertegenwoordiger van de Dienstafnemer zijn, dan wel een Gevolmachtigde. 3. Voor betrouwbaarheidsniveau LoA2 machtigingen MOET de bevoegde vertegenwoordiger geïdentificeerd worden en MOET zijn/haar identiteitsverklaring gevalideerd en geregistreerd worden conform de vereisten voor identificatie bij uitgifte van LoA2 authenticatiemiddelen (zie: paragraaf 2.1.1 en paragraaf 2.1.2) of als alternatief zijn onderstaande vereisten van toepassing op elektronische of niet-elektronische machtigingsaanvragen: a. Elektronisch machtigingsaanvragen: i. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden, MOET er een kopie van een geldig identiteitsdocument zoals genoemd onder paragraaf 2.1.1 en een kopie van een rechtsgeldig door een wettelijk vertegenwoordiger van de Dienstafnemer ondertekend formulier bij de aanvraag gevoegd worden, en de handgeschreven handtekeningen onder deze documenten MOETEN geverifieerd worden door het machtigingenregister. ii. Aan de hierboven opgesomde vereis ten t.a.v. de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer wordt voldaan wanneer de aanvraag elektronisch is ondertekend door de Dienstafnemer die van een Gekwalificeerde Handtekening gebruik maakt. iii. Alternatief: Een andere mogelijkheid is dat de registratie van de unieke kenmerken van de wettelijke vertegenwoordiger geverifieerd MOET worden op basis van het resultaat van een geslaagde bankoverschrijving van een privérekening bij een bank waar de aanvrager dezelfde persoon is als de bankrekeninghouder en waarvoor de financiële instelling bij het openen van de bankrekening de rekeninghouder deugdelijk heeft moeten identificeren, op basis van een geldig identiteitsbewijs.	Ad 1 Betreft een toegestaan alternatief bij LoA2 punt 3 Ad 3 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordiger(s), machtigingenbeheerder of andere Gevolmachtigde namens de wettelijke vertegenwoordiger. Het identiteitsdocument moet voorzien zijn van een handtekening zodat de vergelijking van de handtekening met de handtekening op het aanvraagformulier gemaakt kan worden. Ad 5 Interpretatie: Van de brongegevens in registers waartegen moet worden geverifieerd wordt aangenomen dat deze correct zijn. De gegevens die in de aanvraag worden aangedragen moeten dus in overeenstemming zijn met de brongegevens in de registers.

b. Niet-elektronisch machtigingsaanvragen:
    i. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. De aanvraag MOET ondertekend worden door de wettelijke vertegenwoordiger van de Dienstafnemer door middel van een handgeschreven handtekening.
    ii. De aanvraag MOET worden voorzien van een kopie van een geldig identiteitsdocument. Deze handgeschreven handtekening op de kopie MOET geverifieerd worden met gebruikmaking van het machtigingenregister.
    iii. Er MOET gecontroleerd worden of het identiteitsbewijs(nummer) in de database als gestolen of vermist geregistreerd staat.

4. Een Gevolmachtigde MAG een aanvraag voor een machtiging voor betrouwbaarheidsniveaus LoA 2 indienen. Het machtigingenregister MOET de handgeschreven handtekeningen verifiëren op de Volmacht en op de kopie van het identiteitsdocument van de aanvrager (de wettelijke vertegenwoordiger van de Dienstafnemer), of op de kopie van het identiteitsdocument van de Gevolmachtigde en op het aanvraagformulier. Identificatie van de vertegenwoordiger van de Dienstafnemer MOET plaatsvinden, zoals hierboven onder punt 2 omschreven.
5. Het machtigingenregister MOET de Dienstafnemer of de gemachtigde Rechtspersoon registreren.
    a. De aangeleverde en geregistreerde kenmerken van de Dienstafnemer of de gemachtigde Rechtspersoon MOETEN uniek en feitelijk juist zijn. Identificatie MAG op openbare informatie gebaseerd zijn.
    b. Het machtigingenregister MOET de bij 5a. genoemde kenmerken ten minste verifiëren in Het Handelsregister van de Kamer van Koophandel of Beroepsregister.
6. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten. De aanvraag MOET geaccepteerd worden indien:
    a. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger;
    b. de aanvraag is ondertekend door minimaal twee gezamenlijk bevoegde vertegenwoordigers en de risicobeoordeling volgens punt 7 is laag;
    c. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning;
    d. de aanvraag is ondertekend door minimaal twee beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de risicobeoordeling volgens punt 7 is laag.

	7. Indien de aanvraag is ondertekend door minimaal twee beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de aanvraag wordt geaccepteerd, dan MOET het machtigingenregister met betrekking tot de acceptatie en de mate van bevoegdheid van degenen die ondertekenen een risico-inschatting maken en deze bij de acceptatie van de aanvraag archiveren. 8. Het machtigingenregister MOET in de aanvraag er schriftelijk op wijzen dat de verantwoordelijkheid ten aanzien van welke wettelijk bevoegde vertegenwoordiger zijn /hun handtekening zet(ten), bij de onderneming zelf berust.	
LOA 3	Zelfde als LoA1 en met toevoeging van: 1. Voor betrouwbaarheidsniveau LoA 3 machtigingen, MOET de bevoegde vertegenwoordiger worden geregistreerd en geïdentificeerd conform de vereisten voor identificatie bij uitgifte van LoA3 authenticatiemiddelen (zie vereisten in paragraaf 2.1.1 en 2.1.2.) of als alternatief zijn de onderstaande vereisten van toepassing: i. De vertegenwoordiger die de aanvraag voor de eerste registratie van de Dienstafnemer bij het machtigingenregister ondertekent voor betrouwbaarheidsniveau LoA3 MOET een wettelijke bevoegde vertegenwoordiger van de Dienstafnemer zijn. ii. Elektronische machtigingsaanvragen: 1. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. 2. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van ge scande kopieën van het originele aanvraagformulier die door de wettelijke vertegenwoordiger van de Dienstafnemer door middel van een hand geschreven handtekening zijn ondertekend en daarbij gevoegd de bijbehorende gesc ande kopie van het identiteitsdocument van de wettelijke vertegenwoordiger. iii. Niet-elektronisch machtigingsaanvragen: 1. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van het originele aanvraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de	Ad 1 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordiger(s) en de machtigingenbeheerders.

	bijbehorende kopie van het identiteitsdocument van de vertegenwoordiger. 2. De handgeschreven handtekening op het aanvraagformulier MOET geverifieerd worden aan de hand van de handtekening op de kopie van het identiteitsdocument. 3. De echtheid van identiteitsbewijzen MOET geverifieerd worden, op basis van unieke kenmerken. 4. Er MOET gecontroleerd worden of het identiteitsbewijs (nummer) in de database als gestolen of vermist geregistreerd staat. 2. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten. De aanvraag MOET geaccepteerd worden indien: a. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger; b. de aanvraag is ondertekend door meer dan de helft van het totale aantal gezamenlijk bevoegde vertegenwoordigers en de risicobeoordeling volgens punt 3 is laag; c. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning; d. de aanvraag is ondertekend door meer dan de helft van het totaal aantal beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de risicobeoordeling volgens punt 3 is laag. 3. Indien de aanvraag is ondertekend door meer dan de helft van het totaal aantal beperkt bevoegde, of beperkt gevolmachtigde vertegenwoordigers en de aanvraag wordt geaccepteerd, dan MOET het machtigingenregister met betrekking tot de acceptatie en de mate van bevoegdheid van degenen die ondertekenen een risico-inschatting maken en deze bij de acceptatie van de aanvraag archiveren. 4. Het machtigingenregister MOET in de aanvraag er schriftelijk op wijzen dat de verantwoordelijkheid ten aanzien van welke wettelijk bevoegde vertegenwoordiger zijn /hun handtekening zet(ten), bij de onderneming zelf berust.	
LOA 4	Zelfde als LoA1 en met toevoeging van: 1. Voor betrouwbaarheidsniveau LoA 4 machtigingen MOET de bevoegde vertegenwoordiger worden geregistreerd en fysiek geïdentificeerd conform de vereisten voor identificatie bij uitgifte van LoA4 authenticatiemiddelen (zie paragrafen 2.1.1 en 2.1.2). Specifiek is hierbij het volgende vereist: 2. De vertegenwoordiger die de aanvraag voor de eerste registratie van de Dienstafnemer	Ad 1 Toelichting: De bevoegde vertegenwoordigers zijn hier de wettelijke vertegenwoordigers. De wettelijke vertegenwoordiger moet bij de aanvraag fysiek verschijnen voor identificatie.

bij het machtigingenregister ondertekent voor betrouwbaarheidsniveau LoA 4 MOET een wettelijke bevoegde vertegenwoordiger van de Dienstafnemer zijn.

3. Onderstaande uitdrukkelijke vereisten gelden specifiek voor elektronische of niet-elektronische machtigingsaanvragen:
    a. Voor niet-elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienst afnemer geregistreerd worden.
    b. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van het originele aan vraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de bijbehorende kopie van het identiteitsdocument van de vertegenwoordiger. De hand geschreven handtekening op het aanvraagformulier MOET geverifieerd worden aan de hand van de handtekening op de kopie van het identiteitsdocument.
    c. De echtheid van identiteitsbewijzen MOET geverifieerd worden, op basis van unieke kenmerken.
    d. Er MOET gecontroleerd worden of het identiteitsbewijs(nummer) in de database als gestolen of vermist geregistreerd staat;
    a. Elektronische machtigingsaanvragen:
        i. Voor elektronische machtigingsaanvragen MOETEN de unieke kenmerken van de wettelijke vertegenwoordiger van de Dienstafnemer geregistreerd worden. Aanvragen MOGEN uitsluitend worden geaccepteerd op basis van gescande kopieën van het originele aanvraagformulier en door middel van een handgeschreven handtekening ondertekend door de wettelijke vertegenwoordiger van de Dienstafnemer met de bijbehorende gescande kopie van het identiteitsdocument van de vertegenwoordiger.
    b. Niet-elektronische machtigingsaanvragen
4. Het machtigingenregister MOET de bevoegdheid van de aanvrager verifiëren in het Handelsregister van de Kamer van Koophandel, of, als alternatief, in aanvullende bewijsstukken, zoals statuten en mandaten.
    a. De aanvraag MOET geaccepteerd worden indien:
        i. de aanvraag is ondertekend door een volledig of zelfstandig bevoegde, of een volledig gevolmachtigde vertegenwoordiger;
        ii. de aanvraag is ondertekend door alle gezamenlijk bevoegde vertegenwoordigers;
        iii. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning;
        iv. de aanvraag is ondertekend door alle beperkt bevoegde, of beperkt gevolmachtigde

	vertegenwoordigers van een publieke rechtspersoon. b. De aanvraag MOET worden afgewezen indien: i. de aanvraag is ondertekend door een vertegenwoordiger die beperkt bevoegd is, of een beperkte volmacht heeft, waarbij NIET expliciet is aangegeven dat de vertegenwoordiger gerechtigd is tot het doen van een aanvraag eHerkenning;	

2.1.4 Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	Controledoelstelling: Het machtigingenregister MOET erop toezien dat de betrokkenheid van de vertegenwoordigers met de Dienstafnemer of de tussenpersoon deugdelijk is vastgesteld. 1. De betrokkenheid van de vertegenwoordiger die voor de eerste keer de diensten van het machtigingenregister aanvraagt, met de Dienstafnemer MOET geverifieerd worden door: verificatie van een concreet bedrijfsorganisatorisch kenmerk, zoals bijv. het fysieke postadres, het e-mailadres of het telefoonnummer.	
LOA 2	Hetzelfde als LoA1 en met toevoeging van: 1. Voor private rechtspersonen: a. De betrokkenheid van de aanvrager met de Dienstafnemer MOET worden geverifieerd door het Handelsregister van de Kamer van Koophandel te raadplegen. b. Het machtigingenregister MOET de aangeleverde kenmerken controleren met de geregistreerde kenmerken van de aanvrager in het Handelsregister van de Kamer van Koophandel. 2. Voor publieke rechtspersonen: De betrokkenheid van de aanvrager met de Dienstafnemer MOET worden geverifieerd volgens een van de onderstaande alternatieven: a. Controleer of de identiteitskenmerken van de aanvrager overeenstemmen met het Handelsregister van de Kamer van Koophandel en controleer bestaande beperkingen van de registratie van de machtiging, of anders b. Controleer of de geregistreerde functie in het Handelsregister van de Kamer van Koophandel overeenkomt met de functie van de aanvrager en controleer bestaande beperkingen van de registratie van de machtiging. c. De aanvrager MOET bovendien verklaren (d.m.v. een ondertekend document) dat hij /zij deze functie op het tijdstip	Ad 1 Interpretatie: De gegevens die de aanvrager aandraagt moeten zijn vergeleken met de geregistreerde gegevens in het handelsregister. Van de brongegevens in de KvK register wordt aangenomen dat zij correct zijn. Indien de deelnemer bij de controle in het handelsregister onjuistheden in de gegevens van het handelsregister ontdekt of vermoedt bestaat er geen terugmeldplicht, tenzij om een andere reden al een terugmeldverplichting van toepassing was op de deelnemer. Ad 1c t/m 1f. Interpretatie (principiële afspraak): De aanvrager moet de onbeperkte bevoegdheid hebben om de organisatie te vertegenwoordigen inzake registratie bij het machtigingenregister. De geregistreerde bevoegdheden in het handelsregister kunnen verschillende soorten beperking bevatten zoals financiële beperkingen, beperkingen in type transacties of vormen van gezamenlijke bevoegdheid aangeven. Bij de beperking 'gezamenlijke bevoegdheid' kan de wilsuiting bestaan uit een door alle, in het Handelsregister opgenomen, gezamenlijk bevoegde bestuurders getekende verklaring die de vertegenwoordiger machtigt tot handelen. In het Handelsregister moet het MR de juistheid van de betreffende bestuurders verifiëren. Indien het MR de aanvraag teruglegt bij de aanvrager met het verzoek bewijs aan te leveren over de bevoegdheid van de aanvrager, kan deze bewijsvoering aangeleverd worden in de vorm van: • statuten • opgave (door organisatie bij) KvK • (intern) mandaat • instellingsbesluit(en) • aanstellingsbrief Voor het opstellen van generieke afwegingskaders kan gedacht worden aan: • de beoordeling van de beperking in relatie tot de strekking van de machtiging (dienst)* • ondertekening door meerdere in de KvK opgenomen (beperkt)bevoegd vertegenwoordigers * De Handreiking Betrouwbaarheidsniveaus van ForumStandaardisatie geeft richting aan Dienstverleners die op het Stelsel willen aansluiten bij het bepalen van het juiste LoA van hun dienst. Ad 1a Kerkgenootschappen zijn een bijzondere vorm van private organisaties zoals weergegeven in BW boek 2 artikel 2. Validatie van de bevoegdheden van de

van de aanvraag voor het machtigingenregister bekleedt, of anders
   d. Overeenkomstig het 'Protocol voor controle van interne mandaatbesluiten' dient de aanvrager een document in waarin verklaard wordt dat hij/zij bevoegd is namens de publieke Rechtspersoon een aanvraag te doen voor het Machtigingenregister.
   e. Publieke rechtspersonen kunnen uit meerdere onderdelen bestaan met duidelijk te onderscheiden taken. Het machtigingenregister MOET de daadwerkelijke reikwijdte van de aanvraag controleren. Als de reikwijdte beperkt is tot een bepaald organisatorenonderdeel /vestiging MOETEN de machtigingen eveneens tot dat bepaalde organisatorenonderdeel / die bepaalde vestiging beperkt zijn.
3. Het machtigingenregister MOET de onderstaande functionaliteit bieden:
   a. Registratie van een machtigingenbeheerder
   b. Registratie en beheer van bevoegdheden door de machtigingenbeheerder
4. Het Machtigingenregister registreert één of meerdere personen in de rol van Machtigingenbeheerder:

   a. De wettelijke vertegenwoordiger(s) stelt een persoon in de rol van machtigingenbeheerder aan.

   b. De Machtigingenbeheerder heeft de bevoegdheid om namens/als de wettelijke vertegenwoordiger(s) machtigingen te laten registreren bij de machtigingenregister.

   c. Indien de wettelijke vertegenwoordiger geen andere persoon in de rol van machtigingenbeheerder wenst aan te stellen, vervult de wettelijke vertegenwoordiger de rol van machtigingenbeheerder.

   d. De machtigingenbeheerder wordt, voordat hij een beheerdersmachtiging krijgt, door de machtigingendienst geïdentificeerd op een betrouwbaarheidsniveau dat op zijn minst gelijk is aan het hoogste betrouwbaarheidsniveau van de machtigingen die de wettelijke vertegenwoordiger wil kunnen laten registreren (de reikwijdte) door de machtigingenbeheerder.

   e. De reikwijdte wordt bepaald door de diensten van een beheerdersmachtiging en/of het

wettelijke vertegenwoordiger en zijn associatie met het Kerkgenootschap bij de KvK is niet mogelijk. Namen van bestuurders en kerkleden mogen niet worden gepubliceerd.

1. Kerkgenootschappen of hun koepelorganisatie MOETEN in zijn ingeschreven bij de Kamer van Koophandel om te kunnen worden geregistreerd bij het MR. Het MR MOET het vestigingsadres dat door de aanvrager wordt opgegeven valideren aan het vermelde vestigingsadres in het handelsregister.
2. Indien de aanvraag een stichting, vereniging of vennootschap betreft die onderdeel uitmaakt van een kerkgenootschap MOET de registratie op naam worden gesteld van- en beperkt tot die stichting, vereniging of vennootschap. De MR volgt de voor deze organisatievormen bestaande regels.
3. De persoon die het Kerkgenootschap vertegenwoordigt MOET worden geïdentificeerd conform bestaande stelselregels voor de persoon van wettelijke vertegenwoordiger. Zijn bevoegdheden MOETEN worden beoordeeld conform de bestaande stelselregels.

   Additioneel slechts voor LoA2
   Alternatief 1:
4. De (wettelijke) vertegenwoordiger van het Kerkgenootschap MOET een statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat is opgenomen en;
5. De (wettelijke) vertegenwoordiger overlegt een verklaring die is ondertekend door minimaal de bestuursleden aangevuld met kerkleden (in totaal minimaal 5) dat hij mag optreden als wettelijke vertegenwoordiger. Als alternatief voor de verklaring mag het MR additioneel bewijs accepteren zoals een banktransactie waarmee de vertegenwoordiger aantoont dat hij de beschikking heeft over een bankrekening op naam van het Kerkgenootschap aangevuld met ander bewijs, notulen en agenda's van vergaderingen waaruit de geclaimde bevoegdheid blijkt.
6. Het MR MOET de associatie van de vertegenwoordiger valideren aan de hand van het overlegde statuut en de getekende verklaring.

   Alternatief 2:
7. De koepelorganisatie van het kerkgenootschap, geregistreerd in het handelsregister, MOET met een formele brief aan de MR, het bestaan van het Kerkgenootschap en de bestuurssamenstelling bevestigen en de verantwoordelijkheid op zich voor de juistheid van deze bevestiging nemen.
8. Het MR verifieert de KvK nummer en vestigingsplaats van de koepelorganisatie aan het handelsregister.

   Alternatief 3:
9. De gebruiker levert gegevens van het kerkgenootschap die de gebruiker wil vertegenwoordigen op aan het MR.
10. Het MR controleert deze gegevens bij het ANBI register (uitsluitend digitaal bereikbaar via de beveiligde website van de Belastingdienst "opzoeken ANBI").
11. Het MR neemt contact op met de contactpersoon van het kerkgenootschap zoals deze is geregistreerd in het ANBI register. Deze contactpersoon MOET sc hriftelijk bevestigen dat de gebruiker gerechtigd is om namens het kerkgenootschap op te treden.

    Ad 2 Protocol voor controle van interne mandaatbesluiten: Voor de controle van interne mandaatbesluiten die als alternatief voor controle in het handelsregister worden toegestaan geldt de volgende werkwijze:
12. het mandaatbesluit wordt door degene die opgave doet verstrekt
13. degene die opgave doet duidt aan op basis van welke in het mandaatbesluit genoemde functie hij de opgave doet
14. degene die opgave doet verklaart dat hij op moment van aanvragen daadwerkelijk in betreffende functie is aangesteld
15. het machtigingenregister MOET de betrouwbaarheid van het mandaatbesluit controleren. Deze is voldoende als het betreffende besluit in officiële openbare overheidsbron als Staatscourant of officiële openbaar gemaakte stukken van het bevoegde orgaan van de publiekrechtelijke rechtspersoon kan worden teruggevonden. Bij twijfel aan de betrouwbaarheid MOET het machtigingenregister alsnog de wettelijke vertegenwoordiger vragen om zelf namens de rechtspersoon opgave te doen (indien deze niet al de opgave deed) of zelf een andere vertegenwoordiger van de rechtspersoon contacteren om deze te laten verklaren dat het mandaat geldig is.
16. Het verstrekte en gecontroleerde mandaatbesluit MOET worden gearchiveerd voor de duur van tenminste 7 jaar.

Ad 3 Interpretatie: In de praktijk valt op niveau LoA 1 de rol van machtigingenbeheerder en gemachtigde samen. De beheerdersrol wordt niet aangewezen door de wettelijke vertegenwoordiger van de dienstafnemer en de machtiging kan dus ook zonder toestemming van de wettelijke vertegenwoordiger worden aangevraagd op niveau LoA 1.

Ad 4.

	betrouwbaarheidsniveau van een beheerdersmachtiging. e. Een machtigingenbeheerder heeft de bevoegdheid andere machtigenbeheerders te registreren. 5. machtigingenbeheerder heeft onderstaande bevoegheden: a. De machtigingenbeheerder MAG machtigingen registreren en verlengen binnen de reikwijdte van de toegekende beheerdersmachtiging. b. De machtigingenbeheerder MAG beheerdersmachtigingen voor andere machtigenbeheerders registreren op het betrouwbaarheidsniveau waarvoor de machtigingenbeheerder gemachtigd is, of op een lager betrouwbaarheidsniveau. c. De machtigingenbeheerder MAG machtigingen voor zichtzelf registreren op het betrouwbaarheidsniveau waarvoor de machtigingenbeheerder gemachtigd is, of op een lager betrouwbaarheidsniveau. 6. Verlenging van een beheerdersmachtiging moet voldoen aan onderstaande eisen: a. Een machtigingenbeheerder MAG NIET zijn eigen beheerdersmachtiging verlengen. b. Verlenging door een wettelijk vertegenwoordiger MOET worden gedaan zoals beschreven onder Ad 4. c. Verlenging door een tweede machtigingenbeheerder MAG onder voorwaarden. De tweede machtigingenbeheerder MOET op zijn minst over een beheerdersmachtiging beschikken die een reikwijdte heeft overeenkomstig Ad 4e. 7. De machtigingenbeheerder MOET geauthenticeerd worden voor dat hij toegang tot het machtigingenregister krijgt.	Een bestaande machtigingenbeheerder waarvan tussentijds de organisatie failliet of in surseance van betaling is, mag geen machtigingen registreren. Ook de wettelijk vertegenwoordiger van een vennootschap kan en mag niet meer handelen en machtigingen registreren. De curator is verantwoordelijk voor lopende contracten en hij/zij moet actie ondernemen om te voorkomen dat machtigingenbeheerders en wettelijk vertegenwoordigers machtigingen registreren. Er is geen proactieve controle van de Deelnemer nodig. De bevoegdheid van de machtigingenbeheerder bij organisaties die zijn uitgeschreven uit het handelsregister van de Kamer van Koophandel vervalt. De verantwoordelijkheid hiervoor ligt bij de wettelijk vertegenwoordiger. Er is geen proactieve controle van de Deelnemer nodig.
LOA 3	Hetzelfde als LoA2 met toevoeging van: 1. De betrokkenheid van de aanvrager bij een private rechtspersoon vereist in geval van een Kerkgenootschap additionele verificaties. 2. Indien de bedrijfsvorm een eenmanszaak is, dan gelden de volgende bepalingen: a. de volgende gegevens op het getoonde WID document moeten overeenkomen met de gegevens op het uittreksel van de Kamer van Koophandel: i) De voorletters van de eigenaar ii) De achternaam van de eigenaar	Ad 1 Additioneel voor LoA3 Alternatief 1: 1. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een door een notaris gewaarmerkt statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat zijn opgenomen. 2. Het MR MOET het bestaan en de juistheid van het statuut verifiëren bij de betreffende notaris. Alternatief 2: 1. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een statuut overleggen waarin de wettelijke vertegenwoordigers (bestuursleden) en hun mandaat zijn opgenomen. 2. De (wettelijke) vertegenwoordiger MOET een verklaring overleggen die is ondertekend door minimaal 5 leden dat hij mag optreden als wettelijke vertegenwoordiger. 3. De koepelorganisatie van het kerkgenootschap, geregistreerd in het handelsregister, MOET met een formele brief aan het MR het bestaan van het kerkgenootschap en de bestuurssamenstelling daarvan bevestigen. De

iii) Geboortedatum van de eigenaar
iv) Geboorteplaats van de eigenaar

b. Als aan bepaling 3a is voldaan, dan MOET het BSN worden overgenomen uit het WID document en geregistreerd als het 'identificatienummer' van de onderneming.

3. Indien een eenmanszaak reeds gebruik maakt van de diensten van een Machtigingenregister en het BSN van de eigenaar van de eenmanszaak is nog niet bekend bij het Machtigingenregister, dan kan het BSN worden geregistreerd middels authenticatie met het eTD-identificatiemiddel van de eigenaar, of een formulier met de handschreven handtekening van de eigenaar. In beide gevallen dient een document zoals gespecificeerd onder sub a of sub b te worden aangeleverd:

a. een kopie WID met zichtbaar BSN van de eigenaar van de eenmanszaak.

b. een gewaarmerkt uittreksel bevolkingsregister, niet ouder dan 6 maanden, van de eigenaar van de eenmanszaak, waarop is vermeld: BSN, naam, geboorteplaats en geboortedatum.

koepelorganisatie neemt daarmee de verantwoordelijkheid op zich voor de juistheid van deze bevestiging.
4. De MR verifieert de KvK nummer en vestigingsplaats van de koepelorganisatie in het handelsregister.
5. Als alternatief voor de verklaring van de koepelorganisatie mag het MR additioneel bewijs accepteren zoals een bewijs dat de vertegenwoordiger de beschikking heeft over een bankrekening op naam van het kerkgenootschap aangevuld met notulen en agenda's van vergaderingen waaruit de geclaimde vertegenwoordigingsbevoegdheid blijkt.

Alternatief 3:

1. De MR MOET een bezoek afleggen aan het kerkgenootschap op het vestigingsadres dat in het handelsregister staat vermeld.
2. De MR MOET de vertegenwoordigingsbevoegdheid van de aanvrager valideren aan de hand van de geschreven verklaring van alle bestuursleden of minimaal de bestuursleden aangevuld met kerkleden (in totaal minimaal 5) én de mondelinge verklaring van minimaal 1 aanwezig mede bestuurslid. Als alternatief voor aanwezigheid van het mede bestuurslid mag het MR additioneel bewijs accepteren zoals een bewijs dat de vertegenwoordiger de beschikking heeft over een bankrekening op naam van het kerkgenootschap aangevuld met notulen en agenda's van vergaderingen waaruit de geclaimde vertegenwoordigingsbevoegdheid blijkt.
3. De aanvrager en het mede bestuurslid MOETEN zich identificeren met hun WID conform de bestaande regels voor identificatie.
4. De MR MOET de namen van de bestuursleden valideren aan het statuut aan de betreffende persoonskenmerken in het betreffende WID.
5. De MR legt alle uitgevoerde valuaties en verificaties vast t.b.v. de audit-trail.

Toelichting bij punt 2:

Interpretatie: Vormen van bijzondere omstandigheden zijn bijvoorbeeld 'bankroet' of 'uitstel van betaling'. Het gaat erom dat gecontroleerd wordt of er sprake is van bijzondere omstandigheden én of deze omstandigheden beperkingen meebrengen voor de vertegenwoordigingsbevoegdheid of handelingsbevoegdheid.

Toelichting bij punt 3:

Het BSN wordt geregistreerd als extra identificatienummer bij de identificatienummers van de onderneming die in paragraaf 2.1.3 zijn aangegeven. De belastingdienst behandelt een eenmanszaak als 'burger' en verwerkt in dat geval het BSN en niet de KvK nummer.

Toelichting bij punt 3b:

Deze termijn is gebaseerd op een advies van de rijksoverheid: Hoe lang is een uittreksel uit het bevolkingsregister geldig? | Rijksoverheid.nl

Alternatief 4:

1. Zelfstandige onderdelen van kerkgenootschappen, dan wel parochies, MOETEN zijn ingeschreven in het handelsregister van de Kamer van Koophandel om te kunnen worden geregistreerd bij het machtigingenregister.
2. De aanvraag voor een LoA3 machtiging MOET worden ondertekend door een tekenbevoegd vertegenwoordiger van het landelijke kerkgenootschap, dan wel bisdom.
3. De koepelorganisatie van de landelijke kerkgenootschappen en bisdommen (CIO) MOET zorgdragen dat alle Machtigingenregisters eHerkenning beschikken over een gewaarmerkte lijst met identificerende kenmerken van de vertegenwoordigers die de bij 2 genoemde aanvraag mogen ondertekenen. Deze lijst bevat minimaal de volgende gegevens:
   a. voorna(a)m(en) en/of voorletter(s) en achternaam;
   b. functie;
   c. handtekening.
4. De koepelorganisatie van de landelijke kerkgenootschappen en bisdommen MOET zorgdragen dat:
   a. minstens ieder kwartaal de bij onderdeel 3 genoemde lijst wordt gecontroleerd op actualiteit;
   b. bij wijzigingen in de bij onderdeel 3 genoemde lijst, de Machtigingenregisters de gewijzigde lijst ontvangen.
5. De verantwoordelijkheid voor actualiteit en correctheid van de bij onderdeel 3 genoemde lijst ligt bij de volgende twee partijen:
   a. de koepelorganisatie van de landelijke kerkgenootschappen en bisdommen;
   b. de landelijke kerkgenootschappen en bisdommen.
6. Het Machtigingenregister MOET bij ontvangst van de bij onderdeel 3 genoemde lijst het waarmerk controleren.

		7. De tekenbevoegd vertegenwoordiger van het landelijke kerkgenootschap, dan wel bisdom, MOET worden geïdentificeerd conform bestaande stelselregels voor de persoon van wettelijke vertegenwoordiger. Alternatief 5: 1. De eisen bij Sub 1, 3, 4, 5, 6 en 7 van Alternatief 4 zijn van toepassing. 2. De (wettelijke) vertegenwoordiger van het kerkgenootschap MOET een verklaring overleggen waarin het bestaan van het lokale kerkgenootschap wordt bevestigd en de "gedelegeerde" wettelijk vertegenwoordigers (indien mogelijk op functieniveau) worden benoemd die aanvragen voor eHerkenningsmiddelen en -machtigingen voor het betreffende lokale kerkgenootschap ter goedkeuring mogen ondertekenen. Deze verklaring heeft de volgende vorm: a. De verklaring staat op briefpapier van het (overkoepelende) kerkgenootschap b. Er is een referentiecode (afkorting) opgenomen welke verwijst naar het overkoepelende kerkgenootschap c. De verklaring is ondertekend door een wettelijk vertegenwoordiger van het landelijke kerkgenootschap die is opgenomen op de gewaarmerkte "Lijst CIO-kerken eHerkenning 3". Elektronische ondertekening is hierbij toegestaan d. De verklaring bevat minimaal de volgende gegevens: i. de naam en KvK nummer van het betreffende lokale kerkgenootschap ii. de naam en KvK nummer van de koepelorganisatie (landelijke kerkgenootschap) iii. de bevoegdheden van het lokale kerkgenootschap iv. de functies en/of personen binnen het lokale kerkgenootschap welke worden benoemd als "gedelegeerd" wettelijk vertegenwoordiger v. de bevoegdheden van de "gedelegeerde" wettelijke vertegenwoordigers 3. De (wettelijke) vertegenwoordiger MOET een verklaring overleggen waarin staat dat de aanvrager namens het lokale kerkgenootschap een eHerkenningsmiddel en -machtiging toegekend mag worden. Deze verklaring heeft de volgende vorm: a. De verklaring staat op briefpapier van het lokale kerkgenootschap b. Er is een verwijzing opgenomen naar de verklaring die is beschreven in Sub 2, zodat daarmee een koppeling gemaakt kan worden c. Er is een referentiecode (afkorting) opgenomen welke verwijst naar het overkoepelende kerkgenootschap d. De verklaring bevat minimaal de volgende gegevens van zowel de aanvrager van het eHerkenningsmiddel en -machtiging, de voor akkoord verklarende "gedelegeerde" wettelijk vertegenwoordiger(s), als van de verklarende kerkleden: i. Naam, adres, woonplaats (NAW gegevens) ii. Functie iii. Geboortedatum iv. Documentnummer WID v. Documenttype WID e. De verklaring is door zowel de aanvrager, de bevestigende "gedelegeerde" wettelijk vertegenwoordiger(s), als door de verklarende kerkleden ondertekend. In totaal hebben er minimaal 5 kerkleden getekend. Hierbij is het toegestaan dat de aanvrager en/of "gedelegeerd" wettelijk vertegenwoordigers ook ondertekenen als kerklid. 4. Het MR verifieert het KvK nummer en vestigingsplaats van de koepelorganisatie en het plaatselijke kerkgenootschap in het handelsregister.
LOA 4	Hetzelfde als LoA3 met toevoeging van: 1. De registratie van een Kerkgenootschap op LoA4 MOET door het MR worden uitgesloten vanwege het ontbreken van gezaghebbende bronnen voor het uitvoeren van validaties.	

2.2 Beheer van elektronische identificatiemiddelen

2.2.1 Kenmerken en ontwerp van elektronische identificatiemiddelen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1		Wachtwoorden die wel voldoen aan de eisen voor sterke wachtwoorden MOGEN ook gebruikt worden op niveau LoA1.

	1. Het authenticatiemiddel MOET tenminste een wachtwoord of PIN zijn, (a) gekozen door de gebruiker of (b) automatisch gegenereerd.	

LOA 2	Hetzelfde als LoA 1 met toevoeging van:
	
	1. Als de authenticatiesessie een wachtwoord omvat dat in de browser van de gebruiker wordt ingevoerd dan MOET dat wachtwoord een zogenaamd 'afgedwongen' en 'sterk' wachtwoord of betreffen.
		De invulling van deze norm MOET in sterkte minimaal en aantoonbaar gelijkwaardig zijn aan de good practice die is aangegeven:
		Het wachtwoord:
		
		• MOET ten minste 8 letters bevatten;
		• MOET ten minste 1 kleine letter bevatten [a-z];
		• MOET ten minste 1 hoofdletter bevatten [A-Z];
		• MOET ten minste 1 cijfer bevatten [0-9];
		• MOET ten minste 1 bijzonder teken bevatten [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~]
		• MAG NIET de gebruikersnaam bevatten;
		• MAG NIET gelijk zijn aan een van de 5 eerder gebruikte wachtwoorden.
		
		Of;
		
		• MOET gebruikmaken van wachtwoordzinnen bestaande uit:
		  • zowel hoofdletters als kleine letters en;
		  • eventueel ook andere tekens en;
		  • minimaal een zinlengte van 20 tekens
		
		In het geval van multifactormiddelen moet de sterkte van de wachtwoordcomponent in de risicocontext worden bepaald.
		Multifactor-authenticatie is alleen op LoA3 en LoA4 en vereiste. Het Stelsel kent echter ook een variant op LoA2 (eTD 2+) waar multifactor-authenticatie een vereiste is.

LOA 3	Hetzelfde als LoA2 met toevoeging van:
	
	1. De authenticatie MOET het gebruik van minimaal twee van de volgende authenicatiefactoren omvatten:
	  a. kennis van de gebruiker,
	  b. uniek bezit van de gebruiker, of
	  c. een biometrische eigenschap van de gebruiker.
	2. Het authenticatiemiddel MOET slechts een response geven na een expliciete handeling van de Gebruiker. De handeling van de Gebruiker MOET buiten de werkingssfeer van de applicatie (o.a. browser) plaatsvinden.
	
	Implementatietermijn
	
	Voor punt 1 en 2 geldt:
	
	Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.
	
	De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.
		Ad 2 Toelichting:
		
		Dit betekent dat:
		
		• de Gebruiker op betrouwbare wijze informatie wordt getoond die bevestigd moet worden met een response van de Gebruiker, of;
		• de gebruiker voert zelf informatie in op middel en maakt zo deel uit maakt van de response.
		
		In deze eis bedoelde handelingen van de Gebruiker zijn bijvoorbeeld:
		
		• Het door de gebruiker invoeren van een ontvangen OTP die op een ander device dan waar het op is ontvangen wordt ingevoerd in de applicatie;
		• Het door de gebruiker invoeren van een PIN op een separate cardlezer waarmee het certificaat als authenticatiefactor wordt ingezet;
		• Het door de gebruiker presenteren en laten 'lezen' van zijn biometrische kenmerk als authenticatiefactor.
		
		Indien zowel de authenticatie-afhandeling als de inlog op het zelfde device kan plaats vinden moet de MU/AD dit risico-gedetecteerd hebben en compenserende maatregelen treffen zoals:
		
		• het de gebruikers wijzen op de risico's van het gebruik van het zelfde device voor de inlog via de browser en risico voor de ontvangst en gebruik van de informatie die nodig is voor de afhandeling van de authenticatie.
		
		Voorbeeldsituaties:
		
		• Inloggen via browser van een smartphone en ontvangst en gebruik op het zelfde toestel van een sms-code voor de afhandeling van de authenticatie.
		• Inloggen via de browser van een tablet waar ook de OTP app op staat.

LOA 4	Hetzelfde als LoA3 met toevoeging van:	Ad 1 Toelichting: De eis omvat de doelstellingen:

	1. Het correct functioneren van het authenticatiemiddel moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'High attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 1508-3 en evaluatie norm ISO/IEC 18045).	• het middel MAG NIET gebruikt kunnen worden zonder expliciete actie van de gebruiker in lijn met het multi-factor gebruik; • het middel MAG NIET andere gegevens bevestigen dan wat de gebruiker verwacht; De toekomstige response van het middel MAG NIET vooraf te bepalen zijn; • Specifiek voor LoA3: Het middel MAG NIET bij eventueel klonen in combinatie met het authenticatiemechanisme bruikbaar zijn.. • Specifiek voor LoA4: Het middel MAG NIET te klonen zijn. De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.

2.2.2 Uitgifte, uitreiking en activering

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Deelnemer MAG NIET de eenmaal uitgegeven tokens aan een andere identiteit koppelen (geen hergebruik van pseudoniemen/usernames); a. Deelnemer MOET om dit aan te tonen gedocumenteerde procedures hebben voor het gecontroleerd uitgeven van tokens, wijzigen van identificerende gegevens en het vastleggen van uitgiftes/wijzigingen (AO /IC).	
LOA 2	1. Tokens met betrouwbaarheidsniveaus 2 MOETEN met een lichte verificatie van de identificerende gegevens van de Aanvrager (bijv. naam en /of adres) worden verkregen. Onderstaande vereisten zijn in het bijzonder van toepassing: 2. Een door de uitgever van het token aangemaakte gebruikersnaam en wachtwoord MOET separaat verzonden worden met gebruikmaking van een 'buiten de bandprocedure' naar een van tevoren tijdens het registratieproces door de Aanvrager aangegeven plaats. 3. Een token dat rechtstreeks van internet is gedownload door de Aanvrager na het volgen van de registratieprocedure komt tot stand door een link door te geven naar een plaats die de Aanvrager tijdens het registratieproces heeft opgegeven; in dat geval MOET de link na 24 uur verlopen zijn. 4. De Deelnemer MOET de Gebruiker op de hoogte brengen van het procesverloop van aanvraag tot uitgifte van het middel. 5. De Deelnemer MOET de Gebruiker notificeren dat een middel op zijn naam is uitgegeven.	Ad 1 en 2: Indien het om een middel gaat dat slechts in de context van de Dienstafnemer kan worden gebruikt mag het adres waar naar het token wordt gezonden door de Dienstafnemer worden opgegeven. Ad 4, 5 en 6 Toelichting: Doelstelling van deze eisen is: • De Gebruiker wordt in staat gestelde om de naam van de Authenticatiedienst waar hij het middel heeft aangeschaft te bewaren ter herinnering voor later gebruik. • De Gebruiker wordt in staat gesteld afwijkingen in het proces van uitgifte van een middel te detecteren. • De Gebruiker wordt in staat gesteld om te vast te stellen dat er een middel terecht op zijn naam is uitgegeven. Good practice: Voorbeelden van notificaties: • Het verzenden van een bericht (email of brief) aan de Gebruiker dat bewaard kan worden ter herinnering. In het bericht is de naam van de AD waar het middel is geregistreerd opgenomen. Deze practice geeft daarnaast alleen bescherming bij een aanvraag voor een tweede middel op naam van de gebruiker. • Het gebruik van een mededeling in een terugboeking door AD/MU van een eerdere betaling door Gebruiker met een bankrekening op de opgegeven voor- en achternaam. Deze maatregel geeft enige bescherming bij toepassing voor nieuwe als bestaande Gebruikers, op voorwaarde dat de tenaamstelling van de bankrekening overeenkomt met de naam op het WID. • Het verzenden van een brief naar een adres dat is gekoppeld aan de voor en achternaam van de Gebruiker. Het adres is geverifieerd aan een origineel uittreksel uit de BPR dat de gebruiker heeft overhandigd. Ad 6: Toelichting: De betrouwbaarheid van de associatie met de voornaam een achternaam van de gebruikers neemt toe naarmate de validatie van de associatie onafhankelijker van het registratieproces uitgevoerd kan worden.

	6. De Deelnemer MOET de Gebruiker notificeren van de uitgifte via een kanaal dat betrouwbaar is geassocieerd met de voornaam en achternaam van de gebruiker.	
LOA 3	Het token wordt met een gemiddelde verificatie van de identificerende gegevens van de aanvrager (bijv. naam en/of adres) verkregen.	Onderstaande voorbeelden verduidelijken dit type uitgifte van een token: Het token wordt per aangetekende post verzonden na voorafgaande validatie van het opgegeven adres bij een officiële identiteitsdatabase waar dit fysieke adres geregistreerd staat. Dit betekent: a) Het token wordt verzonden naar adres van de Dienstafnemer dat in het Handelsregister is opgenomen geadresseerd aan de Gebruiker, Machtigingenbeheerder of de Wettelijke vertegenwoordiger of; b) Het token wordt verzonden naar het adres van de Gebruiker zoals dit door de Dienstafnemer is opgegeven. Het risico dat het niet de bevoegde vertegenwoordiger(s) van de Dienstafnemer is die verzocht heeft om de uitgifte van het middel moet worden gemitigeerd. Acceptabele mitigerende maatregelen zijn in elk geval: i. In het geval het verzoek is gedaan door 1 wettelijke vertegenwoordiger of machtigingenbeheerder heeft verzocht om de uitgifte van het middel. Moet de Dienstafnemer van de verzending worden genotificeerd middels een brief naar het adres van de Dienstafnemer dat in het Handelsregister is opgenomen met het verzoek te reageren indien de uitgifte ongedaan gemaakt moet worden. De brief is gesteld geadresseerd aan de Machtigingenbeheerder of Wettelijke vertegenwoordiger van de Dienstafnemer. Alternatief voor een persoonlijke brief is een mail aan de in b) genoemde vertegenwoordigers op hun persoonlijke mailadres in het geverifieerde domein van de Dienstafnemer. ii. In het geval 2 wettelijke vertegenwoordigers, machtigingenbeheerders of een combinatie daarvan het verzoek hebben gedaan is de notificatie aan de dienstafnemer zoals bedoeld bij punt b) i. geen verplichting. c) Het token wordt verzonden naar het adres dat is gekoppeld aan de voor en achternaam van de Gebruiker. Het adres is geverifieerd aan een origineel uittreksel uit de BRP. Alternatieven a) en b) mogen gebruikt worden voor middelen die slechts bruikbaar zijn in de context van de Dienstafnemer. De authenticatiefactoren van het authenticatiemiddel worden gescheiden in tijd verzonden of worden via verschillende communicatiekanalen verzonden. Het is denkbaar dat voor de verzending van de verschillende authenticaticatiefactoren een combinatie van hetgeen onder a) en b) is gesteld wordt gebruikt. Indien een van de authenticatiefactoren naar het email adres van de gebruiker wordt verzonden moet dit email adres zijn geverifieerd. Opgave van het email-adres door de Dienstafnemer op een met b) vergelijkbare wijze is toegestaan mits de gebruiker juistheid van het email-adres voorafgaande aan de verzending van de authenticatiefactor heeft bevestigd. Het token is gedownload van internet nadat het verzoek om een verklaring door de aanvrager ondertekend is met een gekwalificeerde handtekening in overeenstemming met de voorwaarden van de Richtlijn elektronische handtekeningen en geverifieerd door een CSP. Onmiddellijk na de verificatie MOET het token snel aangemaakt worden door de CSP en op de browser van de aanvrager worden gedownload. Het token wordt rechtstreeks door de aanvrager gedownload na het invoeren van een persoonlijk wachtwoord dat aan de aanvrager is uitgereikt tijdens de registratie op ten minste niveau 3.
LOA 4	1. Tokens met betrouwbaarheidsniveau 4 MOETEN met een zware aanvangsverificatie van de identificerendegegevens van de Aanvrager worden verkregen. Onderstaande vereisten zijn in het bijzonder van toepassing: a. De token MOET persoonlijk aan de Aanvrager worden afgegeven, na validatie	

	van de identiteit van de Aanvrager; of; b. de token MOET naar de Aanvrager verzonden en geactiveerd worden na validatie van diens identiteit door fysieke registratie.	

2.2.3 Schorsing, herroeping en reactivering

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2	1. De Deelnemer MOET een werkend proces hebben voor het intrekken van authenticatiemiddelen. 2. Het resultaat van het proces MOET zijn dat een ingetrokken authenticatiemiddel niet meer gebruikt kan worden in het Stelsel. 3. De Deelnemer MAG (optioneel) de mogelijkheid tot schorsing van een authenticatiemiddel aanbieden 4. De deelnemer die het authenticatiemiddel heeft verstrekt MOET het middel intrekken of schorsen ingeval: a. Een verzoek tot intrekking of schorsing is gedaan door de Gebruiker van het authenticatiemiddel; b. Een verzoek tot intrekking of schorsing is gedaan door een vertegenwoordigingsbevoegde van de Gebruiker van het authenticatiemiddel. c. Het middel blijkt te zijn gecompromitteerd; d. Het middel aantoonbaar kwetsbaar is geworden voor manipulatie of misbruik; e. De Gebruiker van het authenticatiemiddel zijn gebruiksverplichtingen niet nakomt. 5. Indien een bevoegde vertegenwoordiger van de Gebruiker verzoekt om schorsing van het middel MOET de Deelnemer aan de vertegenwoordigingsbevoegde duidelijk maken dat de Gebruiker in staat zal zijn om het middel te heractiveren als deze zijn mogelijkheden tot heractivatie in bezit behoudt. 6. De Deelnemer MOET aan kunnen tonen dat middelen die zijn ingetrokken of geschorst vanaf het moment van intrekken of schorsen niet meer gebruikt zijn. 7. De Deelnemer MOET afdoende hebben geverifieerd dat het verzoek tot intrekking of schorsing door de bevoegde vertegenwoordiger is gedaan. De Deelnemer MOET het risico afwegen dat het verzoek niet door de bevoegde vertegenwoordiger is gedaan tegen de schade voor de gebruiker die het afhandelen of het niet afhandelen van het verzoek veroorzaakt. De Deelnemer MOET de risicoafweging vastleggen. a. De risicoafweging MOET een gedocumenteerde procedure zijn waarlangs de beslissing tot stand moet komen en waaraan de uitkomst van een beslissing tot revocatie of schorsing kan worden geverifieerd of; b. De risicoafweging betreft een documentatie per gemaakte afweging die in het dossier van de gebruiker wordt opgenomen. 8. De Deelnemer MOET een het authenticatiemiddel na ontvangst door de Deelnemer van het verzoek tot intrekking of schorsing binnen een (1) werkdag hebben ingetrokken of geschorst. 9. De Deelnemer MOET bij een verzoek tot heractivering van een geschorst authenticatiemiddel dit verzoek valideren als afkomstig van de Gebruiker van het middel of zijn vertegenwoordigingsbevoegde. De wijze van validatie MOET in overeenstemming zijn met het LoA van het geschorste authenticatiemiddel: a. De Deelnemer MOET de Gebruiker of zijn vertegenwoordigingsbevoegde identificeren.	Toelichting: Doel van deze eis is dat de gebruiker van het middel zekerheid krijgt over intrekking of schorsing van het middel als hij daar om verzoekt. Toelichting bij 3: Een vertegenwoordigingsbevoegde kan bijvoorbeeld zijn een Voogd, De Rechtbank of een Bewindvoerder. De identiteit van een Voogd of Bewindvoerder en een beslissing van de Rechtbank kan worden geverifieerd aan een onafhankelijke bron. Good practice voor het verificatie van de identiteit van de Gebruiker bij een verzoek tot intrekking en schorsing/her-activering: • Verstrekken van een code bij de uitgifte van een authenticatiemiddel aan de gebruiker die voor revocatie en schorsingen/her-activering kan worden gebruikt. Tevens wordt de Gebruiker verzocht om beveiligingsvragen te beantwoorden (zogenaamd gedeeld geheim tussen de MU/AD en Gebruiker). De verstrekte code en de antwoorden op de beveiligingsvragen geven samen afdoende zekerheid dat de gene die het verzoek doet tot revocatie en schorsing/her-activering de Gebruiker is. • Een online-dienst waarmee de gebruiker met inzet van zijn authenticatiemiddel(en) een authenticatiemiddel waarvan hij Gebruiker is kan laten intrekken, schorsen en her-activeren. • In het proces voor schorsing (indien ondersteund) MAG soepeler worden omgegaan met de authenticatie van degene die de schorsing meldt met het oog op snellere verwerking. In dat geval moet de afwijking van het normale authenticatieproces expliciet vastgelegd zijn.

	b. De Deelnemer MOET verifiëren bij de geïdentificeerde Gebruiker of deze het betreffende verzoek heeft gedaan. c. Een schorsing MAG eindigen op een moment dat bij het indienen van het verzoek is overeenkomen met de verzoeker. d. De Deelnemer MOET de Gebruiker notificeren over statuswijzigingen over een communicatiekanaal dat is overeengekomen in het proces van het registratie en uitgifte van het middel.	
LOA 3 4	Hetzelfde als LoA1 met toevoeging van: 1. De Deelnemer MOET een het authenticatiemiddel na ontvangst door de Deelnemer van het verzoek tot intrekking of schorsing binnen vierentwintig (24) uur hebben ingetrokken of geschorst:	

2.2.4 Verlenging en vervanging

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Betrouwbaarheidsniveau van het vernieuwingsproces MOET in elk geval gelijk zijn aan het betrouwbaarheidsniveau van eerste uitgave. 2. De levensduur van een credential voordat vernieuwing of intrekking plaatsvindt MOET gebaseerd zijn op een risicoanalyse die de kwaliteit van de onderliggende techniek en noodzaak voor 'proof of life' van de gebruiker in beschouwing neemt. Deze risicoafweging van de levensduur van het middel moet periodiek getoetst worden aan de laatste stand der techniek. 3. Een gebruiker MAG met een bestaand geldig middel vernieuwing aanvragen op hetzelfde betrouwbaarheidsniveau.	
LOA 2 3 4	LoA1 met toevoeging van: 1. De Deelnemer MOET de verwachte levensduur van een authenticatiemiddel jaarlijks vaststellen op basis van een analyse van de kenmerken en kwetsbaarheden van het middel. 2. Een Authenticatiemiddel waarvan is aangetoond dat deze kwetsbaar is geworden voor misbruik of manipulatie MOET door de Deelnemer worden ingetrokken. 3. De vastgestelde levensduur van een authenticatiemiddel MOET zijn gerelateerd aan de te verwachten technische levensduur van het middel maar ZOU niet meer MOETEN zijn dan tien (10) jaar. 4. De Gebruiker MOET minimaal elke tien (10) jaar het gehele proces identificatie tot de uitgifte van een authenticatiemiddel opnieuw doorlopen. 5. De Deelnemer MAG een authenticatiemiddel vernieuwen op basis van een bestaand en geldig authenticatiemiddel. Het vernieuwde authenticatiemiddel MOET aan de Gebruiker worden verstrekt met de zekerheid die behoort bij het LoA van het authenticatiemiddel dat wordt vernieuwd en voldaan wordt aan punt 4. 6. Voor LoA3 en LoA4 middelen die bedoeld zijn voor gebruik in het BSN domein: a. De Deelnemer MOET tenminste een maal per vijf (5) jaar vaststellen dat de Gebruiker nog in bezit is van zijn middel.	Ad 3. Een authenticatiemiddel bestaat uit een technische component en procedurele component. Voor de maximale levensduur van het het middel (technisch en procedureel) is aangesloten bij de levensduur van paspoorten en gekwalificeerde certificaten. Het is vanuit optiek van het Stelsel belangrijker dat de kwetsbaarheid van de verschillende technische componenten van het middel wordt gemonitord door de AD/MU dan dat een specifieke levensduur wordt opgelegd van de technische componenten waaruit een middel kan bestaan. Ad 4. Het is altijd mogelijk dat er in de loop van de tijd fouten gemaakt worden waardoor een persoon niet of niet meer in bezit is van de juiste credentials om over een specifiek middel te mogen beschikken. Daarom is het nodig om personen periodiek opnieuw te identificeren conform het proces van de initiële uitgifte van een middel. Bij de keuze voor de termijn van 10 jaar is aangesloten bij de bestaande praktijk voor het vernieuwen van Nederlandse identiteitsbewijzen. Ad 5. Om dezelfde reden als bij 4. en omdat misbruik door derden niet is uit te sluiten van gestolen, verloren middelen of middelen van bijvoorbeeld overledenen is een extra vorm van controle voorgeschreven die eens in de 5 jaar plaatsvindt. good practice voor middelen die bedoeld zijn voor gebruik in het BSN domein op LoA3 en LoA4: • Uitvoeren van een her-registratie van het middel bij BSNk. Indien een gebruiker niet meer in leven zou zijn geeft BSNk een foutmelding. Deze toets wordt aangevuld met een toets op recent gebruik van het middel in de laatste 12 maanden. Voorbeelden van overige good practices:

	Indien de Deelnemer niet kan vaststellen of de Gebruiker nog in bezit van zijn middel MOET de Deelnemer het authenticatiemiddel intrekken of schorsen. b. De Deelnemer MAG deze eis ook invullen voor ander LoA's en middelen die niet bedoeld zijn voor gebruik in het BSN domein.	• Uitvoeren van een banktransactie die alleen op naam van de Gebruiker staat in combinatie met het gebruik van zijn middel. • De Gebruiker wordt telefonisch, per brief of per email verzocht zijn om binnen een vastgestelde periode (bijv. twee maanden) met zijn middel in te loggen bij zijn AD/MU en een drietal beveiligingsvragen te beantwoorden (zogenaamd gedeeld geheim tussen de MU/AD en Gebruiker) die bij de uitgifte van het middel zijn overeengekomen met de gebruiker.

2.3 Authenticatie

2.3.1 Authenticatiemechanisme

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. De gebruiker MOET in staat worden gesteld om de website/app van de authenticatiedienst en alle andere partijen in het netwerk te authenticeren. 2. De HM MOET in het keuzescherm voor de AD tonen bij welke dienst de Gebruiker gaat inloggen. 3. De AD MOET in het aanlogscherm tonen bij welke Dienstverlener de Gebruiker gaat aanloggen. 4. Optioneel: De AD/MU MAG de Gebruiker aanbieden om de notificatiemethode voor LoA4 (onder d.) toe te passen op de lagere LoA's. 5. Het authenticatiemechanisme MOET 'enige' bescherming bieden tegen ondertaande dreigingen: a. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden. b. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen. c. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller. d. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen. e. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt. f. 'Enige bescherming' MOET worden aangetoond door middel van een risicoanalyse en bijbehorende mitigerende maatregelen. 6. De Deelnemers in het Stelsel MOETEN zekerstellen dat de risico's van identiteitsfraude en misbruik van de tokens worden geanalyseerd en gemitigeerd tot het toepasselijke betrouwbaarheidsniveau.	Ad 1 Dit kan bijvoorbeeld op basis van een TLS certificaat of een digitale handtekening op basis van een vertrouwd certificaat.
LOA 2	Hetzelfde als LoA1	
LOA 3	Hetzelfde als LoA1 met toevoeging van:	Ad 1 Toelichting: Authenticatie onder een merk van het AS wil zeggen onder eHerkenning. Als het middel wordt gebruikt in een andere context moet het

1. Bij gebruik van het authenticatiemiddel MOET de Gebruiker expliciet duidelijk gemaakt worden dat hij een authenticatie in de context van een Stelselmerk uitvoert, ook wanneer zijn applicatie (o.a. de browser) of platform (o.a. PC) waarop de applicatie actief is gecorrumpeerd is. Indien het middel buiten de Stelselcontext wordt gebruik MAG een Stelselmerk NIET getoond worden.
2. De toegang tot diensten van elke afzonderlijke dienstverlener MOET het aanloggen met behulp van het authenticatiemiddel vereisen.
3. Het authenticatiemechanisme MOET bescherming bieden tegen de meeste van deze dreigingen:
    a. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden.
    b. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen.
    c. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller.
    d. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen.
    e. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt.
    f. Bescherming MOET worden aangetoond door een risicoanalyse en bijbehorende mitigerende maatregelen.
4. De MU/AD MOET jaarlijks het authenticatiemechanisme onderwerpen aan een risico analyse daarbij rekening houdend met (nieuwe) aanvalstechnieken en kwetsbaarheden. Dit omvat een vergelijking van de gebruikte cryptografische algoritmen en sleutellengtes met de actuele 'good practice'. Indien de analyse daar aanleiding toe geeft worden middelen aangepast en/of vervangen.
5. Het correct functioneren van het authenticatiemechanisme moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'moderate attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 15408-3 en valuatie norm ISO/IEC 18045).

Implementatietermijn

Voor punt 1 en 2 geldt:

Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.

middel die notificatie achterwege laten of de andere context aangeven. Doel is om hiermee het transactierisico voor de gebruiker verminderen in het geval dat zijn applicatie/browser is gecorrumpeerd.

Ad 2 Toelichting: Single Sign On voor diensten van een enkele dienstverlener op LoA3 en LoA4 is toegestaan. SSO tussen dienstverleners is slechts toegestaan op LoA1 en LoA2. Beide situaties uiteraard met handhaving van de beperking dat de LoA van het middel alleen toegang mag geven tot diensten met een zelfde LoA of een lagere LoA. Single Sign On tussen Dienstverleners moet op LoA3 en LoA4 worden beperkt. Het betrouwbaarheidsniveau wordt met SSO tussen dienstverleners te veel ondermijnd omdat de transactie kwetsbaar wordt voor Man-in-the-front en Man-in-the-browser aanvallen. Daarnaast accepteren Dienstverleners in formeel juridische zin een authenticatie en daarmee kan SSO tussen dienstverleners op LoA3 en LoA4 niet alleen meer een oplossing zijn voor gebruiksgemak.

Ad 5 Toelichting: De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.

	De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.	
LOA 4	LoA3 met toevoeging van: 1. Het auhenticatiemiddel MOET de Gebruiker notificeren (onafhankelijk van de browser die hij gebruikt) van zijn inlogpoging bij een specifieke dienst of dienstverlener . 2. De notificatie MOET zijn gekoppeld aan het gebruik van diensten op het niveau van het middel. 3. De Deelnemer MAG een optie aanbieden om de notificatiedienst door de gebruiker zelf aan en uit te laten zetten voor diensten op het LoA van het middel of lager. 4. De notificatie ZOU de Gebruiker binnen een tijdsbestek MOETEN bereiken zodat de notificatie zijn beslissing om de inlog voort te zetten of af te breken kan beïnvloeden. 5. Het authenticatiemiddel MOET een betrouwbaar (trusted) kanaal bevatten ten behoeve van betrouwbare notificatie en bevestiging, ook wanneer zijn voor inlog gebruikte applicatie of het platform (o.a. PC) waarop de applicatie actief is gecorrumpeerd is. Dit kanaal MOET de mogelijkheid bevatten om de gebruiker elementen in het authenticatieverzoek te laten bevestigen. 6. De Deelnemer MOET de Gebruiker bij het aanbieden van de notificatiedienst er op attenderen dat hij als Gebruiker zelf verantwoordelijk is voor de beveiliging van zijn browser en zelf dus ook verantwoordelijk draagt voor de beslissing om in te loggen. 7. Het correct functioneren van een authenticatiemechanisme (en het authenticatiemiddel) moet weerstand bieden tegen fysieke en logische manipulatie door een aanvaller met een 'High attacker' potentieel in de zin van Annex B van de Common Criteria (ISO 1508-3 en evaluatie norm ISO/IEC 18045). **Implementatietermijn** Voor punt 5 geldt: Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen. De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.	Toelichting: Doel van de eis is om de Gebruiker in staat te stellen een fout of inbreuk in de communicatie te herkennen en bij twijfel de informatietransactie af te breken. Het is altijd mogelijk dat de browser van de Gebruiker gecompromitteerd raakt daarom is voor LoA4 is een extra maatregel opgenomen die bij implementatie gekoppeld mag worden op het middel of op de dienst. Een voorbeeld is verzending van een SMS als een internet browser wordt gebruikt om in te loggen. Bij frequent gebruik van een middel voor diensten op lagere LoA's kan dat door de gebruiker als bezwarend worden ervaren om steeds SMS's te ontvangen, daarom mag een optie aangeboden worden om de dienst door de gebruiker zelf uit te laten zetten. Ook mag de optie worden aangeboden de de gebruiker notificatie te koppelen aan het gebruik van diensten op het LoA van het middel of lager. Ad 5 Toelichting: Het gaat er om dat de gebruiker via het 'trusted' kanaal hoogst betrouwbaar informatie over zijn inlog bij de DV of dienst kan worden gegeven en om hoogst betrouwbare bevestiging kan worden worden gevraagd van een specifiek transactiegegeven. Deze betrouwbaarheid blijf bestaan ook al is de gebruiker slachtoffer van een aanval op zijn inlog-applicatie zoals zijn browser en de PC van de gebruiker (man-in-the-browser attack/man-in-the-front attack). Bij het nemen van maatregelen voor het betrouwbare kanaal moet dus worden uitgegaan van de idee dat de gebruikersomgeving is gecorrumpeerd. Ad 7 Toelichting: De wijze waarop conformiteit met deze eis moet worden aangetoond is aangegeven in paragraaf 2.4.7 Compliance en Audit.

	1. Implementatiedatum voor nieuwe middelen: 31 december 2018 (2 1/2 jaar na vaststelling door TB en rekening houdend met overige implementatie-inspanningen in de periode juli-dec 2016) 2. Implementatiedatum voor bestaandemiddelen: 31 december 2019 (geldigheidstermijn gekwalificeerde certificaten en rekening houdend met overige implementatie-inspanningen in de periode juli-dec 2016) 3. Periodieke evaluatie implementatiedata: Het security officers overleg evalueert elke 6 maanden de noodzaak tot aanpassing van de implementatiedata en adviseert na consultatie van de governance om de implementatie termijn te vervroegen, te verlaten of te handhaven. De evaluatie gebeurt aan de hand van de context van Europese ontwikkelingen), Nederlandse ontwikkelingen en ontwikkeling van het risico dat de kwetsbaarheid (ontbreken van een trusted channel) wordt misbruikt.	

2.4 Beheer en organisatie

2.4.1 Algemene bepalingen

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Partijen die deelnemen in het Stelsel MOETEN het toetredingsproces hebben doorlopen dat is vastgelegd in het Afsprakenstelsel. Het is van belang dat de Deelnemer identificeerbaar is en kan voldoen aan zijn verplichtingen. Daarvoor MOET de Deelnemer bij toetreding en daarna voldoen aan de volgende vereisten: a. De Deelnemer drijft een onderneming en MOET als zodanig zijn ingeschreven in het Nederlandse Handelsregister. De Deelnemer MOET binnen het Stelsel uitsluitend een geregistreerde handelsnaam hanteren. b. De Deelnemer MAG NIET in staat van faillissement verkeren, aan hem MAG NIET een surseance van betaling zijn verleend en voor hem MAG NIET een schuldsaneringsregeling van toepassing zijn. Ook MAG NIET ten aanzien van de deelnemer een faillissement zijn aangevraagd en de Deelnemer MAG NIET zijn gestopt met het betalen van zijn schulden. c. Als combinaties van deelnemers willen toetreden dan is dat mogelijk. In dat geval dienen alle deelnemers te voldoen aan de toetredingseisen.	Ad 1 Het Afsprakenstelsel Elektronische Toegangsdiensten is een publiek private samenwerking onder vigerend Nederlands Recht. Alle verplichtingen die een deelnemer aangaat bij toetredingen zijn vastgelegd in het Juridisch kader. De specifieke vereisten m.b.t privacybescherming en informatiebeveiliging zijn opgenomen in het Privacybeleid respectievelijk het B eleid voor informatiebeveiliging. Het proces voor toetreding is vastgelegd in het Operationeel Handboek, Proces toetreden. Onderdeel van dit proces is een toetsing door de Toezichthouder van de relevante processen, procedures en uitgevoerde technische tests. Ad 2 Hoe deze algemene regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval. De deelnemer kan zijn aansprakelijkheid beperken in de overeenkomst die hij sluit met een dienstafnemer of met een dienstverlener. Daarbij blijft hij gebonden aan de algemene regels van het Nederlandse recht inzake aansprakelijkheid en schadevergoeding. Ad 3 De aansprakelijkheidsregels zijn opgenomen in het Juridisch kader Ad 4 Deze eIDAS eis overlapt de eis met betrekking tot sub-contractanten in 2.4.5. Zowel het Juridisch kader en vooral het Gemeenschappelijk normenkader informatiebeveiliging bevatten voor deze eis relevante specificaties.

	2. Binnen het afsprakenstelsel MOET iedere deelnemer aansprakelijk zijn voor zijn eigen handelen en/of nalaten voor de rol die hij vervult. Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. De deelnemers MOGEN NIET afwijken van deze algemene regels. 3. De beheerorganisatie MOET door de Deelnemer op de hoogte worden gesteld van de mate waarin de Deelnemer onafhankelijk kan opereren. De Deelnemer MOET minimaal informatie verstrekken over: a. De buitenlandse stakeholders in de Deelnemer of moedermaatschappij van de deelnemer;De mate waarin stakeholders in de Deelnemer of moedermaatschappij van deelnemer zeggenschap hebben over de procesgang binnen de Deelnemer; b. de scheiding van processen en verantwoordelijkheden tussen de Authenticatiedienst en de overige onderdelen van de organisatie, in het geval de Authenticatiedienst onderdeel is van een grotere organisatie. c. Daar waar de onafhankelijkheid of betrouwbaarheid van de deelnemer in twijfel is MAG de Toezichthouder van het Stelsel nadere eisen stellen aan de deelnemer om het voldoen aan wettelijke eisen te waarborgen en imagoschade voor het Stelsel te voorkomen. 4. Alle Deelnemers MOETEN voldoen aan de stelseleisen inzake de naleving van verplichtingen bij uitbesteding of gezamenlijk uitvoeren van activiteiten. a. De Deelnemers zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. b. Als een combinatie onder een gemeenschappelijke naam als 'een organisatie' diensten wil verrichten geldt de eis dat: i. De leden van de combinatie vanaf de start van deelname hoofdelijk aansprakelijk MOETEN zijn voor de volledige en correcte nakoming van alle juridische verbintenissen die in het kader van het Stelsel zijn aangegaan. ii. Alle combinanten MOETEN individueel voldoen aan de toetredingseisen. Bij wijziging in de samenstelling van de combinatie MOET de toetredingsprocedure door nieuwe leden van de combinatie opnieuw worden doorlopen.	
LOA 2 3 4	LoA1 met toevoeging van: 1. Deelnemer MOET in het bezit te zijn van een aansprakelijkheidsverzekering die dekkend is voor aansprakelijkheidseisen die kunnen voortvloeien uit het opereren als onderdeel van het Stelsel. 2. Deelnemer MOET beschikken over een continuïteitsplan/exitplan dat in werking treedt op het moment dat deelnemer niet	

	meer aan zijn Stelselverplichtingen kan voldoen of wenst te voldoen. Het continuïteitsplan/exitplan MOET ten minste waarborgen treffen voor het ondersteunen van de bestaande klanten van de deelnemer voor de periode die is afgesproken in contracten met deze klanten. 3. Als de Deelnemer niet beschikt over een aansprakelijkheidsverzekering MOET een deelnemer op andere wijze afdoende aantonen dat eventuele aansprakelijkheidsclaims kunnen worden gedekt (bijvoorbeeld uit eigen middelen).	

2.4.2 Gepubliceerde mededelingen en informatie voor de gebruikers

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Het Afsprakenstelsel MOET openbaar toegankelijk gepubliceerd zijn. Deelnemers MOETEN de stelselvereisten inzake publicatie van dienstbeschrijvingen en gebruiksvoorwaarden naleven.	Ad 1 De bedoelde vereisten voor zijn vastgelegd in de het Operationeel handboek en de Gebruiksvoorwaarden Elektronische Toegangsdiensten. Daarnaast betreft het de naleving van algemene wettelijke verplichtingen inzake gebruiksvoorwaarden en privacy. Specifiek stelselvereisten voor privacybescherming zijn opgenomen in het Privacybeleid van het stelsel.
LOA 2 3 4	Zelfde als LoA1 met toevoeging van: 1. De Deelnemer MOET de Gebruiker online inzicht bieden in: a. de gegevens die over hem zijn vastgelegd ten behoeve van de uitgifte van een authenticatiemiddel of registratie van een machtiging; b. de authenticatiemiddelen die op zijn naam zijn uitgegeven en indien van toepassing door hem afgegeven machtigingen; c. de transacties die met middelen op zijn naam zijn uitgevoerd (datum, tijd, dienstverlener, dienst). 2. Indien een persoon claimt niet meer over zijn middel te beschikken of claimt dat ten onrechte op	Ad 1 Doel van deze eis: De Gebruiker wordt in staat gesteld om anomalieën in het gebruik van zijn middel te ontdekken en met deze informatie in contact te treden met een dienstverlener. De persoon op wiens naam ten onrechte een middel is uitgegeven wordt in staat gesteld registraties op zijn naam en de transacties die met het middel op zijn naam gedaan in te zien. good practice: De Deelnemer geeft zich rekenschap van het feit dat het gaat om toegang tot persoonsgegevens de zin van de AVG. Verwacht mag worden dat de maatregelen die de Deelnemer treft voor bescherming van de toegang tot de transactiegegevens altijd gerelateerd is het LoA van de middel van de Gebruiker. Ad 3 Toelichting bij 3a: Hier is uitgegaan van de situatie dat een fraudeur gebruik heeft gemaakt van identificerende kenmerken van de persoon die claimt dat ten onrechte een middel op zijn naam is uitgereikt. De identificerende kenmerken van de claimant moeten dus overeenkomen met de identificerende kenmerken die zijn gebruikt bij de registratie en uitgifte van het middel. Dat betekent dat de claimant zich kan identificeren als ware hij de daadwerkelijke gebruiker. Een deelnemer mag hier niet van af wijken omdat het risico bestaat dat persoonsgegevens ten onrechte ter inzage worden gegeven. In het geval de identificerende kenmerken niet overeenkomen is een andere juridische basis nodig om de gegevens te verstrekken zoals in het kader van formele opsporing of gerechtelijk bevel.

	zijn naam een middel is uitgegeven MOET de Deelnemer fysiek inzicht geven in de gegevens genoemd onder 2a. 3. De Deelnemer MOET en allen tijde op afdoende wijze vaststellen dat inzage in de gegevens genoemd onder 2a. wordt verstrekt aan de juiste persoon. a. In alle gevallen MOET de Deelnemer een persoon die toegang tot de gegevens vraagt fysiek of online identificeren als ware het de Gebruiker. b. De Deelnemer MOET de Gebruiker toegang verstrekken tot de gegevens op minimaal hetzelfde LoA als het LoA van het middel dat aan de Gebruiker is uitgereikt.		

2.4.3 Beheer van informatiebeveiliging

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2 3 4	1. De Deelnemers en de Beheerorganisatie MOETEN een systeem voor het management van informatiebeveiliging inrichten waarin minimaal hun dienstverlening voor het Stelsel MOET zijn ondergebracht. Het managementsysteem MOET zijn ingericht conform de ISO/IEC 27001:2013 standaard en MOET zijn gecertificeerd of de Deelnemer en de Beheerorganisatie MOETEN beschikken over een Third Party Mededeling met gelijkwaardige conformiteitsverklaring (TPM) van een onafhankelijke Register EDP auditorgelijkwaardige. Hierna wordt kortweg gesproken over een TPM. De toetsing van opzet, bestaan en werking van geïmplementeerde controls en implementatie van de stelselafspraken over de technische invulling maken onderdeel uit van het certificaat of de TPM (inclusief conformiteitsverklaring). 2. De Deelnemer in het Stelsel MOET het risico's op identiteitsfraude onderkennen en in het ontwerp en implementatie van processen voor middelenuitgifte mitigeren. a. De Deelnemer MOET in de risicoanalyse in het kader van de ISO 27001 certificering het procesontwerp van de processen voor registratie en uitgifte van middelen hebben geadresseerd. b. De Deelnemers en Beheerorganisatie MOETEN de op risico gebaseerde beslissingen t.a.v. het ontwerp en de implementatie van mitigerende beheersmaatregelen vastleggen. c. De Deelnemer in het Stelsel MOET iedere afwijking van de vereisten voor de implementatie van risico-verlagende beheersmaatregelen toelichten en vastleggen. d. De Deelnemers in het Stelsel MOETEN erop toezien dat procesgerelateerde gebeurtenissen herleidbaar zijn. Deelnemers MOETEN de procesvoorvallen registreren, wanneer deze betrekking hebben op: de aanvraag van een token het resultaat van de toegepaste verificaties en validaties aanvaarding en weigering van aanvragen.	Ad 1 Dit is een eis die aan alle Deelnemers en Beheerorganisaties wordt gesteld als onderdeel van de basisbeveiliging van het Stelsel.

2.4.4 Bijhouden van de administratie

LoA	Vereiste elementen	Toelichting en good practice

LOA 1 2 3 4	1. Algemene vereisten voor registratie en archivering;De invulling van deze norm voor record keeping MOET de volgende doelstellingen ondersteunen: a. Het voldoen aan wettelijke verplichtingen; b. Dispute resolution in geval van (fraude) claims; c. Het vastleggen van adequate audit trails. 2. Deelnemers aan het Stelsel MOETEN toezien op naleving van het toepasselijke belasting- en privacyrecht. 3. De Deelnemer in het Stelsel MOET kopieën van identiteitsbewijzen archiveren conform de onderstaande eisen: a. Het type identiteitsbewijs en het documentnummer van het identiteitsbewijs MOET geregistreerd en gearchiveerd worden. b. Persoonsgegevens zoals een foto, het Burger Service Nummer (BSN) en de nationaliteit MOETEN bij archivering en opslag conform de AVG verwerkt worden. 4. Op LoA3 en LoA4 MOET de deelnemer de registraties en logging zodanig vastleggen dat deze kunnen worden gebruikt voor bewijsvoering in geval van fraudeonderzoek of claims van misbruik. Het is toegestaan om gevoeliger gegevens vast te leggen als die het doel dienen om te bewijzen dat een middel zorgvuldig is uitgegeven en gebruikt. 5. Specifieke vereisten voor registratie en archivering: De deelnemer aan het Stelsel MOET een log bijhouden van alle uitgevoerde verificaties en validaties. Het betreft minimaal de: a. validaties van inschrijvingen in het Handelsregister van de Kamer van Koophandel. b. validaties van handgeschreven handtekeningen c. validaties van een identiteit door bankoverschrijving d. validaties van elektronische handtekeningen e. validaties van authenticaties in het elektronische registratieproces f. elektronische berichten met een identiteitsverklaring van de Aanvrager ter registratie, waaronder de verplichte bijlage. g. controles van (interne) Machtigingen 6. Archivering van verificaties en validaties is verplicht: a. gedurende de geldigheidsduur van uitgegeven middelen en; b. tot 7 jaar na intrekking of verlopen van het middel. 7. Met het oog op de betrouwbare elektronische communicatie MOETEN de deelnemers voldoen aan volgende eisen ten aanzien van archivering: a. Elke Deelnemer MOET gearchiveerde gegevens beveiligd opslaan zodat zij niet toegankelijk zijn voor onbevoegden. Elke Deelnemer MOET alle door haar ondertekende en alle door haar ontvangen ondertekende berichten 7 jaar archiveren. Na deze periode MOETEN ten minste de persoonsgegevens in deze berichten vernietigd worden. Een Deelnemer MAG NIET persoonsgegevens afkomstig van berichten of bewijsstukken langer bewaren dan noodzakelijk voor het doel waarvoor ze worden verwerkt (conform Wet Bescherming Persoonsgegevens).	Interpretatie: Ad1 Archivering van verificaties en validaties bedoeld voor de opbouw van audittrails is ten behoeve van: • de opsporing en bestrijding van frauduleuze informatietransacties; • de bescherming van de Gebruiker bij misbruik van zijn (digitale) identiteit. De Deelnemer legt de overwegingen voor de vastleggingen in het kader van archivering vast. De Deelnemer specificeert de vastleggingen in het kader van archivering. Ad 3 Persoonsgegevens zoals een foto, het Burger Service Nummer (BSN) en de nationaliteit MOETEN bij archivering en opslag blijvend onleesbaar zijn gemaakt. Deelnemers zijn voor al hun stelselactiviteiten zelf verantwoordelijk voor de naleving van de wettelijke vereisten uit de Algemene verordening gegevensbescherming (AVG). Indien een deelnemer afwijkt van de hetgeen in de toelichting is aangegeven is deze afwijking voor de auditor slechts acceptabel als: • de afwijking is gedocumenteerd en formeel is geaccepteerd door het bevoegde managementniveau van de Deelnemer. • De deelnemer een expliciete afweging heeft gemaakt in het kader van de wet bescherming persoonsgegevens t.a.v. het doel van de opslag en de risico's die dit met zich mee brengt voor personen. De Deelnemer blijft te allen tijde zelf verantwoordelijk voor de inhoud van de gemaakte afweging. Het oordeel van de auditor over naleving van deze norm heeft geen enkele betekenis als verweer indien de Deelnemer door de bevoegde instanties in het kader van de AVG ter verantwoording wordt geroepen. Ad 4 en 5 Toelichting: Afwijken van deze norm is slechts acceptabel indien de noodzaak kan worden aangetoond door de Deelnemer.

2.4.5 Faciliteiten en personeel

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2 3 4	1. De Deelnemer in het Stelsel MAG bij het vervullen van zijn rol (mede) gebruik maken van andere marktpartijen, onderaannemers of samenwerken met partijen waarmee een ander verband bestaat. In dat geval hoeven deze andere partijen niet toe te treden tot het afsprakenstelsel. Essentieel is het uitgangspunt dat alleen toegetreden Deelnemers diensten in het Stelsel verrichten. Bij inschakeling van derde partijen geldt de eis dat: a. De Deelnemer aansprakelijk MOET zijn voor de nakoming van alle verplichtingen in de leveringsketen. De Deelnemer MOET de diensten op eigen naam uit te voeren. b. De Deelnemer de Beheerorganisatie in staat stelt om de naleving van de Stelselafspraken door de Deelnemer op grond van het nalevingsbeleid te monitoren en controleren. 2. De Deelnemer dient het voor de te leveren diensten gebruik te maken van op afdoende opgeleid personeel.	Ad 1 Toelichting: Voor het doorgeven van verplichtingen aan onderaannemers etc. volgt de Deelnemer de vereisten uit het Privacybeleid van het Stelsel en het Gemeenschappelijk Normenkader Informatiebeveiliging. Ad 2 Verondersteld wordt dat de implementatie van de eis grotendeels wordt afgedekt door de ISO 27001 certificatie van de deelnemer en dat de deelnemer het daar waar het gaat om het competenties voor het uitvoeren van verificaties in het identificatieproces dit specifiek maakt (zie paragraaf 2.1.2 en 2.1.3).

2.4.6 Technische controles (technical controls)

LoA	Vereiste elementen	Toelichting en good practice
LOA 1	1. Deelnemers in het Stelsel MOETEN voldoen aan de specificaties voor berichtenuitwisseling zoals is vastgelegd in het Afsprakenstelsel. 2. De bescherming van (persoons-)gegevens MOET expliciet worden meegenomen als een aspect van de risicoanalyse in het kader van de verplichte ISO27001 certificatie van Deelnemers. 3. Verbindingen MOETEN gebruik maken van TLS conform de vereisten uit de koppelvlakspecificaties. 4. Deelnemer moet conform de geldende stand der techniek 'secret information' beschermen en de genomen maatregelen documenteren. 5. Het Stelsel waarborgt dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken.	Ad 1 en 3 Het Afsprakenstelsel bevat meerdere specificaties waaronder de specificaties van interfaces en berichten en communicatiekanalen. Alle Deelnemers hebben zich bij toetreding tot het stelsel verplicht deze specificaties te implementeren. Ad 2 Toelichting: Deelnemers zijn voor al hun stelselactiviteiten zelf verantwoordelijk voor de naleving van de wettelijke vereisten uit de Wet Bescherming Persoonsgegevens. Alleen op LoA3 en LoA4 wordt in het Afsprakenstelsel aantoonbaarheid vereist van risicoafweging t.a.v. bescherming van persoonsgegevens in de veronderstelling dat op deze LoAs bijzondere maatregelen noodzakelijk zullen zijn. Ad 4 'Secret information' omvat persistente wachtwoorden, PINs en (geheime) sleutelmateriaal dat benodigd is voor de authenticatie. Niet bedoeld worden hier eenmalige wachtwoorden (OTPs). Ad 5 De vereisten voor het duurzaam handhaven van de veiligheid is vastgelegd in het Beleid voor informatiebeveiliging en de uitwerking daarvan in het Gemeenschappelijk normenkader informatiebeveiliging.
LOA 2	Zelfde als LoA1 plus 1. De deelnemer MOET risico-beperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. 2. Alle digitale persoonsgegevens en andere gevoelige gegevens MOETEN met cryptografie zijn beschermd tijdens transport. 3. Alle digitale persoonsgegevens en andere gevoelige gegevens in ruste MOETEN met cryptografie zijn beschermd als: i) deze data vanaf het internet te benaderen is ii) deze data op draagbare /verwijderbare media staat. 4. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, MOET zijn beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is.	Ad 2 en 3 Alle 'persoonsgegevens' en 'andere gevoelige gegevens' omvat naast persistente wachtwoorden, PINs en (geheim) sleutelmateriaal dat benodigd is voor de authenticatie ook alle herleidbare persoonsgegevens. Het omvat niet het pseudoniem. Ad 3 Als toegang tot de systemen of media op eenvoudige wijze verkregen kan worden dan dient via cryptografie dit risico beperkt te worden. Betreft bijvoorbeeld een database server die rechtstreeks met een client vanaf het Internet te benaderen is. Is niet van toepassing op een database server die in een beveiligde zone staat waar enkel andere (interne) systemen zoals applicatie servers bij kunnen komen. Met draagbare/verwijderbare media wordt bedoeld: Laptops, usb-sticks, harddisks etc. Is niet van toepassing als deze media in beveiligde ruimtes, zoals een datacenter, zijn geplaatst. Ad 4 Verondersteld wordt dat met de verplichte ISO27001 certificatie voldaan wordt aan deze eis.
LOA 3	Zelfde als LoA2 punten 2 en 3 en met toevoeging van: 1. De deelnemer MOET risico-beperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. De Deelnemer MOET zijn maatregelen baseren op een analyse van de risico's in het registratie en uitgifte proces ten aanzien van de genoemde dreiging. 2. Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt MOET zijn beschermd tegen ongeoorloofde manipulatie.	Ad 1 Toelichting: Voorkomen wordt dat één en dezelfde medewerker zonder enige vorm van controle, toezicht of functiescheiding in staat is om de registratie van een gebruiker te doen en vervolgens een authenticatiemiddel kan creëren en uitreiken.Dat het onwaarschijnlijk wordt gemaakt dat technisch beheerders ongezien rechtstreeks ingrijpen op databases om daarmee een werkend authenticatiemiddel te creëren. Dat betekent dat ofwel de technisch beheerder deze handeling niet kan verrichten ofwel dat een dergelijke handeling van de beheerder vrijwel direct wordt gesignaleerd en onder de aandacht van het management wordt gebracht. Ad 2 Verondersteld wordt dat met de verplichte ISO27001 certificatie voldaan wordt aan deze eis.
LOA 4	Hetzelfde als LoA 2 punten 2 en 3 en LoA3 punt 2 en met toevoeging van: 1. De deelnemer MOET risicobeperkende maatregelen nemen voor de dreiging dat een medewerker met valse voorwendselen een authenticatiemiddel creëert op naam van een fictief persoon, of op naam van een bestaand persoon zonder dat deze daarom heeft verzocht. De Deelnemer MOET maatregelen nemen die functiescheiding handhaven tussen medewerkers die de uitgifte van het authenticatiemiddel controleren en medewerkers die de	Ad 1 Toelichting: Voorkomen wordt dat één en dezelfde medewerker zonder enige vorm van controle, toezicht of functiescheiding in staat is om de registratie van een gebruiker te doen en vervolgens een authenticatiemiddel kan creëren en uitreiken. Dat het onwaarschijnlijk wordt gemaakt dat technisch beheerders ongezien rechtstreeks ingrijpen op databases om daarmee een werkend authenticatiemiddel te creëren. Dat betekent dat ofwel de technisch beheerder deze handeling niet kan

	uitgifte van het authentictiemiddel goedkeuren. Deze eis is ontleent aan het Programma van Eisen PKIoverheid v4.3, deel 3 – basiseisen, eis-nummer 5.2.4-pkio77 en onderliggende ETSI eisen. Van registratie- en uitgifteprocessen voor LoA4 authenticatiemiddelen die zijn gebaseerd op een gekwalificeerd certificaat mag worden verondersteld dat die aan deze eis voldoen.	verrichten ofwel dat een dergelijke handeling van de beheerder vrijwel direct wordt gesignaleerd en onder de aandacht van het management wordt gebracht.

2.4.7 Compliance en audit

LoA	Vereiste elementen	Toelichting en good practice
LOA 1 2	1. De Deelnemer MOET bij toetreding tot het Stelsel zijn processen voor uitgifte van middelen en de technische beschrijving van de middelen en het authenticatiemechanisme ter beoordeling aanbieden aan de Toezichthouder en de externe conformiteitsbeoordelaar. Als toegetreden partij MOET de Deelnemer bij wijziging van zijn processen deze opnieuw aanbieden ter beoordeling door de Toezichthouder. 2. De Deelnemer MOET bij essentiële wijziging in processen of de gebruikte technologie van authenticatiemechanisme of authenticatiemiddel opnieuw zijn processen en technische documentatie ter beoordeling aanbieden aan de Toezichthouder en de conformiteitsbeoordelaar. 3. De deelnemer moet zijn dienstverlening aantoonbaar binnen de scope van de verplichte ISO 27001 certificatie hebben gebracht.	Ad 1 en 2 Toelichting: • De wijze waarop deelnemers processen aan de Toezichthouder aanbieden volgt de betreffende vereisten uit het Operationeel handboek van het stelsel. • De eisen aan de conformiteitsbeoordelaar, de uit te voeren toetsen en conformiteitsrapportage zijn beschreven in de Handreiking Conformiteitstoetsing authenticatiemiddel en mechanisme. (zie ook resp. par 2.2.1 en 3.2.1). • In het kader van het Toezicht op het Stelsel vinden periodieke nalevingscontroles plaats door de toezichthouder. Ad 3 Toelichting: In het kader van ISO 27001 certificatie vinden periodieke interne audits plaats die de voor de dienst relevante processen raken.
LOA 3 4	Zelfde als LoA1 met toevoeging van: 1. De MU/AD moet ten behoeve van de conformiteitsbeoordeling en het toezicht een actueel overzicht kunnen opleveren van de aan het authenticatiemiddel en autenticatiemechanisme, uitgevoerde wijzigingen, met daarbij een beschrijving van de impact op de conformiteit aan de gestelde eisen. 2. Bij de conformiteitsbeoordeling wordt onderscheid gemaakt tussen verschillende typen onderzoek, te weten: een initieel onderzoek, een herhalingsonderzoek en een heronderzoek. a. Een initieel onderzoek is een eerste beoordeling over de volledige scope van het object van onderzoek op basis van de gestelde eisen; b. Een herhalingsonderzoek vindt uitsluitend plaats bij uitgevoerde wijzigingen aan het object van onderzoek die van invloed (kunnen) zijn op de conformiteit aan de gestelde eisen. De scope is beperkt tot de wijzigingen aan het object van onderzoek; c. Een heronderzoek vindt minimaal binnen drie jaar na uitgifte van de rapportage initieel onderzoek plaats over de volledige scope van het object van onderzoek. 3. De conformiteitsbeoordelaar die de conformiteitsbeoordeling uitvoert: a. Heeft aantoonbaar ruime ervaring met het uitvoeren van technische beoordelingsopdrachten van authenticatiemiddelen of vergelijkbare objecten van onderzoek; b. Zal voor de opdracht personeel inzetten met ruime ervaring en de voor de beoordeling benodigde competenties; c. Is bij het uitvoeren van de beoordeling en in haar oordeelsvorming geheel onafhankelijk van haar opdrachtgever en de MU/AD; d. Heeft een intern kwaliteitssysteem en/of vaktechnische richtlijnen en procedures voor het uitvoeren van beoordelingsopdrachten, met inbegrip van registratie van ondersteunend bewijs, rapportering aan opdrachtgever en aan derden en – waar nodig - interne (peer) review; e. Verstrekt toestemming dat toezichthouder op elk moment, binnen 7 jaar na het uitbrengen van de rapportage van conformiteitsbeoordelaar inzage kan vorderen in de rapportage en in het bijbehorende dossier waarin het ondersteunend bewijs is vastgelegd; f. Levert voorafgaand aan de opdrachtverstrekking aan de opdrachtgever of de MU/AD een formele verklaring op waarin conformiteit aan sub a tot en met sub e op het	Ad 1 t/m 5 Toelichting: Ten behoeve van de voorbereiding op de conformiteitsbeoordeling is een 'Handreiking voorbereiding Conformiteitsbeoordeling' beschikbaar. Ad 3 Toelichting bij sub g: Indien van een conformiteitsbeoordelaar zoals bedoeld in sub g gebruik wordt gemaakt blijven sub a, e, f en h wel onverkort van toepassing. Ad 6 Toelichting: Dit artikel beschrijft de situatie dat de autor tot een positieve verklaring komt. Het is bij het afgeven van conformteitverklaringen een gangbare auditpraktijk dat er niet wordt gewerkt met vooraf bepaalde termijnen genoemd (bijvoorbeeld 3 maanden voor een kritieke afwijking). Een realistische oplostijd is namelijk afhankelijk van de activiteit die moet worden uitgevoerd (fundamentele systeemontwikkeling kost bijvoorbeeld meer tijd dan een aanpassing instellingen van applicaties en hardware). Daarom gaat vereist het vaststellen van deadlines maatwerk. Aangezien er een positieve auditor tot een positieve verklaring is gekomen zal de auditor de juiste uitvoering van het verbeterplan pas bij de volgende controle nagaan. De toezichthouder zal daarom geheel naar eigen inzicht de uitvoering van het verbeterplan controleren. Ad 7 Toelichting: Dit artikel beschrijft de situatie waarin de auditor tot een negatieve verklaring komt. Het rapport met de negatieve verklaring is formeel en definitief en wordt door de deelnemer aan de toezichthouder gezonden. Het is aan de Toezichthouder om al dan niet consequenties aan de negatieve verklaring van de auditor te verbinden. Het ligt daarom voor de hand dat de Deelnemer de Toezichthouder op de hoogte houdt van de afspraken die hij maakt met de auditor over de wijze waarop de oplossing en her-boordeling plaats gaat vinden.

moment van opdrachtverstrekking en gedurende de conformiteitsbeoordeling verklaard en onderbouwd wordt;
   g. Een testlaboratorium ingevolge ISO 17025 voor de scope "testing of information technology products" wordt vermoed aan sub b tot en met sub d te voldoen.
   h. De conformiteitsbeoordelaar beschikt over een bedrijfs- of beroepsaansprakelijkheidsverzekering.
4. Een onderzoek van de conformiteitsbeoordelaar wordt zodanig gepland en uitgevoerd dat een redelijke mate van zekerheid kan worden verkregen dat het object van onderzoek op het in de rapportage aangegeven moment aan de gestelde eisen voldoet.
5. De rapportage van de conformiteitsbeoordelaar bevat minimaal:
   a. De doelstelling van de opdracht, een beschrijving van het object van onderzoek (uniek identificerend, met datum en versienummer), de eisen op basis waarvan het object van onderzoek is beoordeeld en het plan van aanpak met de gevolgde stappen en de gehanteerde onderzoeksmethoden en aanvalstechnieken;
   b. Het eindoordeel over de mate waarin het object op het aangegeven moment aan de gestelde eisen voldoet, met onderbouwing;
   c. Belangrijkste bevindingen en aanbevelingen;
   d. Detailbevindingen, met vermelding van referenties naar het geregistreerde bewijs over de conformiteit aan de betreffende eis.
6. Opdrachtgever MOET op basis van de rapportage een verbeterplan op te stellen voor de geconstateerde afwijkingen, met daarin minimaal een oorzaakanalyse, adequate corrigerende maatregelen voor de geconstateerde afwijkingen en een oplostermijn en deadline. De gespecificeerde oplostermijn staat nadrukkelijk in verhouding tot de classificatie van de afwijking en de benodigde middelen om deze op te lossen. De termijnen voor het opstellen van het verbeterplan en de oplossingen zijn ter beoordeling aan de autitor. De opdrachtgever MOET het door de auditor geaccepteerde verbeterplan aan de toezichthouder ter beschikking te stellen.
7. Indien de conformiteitsbeoordelaar in de rapportage oordeelt dat het object van onderzoek - op het in de rapportage aangegeven moment- niet of slechts gedeeltelijk aan de gestelde eisen voldoet, MOET Opdrachtgever in overleg te treden met de conformiteitsbeoordelaar om een herbeoordeling uit te laten voeren van de corrigerende maatregelen als uitbreiding van de uitgevoerde conformiteitsbeoordeling, danwel een hernieuwd initieel onderzoek te laten uitvoeren door een conformiteitsbeoordelaar. De conformiteitsbeoordelaar kan daarbij eisen dat het verbeterplan vooraf ter beoordeling en goedkeuring wordt voorgelegd.

Implementatietermijn

Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.

De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.

Eisen Identificatie op Afstand

Onderstaande eisen zijn een selectie van de eisen in ETSI TS 119 461 v1.1.1. De eisen zijn integraal overgenomen uit de norm en derhalve in de Engelse taal. De niet genoemde hoofdstukken en eisen worden reeds ingevuld door bestaande eisen in het Afsprakenstelsel. Zie Eisen Identificatie op Afstand niet van toepassing.

De bovenste rij in de tabellen bevat het hoofdstuk, de paragraaf en/of subparagraaf. De eerste kolom bevat de eisen. De tweede kolom bevat een toelichting op, of voorbeeld bij de eisen in de eerste kolom.

In de eisen dienen de woorden "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**can**" en "**cannot**" te worden geïnterpreteerd zoals beschreven in clause 3.2 van ETSI Drafting Rules.

- SHALL: een absolute vereiste
- SHALL NOT: een absoluut verbod
- SHOULD: sterke wens, tenzij er valide reden is in specifiek geval af te wijken
- SHOULD NOT: ongewenst, tenzij er valide reden is om het in specifiek geval toe te laten
- MAY: een vrije keuze, een optie
- NEED NOT: niet verplicht
- CAN: mogelijkheid
- CANNOT: onmogelijkheid

Terms ETSI TS 119 461 v1.1.1

Definitie van de termen die gehanteerd worden in de norm. De termen zijn integraal overgenomen uit de norm en derhalve in de Engelse taal.

- applicant: person (legal or natural) whose identity is to be proven
- authoritative evidence: evidence that holds identifying attribute(s) that are managed by an authoritative source
- authoritative source: any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity
- (identity) attribute: quality or characteristic ascribed to a person
- baseline LoIP: Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of general good practice requirements for the identity proofing process and considered suitable for the trust services policies currently defined by ETSI standards
- binding to applicant: part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence
- digital identity document: identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form
- electronic identification means (eID means): material and/or immaterial unit containing person identification data and which is used for authentication for an online service
- eID scheme: governance model and technical specifications allowing interoperability between eID means from different eID providers
- (identity) evidence: information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct
- False Acceptance Rate (FAR): proportion of verification transactions with false biometric claims erroneously accepted
- False Rejection Rate (FRR): proportion of verification transactions with true biometric claims erroneously rejected
- identity: attribute or set of attributes that uniquely identify a person within a given context
- identity document: physical or digital document issued by an authoritative source and attesting to the applicant's identity
- identity proofing context: external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself
- identity proofing (process): process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes
- identity proofing policy: set of rules that indicates the applicability of an identity proofing service to a particular community and/or class of application with common security requirements
- legitimate evidence holder: person for whom the evidence is issued
- Level of Identity Proofing (LoIP): confidence achieved in the identity proofing
- liveness detection: measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture
- physical identity document: identity document issued in physical and human-readable form
- physical presence: identity proofing where the applicant is required to be physically present at the location of the identity proofing
- presentation attack: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system
- Presentation Attack Detection (PAD): automated determination of a presentation attack
- proof of access: any source irrespective of its form that can be trusted for reliable data, information and/or evidence that can be used in an identity proofing process, provided that the applicant is able to demonstrate access to the source
- pseudonym: fictitious identity that a person assumes for a particular purpose, which differs from their original or true identity
- remote identity proofing: identity proofing process where the applicant is physically distant from the location of the identity proofing
- subject: legal or natural person that is enrolled to a trust service
- subscriber: legal or natural person bound by an agreement with a trust service provider to any subscriber obligations
- supplementary evidence: evidence that is used in addition to authoritative evidence to strengthen the reliability of the identity proofing and/or as evidence for attributes that are not evidenced by the authoritative evidence
- trusted register: public register, database, or other source that is trusted for the conveyance of identity attributes in the identity proofing context
- trust service component: one part of the overall service of a TSP
- validation: part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid

hoofdstuk / paragraaf / norm	toelichting ETSI	toelichting eTD
8 Identity proofing service requirements **8.2 Attribute and evidence collection** **8.2.3 Use of physical and digital identity documents as evidence**		
[CONDITONAL] If physical and/or digital identity documents are used as evidence, the requirements in the present clause apply.		Met een fysiek document wordt hier bedoeld het uitlezen van de 'Visual Inspection Zone' (VIZ). Dat is te beschouwen als het voor mensen gemakkelijk leesbare gedeelte van het identiteitsbewijs. Met digitaal wordt hier bedoeld het uitlezen van de chip en/of de 'Machine Readable Zone' (MRZ).
COL-8.2.3-01: An identity document used as evidence may be in physical or digital form.	NOTE 1: A physical or digital identity document as defined in the present document will usually represent a natural person only. Identity documents that evidence that a natural person represents a legal person can be envisaged but cannot be assumed to be generally available.	De term 'legal person' is in deze context niet relevant voor de Nederlandse situatie. De term 'present document' dient gelezen te worden als het bron document, oftewel de ETSI TS 119 461 standaard v1.1.1.
COL-8.2.3-02: The document used as authoritative evidence shall contain a face photo and/or other information that can be compared with the applicant's physical appearance.	NOTE 2: Required for verification against the applicant's physical appearance for binding to applicant. The binding is by biometric technology or by manual verification, or a combination of the two, see clause 8.4 of the present document. NOTE 3: This does not exclude the use of supplementary documents without a face photo or similar information. NOTE 4: The present document only specifies requirements for binding to applicant using face biometrics and/or manual face verification. Requirement COL-8.2.3-02 does not exclude the possibility of using other biometrics, e.g. fingerprint or iris, but the present document does not specify requirements for such use cases.	Sommige identiteitsdocumenten bevatten alleen een foto en verder geen andere details m.b.t. de fysieke kenmerken van de houder. Overige informatie over de uiterlijke kenmerken op het identiteitsdocument is voor ETD /eHerkenning geen vereiste.
COL-8.2.3-03: For each identity proofing context supported, a list of the identity documents that are accepted shall be documented and published.	EXAMPLE: The list can consist of document types, e.g. all passports, or named documents, e.g. passports and national identity cards from specific countries.	Voor ETD/eHerkenning is de eis alleen van toepassing op identificatie op afstand en worden alleen paspoorten en nationale identiteitskaarten, zoals vermeld bij PRADO, geaccepteerd. PRADO is beschikbaar op de volgende locatie: https://www.consilium.europa.eu/prado/nl
[CONDITIONAL] COL-8.2.3-04: If physical identity documents are used as evidence, only passports, national identity cards and other official identity documents that according to the identity proofing context offer comparable reliability of the identity shall be accepted; where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process of passport and/or identity card.	NOTE 5: The comparable reliability of other identity documents can be based on a comparison of protection against known threats. NOTE 6: Some countries issue national identity cards or have valid national identity cards that are below current practice in the security of national identity documents. Identity proofing context requirements can be to not accept such national identity cards.	Voor ETD/eHerkenning is de eis alleen van toepassing op identificatie op afstand en worden alleen paspoorten en nationale identiteitskaarten, zoals vermeld bij PRADO, geaccepteerd.
[CONDITIONAL] COL-8.2.3-05: If physical identity documents are used as evidence, the documents shall be presented in their original form.	NOTE 7: Meaning the applicant is required to present the original in the identity proofing process to evidence proof of possession of the identity document; the identity proofing process can subsequently capture another representation of the document, e.g. by a video sequence, photo, or scan.	
[CONDITIONAL] COL-8.2.3-06: If digital identity documents are used as evidence, only eMRTD digital identity documents according to ICAO 9303 part 10 [2] and other digital documents that according to the identity proofing context offer comparable reliability of the identity shall be accepted; where the judgement on comparable reliability shall be based on an assessment of the	NOTE 8: The comparable reliability of other identity documents can be based on a comparison of protection against known threats.	Voor ETD/eHerkenning wordt eMRTD alleen geaccepteerd overeenkomstig ICAO 9303 part 10 [2] en als de data uit de chip gevalideerd kan worden door een controle van de digitale handtekening van het betreffende land. Andere documenten met vergelijkbare betrouwbaarheid MOGEN toegestaan worden. Het is aan de

security features and issuance process of the other identity document towards the security features and issuance process required by ICAO 9303 part 10.		deelnemer om deze betrouwbaarheid aan te tonen. Standaard toegestane document (en), naast de documenten overeenkomstig ICAO 9303 part 10 [2]; - Nederlandse rijbewijs; Model 6I van 14 november 2014 ICAO 9303 is beschikbaar op de volgende locatie: https://www.icao.int/publications/pages/publication.aspx?docnum=9303 ICAO 9303 definities: **MRTD = Machine Readable Travel Document** Official document, conforming with the specifications contained in Doc 9303, issued by a State or organization which is used by the holder for international travel (e. g. MRP, MRV, MROTD) and which contains *mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine*. **eMRTD = Electronic Machine Readable Travel Document** An MRTD (passport, visa or card) that has a *contactless integrated circuit embedded in it and the capability of being used for biometric identification of the MRTD holder* in accordance with the standards specified in the relevant Part of Doc 9303 — Machine Readable Travel Documents.
8.3 Attribute and evidence validation **8.3.1 General requirements**		
VAL-8.3.1-08: The identity proofing process shall verify that the evidence is genuine and presented in its original form.	NOTE 1: An evidence of a type that actually exists, and that is not counterfeit, has not been tampered with and, where applicable, is not a copy of the original.	
VAL-8.3.1-09: The authenticity and integrity of the evidence shall be verified.		
[CONDITIONAL] VAL-8.3.1-10: If the evidence has explicit security features/elements, these elements shall be verified.	NOTE 2: This need not be all security elements of, e. g. a physical identity document. A selection of elements sufficient for assessing that the evidence is genuine can be applied.	Deze eis geldt zowel voor fysieke identificatie, als identificatie op afstand. Het uitgangspunt is dat, onafhankelijk van de gebruikte identificatiemethode, alle veiligheidskenmerken van het identiteitsdocument de gecontroleerd zouden moeten worden. De Toetreder dient dit middels een analyse van de risico's, gecombineerd met de mogelijkheden die de identificatiemethode biedt, toe te lichten.
8.3.2 Validation of digital identity document		
[CONDITONAL] If digital identity documents are used as evidence, the requirements in the present clause apply.		Met digitaal wordt hier bedoeld het uitlezen van de chip en/of de ‘Machine Readable Zone’ (MRZ).
[CONDITIONAL] VAL-8.3.2-01: If the digital identity document is used in a remote identity proofing process, the data from the identity document shall be transferred to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the document content.		
VAL-8.3.2-02: The digital identity document shall only be accepted if the issuer's digital signature on the document is successfully validated	NOTE 1: Usually this means that the validation result is TOTAL-PASSED as defined by ETSI EN 319 102-1 [i.5]. NOTE 2: For an eMRTD document following ICAO 9303 part 10 [2], country signing certificates, e.g.	Bij NOTE 1: ETSI EN 319 102-1 is beschikbaar op de volgende locatie: https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

	downloaded from the ICAO PKD (Public Key Database), are needed for validation.	
[CONDITIONAL] VAL-8.3.2-03: If an online status service to confirm the document's validity exists and is practically available, the process shall use this service to verify that the document is currently valid.	NOTE 3: Meaning not revoked, suspended, or reported as lost/stolen. Not all document issuers have available lookup services to check validity, and in some cases access to lookup services is restricted. Regarding current validity, note that there can be a delay in the order of days between the events of revoking a document and updating a status service. NOTE 4: If digital identity documents from many different sources are accepted, online access (interactive or by API) to all the different status services can be impractical for documents that occur infrequently.	Voor ETD/eHerkenning wordt deze eis ingevuld middels een gestolen/vermist-controle vanaf betrouwbaarheidsniveau LoA3.
[CONDITIONAL] VAL-8.3.2-04: If the digital identity document is required to be read from a chip embedded in a physical identity document, the identity proofing process shall ensure that neither the applicant nor an external attacker can inject into the process a copy of a digital identity document that has previously been obtained and stored by the attacker.	NOTE 5: Fulfilment of this requirement can depend on the protocol supported by the chip; reliable fulfilment can be difficult if the chip does not support a protocol that supports cloning detection. NOTE 6: Fulfilment of this requirement can rely on the applicant's use of software that is approved for the identity proofing process, e.g. mobile app functionality.	
VAL-8.3.2-05: Information obtained from the digital identity document shall be recorded as needed for binding to applicant and to evidence the identity proofing process.	NOTE 7: In addition to identity attributes, required information to be recorded is typically at least issuer, validity period, and the document's unique identification number.	Bij NOTE 7: voor ETD/eHerkenning wordt 'is suer' geïnterpreteerd als het land van uitgifte van het WID. De ICAO-standaard haalt voor de landcodes de standaard ISO 3166-1 aan.
VAL-8.3.2-06: The face photo contained in the digital identity document shall be extracted to enable binding to applicant.		
8.3.3 Validation of physical identity document		
[CONDITONAL] If a physical identity document is used as evidence, the requirements in the present clause apply.	NOTE 1: A physical identity document can be used with the applicant's physical presence and remotely by the applicant presenting the document in front of a camera.	
VAL-8.3.3-01: The process shall verify that the physical identity document presented is visually equal to the expected visual appearance of the document type.		
[CONDITONAL] VAL-8.3.3-02: If a physical identity document is used as evidence in a remote validation process, the process shall ensure that the applicant has the document in hand and presents the document in real-time in front of a camera.	NOTE 2: It is required that this happens at the time of the identity proofing; submission of a pre-recorded photo or video stream of an identity document is considered not to meet the requirements for identity proofing to Baseline LoIP. NOTE 3: This can rely on the applicant's use of software approved for the identity proofing process, e.g. mobile app functionality.	Remote validation is in deze context het op afstand beoordelen van de echtheid van het fysieke identiteitsdocument. Zie ook de definitie van validation.
VAL-8.3.3-03: The process shall ensure that the document presented by the applicant is a genuine, physical identity document that is not counterfeited or falsified/modified.		
[CONDITIONAL] VAL-8.3.3-04: If the physical identity document is used in a remote identity proofing process, the applicant's presentation of the identity document in front of a camera shall include recording of a video sequence to visualize the physical characteristics of the identity document and its security features. The recording shall cover each relevant side of the identity document presented by the applicant.	EXAMPLE 1: The applicant can be given instructions for the movement of the identity document, where the specific actions and/or their sequence are unpredictable to the applicant. NOTE 4: With the current state of technology, the use of a still photo of the identity document is not considered sufficient for Baseline LoIP. This can change in the future with the development of image analysis technology. EXAMPLE 2: Both the front and back sides of a national identity card will usually need to be presented.	

[CONDITIONAL] VAL-8.3.3-05: If the physical identity document is used in a remote identity proofing process, the process shall ensure that the video stream is transmitted to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the video stream.	NOTE 5: In particular, to protect against replay attack with the injection of another video stream in the process.	
[CONDITONAL] VAL-8.3.3-06: If the process is performed with manual validation of the physical identity document, the registration officer shall have access to authoritative sources of information on document appearance and document validation.	EXAMPLE 3: PRADO (Public Register of Authentic Travel and Identity Documents Online) for the EU and the EEA countries.	Bij EXAMPLE 3: PRADO is beschikbaar op de volgende locatie: https://www.consilium.europa.eu/prado/nl
VAL-8.3.3-07: Security elements of physical identity documents shall be verified to the extent needed to obtain sufficient reliability in the genuineness of the document; the verification process shall be documented.	EXAMPLE 4: Security elements can be watermarks, holograms, printing techniques, visual and infrared light patterns, and see-through elements.	
[CONDITONAL] VAL-8.3.3-08: If the process is performed with the physical presentation of physical identity documents, the registration officer shall verify optical and haptic/tactile security features if any.		
[CONDITIONAL] VAL-8.3.3-09: If an online status service to confirm the physical identity document's validity exists and is practically available, the process shall use this service to verify that the document is currently valid.	NOTE 6: Meaning not revoked, suspended, or reported as lost/stolen. Not all document issuers have available lookup services to check validity, and in some cases access to lookup services is restricted. Regarding current validity, note that there can be a delay in the order of days between the events of revoking a document and updating a status service. NOTE 7: If physical identity documents from many different sources are accepted, online access (interactive or by API) to all the different status services can be impractical for documents that occur infrequently.	
VAL-8.3.3-10: Information printed on physical identity documents shall be recorded as needed for binding to applicant and to evidence the identity proofing process.	NOTE 8: Information can be extracted by manual transcription, automatically for example by optical scanning and OCR techniques, and in some cases by photo/photocopy of the document. NOTE 9: In addition to identity attributes, required information to be recorded is typically at least issuer, validity period, and the document's unique identification number.	
[CONDITONAL] VAL-8.3.3-11: If face biometrics is applied to bind the physical identity identity document to the applicant, the face photo printed on the identity document shall be extracted.		
[CONDITONAL] VAL-8.3.3-12: If the physical identity document is used in a remote identity proofing process, and the identity document has an MRZ (machine readable zone), the information from the MRZ should be extracted and validated.		
[CONDITONAL] VAL-8.3.3-13: If the physical identity document is validated by manual procedures, the validation task should be assigned randomly among available registration officers.		
[CONDITONAL] VAL-8.3.3-14: If validation of physical identity documents is done manually, the validation shall be carried out by a registration officer that has received appropriate training covering at least the following: a) Fraud prevention and detection of forgery. b) Data protection. c) Communication training (when the registration officer is required to communicate with the		

applicant). d) Training on software and equipment used. e) Training on verification of documents and their security elements.		
[CONDITONAL] VAL-8.3.3-15: If validation of physical identity documents is done manually, the training of the registration officers shall be repeated or refreshed at least annually.		
[CONDITONAL] VAL-8.3.3-16: If validation of physical identity documents is done manually, and the process is performed with the physical presentation of the document, the registration officer should have available tools to enhance the reliability of the validation.	EXAMPLE 5: Magnifying glass and an ultraviolet lamp.	
[CONDITONAL] VAL-8.3.3-17: If validation of physical identity documents is done manually, and the document is used in a remote identity proofing process, the registration officer shall have available tools to enhance the reliability of the validation.	EXAMPLE 6: Computerized tool to zoom in on details of the document.	
VAL-8.3.3-18: Automated means and machine-learning technology should be used to analyse the characteristics of physical identity documents against their expected appearance, including analysis of security elements of documents and potential manipulation of documents.	NOTE 10: This requirement implies that a purely manual process for validating a physical identity document is allowed both for physical presence and for remote identity proofing. However, the use of (additional) automated means is recommended. NOTE 11: The document type, e.g. a passport of a specific country, can be an input parameter to the analysis, or the analysis can determine the type by automated means. NOTE 12: Automated and manual analysis can be used in combination, e.g. with fall-back to manual analysis if the automated process yields an uncertain result, or by using automated analysis as a tool for a human registration officer.	
[CONDITONAL] VAL-8.3.3-19: If automated means and machine-learning technology are used to analyse physical identity documents, the video stream recorded according to requirement VAL-8.3.3.-04 shall be of sufficient quality for the analysis.		
[CONDITONAL] VAL-8.3.3-20: If automated means and machine-learning technology are used to analyse physical identity documents, the algorithms and technology shall be systematically tested against reference datasets and be kept updated to cope with changes in the threats and risk situation.		
8.4 Binding to applicant **8.4.1 General requirements**		
BIN-8.4.1-01: The identity proofing process shall verify that the applicant is the legitimate evidence holder.		
BIN-8.4.1-02: The identity proofing process shall verify that the evidence is in the possession of the applicant.	NOTE 1: For the evidence types existing eID means and existing digital signature means, no specific binding requirements are needed since the validation of the evidence also verifies the binding. This is under the assumption that only the applicant can use the eID means or digital signature means. NOTE 2: For the supplementary evidence types trusted register, proof of access, and documents and attestations, no specific binding requirements are needed. If the binding of the authoritative evidence (identity document, eID means, or digital signature means) to the applicant is successful, and the supplementary evidence is validated and identifies the same person, the supplementary evidence is considered bound to the applicant.	Bij NOTE 1: 'existing eID means' is voor ETD/eHerkenning niet van toepassing in relatie tot identificatie op afstand.

8.4.2 Capture of face image of the applicant		
[CONDITONAL] If the applicant is a natural person, and an identity document is used as evidence, and the identity proofing process is carried out remotely, the following requirements apply.		
BIN-8.4.2-01: A video stream of the applicant's face shall be captured.	NOTE 1: The video stream and images extracted from the stream can be used for binding to applicant by both face biometrics and manual means.	
BIN-8.4.2-02: The video capture process shall apply liveness detection measures to ensure that the video stream is of a live person present in front of the camera at the time of the identity proofing.	NOTE 2: It is required that this happens at the time of the identity proofing; submission of a pre-recorded video stream is considered not to meet the requirements for identity proofing to Baseline LoIP. A part of liveness detection can be instructing the applicant to perform certain actions, where the specific actions or their sequence are unpredictable to the applicant.	
BIN-8.4.2-03: The video stream capture should apply measures to detect artificially generated or manipulated face appearance.	NOTE 3: Such attacks are sometimes termed "deep fake" attacks.	
[CONDITIONAL] BIN-8.4.2-04: If the video stream is captured on the applicant's device, the identity proofing process shall ensure that the video stream is transmitted to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the video stream.	NOTE 4: In particular to protect against replay attack with an injection of another video stream in the process. NOTE 5: This can rely on the applicant's use of software approved for the identity proofing process, e.g. mobile app functionality.	
[CONDITIONAL] BIN-8.4.2-05: If face biometrics is used for binding to applicant, at least one image of sufficient quality for binding to applicant shall be extracted from the video stream.		
BIN-8.4.2-06: The video stream capture shall apply PAD measures in compliance with ISO/IEC 30107-3 [3].		
BIN-8.4.2-07: The PAD should be evaluated according to ISO/IEC 19989-3 [i.18].	NOTE 6: ISO/IEC 19989-3 [i.18] specifies security evaluation of PAD applying Common Criteria (ISO /IEC 15408 [i.24]).	Presentation Attack Detection (PAD): automated determination of a presentation attack
BIN-8.4.2-08: Test results for the PAD shall achieve an APCER (attack presentation classification error rate) as defined by ISO/IEC 30107-3 [3] at the level of industry best practice.	NOTE 7: No specific number is specified for the APCER. Rapid technology improvement can lead to significant progress in industry best practice APCER performance even in the short term.	**APCER = attack presentation classification error rate** proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario Bron: ISO30107-3: Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, paragraaf 3.2.1
BIN-8.4.2-09: Test results for the PAD should achieve BPCER (bona fide presentation classification error rate) as defined by ISO/IEC 30107-3 [3] at the level of industry best practice.	NOTE 8: The BPCER has no impact on security but on user-friendliness.	**BPCER = bona fide presentation classification error rate** proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario Bron: ISO30107-3: Information technology — Biometric presentation attack detection — Part 3: Testing and reporting, paragraaf 3.2.2 Dit is een kwaliteitsnorm voor gebruikersvriendelijkheid. De toetreder dient via een risicoanalyse aan te tonen dat hierop zicht wordt gehouden.
BIN-8.4.2-10: The PAD measures and APCER and BPCER rates shall be kept up to date concerning advances in the threat landscape and available technology.		

8.4.3 Binding to applicant by automated face biometrics		
[CONDITONAL] If binding to applicant is by automated face biometrics, the following requirements apply:	NOTE 1: Use of other biometric means than face biometrics is currently out of scope but can be a future possibility.	
BIN-8.4.3-01 The process shall provide a reliable, automated comparison between the face image extracted from the identity document presented by the applicant and a face image captured according to the requirements of clause 8.4.2 of the present document.		
BIN-8.4.3-02: Only data capture and preliminary data quality assessment shall be done in equipment controlled by the applicant.		
BIN-8.4.3-03: Biometric signal processing, comparison, data storage, and decision SHALL be carried out in secure processing equipment.	EXAMPLE 1: To protect against threats to the biometric system as described in clause 5.1 in ISO /IEC 30107-1 [i.16].	
[CONDITONAL] BIN-8.4.3-04: If biometric face recognition is used with the physical presence of the applicant, properly secured equipment shall be used to read the identity document presented by the applicant and obtain a face image of the applicant.		
[CONDITONAL] BIN-8.4.3-05: If biometric face recognition is used with the physical presence of the applicant, locally installed and properly secured equipment may be used for the biometric face recognition processing.	EXAMPLE 2: For fulfilment of the two requirements above, a biometric kiosk as commonly used at passport offices, or equipment similar to that used for automated border control, can be used.	
BIN-8.4.3-06: The biometric algorithms and technologies applied shall be systematically tested against reference datasets and kept updated to cope with changes in the threats and risk situation.	NOTE 2: See for example, clauses for face biometrics in ISO/IEC 19795-1 [i.17].	
BIN-8.4.3-07: Test results for the biometric face recognition shall show a FAR (false acceptance rate) at the level of industry best practice.	NOTE 3: No specific number is specified for FAR. Rapid technology improvement can lead to significant progress in industry best practice FAR performance even in the short term. NOTE 4: An example of industry best practice reference can be the one-to-one face matching results reported from the NIST Face Recognition Vendor Test.	ETSI 119 461 definities: **False Acceptance Rate (FAR)** proportion of verification transactions with false biometric claims erroneously accepted NOTE: Source ISO/IEC 19795-1 [i.17].
BIN-8.4.3-08: Test results for the biometric face recognition should show a FRR (false rejection rate) at the level of industry best practice.	NOTE 5: False rejection rate has no impact on security but on user-friendliness.	ETSI 119 461 definities: **False Rejection Rate (FRR)** proportion of verification transactions with true biometric claims erroneously rejected NOTE: Source ISO/IEC 19795-1 [i.17]. De Toetreder dient via een risicoanalyse aan te tonen dat hierop zicht wordt gehouden.
BIN-8.4.3-09: The biometric face recognition may apply measures to detect morphed photos in identity documents.	NOTE 6: A morphed photo is created by merging the face photos of two or more different persons into one photo. Since some countries allow persons to bring their own photo for issuing a passport or national identity card, there is a risk that documents are issued with morphed photos. With a morphed photo, there is a risk that both/all the persons can be recognized both by a human registration officer and by face biometrics with a reliability above the applied threshold, meaning more than one person can use the identity document containing the morphed photo. NOTE 7: Morphing detection means are best applied in the binding to applicant step of an identity proofing process when a new photo, known not to be morphed, of the applicant can be compared to the potentially morphed reference photo.	Het voorkomen van morphed foto's op het WID is een primaire taak van de uitgever van het WID.

8.4.4 Binding to applicant by manual face verification		
[CONDITONAL] If manual binding of the applicant to an identity document is used, the following requirements apply:		
BIN-8.4.4-01: The registration officer shall compare the face photo obtained from the applicant's identity document with the applicant's physical appearance, either from the applicant's the physical presence or from a video sequence.		
BIN-8.4.4-02: The registration officer performing the binding to applicant shall receive training before being allowed to make any comparison, with training repeated or refreshed at least yearly.	EXAMPLE 1: See the FISWG Minimum Training Criteria for Assessors Using Facial Recognition Systems [i.22] or for more extensive description the ENFSI Best Practice Manual for Facial Image Comparison [i.23], Appendix A.	Bij EXAMPLE 1: • Het FISWG-document waaraan gerefereerd wordt is beschikbaar op de volgende locatie: https://fiswg.org/documents.html • Het ENFSI-document waaraan gerefereerd wordt is beschikbaar op de volgende locatie: https://enfsi.eu/documents/best-practice-manuals
BIN-8.4.4-03: The registration officer shall perform a morphological analysis according to a defined feature list.	EXAMPLE 2: As recommended by the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] and the corresponding checklist in [i.21].	Bij EXAMPLE 2: De documenten waaraan gerefereerd wordt zijn beschikbaar op de volgende locatie: https://fiswg.org/documents.html
BIN-8.4.4-04: The registration officer shall be allowed to spend sufficient time for the face comparison.	NOTE 1: In general, an assessment according to the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] can be sufficient, while a review according to the same document can be required at least for remote identity proofing.	
BIN-8.4.4-05: The registration officer shall have tools available to magnify images to view details.	NOTE 2: With physical presence and physical identity document, this can be a magnifying glass for the face image printed on the document. If face images are used, computerized tools are assumed.	
[CONDITIONAL] BIN-8.4.4-06: If binding to applicant is done by comparing face images or video sequences, the registration officer should use computerized tools in the face comparison.	EXAMPLE 3: Tool for superimposition of images described by the FISWG Facial Comparison Overview and Methodology Guidelines [i.20].	Bij EXAMPLE 3: De documenten waaraan gerefereerd wordt zijn beschikbaar op de volgende locatie: https://fiswg.org/documents.html
8.5 Issuing of proof **8.5.1 Result of the identity proofing**		
ISS-8.5.1-01: The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.	EXAMPLE 1: The result can be digitally signed and encrypted at the message level or be transmitted over a properly secured communication channel. NOTE 1: The present document places no requirement on the format of the result of the identity proofing. Example formats can be a document (e.g. PDF), structured data (e.g. XML, JSON), or an identity assertion (e.g. OIDC, SAML). NOTE 2: The result of the identity proofing process can convey the attributes that are verified and the LoIP, but can even be a simple 'success' or 'failure' statement meaning that identity attributes provided by the TSP at the start of the identity proofing process are verified (or not) against the applicant to the required LoIP. NOTE 3: The present document makes no assumption on the attributes to convey, whether the applicant is a natural person, a legal person, or a natural person representing a legal person (roles or authorizations can be relevant in the latter case). NOTE 4: The present document makes no assumptions on the information to convey for identity proofing processes that do not complete successfully.	Bij NOTE 2: voor ETD/eHerkenning kan de term TSP gelezen worden als middeluitgever (MU). Bij NOTE 3: 'legal person' is in deze context niet relevant voor de Nederlandse situatie.
ISS-8.5.1-02: The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes	EXAMPLE 2: By referring to the Baseline LoIP defined by the present document.	Bij EXAMPLE 2: ETSI 119 461 definities:

required for the unique identification of the applicant in the identity proofing context.		**baseline LoIP** Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of general good practice requirements for the identity proofing process and considered suitable for the trust services policies currently defined by ETSI standards
ISS-8.5.1-03: The result of the identity proofing process may convey LoIP separately for individual identity attributes that are not required for unique identification in the identity proofing context and where these LoIPs differ from the overall result of the identity proofing process.		
8.5.2 Evidence of the identity proofing process		
ISS-8.5.2-01: Evidence of the identity proofing process shall be gathered and retained in compliance with the identity proofing context.	NOTE 1: Evidence can be retained in digital or paper format. NOTE 2: The need to retain evidence of identity proofing processes that did not complete successfully can be determined by the identity proofing context. NOTE 3: Gathering and retention of evidence is required to comply with applicable data protection legislation, notably GDPR if the identity proofing process is carried out under the legislation of an EU Member State	De bewaartermijnen dienen conform AVG te worden vastgesteld.
ISS-8.5.2-02: The evidence of the identity proofing process shall document the identity evidence used in the identity proofing process and the issuer or source of that evidence.	EXAMPLE 1: An identity document can be identified by the issuer name and document number, or by retaining a copy of the document, possibly in the form of a video sequence or image if a physical identity document is used. Retaining a copy can, depending on the identity proofing context, be required, allowed, or forbidden.	
ISS-8.5.2-03: The evidence of the identity proofing process should completely document the identity proofing process.	EXAMPLE 2: Including video sequences used in a remote identity proofing process; however, retaining video sequences or images of a human applicant can, depending on the identity proofing context, be required, allowed, or forbidden.	
ISS-8.5.2-04: Evidence of the identity proofing process shall be retained for the necessary retention time given by the identity proofing context.	EXAMPLE 3: A typical requirement from a TSP is to retain evidence of the identity proofing process as long as the applicant remains a subject/subscriber of the TSP plus several of years after that time.	De bewaartermijnen dienen conform AVG te worden vastgesteld. Bij EXAMPLE 3: voor ETD/eHerkenning kan de term TSP gelezen worden als middeluitgever (MU).
ISS-8.5.2-05: The evidence of the identity proofing process shall be stored in a tamper-proof way.		
ISS-8.5.2-06: The evidence of the identity proofing process shall be stored in a way that guarantees the confidentiality of the information.		
ISS-8.5.2-07: The evidence of the identity proofing process shall be stored in a way that ensures the possibility to search, retrieve, and re-verify the identity proofing result.	NOTE 4: Offline storage or other means that will result in a prolonged response time are acceptable.	
ISS-8.5.2-08: At the end of the retention time defined by ISS 8.5.2-04, the evidence of the identity proofing process and all personal data on the applicant shall be deleted.		

Eisen Identificatie op Afstand niet van toepassing

Onderstaande eisen zijn een selectie van de eisen in ETSI TS 119 461 v1.1.1. welke niet van toepassing zijn verklaard voor Elektronische Toegangsdiensten, met een onderbouwing waarom deze niet van toepassing zijn verklaard.

hoofdstuk / paragraaf / norm	toelichting ETSI	eTD onderbouwing 'reeds bestaande eisen in afsprakenstelsel'
5 Operational risk assessment		**Eisen zijn onderdeel van het Afsprakenstelsel ETD.**
6 Policies and practices		**Eisen zijn onderdeel van het Afsprakenstelsel ETD.**
7 Identity proofing service management and operation		**Eisen zijn onderdeel van het Afsprakenstelsel ETD.**
8 Identity proofing service requirements **8.1 Initiation**		
INI-8.1-01: The applicant shall be informed of, and shall accept, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.		Eis is onderdeel van het Normenkader Betrouwbaarheidsniveaus, paragraaf 2.1.1.
INI-8.1-02: If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant shall be allowed to select which of the alternative processes to use.	NOTE 1: A physical or digital identity document as defined in the present document will usually represent a natural person only. Identity documents that evidence that a natural person represents a legal person can be envisaged but cannot be assumed to be generally available.	Het is aan de leveranciers om een passend proces aan de klanten aan te bieden.
INI-8.1-03: The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.	EXAMPLE 1: Information on the applicable data protection rules, notably GDPR if the identity proofing process is carried out under the legislation of an EU Member State. EXAMPLE 2: The identity proofing process can require the use of a specific type of device (e.g. a smartphone) with the installation of specific software (e.g. an app).	Eis is onderdeel van het Normenkader Betrouwbaarheidsniveaus, paragraaf 2.2.2.
8.2 Attribute and evidence collection **8.2.1 General requirements**		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.1 en 2.1.2.**
COL-8.2.1-01: The identity attributes required for the identity proofing context shall be defined and collected.		
COL-8.2.1-02: The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.		
COL-8.2.1-03: The identity attributes shall be validated by use of one or more authoritative evidence.	NOTE 1: An identity proofing process can use multiple evidence, including several evidence of the same type, e. g. several identity documents, either routinely, or with further evidence added if identity proofing using the initial evidence yields insufficient reliability of the result.	
COL-8.2.1-04: The evidence collected shall meet the requirements of the identity proofing context.	NOTE 2: The identity proofing context can pose requirements for the use of specific types of evidence, e.g. resulting from applicable legislation.	
COL-8.2.1-05: The evidence shall be issued by entities trusted in the identity proofing context.	NOTE 3: Meaning that the evidence can be validated and that the reliability of the attributes conveyed can be assessed.	
COL-8.2.1-06: A list of the identity proofing use cases supported, the evidence that can be trusted, and, as far as possible, the identity proofing contexts supported shall be published.	NOTE 4: Identification of use cases can be by reference to clause 9 of the present document.	

	NOTE 5: While the list of evidence that can be trusted is required to be comprehensive, a specific identity proofing context can place restrictions on the selection of evidence applicable to the identity proofing context.	
COL-8.2.1-07: The freshness of the identity information obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.	EXAMPLE: A passport can have a lifetime of 10 years, and an eID or signing certificate can have a lifetime of 2-5 years, meaning the identity attributes obtained from this evidence can have changed since the evidence was issued. Some evidence issuers can apply revocation and re-issuing if information changes. NOTE 6: If the information conveyed from an evidence does not fulfil the information freshness requirements of the identity proofing context, the situation can be compensated by the use of supplementary evidence.	
8.2.2 Attribute collection **8.2.2.1 Attribute collection for natural person**		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.1.**
[CONDITONAL] If the applicant is a natural person, the requirements in the present clause apply.		
COL-8.2.2.1-01: For each identity proofing context supported, the means used to collect identity attributes for a natural person shall be documented and published.	EXAMPLES: • From a physical identity document by transcription or scanning (e.g. OCR reading). • From a digital identity document. • From the use of an eID authenticating the applicant. • From a certificate supporting a digital signature applied by the applicant. • Directly from the applicant by typing in information or otherwise. • From authoritative information sources such as public registers. • From existing information in auxiliary data sources such as customer records and databases. • From other documents supplied by the applicant or from other sources.	
COL-8.2.2.1-02: The following attributes shall at a minimum be collected if the applicant is a natural person: a) family name(s), first name(s), which should be current names; b) further information as needed to uniquely identify the applicant as a natural person in the identity proofing context.	NOTE 1: There can be cases where the name attributes collected need to match the name provided by an evidence, which is not necessarily the current name when a name change occurred after the evidence was issued. NOTE 2: Requirements for the presence of naming attributes can depend on the identity proofing context. In some contexts, a full name (all family names and first names) can be required, while in other contexts full name is not needed. In rare cases, a person can have only one name, classified as either first name or family name. NOTE 3: Depending on the identity proofing context, unique identification can be in the form of a single attribute such as a national identity number, or as one or more additional attributes that together with the name provide unique identification. NOTE 4: ETSI EN 319 412-2 [i.9] specifies X.509 certificate profile for natural persons. In addition to the name of the subject, a country attribute with undefined semantics is mandatory, and usually a serialNumber attribute is required to guarantee a unique identity. While values for the country and the serialNumber attributes can be part of the attributes collected, these values can also be generated and added by the certification authority. NOTE 5: Although the outcome of the identity proofing can be a pseudonym identity, identity proofing conforming to the present document requires identification of the real identity of the person as determined by applicable identity documents, official registers or other authoritative sources.	
COL-8.2.2.1-03: The attributes to collect shall be as determined by the identity proofing context.	NOTE 6: Given the identity proofing context, the legal basis for collecting certain attributes can be laws or regulations allowing collection or consent by the applicant.	

	Applicant's consent can be extended to the collection of attributes additional to the minimum set needed for the identity proofing context.	
COL-8.2.2.1-04: The identity proofing process shall not collect identity attributes that are not included in the result of the identity proofing, except when such attributes are required for attribute and evidence validation and/or binding to applicant.		
8.2.2.2 Attribute collection for legal person		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.3.**
[CONDITONAL] If the applicant is a legal person, the requirements in the present clause apply.		
COL-8.2.2.2-01: For each identity proofing context supported, the means used to collect identity attributes for a legal person shall be documented and published.	NOTE: Depending on the identity proofing context, attribute collection for a legal person may vary from basic company information to an extensive record of information about the legal person, including information such as beneficial owners and personnel in key roles. EXAMPLE 1: Attributes can be collected from business registers, commercial information providers, documents and attestations, or by manual input in the course of the identity proofing process.	
COL-8.2.2.2-02: The attributes collected shall uniquely identify the applicant as a legal person in the identity proofing context.		
COL-8.2.2.2-03: The following attributes shall, as a minimum, be collected if the applicant is a legal person: a) full name of the legal person; b) country of registration of the legal person; c) unique identifier and type of identifier for the legal person (unless such identifier does not exist).	EXAMPLE 2: Unique identifier can be national registration number, tax number, VAT number, or LEI (Legal Entity Identifier).	
8.2.2.3 Attribute collection for natural person representing legal person		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.4.**
[CONDITONAL] If the applicant is a natural person representing a legal person, the requirements in the present clause apply.		
COL-8.2.2.3-01: Identity attributes for the natural person shall be collected according to the requirements in clause 8.2.2.1 of the present document.		
COL-8.2.2.3-02: Identity attributes for the legal person shall be collected according to the requirements in clause 8.2.2.2 of the present document.		
COL-8.2.2.3-03: The role of the natural person with respect to the legal person and identification of the source of the authorization of the natural person to represent the legal person shall be collected.		
8.2.4 Use of existing eID means as evidence		**De eisen in deze paragraaf gaan over het gebruik van andere elektronische identificatiemiddelen voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD/eHerkenning biedt geen ruimte voor het gebruik van andere elektronische identificatiemiddelen voor het aantonen van de identiteit.**
[CONDITONAL] If existing eID means for	NOTE 1: A physical identity document can be used with	

authentication is used as evidence, the requirements in the present clause apply.	the applicant's physical presence and remotely by the applicant presenting the document in front of a camera.	
COL-8.2.4-01: For each identity proofing context supported, the conditions that an eID or eID scheme is required to fulfil to be accepted for identity proofing shall be documented and published.	NOTE 1: Most eID solutions today represent a natural person, although eID means for a legal person or a natural person representing a legal person is possible. EXAMPLE 1: The documentation can list named eIDs or eID schemes or describe the necessary characteristics of eIDs or eID schemes by referring to a required LoA as defined by an assurance level framework. EXAMPLE 2: Acceptance for an identity proofing context can require that certain identity attributes are asserted by the eID means. EXAMPLE 3: The identity proofing context can state that only eIDs notified according to the eIDAS Regulation [i.1] Article 9 can be used.	
COL-8.2.4-02: The eID shall conform to eIDAS LoA substantial or high or conform to an LoA defined by another assurance level framework and offering comparable assurance to the relevant eIDAS LoA level.	NOTE 2: eIDAS LoAs are specified by CIR (EU) 2015 /1502 [i.3]. The identity proofing context can require conformance to specifically the eIDAS LoA framework and can also require that eIDs are notified according to the eIDAS Regulation [i.1] Article 9. EXAMPLE 4: The eID can conform to a national assurance level framework of an EU Member State or an assurance level framework of a non-EU state; in both cases, the assurance level framework can be aligned with the eIDAS LoAs. NOTE 3: The comparable assurance to an eIDAS LoA level can be assessed by an independent, accredited conformity assessment body. NOTE 4: The identity proofing context can place further requirements on the issuing of the eID, e.g. to avoid a long chain of eID renewals where the presence (physical or remote) of the eID subject is a long time in the past, or to avoid a long chain of eIDs that are all issued based on another eID.	
[CONDITIONAL] COL-8.2.4-03: If required attributes to be collected cannot be confirmed by the authentication using the eID means, these attributes shall be collected from other sources and validated by use of other evidence in accordance with the identity proofing context.	NOTE 5: Typically, this happens when required attributes are not present in the identity assertion obtained from the authentication protocol.	
[CONDITIONAL] COL-8.2.4-04: If the eID means is used for an identity proofing process supporting an EU qualified trust service, the eID shall conform to eIDAS LoA substantial or high.	NOTE 6: When the qualified trust service is the issuance of a qualified certificate, eIDAS Article 24.1 (b) states that the eID means is required to be issued based on a prior physical presence of the natural person or an authorized representative of the legal person.	
8.2.5 Use of existing digital signature means as evidence		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.2.**
[CONDITONAL] If an existing digital signature means with a supporting certificate is used as evidence, the requirements in the present clause apply.		
COL-8.2.5-01: For each identity proofing context supported, the conditions under which digital signatures and certificates are accepted shall be documented and published.	NOTE 1: A digital signature can be applied by a natural person (electronic signature as defined by eIDAS), a legal person (electronic seal as defined by eIDAS), or a natural person representing a legal person, depending on the information included in the certificate and the semantics of this information. NOTE 2: The conditions can be stated in the form of a signature policy; see ETSI TS 119 172-1 [i.13].	

	NOTE 3: The present document makes no assumption on the format or content of the document signed. Identity attributes are evidenced by the certificate, not by the signed document. EXAMPLE 1: Regarding digital signature, the identity proofing context can require that a qualified electronic signature/seal, according to the eIDAS regulation, is used. EXAMPLE 2: Regarding certificate, the list can consist of named certificate issuers or describe the necessary characteristics of the certificate, e.g. by referring to a policy level as defined by ETSI EN 319 411-1 [i.7] or ETSI EN 319 411-2 [i.8]. EXAMPLE 3: Acceptance for an identity proofing context can pose requirements for certificate content, e.g. require that certain identity attributes are present for the named subject.	
[CONDITONAL] COL-8.2.5-02: If a digital signature with a supporting certificate is accepted as evidence of identity for a natural person representing a legal person, the certificate should evidence the connection between the natural and the legal person.	NOTE 4: For an X.509 certificate, this will typically imply that the Subject field of the certificate identifies both the natural and the legal person; however, such identification in itself does not evidence that the natural person is authorized to represent the legal person for the identity proofing.	
COL-8.2.5-03: The certificate shall at least conform to the NCP policy level as defined by ETSI EN 319 411-1 [i.7].	NOTE 5: The identity proofing context can place further requirements on the issuing of the certificate, e.g. to avoid a long chain of certificate renewals where the presence (physical or remote) of the certificate subject is a long time in the past, or to avoid a long chain of certificates that are all issued based on another certificate. A requirement for the certificate to be issued based on one of the use cases defined in the present document can be recommended.	
[CONDITIONAL] COL-8.2.5-04: If required attributes to be collected are not present in the certificate, these attributes shall be collected from other sources and validated by the use of other evidence in accordance with the identity proofing context.		
[CONDITIONAL] COL-8.2.5-05: If the digital signature with certificate is used for an identity proofing process supporting an EU qualified trust service, the digital signature shall be a qualified electronic signature as defined by the eIDAS Regulation if the applicant is a natural person or a natural person representing a legal person, or a qualified electronic seal as defined by the eIDAS Regulation if the applicant is a legal person.	NOTE 6: When the qualified trust service is the issuance of a qualified certificate, eIDAS Article 24.1 (c) states that the qualified certificate is required to be issued based on identity proofing either by a prior physical presence of the natural person or of an authorized representative of the legal person, or by an eID means conforming to eIDAS substantial or high that is in turn based on identity proofing by the physical presence of the natural person or an authorized representative of the legal person.	
8.2.6 Use of trusted register as supplementary evidence		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.1.**
[CONDITONAL] If a trusted register is used as supplementary evidence, the requirements in the present clause apply.		
COL-8.2.6-01: For each identity proofing context supported, a list of the trusted registers used to collect and/or validate attributes, and whether lookup in these registers is mandatory or optional, shall be documented and published.	NOTE 1: Availability of trusted registers can vary between countries, ranging from no availability to lookup in particular sources, e.g. national population registers or business registers, mandated by national regulation. EXAMPLE 1: Trusted registers can be used both to validate attributes that are already collected to ensure that the attribute values are correct and up to date, and to fetch additional attributes.	
COL-8.2.6-02: Only official national or nationally approved registers should be accepted as trusted registers.	EXAMPLE 2: Depending on the identity proofing context, information sources such as existing customer databases of TSPs or other service providers can be defined as trusted registers.	

[CONDITIONAL] COL-8.2.6-03: If the applicant is a legal person, the attributes collected for the legal person shall be verified against an authoritative business register to the extent that the legal person is registered and that the required attributes are present in the register.	NOTE 2: There can be a need to do identity proofing of entities that do not possess a unique identifier and that are not present in any business register, e.g. public sector agencies in some countries.	
8.2.7 Use of proof of access as supplementary evidence		**De eisen in deze paragraaf gaan over het gebruik van vertrouwde toegangsmethoden voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD/eHerkenning maakt geen gebruik controle van vertrouwde toegangsmethoden voor het antonen van de identiteit.**
[CONDITONAL] If proof of access is used as supplementary evidence, the requirements in the present clause apply.		
COL-8.2.7-01: For each identity proofing context supported, a list of the proof of access mechanisms that are required or accepted as supplementary evidence of identity and the attributes that are collected or validated from these mechanisms shall be documented and published.	NOTE: Proof of access will usually be relevant only for natural persons. EXAMPLE 1: Proof of access to a bank account with identity information obtained from the bank. EXAMPLE 2: Proof of access to a mobile phone with identity information obtained from the mobile operator's subscription register.	
COL-8.2.7-02: The attributes returned from the proof of access shall be reliably linked to the applicant.	EXAMPLE 3: Proof of access to a bank account owned by another person could result in attributes for the other person to be returned.	
COL-8.2.7-03: The reliability of attributes obtained from proof of access mechanisms shall be evaluated with all cases of attributes considered to have lower reliability than the outcome of the general identity proofing process documented and published.	EXAMPLE 4: The general outcome of an identity proofing process is Baseline, but a mobile phone number obtained from proof of access can have lower reliability.	
8.2.8 Use of documents and attestations as supplementary evidence		**De eisen in deze paragraaf gaan over het gebruik documenten en verklaringen voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD /eHerkenning maakt geen gebruik documenten en verklaringen voor het aantonen van de identiteit.**
[CONDITONAL] If documents and attestations are used as supplementary evidence, the requirements in the present clause apply.		
COL-8.2.8-01: For each identity proofing context supported, a list of the documents or attestations required or accepted as supplementary evidence of identity and the attributes that are collected or validated from this documentation shall be documented and published.	EXAMPLE 1: For a natural person, in some countries, utility bills or similar can be required as evidence of address. EXAMPLE 2: Attestations can be used as evidence that a legal person exists and for further information on its legal status, and as evidence that a natural person is entitled to represent the legal person.	
[CONDITIONAL] COL-8.2.8-02: If the applicant is a legal person, a statement from a natural person verified to represent the legal person may be accepted as evidence.		
COL-8.2.8-03: The reliability of attributes obtained from documents and attestations shall be evaluated with all cases of attributes considered to have lower reliability than the outcome of the general identity proofing process documented and published.	EXAMPLE 3: The general outcome of an identity proofing process is Baseline, but an address obtained from a utility bill can have lower reliability.	
COL-8.2.8-04: Acceptance of digital documents and attestations should be limited to digital documents and attestations that are evidenced by the issuer's digital signature.	NOTE: The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted.	

8.2.9 Evidence collection for natural person representing legal person		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.4.**
[CONDITIONAL] If the applicant is a natural person purporting to represent a legal person, the requirements in the present clause apply.		
COL-8.2.9-01: Evidence for the natural person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.		
COL-8.2.9-02: Evidence for the legal person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.		
COL-8.2.9-03: For each identity proofing context supported, the accepted means to evidence the link between the natural person's identity and the legal person's identity shall be documented and published.	EXAMPLE 1: Trusted registers like business registries, or required documents and attestations.	
COL-8.2.9-04: For each identity proofing context supported, the positions, roles, or other relationships accepted for a natural person to represent a legal person shall be documented and published.	EXAMPLE 2: Directors, executives, board members, or a natural person with authorization duly delegated from another natural person in an authorized role.	
COL-8.2.9-05: For each identity proofing context supported, any freshness (current) requirement applicable to any statement or document regarding the natural person's relationship to the legal person shall be documented and published.		
COL-8.2.9-06: If the legal person is listed in an authoritative business register, the role of the natural person concerning the legal person shall be collected from or validated against this business register to the extent that the required attributes are present in the register.	NOTE 1: Practices for registration vary between countries. As one example, public sector entities are not registered in business registers in all countries.	
COL-8.2.9-07: The role of the natural person concerning the legal person may be collected from or verified against other information sources than authoritative business registers.	NOTE 2: This, in particular, applies to legal persons that are not present in such business registers. EXAMPLE 3: Information source can be public notaries, other registers than business registers, the official web site of the legal person, contacts with representatives of the legal person other than the concerned natural person etc.	
COL-8.2.9-08: Documents and attestations from the concerned legal person may be used as evidence of a natural person's authorization to represent the legal person.		
8.3 Attribute and evidence validation **8.3.1 General requirements**		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.1.**
VAL-8.3.1-01: All necessary identity attributes shall be validated to the required reliability by the presented evidence.		
VAL-8.3.1-02: Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.		
VAL-8.3.1-03: The handling of differences in encoding of identity attributes between collected attributes and attributes from evidence, and between different evidence, shall be described.	EXAMPLE 1: Typical sources of differences are transcription between alphabets or from non-alphabetical scripts (e.g. Chinese) to an alphabet, transcription of national language characters (e.g. Norwegian æ, ø, å) into Latin characters, and transcription of diacritics (e.g. French é, è, ê) into Latin characters.	

VAL-8.3.1-04: The handling of differences in name attributes between collected attributes and attributes from evidence, and between different evidence, shall be described.	EXAMPLE 2: Missing names (middle names or first names), change of name not reflected (e.g. evidence contains a name before a later change of name), use of initials, truncation (e.g. limited number of characters that can be printed on an identity document), use of prefix (e.g. Dr) or suffix (e.g. Jr).	
VAL-8.3.1-05: The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.		
VAL-8.3.1-06: The identity proofing process shall verify that the evidence is issued by an authoritative source that is trusted according to the identity proofing context.		
[CONDITONAL] VAL-8.3.1-07: If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.	EXAMPLE 3: Valid from and valid to attributes of a digital signature certificate, date of expiry of an identity document.	
VAL-8.3.1-11: The identity proofing process shall as far as possible verify that the evidence is valid at the time of the identity proofing.	EXAMPLE 4: An identity document can be declared lost, stolen, or revoked, but not all document issuers provide an online status service that can be used to check current status, and if an online status service exists, its availability can be restricted.	
VAL-8.3.1-12: Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.	NOTE 3: This requirement does not prohibit remote access to this environment by registration officers.	
8.3.4 Validation of eID		**De eisen in deze paragraaf gaan over het gebruik van andere elektronische identificatiemiddelen voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD/eHerkenning biedt geen ruimte voor het gebruik van andere elektronische identificatiemiddelen voor het aantonen van de identiteit.**
[CONDITONAL] If authentication by use of an existing eID means is used as evidence, the requirements in the present clause apply.		
VAL-8.3.4-01: An authentication protocol that confirms that the holder of the eID means is successfully authenticated and that the eID means used is valid (not expired, suspended, or revoked) shall be executed.	NOTE 1: Successful authentication implies that the eID means as evidence is validated, that the identity information conveyed from the eID means is validated, and that the identity information is bound to the applicant. NOTE 2: The eID means can represent a natural person, a legal person, or a natural person representing a legal person.	
8.3.5 Validation of digital signature with certificate		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.2.**
[CONDITONAL] If a digital signature with certificate is used as evidence, the requirements in the present clause apply.		
VAL-8.3.5-01: The digital signature shall be created as part of the identity proofing process.	NOTE 1: This is to avoid threats from the use of documents previously signed by the applicant.	
VAL-8.3.5-02: The digital signature shall be validated and the signing certificate shall only be used as evidence for identity attributes if the signature is valid.	NOTE 2: Usually, this means that the validation result is TOTAL-PASSED as defined by ETSI EN 319 102-1 [i.5]. NOTE 3: If the digital signature is valid, the information obtained from the certificate supporting the digital signature can be considered valid and bound to the applicant. NOTE 4: The certificate can represent a natural person, a legal person, or a natural person representing a legal person.	

[CONDITIONAL] VAL-8.3.5-03: If the identity proofing context requires a digital signature supported by a qualified certificate according to the eIDAS Regulation, the signature should be validated according to ETSI TS 119 172-4 [i.14].		
8.3.6 Validation of information obtained from trusted registers		**De eisen in deze paragraaf zijn onderdeel van het normenkader betrouwbaarheidsniveaus, paragraaf 2.4.3 en 2.4.6.**
[CONDITONAL] If trusted registers are used in an identity proofing process, the requirements in the present clause apply.		
[CONDITONAL] VAL-8.3.6-01: If the communication towards the trusted register is online, the communication channel shall be secured by using an up to date version of the TLS protocol or another protocol offering a comparable level of security.		
[CONDITONAL] VAL-8.3.6-02: If the communication towards the trusted register is online, the trusted register shall be authenticated.	EXAMPLE 1: By a website certificate.	
[CONDITONAL] VAL-8.3.6-03: If the communication towards the trusted register is message-based, all messages shall be authenticated and integrity protected.	EXAMPLE 2: By use of digital signatures. The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted.	
[CONDITONAL] VAL-8.3.6-04: If the communication towards the trusted register is message-based, all messages containing personal identity information shall be encrypted.		
VAL-8.3.6-05: The integrity and authenticity of the information obtained from the trusted register shall be validated.		
VAL-8.3.6-06: The procedure to apply in case of discrepancies between the information obtained from trusted registers and information from other evidence shall be documented.	EXAMPLE 3: A trusted register can override information obtained from other evidence. The identity proofing context can pose requirements.	
8.3.7 Validation of proof of access		**De eisen in deze paragraaf gaan over het gebruik van vertrouwde toegangsmethoden voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD/eHerkenning maakt geen gebruik controle van vertrouwde toegangsmethoden voor het antonen van de identiteit.**
[CONDITONAL] If proof of access is used in an identity proofing process, the requirements in the present clause apply.		
VAL-8.3.7-01: A proof of access protocol shall be executed to ensure that the applicant controls the item in question.	EXAMPLE 1: To confirm possession of mobile phone number, email address, or bank account.	
VAL-8.3.7-02: The identity information obtained shall be transferred or otherwise be made available for the identity proofing process in a way that ensures the authenticity of the source of information and integrity and confidentiality of the information.		
VAL-8.3.7-03: The integrity and authenticity of the identity attributes obtained shall be validated.	EXAMPLE 2: Information from an existing customer record of a bank or a telecommunications service provider.	
[CONDITIONAL] VAL-8.3.7-04: If proof of access to a bank account is used as supplementary evidence, the applicant's access to the bank account shall be reliably authenticated.	EXAMPLE 3: By use of eID means fulfilling requirements for PSD2 (EU Payment Services Directive) SCA (Strong Customer Authentication) [i.2]. EXAMPLE 4: A payment made by the applicant to an account associated with the identity proofing process can be part of the proof of access protocol.	

VAL-8.3.7-05: The procedure to apply in case of discrepancies between the identity attributes obtained from proof of access and identity attributes from other evidence shall be documented.	EXAMPLE 5: The information obtained from proof of access can be regarded as authoritative and override other sources of information, or other evidence can be regarded as authoritative, or an arbitration procedure can be used. The identity proofing context can pose requirements.	
8.3.8 Validation of documents and attestations		**De eisen in deze paragraaf gaan over het gebruik documenten en verklaringen voor het aantonen van de identiteit. Het proces voor identificatie op afstand bij ETD /eHerkenning maakt geen gebruik documenten en verklaringen voor het aantonen van de identiteit.**
[CONDITONAL] If documents and attestations are used in an identity proofing process, the requirements in the present clause apply.		
VAL-8.3.8-01: The identity proofing process shall verify that the document or attestation presented is of an accepted type and is issued by an actor trusted according to the identity proofing context.		
VAL-8.3.8-02: The identity of the issuer of the document or attestation, and the authenticity and integrity of the contained information, shall be verified.	NOTE 1: For a digital document, this can imply validating a digital signature on the document or attestation. The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted. NOTE 2: For a physical document, this can be by physical signatures or seals, logos and other visual elements, and by examining the document to detect falsification and tampering.	
[CONDITIONAL] VAL-8.3.8-03: If a document or attestation is in physical form or digital form rendered for human validation, the identity proofing process shall verify that the document presented is visually equal to the expected visual appearance.		
[CONDITIONAL] VAL-8.3.8-04: If a document or attestation is in physical form and the document type contains security elements, these security elements shall be verified to the extent required by the identity proofing context.		
VAL-8.3.8-05: The procedure to apply in case of discrepancies between the identity attributes obtained from documents and attestations and identity attributes from other evidence shall be documented.	EXAMPLE: The information obtained from documents and attestations can be regarded as authoritative and override other sources of information, or other evidence can be regarded as authoritative, or an arbitration procedure can be used. The identity proofing context can pose requirements.	
8.4 Binding to applicant **8.4.5 Binding to applicant for legal person and natural person representing legal person**		**De eisen in deze paragraaf zijn onderdeel van het Normenkader betrouwbaarheidsniveaus, paragraaf 2.1.4.**
[CONDITONAL] If the applicant is a legal person or a natural person representing a legal person, the following requirements apply:		
BIN-8.4.5-01: Validated evidence shall prove that the legal person exists and that the application to the trust service is a willful act carried out on behalf of the legal person.		
[CONDITIONAL] BIN-8.4.5-02: If the applicant is a natural person representing a legal person, the identity of the natural person shall be proven according to the requirements of the present document.		
[CONDITIONAL] BIN-8.4.5-03: If the applicant is a natural person representing a legal person,		

validated evidence shall prove the natural person's authorization to represent the legal person.		
[CONDITIONAL] BIN-8.4.5-04: If the applicant is a natural person representing a legal person, and the legal person is listed in an authoritative business register, the natural person's authorization to represent the legal person should be proven by information from that register.	NOTE: This implies that the natural person has one of the roles listed in the business register and that this role is authorized to represent the legal person in the identity proofing context.	
9 Use cases for identity proofing to Baseline LoIP		**Eisen zijn onderdeel van het Afsprakenstelsel ETD.**

Specificaties voor het beheer van bevoegdheden

EH1 vervalt per 1-7-2021

Met ingang van 1 juli 2021 komt het gebruik van het betrouwbaarheidsniveau eH1 te vervallen en moeten de middelen en machtigingen minimaal voldoen aan de normen van het betrouwbaarheidsniveau eH2.

Norm	LoA	Vereisten	Best practices
3	LOA 1 2 3 4	Vereisten voor de kwaliteit van registratie van machtigingen	
3.1		**Generieke vereisten**	
3.1.2	LOA 1 2 3 4	Controledoelstelling: Het machtigingenregister MOET erop toezien dat het beheers proces van machtigingen deugdelijk wordt uitgevoerd.	
3.1.2.3	LOA 1 2 3 4	De machtigingenbeheerder MAG slechts geautoriseerd worden om zich te registreren en om bevoegdheden te registreren die zich op hetzelfde of op een lager niveau bevinden dan zijn eigen autorisatieniveau.	Interpretatie: In de praktijk valt op niveau LoA 1 de rol van machtigingenbeheerder en gemachtigde samen.
3.1.2.4	LOA 1 2 3 4	De machtigingenbeheerder MOET geauthenticeerd worden voor dat hij toegang tot het machtigingenregister krijgt.	Interpretatie: In de praktijk valt op niveau LoA 1 de rol van machtigingenbeheerder en gemachtigde samen.
3.1.2.5	LOA 1 2 3 4	De geldigheid van geregistreerde machtigingen MOET tot een nader omschreven periode worden beperkt, waarbij een maximale geldigheidsperiode van 5 jaar geldt.	Advies: De bewaking van de geldigheidsduur kan op verschillende wijzen worden vormgegeven en hoeft niet een specifiek bewakingsproces te zijn. Bijvoorbeeld een abonnementsstructuur kan een manier zijn om periodiek de geldigheidsduur te bewaken.
3.1.2.6	LOA 1 2 3 4	Het machtigingenregister MOET het resultaat van een registratie of wijziging aan machtigingenbeheerder bevestigen.	Interpretatie: Bij online beheer van machtigingen door de beheerder wordt automatisch voldaan aan deze norm. Als het Machtigingenregister in opdracht van de beheerder wijzigingen uitvoert moet deze norm een specifiek uitwerking krijgen.
3.1.2.7	LOA 1 2 3 4	De machtigingenbeheerder MOET op ieder moment inzage hebben in de feitelijk geregistreerde machtigingen binnen zijn verantwoordelijkheidsdomein.	Interpretatie: Bij online beheer van machtigingen door de beheerder wordt automatisch voldaan aan deze norm. Als het machtigingenregister in opdracht van de beheerder wijzigingen uitvoert moet deze norm een specifiek uitwerking krijgen.
3.1.3	LOA 1 2 3 4	Controledoelstelling: Het machtigingenregister MOET erop toezien dat de reikwijdte van de machtigingen deugdelijk wordt geregistreerd.	
3.1.3.1	LOA 1 2 3 4	De tijdens de registratie van een machtiging verschafte gegevensverklaringen MOETEN bestaan uit: • Kenmerken ter identificatie van de vertegenwoordigde Dienstafnemer • Kenmerken ter identificatie van de vertegenwoordiger(s) van de Dienstafnemer welke van toepassing zijn op een machtiging. • Dit vereiste hoeft niet in acht genomen te worden als de vertegenwoordiger slechts op LoA 1 geïdentificeerd is. • Kenmerken ter identificatie van de Gemachtigde. • De reikwijdte van de machtiging: de omvang van de diensten en procedures waar de vertegenwoordiger voor gemachtigd is. • Aard van de machtiging: kenmerken van de machtiging zoals het 'recht op vervanging' en 'bevoegdheid om zelfstandig op te treden'. • Ingangsdatum en geldigheidsdatum van de machtiging.	
3.1.3.2	LOA 1 2 3 4	De reikwijdte van de machtigingen kan beperkt worden tot één Vestiging of een Dienstafnemer. In het geval van een gemachtigde tussenpersoon of een gemachtigde derde MOGEN de machtigingen niet tot één Vestiging of tussenpersoon beperkt worden.	Interpretatie: Deze norm betreft ketenmachtigingen. Bijvoorbeeld de machtiging van een accountantskantoor kan niet beperkt worden tot één vestiging van die accountant.
3.3		**Controledoelstelling: Het machtigingenregister MOET erop toezien dat aanvragers deugdelijk geregistreerd, geïdentificeerd en geauthenticeerd zijn, en dat de identiteitsverklaringen behoorlijk geverifieerd zijn conform de betrouwbaarheidsniveaus voor het uitgegeven middel.** **Specifiek is hierbij het volgende vereist**	
3.3.1	LOA 2 3 4	Controledoelstelling: Het machtigingenregister MOET erop toezien dat de machtigingen deugdelijk beheerd worden door de Dienstafnemer.	

3.3.1.1	LOA 2 3 4	Voor de elektronische administratie van machtigingen op betrouwbaarheidsniveaus LoA 2, 3 en 4: • Nadat opdracht is verleend tot de dienstverlening van het machtigingenregister zal de Dienstafnemer vertegenwoordigd worden door de perso(o)n(en) die de functie van machtigingenbeheerder bekleedt: • De machtigingenbeheerder MOET in het bezit zijn van een middel uit het stelsel. • De machtigingenbeheerder MOET bevoegd zijn in het Machtigingenregister.	
3.3.1.2	LOA 2 3 4	Voor de niet-elektronische administratie van machtigingen op betrouwbaarheidsniveaus LoA 2, 3 en 4: • Nadat opdracht is verleend tot de dienstverlening van het machtigingenregister zal de Dienstafnemer vertegenwoordigd worden door de perso(o)n(en) die de functie van machtigingenbeheerder bekleedt/bekleden: • De machtigingenbeheerder MOET bevoegd zijn in het machtigingenregister.De machtigingenbeheerder MOET ieder ingediend ver zoek met een handgeschreven handtekening ondertekenen. • Het machtigingenregister MOET de handgeschreven handtekening steeds verifiëren door deze te vergelijken met de gearchiveerde handgeschreven handtekening van de machtigingenbeheerder.	
3.3.2	LOA 1 2 3 4	Controledoelstelling: Het machtigingenregister MOET erop toezien dat de machtigingen beheerd worden door de juiste Dienstafnemer.	
3.3.2.1	LOA 1	Elektronisch verzoek De Dienstafnemer MOET geïdentificeerd worden op basis van de bevoegdheid van de machtigingenbeheerder.	
3.3.2.2	LOA 1	Niet-elektronisch verzoek De Dienstafnemer MOET geïdentificeerd worden volgens hoofdstuk 2, paragraaf 2.1.3 Bewijs van verificatie van identiteit (rechtspersoon).	
3.3.2.3	LOA 2 3 4	De Dienstafnemer MOET ten minste op betrouwbaarheidsniveau 2 geïdentificeerd worden op basis van een machtiging van machtigingenbeheerder. In het geval dat de reikwijdte van de bevoegdheid beperkt is tot één Vestiging MOET de identificatie uitgevoerd worden volgens ho ofdstuk 2, paragraaf 2.1.3 Bewijs van verificatie van identiteit (rechtspersoon).	
3.3.3	LOA 1 2 3 4	Controledoelstelling: Het machtigingenregister MOET erop toezien dat machtigingen of wijzigingen uitsluitend door de geregistreerde vertegenwoordiger van de Dienstafnemer aangevraagd kunnen worden.	
3.3.3.1	LOA 1 2 3 4	Elektronische verzoeken: De machtigingenbeheerder MOET geauthenticeerd worden op basis van zijn middel uit het stelsel en in overeenstemming met het toepasselijk betrouwbaarheidsniveau in het machtigingenregister.	
3.3.3.2	LOA 1	Niet-elektronische verzoeken: De machtigingenbeheerder MOET geauthenticeerd worden volgens de vereisten in paragraaf 2.1.3 bij LoA1. Specifieke uitzondering: machtigingenbeheerder hoeft niet opnieuw een kopie van zijn identiteitsdocument op te sturen in het geval dat het machtigingenregister hem/haar anderszins kan identificeren.	
3.3.3.3	LOA 2	Niet-elektronische verzoeken: De machtigingenbeheerder MOET geauthentiseerd worden volgens de vereisten van paragraaf 2.1.3 bij LoA2, plus en een van de onderstaande verificaties van een kopie van het identiteitsdocument. • Verificatie in het register voor gestolen of vermiste identiteitsbewijzen. • verificatie met het gebruik van een door de machtigingenbeheerder gedane bankoverschrijving. Bij herhaalde verificatie in het register voor gestolen of vermiste identiteitsbewijzen, hoeft de machtigingenbeheerder, zolang het	

		identiteitsdocument niet verlopen is, niet opnieuw een kopie van zijn identiteitsdocument op te sturen.	
3.3.3.4	LOA 3	De machtigingenbeheerder MOET geauthenticeerd worden volgens de vereisten van paragraaf 2.1.3 bij LoA3. Naast het voorgaande MAG het Machtigingen register NIET een andere alternatieve procedure gebruiken.	
3.3.3.5	LOA 4	In aanvulling op 3.3.3.1 De machtigingenbeheerder MOET de aanvraag elektronisch ondertekenen met een gekwalificeerde handtekening. Niet-elektronische verzoeken: De machtigingenbeheerder MOET geauthenticeerd worden middels de alternatieven genoemd in paragraaf 2.1.3 bij LoA4. Naast het voorgaande MAG het Machtigingen register NIET een andere alternatieve procedure gebruiken.	
3.4		**Controledoelstelling: Het machtigingenregister MOET bewaken dat de kwaliteit van de verlenging van machtigingen dezelfde is als bij de eerste registratie.**	
3.4.1	LOA 1	De machtigingenbeheerder MOET ten minste op betrouwbaarheidsniveau LoA 1 geauthenticeerd zijn. De betrokkenheid van de machtigingenbeheerder bij de Dienstafnemer MOET ten minste op betrouwbaarheidsniveau LoA 1 ingeschaald zijn.	
3.4.2	LOA 2	De machtigingenbeheerder MOET ten minste op betrouwbaarheidsniveau LoA 2 geauthenticeerd zijn. De betrokkenheid van de machtigingenbeheerder bij de Dienstafnemer MOET ten minste op betrouwbaarheidsniveau LoA 2 ingeschaald zijn.	
3.4.3	LOA 3	De machtigingenbeheerder MOET ten minste op betrouwbaarheidsniveau LoA 3 geauthenticeerd zijn. De procedure om de betrokkenheid van de machtigingenbeheerder bij de Dienstafnemer vast te stellen MOET ten minste in overeenstemming zijn met betrouwbaarheidsniveau LoA 3.	
3.4.4	LOA 4	De machtigingenbeheerder MOET ten minste op betrouwbaarheidsniveau LoA 4 geauthenticeerd zijn. De procedure om de betrokkenheid van de machtigingenbeheerder bij de Dienstafnemer vast te stellen MOET ten minste in overeenstemming zijn met betrouwbaarheidsniveau L oA 3.	
3.4.5	LOA 2 3 4	De te verlengen machtiging MOET ten minste geïdentificeerd worden: • In overeenstemming met identificatie van de Dienstafnemer op betrouwbaarheidsniveau LoA 2; en • Met de unieke identiteitskenmerken van de persoon die bevoegd gaat worden.	
3.5		**Controledoelstelling: Het machtigingenregister MOET erop toezien dat intrekking- en schorsingsprocedures in overeen stemming met de juiste betrouwbaarheidsniveaus worden doorgevoerd.**	
3.5.1	LOA 1 2 3 4	Het machtigingenregister MOET verzoeken voor intrekking of schorsing van machtigingen afkomstig van de volgende partijen accepteren: • de Rechtbank; • de wettelijke vertegenwoordiger(s) van de Dienstafnemer, waaronder mede begrepen de curator; • de Gevolmachtigde namens de wettelijke vertegenwoordiger; • de Machtigingenbeheerder.	
3.5.2	LOA 1	Een intrekking MOET middels een handmatig ondertekende brief of e-mail worden verzocht. De in vereiste 3.5.1 genoemde partij MOET ten minste op betrouwbaarheidsniveau LoA 1 geauthenticeerd zijn.	Interpretatie: In het proces voor schorsing (indien ondersteund) mag soepeler worden omgegaan met de authenticatie van degene die de schorsing meldt met het oog op snellere verwerking. In dat geval moet de afwijking van het normale authenticatieproces expliciet vastgelegd zijn. Advies: Het is voorstelbaar dat bij een verzoek Rechter tot schorsing of intrekking de identificatieprocedure niet conform de aangegeven vereisten kan worden uitgevoerd. Kern is dat dan een mate van zekerheid wordt bereikt over de authenticiteit van

			het verzoek dat overeenkomt met het juiste LoA. Bijvoorbeeld verificatie van een of meer identificerende kenmerken via een of meer andere kanalen dan waarlangs het verzoek is gedaaan.
3.5.3	LOA 2	De partijen die een intrekkings- of schorsingsverzoek van bevoegdheid mogen indienen (zie vereiste 3.5.1.) MOETEN ten minste op betrouwbaarheidsniveau LoA 2 geauthenticeerd zijn (zie hoofdstuk 2, paragraaf 2.1.1 en 2.1.2)	Interpretatie: In het proces voor schorsing (indien ondersteund) mag soepeler worden omgegaan met de authenticatie van degene die de schorsing meldt met het oog op snellere verwerking. In dat geval moet de afwijking van het normale authenticatieproces expliciet vastgelegd zijn. Advies: Het is voorstelbaar dat bij bijvoorbeeld een verzoek Rechter tot schorsing of intrekking de identificatieprocedure niet conform de aangegeven vereisten kan worden uitgevoerd. Kern is dat dan een mate van zekerheid wordt bereikt over de authenticiteit van het verzoek dat overeenkomt met het juiste LoA. Bijvoorbeeld verificatie van een of meer identificerende kenmerken via een of meer andere kanalen dan waarlangs het verzoek is gedaaan.
3.5.4	LOA 3 4	De in vereiste 3.5.1 genoemde partij MOET ten minste op betrouwbaarheidsniveau LoA 3 geauthenticeerd zijn (zie hoofdstuk 2, paragraaf 2.1.1 en 2.1.2).	Interpretatie: In het proces voor schorsing (indien ondersteund) mag soepeler worden omgegaan met de authenticatie van degene die de schorsing meldt met het oog op snellere verwerking. In dat geval moet de afwijking van het normale authenticatieproces expliciet vastgelegd zijn. Advies: Het is voorstelbaar dat bij een verzoek Rechter tot schorsing of intrekking de identificatieprocedure niet conform de aangegeven vereisten kan worden uitgevoerd. Kern is dat dan een mate van zekerheid wordt bereikt over de authenticiteit van het verzoek dat overeenkomt met het juiste LoA. Bijvoorbeeld verificatie van een of meer identificerende kenmerken via een of meer andere kanalen dan waarlangs het verzoek is gedaaan.
3.5.5	LOA 1	Er zijn geen vereisten voor de doorlooptijd van de verwerking van het intrekkingsverzoek.	
3.5.6	LOA 2 3 4	Intrekking MOET als volgt worden verwerkt: Alternatief 1 voor elektronische verzoeken: Intrekking MOET onmiddellijk worden verwerkt: Alternatief 2 voor elektronische verzoeken: Intrekking MOET binnen een dag na ontvangst van het verzoek worden ver werkt.	
3.5.7	LOA 1 2 3 4	Een verzoek tot heractivering van geschorste machtiging MOET worden gedaan door machtigingenbeheerder of een andere wettelijke vertegenwoordiger van de Dienstafnemer die volgens de vereisten voor eerste identificatie in overeenstemming met het toepasselijke betrouwbaarheidsniveau (zie hoofdstuk 2, paragraaf 2.1.1) is geïdentificeerd.	
3.6		**Controledoelstelling: Het machtigingenregister MOET misbruik van niet-actieve machtigingen voorkomen.**	
3.6.1	LOA 3 4	De Machtigingendienst waarborgt dat het bedrijf of de organisatie de geregistreerde machtigingen actueel houdt: 1. Het machtigingenregister verzoekt de machtigingenbeheerder in elk geval tweejaarlijks de geregistreerde set van machtigingen te bevestigen, dan wel te laten wijzigingen, of te laten de-registreren indien over een periode van 24 maanden geen van de machtigingen uit deze set is gebruikt. 2. In het geval de machtigingenbeheerder zijn bevoegdheid om de organisatie, of het bedrijf, te vertegenwoordigen 24 maanden niet heeft gebruikt, verzoekt de Machtigingendienst ook de wettelijke vertegenwoordiger van de onderneming, of rechtspersoon die in het handelsregister is opgenomen om de betreffende bevoegdheid te bevestigen, dan wel te laten de-registreren. Indien de wettelijke vertegenwoordiger zelf de machtigingenbeheerder is, vervalt deze eis. 3. In het geval de machtigingenbeheerder, of de wettelijke vertegenwoordiger, niet op een herhaald verzoek, zoals bedoeld in sub 1 en sub 2, reageert, moet de Machtigingendienst een machtiging die niet is gebruikt intrekken. Als ook wordt geconstateerd dat de onderneming, of rechtspersoon niet meer als zodanig in het handelsregister is ingeschreven, moeten alle machtigingen worden ingetrokken.	
3.7		**Controledoelstelling: Het Machtigingenregister MOET bedrijfsdiscontinuïteit of misbruik van de machtigingen voorkomen die voortkomen uit een uitgestelde verwerking van de verzochte wijzigingen.**	
3.7.1	LOA 1	Een wijzigingsverzoek voor machtigingen MOET zo spoedig mogelijk verwerkt worden.	

3.7.2	LOA 2 3 4	Een elektronisch wijzigingsverzoek voor machtigingen MOET onmiddellijk verwerkt worden.	
3.7.3	LOA 2 3 4	Een niet-elektronisch wijzigingsverzoek voor machtigingen moet binnen twee werkdagen worden verwerkt.	

Eisen voor geldigheid van verklaringen voor Dienstverleners

EH1 vervalt per 1-7-2021

Met ingang van 1 juli 2021 komt het gebruik van het betrouwbaarheidsniveau eH1 te vervallen en moeten de middelen en machtigingen minimaal voldoen aan de normen van het betrouwbaarheidsniveau eH2.

Norm	LoA	Vereisten	Best practices
4	LOA 1 2 3 4	De ontvangende partij MOET een verklaring alleen gebruiken als deze voldoet aan de eisen van die bij het betrouwbaarheidsniveau horen (van deze verklaring). De ontvangende partij ZOU waar mogelijk striktere normen MOETEN hanteren dan de ruimte die geboden wordt in de vereisten van de in 4.1 en 4.2 gedefinieerde betrouwbaarheidsniveaus van de verklaringen.	Richtlijn is dat de ruimte niet groter zou moeten zijn dan noodzakelijk. Dat betekent dat de Dienstaanbieder striktere normen zou moeten hanteren als de situatie dat toestaat.
4.1		**Vereisten authenticatie- en machtigingsverklaring**	
4.1.1	LOA 3 4	Geldigheidseisen aan een authenticatie- en machtigingsverklaring (of een daar van afgeleide credential of token) MOETEN afgedwongen worden door elke partij die de verklaringen ontvangt en/of door levert. Dit geldt voor alle Deelnemers maar heel specifiek ook voor Dienstverlener & Dienstbemiddelaar.	Dit geldt voor alle verklaringen die een partij zelf gebruikt maar ook de verklaringen die zo'n partij doorgeeft aan een volgende partij. Zo zijn een Makelaar en Dienstbemiddelaar verantwoordelijk voor het doorleveren van slechts authenticatie- en machtigingsverklaring waarvan ze zelf hebben vastgesteld dat deze voldoen aan de geldigheidseisen, voor zover dat mogelijk is.
4.1.1.1	LOA 3 4	• Een Verklaring MAG NIET gebruikt worden buiten de gebruikerssessie waarin de Dienstverlener of Dienstaanbieder hem ontvangt. • Een Verklaring in een Gebruikerssessie MOET binnen 4 uur ververst worden.	In een aantal gevallen zal 4 uur zelfs heel ruim zijn. De DV moet zelf een afweging maken of 4 uur voor zijn proces niet veel te ruim is. Een DV die slechts kleine online formulieren beschikbaar stelt zou een veel scherpere geldigheidstermijn moeten kiezen.
4.2		**Vereisten associatieverklaring**	
4.2.1	LOA 1 2 3 4	De Dienstbemiddelaar MOET met een associatieverklaring de Authenticatie (en optioneel) Machtigingsverklaring onlosmakelijk verbinden aan de een transactie of een document overeenkomstig het geldende betrouwbaarheidsniveau.	Ook hier moet de ruimte niet groter zijn dan noodzakelijk. Dat betekent dat de Dienstaanbieder strenger zou moeten zijn als zijn situatie dat toestaat.
4.2.1.1	LOA 1 2 3	Een associatieverklaring (met bericht) die ontstaat binnen een gebruikerssessie MAG NIET ingezonden worden naar de Dienstaanbieder buiten de sessie waarin hij ontstaat TENZIJ • de indienende partij (Dienstbemiddelaar) de Gebruiker gegarandeerd kan informeren over eventuele inzendproblemen, binnen een redelijke termijn voor het betreffende bericht., OF • de Dienstverlener samen met en de indienende partij de ontvangst het betreffende bericht door de DV garanderen.	De beoordeling van een 'redelijke termijn' (voor het informeren van de Gebruiker over inzendproblemen bij een bericht) is een eigen afweging van de Dienstaanbieder. Centraal bij het vaststellen van deze redelijke termijn staat het nadelige gevolg voor de Gebruiker als hij er te laat achter komt dat een bericht /transactie niet ontvangen is door de Dienstaanbieder.
4.2.1.1.1	LOA 1 2	Een associatieverklaring MAG NIET ouder zijn dan 5 dagen	Dit zijn maximale termijnen een Dienstaanbieder zou zelf strengere eisen moeten stellen aan de maximale leeftijd van de associatieverklaring als de situatie dat toestaat.
4.2.1.1.2	LOA 3	Een associatieverklaring MAG NIET ouder zijn dan 1 dag	
4.2.1.1.3	LOA 1 2 3	Een Dienstaanbieder MAG onder 'speciale omstandigheden' een associatieverklaring accepteren tot maximaal 10 dagen oud.	De beoordeling van een 'speciale omstandigheid' is een eigen afweging van de Dienstaanbieder. De speciale omstandigheid moet niet de standaard afhandeling zijn, maar slechts gebruikt in uitzonderingsgevallen zoals bijvoorbeeld een incident met

			tijdelijke onbeschikbaarheid van de Dienstaanbieder zelf. In dat geval kan de DA besluiten om associatieverklaringen te accepteren die tijdens de onbeschikbaarheidsperiode nog wel geaccepteerd zouden zijn. Anders moeten de Dienstbemiddelaars hun berichten opnieuw laten accorderen door de Gebruiker.
4.2.1.2	LOA 4	Een associatieverklaring op LoA4 die ontstaat binnen een gebruikerssessie MAG NIET ingezonden worden naar de Dienstaanbieder buiten de sessie waarin hij ontstaat.	
4.3		**Vereisten geldigheid van verklaringen van Dienstverleners**	
4.3.1	LOA 1	Transportberichten: De geldigheid van transportberichten moet niet langer zijn dan strikt noodzakelijk: ruim genoeg om een efficiënte gebruikerservaring te garanderen en kort genoeg om een aanvaller minimale gelegenheid te bieden. Authenticatie Tokens: Authenticatie Tokens die zijn afgeleid van authenticatiemiddelen MOETEN op de zelfde termijn als het middel ingetrokken of geschorst kunnen worden. Een 'sessie' MAG daarom een hele dag duren. Extented Sessie: Een 'extented sessie' op een specifiek apparaat MAG (zonder expliciete herauthenticatie van de gebruiker) onbeperkt duren, maar dan MOET deze extended sessie minimaal elke maand 'in gebruik' zijn geweest.	OAuth2 tokens tbv native DV-app: • Een Authorization Grant ZOU na 5 minuten MOETEN vervallen. • Een Access Token MOET na 24 uur vervallen. • Refresh Token MOET na een maand vervallen • Een geldig Refresh Token MAG (binnen die maand) wel onbeperkt ververst worden zonder expliciete herauthenticatie van de Gebruiker.
4.3.2	LOA 2	Hetzelfde als LoA1, uitgezonderd de eisen over de 'extended sessie' Extented Sessie: • Een 'extented sessie' op een specifiek apparaat ZOU (zonder expliciete herauthenticatie van de gebruiker) uiterlijk een 7 dagen MOGEN duren. • Een 'extented sessie' op een specifiek apparaat MAG (zonder expliciete herauthenticatie van de gebruiker) uiterlijk een jaar duren, maar dan MOET deze extended sessie minimaal elke maand 'in gebruik' zijn geweest.	OAuth2 tokens tbv native DV-app: • Een Authorization Grant ZOU na 5 minuten MOETEN vervallen. • Een Access Token MOET na 24 uur vervallen. • Een Refresh Token ZOU na 7 dagen MOETEN vervallen • Een Refresh Token MOET binnen een maand vervallen • Een geldig Refresh Token MAG ververst worden met een maximum verlenging van 1 jaar zonder expliciete herauthenticatie van de Gebruiker.
4.3.3	LOA 3	Hetzelfde als LoA1, uitgezonderd de eisen over de 'extended sessie' Extented Sessie: • Een 'extented sessie' op een specifiek apparaat ZOU (zonder expliciete herauthenticatie van de gebruiker) uiterlijk 8 uur MOGEN duren, tenminste zolang het apparaat niet uit is geweest. • Een 'extented sessie' op een specifiek apparaat MAG (zonder expliciete herauthenticatie van de gebruiker) uiterlijk 7 dagen duren, maar dan MOET deze extended sessie minimaal elke 24 uur 'in gebruik' zijn geweest.	OAuth2 tokens tbv native DV-app: • Een Authorization Grant MOET na 5 minuten vervallen. • Een Access Token MOET na 4 uur vervallen • Een Refresh Token ZOU na 8 uur MOETEN vervallen en als het apparaat uit is geweest. • Een Refresh Token MOET binnen 24 uur vervallen • Een geldig Refresh Token MAG ververst worden met een maximum verlenging van 7 dagen zonder expliciete herauthenticatie van de Gebruiker.
4.3.4	LOA 4	Hetzelfde als LoA1, uitgezonderd de eisen over de 'Authenticatie Tokens' en 'Extended Sessie' Authenticatie Tokens: Een 'sessie' MAG uiterlijk 1 uur duren, maar dan MOET deze sessie constant in gebruik1 zijn geweest (voor zover detectie mogelijk is). Extented Sessie: Een 'extented sessie' op een specifiek apparaat MAG NIET bestaan.	OAuth2 tokens tbv native DV-app is momenteel nog niet ondersteund voor native apps, anders: • Een Authorization Grant MOET na 5 minuten vervallen. • Een Access Token ZOU na 15 minuten MOETEN vervallen en als de App inactief1 is geweest. • Een Access Token MOET binnen 1 uur vervallen • Een Refresh Token MAG NIET gebruikt worden

Voetnoot:

1. Een App is inactief als deze op de achtergrond is geweest of als het scherm uit is geweest.

Attributenbeleid

Het leveren van attributen houdt in: het leveren van unieke, gegevens van natuurlijke en niet-natuurlijke personen, zoals achternaam, KVK-nummer, organisatie en het voldoen aan een leeftijdsgroep. Deze persoonsgegevens kunnen zelfverklaard zijn of geverifieerd tijdens de registratie of op een later moment op een bepaald betrouwbaarheidsniveau.

Er zijn verplicht en optioneel te verstrekken attributen. Verplicht te verstrekken attributen zijn gegevens die een Deelnemer MOET verstrekken. Optioneel te verstrekken attributen zijn gegevens die een Deelnemer MAG verstrekken. Deze Optionele functionaliteit kan door meerdere rollen (deelnemers) in het netwerk geleverd worden geleverd ten behoeve van Dienstverlener (DV).

Voor herkenningsmakelaars is attribuutverstrekking een verplichte functionaliteit om in te richten en te leveren. De Deelnemers mogen alle attributen uitwisselen die beschreven zijn in de Attribuutcatalogus. Ze hoeven hiervoor niet opnieuw toe te treden of een proceswijziging in te dienen. Indien een nieuw attribuut aan de Attribuutcatalogus moet worden toegevoegd, dient wel een proceswijzigingsverzoek te worden ingediend, waarbij gespecificeerd dient te worden welk attribuut wordt toegevoegd en welke processen hiervoor worden ingericht. Zie proces Proces toetreden.

Welke afspraken en eisen gelden er binnen het afsprakenstelsel?

- Het verstrekken van attributen gebeurt altijd op basis van *user consent*: de gebruiker of de vertegenwoordiger van de gebruiker moet expliciet toestemming geven om deze informatie door te geven aan de organisatie die erom vraagt (dienstverlener). Als een vertegenwoordiger deze toestemming geeft, moet deze hiervoor gemachtigd zijn.
- Het stelsel verstrekt attributen op verzoek van een dienstverlener. Het is de verantwoordelijkheid van de dienstverlener om te beoordelen of er doelbinding is, niet meer gegevens te vragen dan nodig en de dienstafnemer (gebruiker) te informeren wat er met de gegevens wordt gedaan (conform AVG, voor wettekst zie https://wetten.overheid.nl/BWBR0040940/2019-02-19).
- Aan dienstafnemers (gebruikers) moet steeds inzage, correctie en intrekking geboden worden van de over hen geregistreerde persoonsgegevens.
- Het is niet toegestaan aan gebruikers of (wettelijke) vertegenwoordigers vooraf globaal toestemming te vragen voor verstrekken van alle mogelijke attributen. De user consent dient specifiek te zijn voor een bepaald attribuut en mag beperkt zijn tot een bepaalde dienst en/of dienstverlener. Nadat de eerste keer met de verstrekking van een bepaald attribuut is ingestemd mag de betrokkene aangeven dat dit in vervolg voor dat specifieke doel niet opnieuw gevraagd hoeft te worden. Het bewaren van deze instelling is gebonden aan de termijn als gespecificeerd in het Normenkader betrouwbaarheidsniveaus (doorlooptijd van mutaties van bevoegdheden bij herhaalde registratie).

Verantwoordelijkheden middelenuitgever

- Registreren van door aanvrager van het authenticatiemiddel verstrekte persoonsgegevens behorende bij de houder van het middel. Deze persoonsgegevens kunnen zelfverklaard zijn of geverifieerd tijdens de registratie of op een later moment op een bepaald betrouwbaarheidsniveau.
- Als gebruiker een specifieke dienst benadert die bepaalde attributen wilt ontvangen, dan wordt consent gevraagd waarbij getoond wordt i) voor welke dienstverlener en ii) welke dienst en iii) voor welk attribuut. Daarbij is het mogelijk vanuit usability oogpunt om de gebruiker meteen te laten kiezen om dit attribuut in navolgende verzoeken met de dienstverlener te delen, ook voor andere diensten.

Verantwoordelijkheden authenticatiedienst

- Het verstrekken van attributen over de geauthenticeerde gebruiker na een geslaagde authenticatie indien dit door de dienstverlener gevraagd wordt en indien het op grond van bij middelenuitgever of authenticatiedienst geregistreerde user consent of tijdens authenticatie gevraagde consent is toegestaan.
- Het aanbieden aan de geauthenticeerde gebruiker van inzage, correctie en intrekking van de over hen geregistreerde persoonsgegevens en het registreren of er toestemming is verleend voor het zonder steeds opnieuw vragen verstrekken van deze persoonsgegevens, aan een specifieke dienstverlener en dienst (dit proces kan elektronisch of op papier worden aangeboden).
- Een Authenticatiedienst MOET zijn attribuutverstrekking beperken tot de gegevens die zij beheert uit hoofde van het uitvoeren van haar rol.

Verantwoordelijkheden machtigingenregister

- Het registreren van gegevens van de vertegenwoordigde dienstafnemer of intermediaire partij gegevens welke verstrekt kunnen worden binnen de context van een machtiging. Deze kunnen zelfverklaard zijn, geverifieerd tijdens registratie of op een later moment of gevalideerd op het moment van authenticatie;
- per gegeven registreren van user consent van de wettelijke vertegenwoordiger of machtigingenbeheerder voor het daadwerkelijk verstrekken van die gegevens aan alle dienstverleners (indien gewenst kan worden geregistreerd dat een gegeven alleen aan specifieke dienstverlener(s) mag worden geleverd);
- Na aantreffen van machtiging verstrekken van attributen behorende bij de context waarop de machtiging betrekking heeft indien dit door de dienstverlener gevraagd wordt en indien het op grond van geregistreerde user consent is toegestaan (indien user consent niet vooraf is geregistreerd moet dit op moment van transactie worden gevraagd).
- Indien attribuutverstrekking wordt aangeboden moet aan vertegenwoordigde dienstafnemers of intermediaire partijen waarvoor machtiging worden geregistreerd en hun beheerders inzage, correctie en mogelijkheid tot verwijderen geboden kunnen worden van de over hen geregistreerde (persoons)gegevens en of er toestemming is verleend voor het zonder steeds opnieuw vragen verstrekken van deze gegevens, aan een specifieke dienstverlener en dienst (dit proces kan elektronisch of op papier worden aangeboden).

Verantwoordelijkheden herkenningsmakelaar

- Het registreren welke attributen een dienstverlener wil uitvragen bij iedere authenticatie.
- Het doorgeven van attributen precies zoals ze ontvangen zijn van authenticatiediensten of machtigingenregisters.

Templates en formulieren

Onderstaande documenten kunnen worden opgeslagen als PDF of als Word document voor verdere verwerking. Klik hiervoor rechtsboven op **Tools > Export to PDF** of **Tools > Export to Word**.

- Template deelnemersovereenkomst — De overeenkomst tussen deelnemers en beheerorganisatie op basis waarvan deelnemers gehouden zijn het afsprakenstelsel toe te passen. Deze deelnemersovereenkomst verwijst naar het afsprakenstelsel maar is er (strikt genomen) zelf geen onderdeel van.
- Template verzoek tot (uitbreiding) toetreding
- Template wijziging rechtspersoon deelnemer
- Template zelfverklaring Dienstverlener

Template deelnemersovereenkomst

20180104 Deelnemersovereenkomst Afsprakenstelsel Elektronische Toegangsdiensten.docx

Deelnemersovereenkomst Afsprakenstelsel elektronische toegangsdiensten

Partijen

De Staat der Nederlanden, te dezen vertegenwoordigd door de staatssecretaris van Binnenlandse Zaken, voor deze <f unctie> , <naam>,

en

<Naam deelnemer> gevestigd te <adres>, te dezen vertegenwoordigd door <naam> , voor deze <functie>, <naam>,

verder te noemen: deelnemer,

Overwegende dat

I. dienstverleners in toenemende mate langs elektronische weg diensten wensen te verlenen aan dienstafnemers;

II. een betrouwbare herkenning van de dienstafnemer daarbij noodzakelijk is;

III. in deze behoefte wordt voorzien door middel van een afsprakenstelsel en een netwerk voor elektronische toegangsdiensten;

IV. in het netwerk voor elektronische toegangsdiensten vijf rollen worden onderscheiden, te weten de middelenuitgever, de authenticatiedienst, de ondertekendienst, het machtigingenregister en de herkenningsmakelaar;

V. in het netwerk voor elektronische toegangsdiensten de positie van dienstverlener wordt onderscheiden;

VI. de deelnemer elektronische toegangsdiensten wenst te verlenen en wenst te worden toegelaten tot het netwerk voor elektronische toegangsdiensten om één of meer rollen te vervullen;

VII. het deelnemers alleen wordt toegestaan een rol in het netwerk voor elektronische toegangsdiensten te vervullen indien zij de toetredingsprocedure met goed gevolg hebben doorlopen;

VIII. in het afsprakenstelsel elektronische toegangsdiensten is vastgelegd aan welke verplichtingen de deelnemer dient te voldoen voor de desbetreffende rol;

IX. de staatssecretaris van Binnenlandse Zaken zorg draagt voor het beheer van het afsprakenstelsel elektronische toegangsdiensten en het toezicht op de naleving van de daarin opgenomen verplichtingen door de deelnemers.

Verklaren te zijn overeengekomen als volgt

Artikel 1. Definities

1.1 Alle onderstreepte begrippen die in deze Deelnemersovereenkomst zijn opgenomen, hebben de betekenis zoals opgenomen in het afsprakenstelsel elektronische toegangsdiensten. De begrippen worden slechts de eerste keer dat zij in de Deelnemersovereenkomst voorkomen, onderstreept. Alle definities kunnen zowel in enkel- als meervoud gehanteerd worden.

Artikel 2. Voorwerp van de Deelnemersovereenkomst

2.1 De deelnemer verkrijgt hierbij het recht binnen het netwerk voor elektronische toegangsdiensten voor eigen rekening en risico elektronische toegangsdiensten aan te bieden en de rol(len) te vervullen waarvoor hij de toetredingsprocedure met goed gevolg heeft doorlopen.

2.2 De deelnemer is gehouden onverkort alle verplichtingen na te komen die op grond van deze Deelnemersovereenkomst, het afsprakenstelsel , de Gebruiksvoorwaarden en alle overige bindende regelingen die op enig moment voor zijn rol zijn vastgesteld en in werking zijn getreden.

2.3 De deelnemer is op de hoogte van en erkent de governance van het afsprakenstelsel, zoals vastgelegd in het Instellingsbesluit besturing afsprakenstelsel elektronische toegangsdiensten, alsmede het toezicht zoals vastgelegd in het afsprakenstelsel.

2.4 Het is de deelnemer niet toegestaan andere rollen te vervullen en/of elektronische toegangsdiensten op andere betrouwbaarheidsniveaus te vervullen en/of andere functionaliteiten aan te bieden zonder hiervoor de toetredingsprocedure te doorlopen.

2.5 De staatssecretaris van Binnenlandse Zaken zal zich inspannen de op hem rustende verplichtingen voortvloeiend uit zijn verantwoordelijkheid voor het afsprakenstelsel naar beste vermogen na te komen, met inachtneming van de belangen van alle betrokken partijen.

2.6 Van deze Deelnemersovereenkomst maken onlosmakelijk onderdeel uit de volgende documenten:

a) het afsprakenstelsel zoals dat formeel op enig moment is vastgesteld en van toepassing is op en in werking getreden is voor een bepaalde rol;

b) de Gebruiksvoorwaarden.

2.7 Bij strijdigheden tussen de in het vorige lid genoemde documenten, prevaleert het eerder genoemde document boven het later genoemde document.

2.8 Een bepaling in de Deelnemersovereenkomst die strijdig is met het afsprakenstelsel en/of het geldende recht, laat de overige bepalingen van de Deelnemersovereenkomst onverlet.

Artikel 3. Gebruiksrecht voor het voeren van het Merk

3.1 Onder het Merk wordt verstaan: het (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan de staatssecretaris van Binnenlandse Zaken het merkenrecht uitoefent.

3.2 De deelnemer heeft het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van de Deelnemersovereenkomst, het Merk te gebruiken in verband met het uitvoeren van elektronische toegangsdiensten en het vervullen van de overeengekomen rol(len), in overeenstemming met deze Deelnemersovereenkomst en de daaruit voortvloeiende voorschriften.

3.3 De deelnemer is niet bevoegd derden toestemming te geven het Merk te gebruiken.

3.4 De deelnemer zal niets doen dan wel nalaten waardoor de rechten van de staatssecretaris van Binnenlandse Zaken ten aanzien van het Merk kunnen worden aangetast en/of de ter zake van het Merk opgebouwde goodwill negatief zou kunnen worden beïnvloed.

Artikel 4. Aanvang, looptijd en duur van de Deelnemersovereenkomst

4.1 Deze Deelnemersovereenkomst treedt in werking op de datum van ondertekening en eindigt op <vul datum in>.

Artikel 5. Beëindiging van de Deelnemersovereenkomst

5.1 De deelnemer is te allen tijde gerechtigd de Deelnemersovereenkomst tussentijds schriftelijk te beëindigen met inachtneming van een opzegtermijn van 3 kalendermaanden.

5.2 De staatssecretaris van Binnenlandse Zaken kan de Deelnemersovereenkomst in de navolgende situaties beëindigen:

1. Indien de deelnemer enige verplichting uit de Deelnemersovereenkomst of het afsprakenstelsel bewust en/of consequent niet nakomt.
2. De toezichthouder de staatssecretaris van Binnenlandse Zaken hiertoe adviseert naar aanleiding van een klacht, geschil of handhavingverzoek.
3. De deelnemer failliet is verklaard, aan hem surseance van betaling is verleend of onder een schuldsaneringsregeling valt.

5.3 Na beëindiging van de Deelnemersovereenkomst zal de deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de desbetreffende rol(len) staken, dan wel zo snel mogelijk staken als praktisch haalbaar is. De deelnemer zal alle medewerking verlenen om de continuïteit van de toegangsdienstverlening zeker te stellen, onder meer door mee te werken aan overdracht van de toegangsdienstverlening aan een andere deelnemer en beschikt in dit kader over een continuïteits- en/of exitplan.

Artikel 6. Aansprakelijkheid deelnemers jegens derden en beheerorganisatie

6.1 De deelnemer aanvaardt door ondertekening van deze Deelnemersovereenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die de deelnemer vervult. De deelnemer aanvaardt deze aansprakelijkheid ook in die situaties waarbij dit handelen en/of nalaten schade veroorzaakt aan andere deelnemers en/of bedrijven en /of dienstverleners en/of de beheerorganisatie. Bedrijven, dienstverleners, andere deelnemers en de beheerorganisatie kunnen zich jegens de deelnemer onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De deelnemer vrijwaart de staatssecretaris van Binnenlandse Zaken voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van de elektronische toegangsdiensten.

Artikel 7. Overige bepalingen

7.1 De staatssecretaris van Binnenlandse Zaken is bevoegd te onderzoeken of deelnemer de afspraken van het afsprakenstelsel naleeft en/of deelnemer voldoet aan de eisen en voorwaarden die aan zijn rol worden gesteld in het afsprakenstelsel. De deelnemer verleent hieraan zijn medewerking.

7.2 Verplichtingen uit deze Deelnemersovereenkomst die naar hun aard bedoeld zijn om ook na afloop van deze Deelnemersovereenkomst voort te duren, behouden hun werking na afloop van deze Deelnemersovereenkomst.

7.3 Op deze overeenkomst is Nederlands recht van toepassing.

Aldus overeengekomen in tweevoud,

Namens de Staatssecretaris van Binnenlandse Zaken Naam: Functie: Datum: Plaats:	Namens de deelnemer, Naam: Functie: Datum: Plaats:
	<Naam deelnemer>

Template verzoek tot (uitbreiding) toetreding

Dit verzoek tot toetreding stelt (potentiële) deelnemers van Elektronische Toegangsdienstenin staat zich aan te melden voor (uitbreiding van) deelname aan het Netwerk. Dit ingevulde formulier vormt een onderdeel van het toetredingsproces voor Elektronische Toegangsdiensten, zoals beschreven in Proces toetreden.

Bedrijf

Naam:	
Handelsnaam:	
KvK nummer:	

Contactpersoon

Naam:	
Functie:	
E-mailadres:	
Telefoonnummer:	

Huidige rollen

Bovengenoemd bedrijf is op datum van ondertekening toegetreden tot het Netwerk in de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH2	eH2+	eH3	eH4
Herkenningsmakelaar	O			
Middelenuitgever	O	O	O	O
Authenticatiedienst	O	O	O	O
Machtigingenregister	O	O	O	O

Huidige optionele functionaliteit

Bovengenoemd bedrijf levert op datum van ondertekening de volgende optionele functionaliteit:

	Herkennings makelaar	Middelen uitgever	Authenticatie dienst	Machtigingen register
eHerkenning				
Bedrijven (G2B, B2B)	O			
Consumenten (B2C)		O	O	
Aanvullende features				
Gevalideerde attributen		O	O	O
Single sign-on			O	

Nieuwe rollen

Ondergetekende verklaart dat bovengenoemd bedrijf voornemens is het in het afsprakenstelsel beschreven Proces toetreden te doorlopen voor de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH2	eH2+	eH3	eH4
Herkenningsmakelaar	O			
Middelenuitgever	O	O	O	O
Authenticatiedienst	O	O	O	O

Machtigingenregister	O	O	O	O

Nieuwe optionele functionaliteit

Ondergetekende verklaart dat bovengenoemd bedrijf voornemens is het in het afsprakenstelsel beschreven Proces toetreden te doorlopen voor de volgende optionele functionaliteit:

	Herkennings makelaar	**Middelen uitgever**	**Authenticatie dienst**	**Machtigingen register**
eHerkenning				
Bedrijven (G2B, B2B)	O			
Consumenten (B2C)		O	O	
Aanvullende features				
Gevalideerde attributen		O	O	O
Single sign-on			O	

Geheimhoudingsverklaring

Ondergetekende verklaart alle informatie die hem in het kader van de toetreding en het gebruik het Afsprakenstelsel elektronische toegangsdiensten beschikbaar wordt gesteld, dan wel waarvan Ondergetekende kennis neemt, ongeacht of dit mondeling of schriftelijk gebeurt, als vertrouwelijk te behandelen, alleen te gebruiken voor het doel waarvoor de informatie is verstrekt en niet aan derden ter beschikking te stellen. Deze Geheimhoudingsverklaring betreft mede, dus niet uitsluitend, de informatie die als “Intern” of “Vertrouwelijk” is gekwalificeerd.

Ondertekening

Ondergetekende verzoekt de beheerorganisatie op basis van de door invulling van dit formulier verschafte informatie en de bijgevoegde bijlagen bovengenoemd bedrijf toe te laten treden als deelnemer van het Afsprakenstelsel Elektronische Toegangsdiensten voor de hierboven aangekruiste rollen, betrouwbaarheidsniveaus en optionele functionaliteit.

Datum:	
Plaats:	
Naam:	
Handtekening:	

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

Template wijziging rechtspersoon deelnemer

Wijziging rechtspersoon deelnemer

De deelnemer verklaart door ondertekening van dit formulier dat:

- de rechtspersoon waaraan de onderneming van de deelnemer toebehoort, wijzigt;
- de deelnemer de Beheerorganisatie verzoekt de deelnemersovereenkomst op naam te zetten van de nieuwe rechtspersoon;
- de organisatie en bedrijfsprocessen van de deelnemer, zoals daarvan tijdens het Proces toetreden verslag van is gedaan en zoals daarvan testen hebben plaatsgevonden, niet zijn gewijzigd;
- hij in het kader van de nieuwe rechtspersoon onveranderd conform het Afsprakenstelsel Elektronische Toegangsdiensten zal handelen.

(1) Huidige rechtspersoon

Naam	_____
KvK nummer	_____

(2) Nieuwe rechtspersoon

Naam	_____
KvK nummer	_____

(3) Contactpersoon

Naam	_____
E-mailadres	_____
Telefoonnummer	_____

(4) Rollen en/of betrouwbaarheidsniveaus

Ondergetekende verklaart dat de deelnemer het toetredingproces heeft doorlopen voor de volgende rollen en voor de volgende betrouwbaarheidsniveaus:

	eH2	**eH2+**	**eH3**	**eH4**
Herkenningsmakelaar	O			
Middelenuitgever	O	O	O	O
Authenticatiedienst	O	O	O	O
Machtigingenregister	O	O	O	O

(5) Verplichting ten aanzien van testen en conformiteit

De ondergetekende verklaart op grond van de reeds doorlopen toetredingsprocedure:

- onverminderd zijn medewerking te verlenen aan penetratietesten van de systemen;
- onverminderd zal handelen conform het afsprakenstelsel zoals dat op enig moment formeel is vastgesteld.

(6) Ondertekening

Datum:	_____
Plaats:	_____
Naam:	_____
Handtekening:	_____

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

Bijgevoegd:

O Kopie uittreksel handelsregister (liefst ingescand/elektronisch exemplaar)

O Kopie volmacht (liefst ingescand/elektronisch exemplaar)

Template zelfverklaring Dienstverlener

Ondergetekende,

Bedrijf

Naam:	
Handelsnaam:	
KvK nummer:	

Contactpersoon

Naam:	
Functie:	
E-mailadres:	
Telefoonnummer:	

verklaart hierbij voor zijn rol als Dienstverlener (waaronder ook kan worden verstaan een combinatie van Dienstaanbieder en Dienstbemiddelaar) als bedoeld in het Afsprakenstelsel Elektronische Toegangsdiensten (“afsprakenstelsel”), aantoonbaar te voldoen en te blijven voldoen aan alle op hem rustende verplichtingen en vereisten van het afsprakenstelsel.

Meer in het bijzonder verklaart ondergetekende dat hij voldoet en blijft voldoen aan de volgende verplichtingen:

1. De Dienstverlener beheerst binnen zijn vermogens de juistheid en de actualiteit van metadata en de gegevens voor de Dienstcatalogus (Proces doorvoeren nieuwe dienstencatalogus).
2. De dienstverlener beheerst de beveiligingsrisico’s van de technische componenten onderliggende aan de online diensten die hij aansluit; waaronder de betrokken eigen systemen, netwerkverbindingen, websites en de koppeling met de Herkenningsmakelaar (Proces instandhouding en naleven, Aansluiten als dienstverlener, Beleid voor informatiebeveiliging), meer specifiek de volgende normen uit de ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC):
    a. De Dienstverlener voert beheerst wijzigingen door op de relevante systemen en wijzigingen worden steeds getest voordat deze in productie worden genomen (B0-5).
    b. De Dienstverlener draagt zorg voor hardening van alle relevante ICT-componenten tegen aanvallen en beschikt hiervoor over een security baseline voor de relevante systemen (B0-6).
    c. De Dienstverlener heeft een patchmanagementproces ingericht zodat steeds de laatste (beveiligings-)patches zijn geïnstalleerd (B0-7).
    d. De Dienstverlener beheerst de toegangsbeveiliging / toegangsbeheer van de relevante systemen (B0-12).
    e. De Dienstverlener draagt zorg voor het gebruik van veilige beheermechanismen zoals het gebruik van veilige netwerkprotocollen, beheerinterfaces die via het internet uitsluitend door middel van sterke authenticatie te benaderen zijn en het uitsluiten dat er gebruik wordt gemaakt van zogenaamde ‘backdoors’ om de systemen te benaderen (B2-1).
    f. De Dienstverlener draagt er zorg voor dat bij de ontwikkeling van web-applicaties gebruik wordt gemaakt van veilige ontwikkeltechnieken, zoals beschreven in de OWASP top 10 (samenvattend B3-1 t/m 7).
    g. De Dienstverlener heeft sleutelbeheer ingericht waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers zijn geplaatst en neemt maatregelen ter beveiliging van de privé sleutel (private key) (B5-1).
    h. De Dienstverlener draagt zorg voor versleuteling van sessie cookies (B5-4).
    i. De Dienstverlener voert actief controles uit op logging, gericht op de operatie en beveiliging van systemen (B7-8).
    j. De Dienstverlener draagt er zorg voor dat bij uitbesteding van activiteiten de relevante verplichtingen worden vastgelegd (in een overeenkomst) (B0-14).
3. De Dienstverlener beheerst de geheimhouding van vertrouwelijke stelsel gerelateerde informatie en de zorgvuldige omgang met persoonsgegevens van dienstafnemers (Aanvullende verplichtingen).
4. De Dienstverlener beheerst de juiste koppeling van een authenticatiemiddel van de dienstafnemer aan het account van die dienstafnemer bij de Dienstverlener (Aanvullende verplichtingen).
5. De Dienstverlener beheerst de risico’s van de online dienst die hij aansluit. De Dienstverlener heeft het betrouwbaarheidsniveau van de dienst vastgesteld op basis van de analyse van deze risico’s (Aanvullende verplichtingen).
6. Indien (bijzondere) persoonsgegevens worden verwerkt, verklaart de Dienstverlener hiertoe gerechtigd te zijn en bewerkersovereenkomsten afgesloten te hebben met relevante partijen.

Voorts aanvaardt ondergetekende dat de Herkenningsmakelaar gedurende de looptijd van de overeenkomst met de dienstverlener beoordeelt of de dienstverlener blijft voldoen aan de op hem rustende verplichtingen op grond van het afsprakenstelsel.

Indien de Herkenningsmakelaar hieromtrent twijfelt of van mening is dat dit niet langer het geval is, geeft hij dit terstond door aan de Toezichthouder. Indien de Toezichthouder oordeelt dat de Herkenningsmakelaar dient te handhaven, zal de Herkenningsmakelaar terstond zijn dienstverlening aan de Dienstverlener schorsen of beëindigen .

Datum:	
Plaats:	

Naam:	
Handtekening:	

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

Toelichting

In het Juridisch kader van het Afsprakenstelsel Elektronische toegangsdiensten (hierna: afsprakenstelsel) is het indirect toezicht opgenomen. Indirect toezicht houdt in dat de Toezichthouder er op toe ziet dat de Deelnemers van het afsprakenstelsel op afdoende wijze de naleving van de stelselvoorwaarden door hun Gebruikers van het afsprakenstelsel controleren.

Voor het indirecte toezicht op de Dienstverlener betekent dit concreet dat de Toezichthouder verantwoordelijk is voor de borging van de naleving van de verplichting van de Herkenningsmakelaar om:

1. de naleving van de dienstverleningsovereenkomst die de Herkenningsmakelaar met de Dienstverlener heeft te monitoren, inclusief de hierop van toepassing zijnde Gebruiksvoorwaarden Elektronische Toegangsdiensten, alsmede
2. te monitoren dat de dienstverlener blijvend voldoet aan de positieve testresultaten voor aansluiting .

Om ervoor te zorgen dat de Herkenningsmakelaar opvolging geeft aan de verplichting genoemd onder punt 1. is deze zelfverklaring opgesteld. Deze zelfverklaring is hiermee een nadere uitwerking van de wijze waarop binnen het afsprakenstelsel door de Herkenningsmakelaar invulling wordt gegeven aan het indirecte toezicht op de Dienstverlener ten aanzien van de naleving van de dienstverleningsovereenkomst die de Herkenningsmakelaar met de Dienstverlener heeft te monitoren, inclusief de hierop van toepassing zijnde Gebruiksvoorwaarden Elektronische Toegangsdiensten.

Gelet op het bovenstaande dient de Herkenningsmakelaar in het kader van het indirecte toezicht derhalve de volgende documenten aan de Toezichthouder te kunnen overleggen:

- een rechtsgeldig ondertekende Zelfverklaring door de Dienstverlener;
- een rechtsgeldig ondertekende dienstverleningsovereenkomst inclusief Gebruiksvoorwaarden Afsprakenstelsel Elektronische toegangsdiensten, en
- positieve testresultaten voor aansluiting .

Om deze documenten aan de Toezichthouder te kunnen overleggen dient de Dienstverlener in het kader van het indirecte toezicht bovengenoemde documenten aan de Herkenningsmakelaar te overleggen.

Hiermee is de zelfverklaring, in combinatie met de dienstverleningsovereenkomst, de Gebruiksvoorwaarden van het afsprakenstelsel en de testresultaten voor aansluiting, een middel om indirect toezicht te kunnen houden op de naleving van de afspraken van het afsprakenstelsel door de Dienstverlener.

De zelfverklaring wordt eenmalig ondertekend tenzij er sprake is van één van de situaties als genoemd in Indirect toezicht op de Dienstverlener.

snippets

veelgebruikte snippets voor het rebranden

Elektronische Toegangsdiensten

Netwerk

Afsprakenstelsel Elektronische Toegangsdiensten

Herkenningsdiensten

www.eherkenning.nl

Herkenningsmakelaar

Instellingsbesluit Elektronische Toegangsdiensten

Afsprakenstelsel Elektronische Toegangsdiensten

Afsprakenstelsel Elektronische Toegangsdiensten

Elektronische Toegangsdiensten

Elektronische Toegangsdiensten

footer







EHerkenning

EHerkenning

EHerkenning

EHerkenning	**Afsprakenstelsel eHerkenning** | Alle rechten voorbehouden	Paginanummer





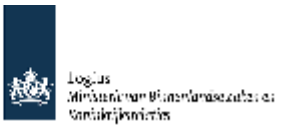
idensys

idensys


idensys


idensys

header



Herkenningsmakelaar

Herkenningsmakelaar

Netwerk

Netwerk

snippet.ad.mr.participants

We-ID | Reconi | Digidentity | KPN | QuoVadis | Zetsolutions

snippet.antwoord

Antwoord:

snippet.beperking.dienstbemiddeling

Note: At this moment the use of ASTA-sets and Service Intermediation is limited to the EB for eIDAS Outgoing.

snippet.betrouwbaarheidsniveaus

	eH2	eH2+	eH3	eH4
Herkenningsmakelaar	O			
Middelenuitgever	O	O	O	O
Authenticatiedienst	O	O	O	O
Machtigingenregister	O	O	O	O

snippet.bewaartermijnen

Bewaartermijnen:

- Alle benodigde gegevens t.b.v. identificatie bij uitgifte middel en/of registratie machtiging: 7 jaar (na verlopen/intrekking middel/machtiging) tbv fraudeonderzoek en beslechting van geschillen (N.B.: hierbij wordt geen onderscheid gemaakt in het niveau van het middel of machtiging, immers het doel is hetzelfde);
- Gegevens betreffende authenticatie: 7 jaar tbv fraudeonderzoek.

snippet.branding

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

* Citizen: r1.12 only EU-citizens via eIDAS BerichtenService

snippet.bsnk_specs



The most recent version of the technical BSNk specifications are available on https://wiki.bsn-koppelregister.nl/ or on request (beheerorganisatie BSNk through servicecentrum@logius.nl). The information below is for information only.

snippet.bzk

het ministerie van Binnenlandse Zaken

snippet.calamiteit

- Verwachte verstoringsduur > 4 uur binnen het Beschikbaarheidsvenster en/of;
- Betrokkenheid van tenminste twee deelnemers en/of;
- Directe en ernstige hinder en/of;
- Impact op vertrouwelijkheid en integriteit en/of;
- Meldplichtig datalek als bedoeld in de Meldplicht datalekken.

snippet.checklist

Test date:	_____ / _____ / _____
Build version:	_____
Tester:	_____
Signature:	

snippet.checklist.ad

AD - Keyname-Key Mismatch A
AD - Keyname-Key Mismatch B
AD - Wrong digest
AD - Missing fields
@ProviderName
@IssueInstant
@ID
@AssertionConsumerServiceIndex
@AttributeConsumingServiceIndex
- Issuer
- RequestedAuthnContext
- AuthnContextClassRef
AD - Empty fields
@ProviderName
@IssueInstant
@ID
@AssertionConsumerServiceIndex
@AttributeConsumingServiceIndex
- Issuer
@Comparison
- AuthnContextClassRef
AD - Random value swaps

snippet.checklist.hm

HM - Keyname-Key Mismatch A
HM - Keyname-Key Mismatch B
HM - Wrong digest
HM - Missing fields
@IssueInstant
@ID
@AssertionConsumerServiceIndex
@AttributeConsumingServiceIndex
@IsPassive
@ProtocolBinding
@Consent
- Issuer
- RequestedAuthnContext
- AuthnContextClassRef
HM - Empty fields
@IssueInstant
@ID
@AssertionConsumerServiceIndex
@AttributeConsumingServiceIndex
- Issuer
@Comparison
- AuthnContextClassRef

snippet.checklist.mr

MR - Keyname-Key Mismatch A
MR - Keyname-Key Mismatch B
MR - Wrong digest
MR - Missing fields
@IssueInstant
@ID
– Issuer
– Extensions
– xacml-context:Attribute (1)
– xacml-context:AttributeValue
– xacml-context:Request
– xacml-context:Subject
– xacml-context:Attribute (2)
– xacml-context:AttributeValue
– xacml-context:Resource
– xacml-context:Attribute (3)
– xacml-context:AttributeValue
– xacml-context:Attribute (4)
– xacml-context:AttributeValue
– xacml-context:Action
– xacml-context:Attribute
– xacml-context:AttributeValue
– xacml-context:Environment
MR - Empty fields
@IssueInstant
@ID
– Issuer
– Extensions
– xacml-context:Attribute (1)
– xacml-context:AttributeValue
– xacml-context:Request
– xacml-context:Subject
– xacml-context:Attribute (2)
– xacml-context:AttributeValue
– xacml-context:Resource
– xacml-context:Attribute (3)
– xacml-context:AttributeValue
– xacml-context:Attribute (4)
– xacml-context:AttributeValue

– xacml-context:Action
– xacml-context:Attribute
– xacml-context:AttributeValue
– xacml-context:Environment
MR - Random value swaps

snippet.colofon

Afsprakenstelsel			Document	
Versie	1.13 20 oktober 2022		Auteur	Beheerorganisatie
Datum vaststelling	20-okt-2022		Classificatie	Openbaar
Datum publicatie	7-dec-2022		Status	Definitief

snippet.colofon.gebruikersvoorwaarden

Gebruikersvoorwaarden				
Versie	G1.7		Geldig vanaf versie van het AS	1.13p

snippet.determine.appropriate.identifiers

Determine appropriate.Identities for (ECTA- or ASTA-) Sets for Recepient (DV of DA)

DetermineAppropriateIdentifiers (sets, Recipient.ServiceProviderID)

- GROUP ecta/acta-sets BY setNumber in sets
- ORDER sets ASSENDING BY setNumer
- FOR EACH set IN sets
    - # check IF all IdentityTypes in set can and may be provided for het user
    - FOR EACH IdentifierType IN set
        - IF IdentifierType=BSN AND Recipient.ServiceProviderID NOT on the BSN AutorisationList THEN respond with a unrecoverable error (Attributes not supported). See Error handling for more details.
        - IF IdentifierType can not be provided for this user THEN next set
    - # all IdentifierTypes are checked, current Set = *appropriate* set
    - # Add the Identifiers of the user for all IdentifierTypes (Identificerende kenmerken) in the *appropriate set to appropriate.Identities*
    - FOR EACH IdentifierType IN set
        - appropriate.Identities[IdentifierType] = IdentifierValue of IdentifierType for the user and Receipient combination
    - RETURN appropriate.Identities
- # No appropriate Set can be provides for this user - start error handling
- respond with a recoverable error (Attributes not supported). See Error handling for more details.

snippet.diensten

Herkenningsdiensten

snippet.doelomschrijving

De rechtmatigheidsgrondslag is de toestemming van de betrokkene zoals bepaald door de AVG.

snippet.duur.publicatie

De vergaderstukken van het beraad worden (krachtens art. 9 van het Instellingsbesluit) gepubliceerd op de website van eHerkenning (www.eherkenning.nl) gedurende een periode van 1 jaar. De stukken zijn daarna op te vragen bij de secretaris van het betreffende beraad. De leden worden hierover geïnformeerd.

snippet.ecta

An SP may request multiple EntityConcernedTypes in an identifier set. The SP may also indicate to honor restrictions. When an Attribute with a ServiceRestriction is included in the AttributeStatement, users can access the service under the restrictions as specified for that type of restriction. Currently, the only restrictions supported are ServiceRestriction:Vestigingsnr and ServiceRestriction:SubdossierNr (deprecated). The ServiceRestriction:Vestigingsnr CAN be indicated in the Service catalog, in such case both the ServiceRestriction:Vestigingsnr and ServiceRestriction:SubdossierNr will be returned, if applicable.

snippet.email.bo

info@eherkenning.nl

snippet.gebruikservaring.attributen

De gebruiker kan bevraagd worden over de te leveren attributen, bijvoorbeeld voor het geven van toestemming of het verstrekken van een attribuut dat nog niet eerder was vastgelegd. Dit heeft gevolgen voor de gebruikerservaring en de doorlooptijd van het authenticatieverzoek. Partijen dienen hier rekening mee te houden.

snippet.handreikingloa

De Handreiking Betrouwbaarheidsniveaus van Forum Standaardisatie geeft richting aan Dienstverleners die op het Stelsel willen aansluiten bij het bepalen van het juiste LoA niveau van hun dienst.

snippet.hm.participants

Signicat | Reconi | Digidentity | iWelcome | KPN

snippet.implementatietermijn.RFC2040.1

Het Tactisch Beraad heeft 22 juni 2016 besloten de implementatietermijn te bepalen wanneer er duidelijkheid is over de wet GDI, waarin ook de businesscase voor de toepassing van de eIDAS betrouwbaarheidsniveaus in overweging wordt genomen.

De uiterlijke implementatiedatum van de RFC 2040 is gekoppeld aan de publicatie van de wet GDI, verwacht per 31 december 2017.

snippet.implementatietermijn.RFC2040.2

Voor de toegevoegde eis 3.2.1 LoA 4 punt 5 geldt een specifieke overweging:

1. Implementatiedatum voor nieuwe middelen: 31 december 2018
2. Implementatiedatum voor bestaande middelen: 31 december 2019
3. Periodieke evaluatie implementatiedata: Het security officers overleg evalueert elke 6 maanden de noodzaak tot aanpassing van de implementatiedata en adviseert na consultatie van de governance om de implementatie termijn te vervroegen, te verlaten of te handhaven. De evaluatie gebeurt aan de hand van de context van Europese ontwikkelingen), NL ontwikkelingen en ontwikkeling van het risico dat de kwetsbaarheid (ontbreken van een trusted channel) wordt misbruikt.

snippet.instellingsbesluit

Instellingsbesluit Elektronische Toegangsdiensten

snippet.Interface specification HM-MR response

Response (2)

@ID	SAML: Unique message attribute
@InResponseTo	SAML: Unique attribute of the XACMLAuthzDecisionQuery to which this response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the HM on which the message is offered. MUST match the SAML metadata.
@Consent	Elektronische Toegangsdiensten: MUST NOT be included
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the MR. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the MR for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included
Status	Elektronische Toegangsdiensten: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	Elektronische Toegangsdiensten: MUST contain an assertion about the authorization (see the next section).

Rules for processing responses

A receiving HM:

- MUST verify the structure and contents of the response.

A responding MR MUST:

- The MR MUST communicate the Level of Assurance of the registered authorization. A MR MUST NOT communicate a level for which it is not certified.
    - In case of a chain of authorizations, the MR MUST communicatie the minimum of the LoA of all Representation authorizations in the applicable chain (so far).
    - In case of a request for a portal service, a MR MUST communicate the Level of Assurance as the minimum Level of Assurance of all applicable service authorizations chosen by the user.

Authorization assertion

Assertion	**@Version**	SAML: Version of the SAML protocol. The value MUST be '2.0'.
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the MR. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
	Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the MR for the enveloped assertion.
	Subject	Elektronische Toegangsdiensten: MUST contain a different transient <NameID> from the AD Assertion as received in the Request or preceding MR assertion in case of chain authorization. Each assertion MUST contain a new transient identifier, that is unique for the issuer during at least the past 12 months.
	Conditions	Elektronische Toegangsdiensten: MAY be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver. Other conditions MUST NOT be included.
	Advice	Elektronische Toegangsdiensten: MUST be included, containing an AssertionIDRef referencing the Assertion this declaration is directly linked to.

	XACMLAuthz-Decision Statement	Elektronische Toegangsdiensten: MUST contain an SAML Statement of the type XACMLAuthzDecisionStatementType. See below.

XACMLAuthzDecision Statement	**Response**	**Result**	**@ResourceID**	Elektronische Toegangsdiensten: MUST NOT be included
			Decision	XACML: One of the values allowed in XACML 2.0. In the event of a cancellation or error, the element MUST be populated with the value 'Deny'. See also Error handling.
			Status	XACML: must be filled with one of the values that are allowed according to the XACML 2.0 specifications
			Obligations	Obligation urn:etoegang:core:RequireConfirmationFromNextMR FulfillOn=Permit AttributeAssignment urn:etoegang:core:AuthorizationRegistryID = <MR2> (see EntityID) Elektronische Toegangsdiensten: In the event of chain authorization, such is established by the first MR, which then specifies, by means of an Obligation, that the second link MUST be verified or Decision = 'Permit' is otherwise invalid.
	Request		**Subject**	Elektronische Toegangsdiensten: Any received AuthenticationMeansID MUST be deleted and not returned in the response to the HM. If the Decision is 'Permit' THEN Depending on the Rules for processing request: • an ActingEntityID • an ActingSubjectID.EncryptedID@SP • one LegalSubjectID with one or more AttributeValues with an EncryptedID@SP • a LinkedDeclarationSignatureValue

			Resource	Elektronische Toegangsdiensten: MUST contain the attribute-elements contained in the resource element from the request.
				
				If the Decision is 'Permit'
				
				• ServiceID MUST be included as multi-valued XACML attribute
				• ServiceUUID MUST be included as multi-valued XACML attribute
				• LevelOfAssuranceUsed MUST be included. See Level of assurance
				• Depending on the Rules for processing request:
				  • an EntityConcernedID
				  • one or more ServiceRestrictions
				  • an IntermediateEntityID.EncryptedID
				  • one or more Encrypted Attributes
				
				NextAuthorizationRegistryID MAY be included. See EntityID.
				
				Other attributes MUST NOT be included.

			Action	Elektronische Toegangsdiensten: MUST be the same as the Action element in the request. See XACMLAuthzDecisionQuery (above).
			Environment	Elektronische Toegangsdiensten: MUST be empty.

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID=" " InResponseTo=" " Version="2.0"
IssueInstant=" " Destination=" ">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> </saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI=" ">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue> </ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
```

```
        <ds:SignatureValue> </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName> </ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"> </samlp:StatusCode>
    </samlp:Status>
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID=" " IssueInstant=" ">
        <saml:Issuer> </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                <ds:Reference URI=" ">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                    <ds:DigestValue> </ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue> </ds:SignatureValue>
            <ds:KeyInfo>
                <ds:KeyName> </ds:KeyName>
            </ds:KeyInfo>
        </ds:Signature>
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"> </saml:NameID>
        </saml:Subject>
        <saml:Conditions NotBefore=" " NotOnOrAfter=" "> </saml:Conditions>
        <saml:Statement xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os" xmlns:xsi="http://www.
w3.org/2001/XMLSchema-instance" xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
            <xacml-context:Response xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <xacml-context:Result>
                    <xacml-context:Decision>Permit</xacml-context:Decision>
                    <xacml-context:Status>
                        <xacml-context:StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"> </xacml-
context:StatusCode>
                    </xacml-context:Status>
                </xacml-context:Result>
            </xacml-context:Response>
            <xacml-context:Request xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <xacml-context:Subject>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ActingEntityID" DataType="
http://www.w3.org/2001/XMLSchema#string" Issuer=" ">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Subject>
                <xacml-context:Resource>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceID" DataType="http://www.w3.
org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:ServiceUUID" DataType="http://www.
w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:LevelOfAssurance" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:core:LevelOfAssuranceUsed" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                    <xacml-context:Attribute AttributeId="urn:etoegang:1.9:EntityConcernedID:KvKnr" DataType="
http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue> </xacml-context:AttributeValue>
                    </xacml-context:Attribute>
```

```
                    <xacml-context:ResourceContent>
                        <saml:EncryptedAttribute>
                            <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" Id="
_DE46C6F5E2E3111255D3A715C4760656">
                                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                    <xenc:EncryptedKey>
                                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-
oaep-mgf1p"/>
                                        <ds:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                                            <ds:KeyName>62355fbd1f624503c5c9677402ecca00ef1f6277</ds:KeyName>
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>.....</xenc:CipherValue>
                                        </xenc:CipherData>
                                    </xenc:EncryptedKey>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>.......</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                        </saml:EncryptedAttribute>
                    </xacml-context:ResourceContent>
                </xacml-context:Resource>
                <xacml-context:Action>
                    <xacml-context:Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                        <xacml-context:AttributeValue>Authenticate</xacml-context:AttributeValue>
                    </xacml-context:Attribute>
                </xacml-context:Action>
                <xacml-context:Environment> </xacml-context:Environment>
            </xacml-context:Request>
        </saml:Statement>
    </saml:Assertion>
</samlp:Response>
```

snippet.Interface specifications DV-HM response

For chain authorizations (Vervallen_Interface specifications HM-MR chain authorization), the identification number of the represented service consumer are included in the assertion for the HM in the same way as for single authorizations. The additional information about the chain is stored in a separate attribute.

Note: The HM will not identify the MRs from which the underlying assertions originate. Additional attributes relate to the represented service consumer or the user. There is no mechanism to include an additional attribute that relates specifically to an intermediary.

Element/@Attribute	0..n	Description
@ID	1	SAML: Unique message characteristic. MUST identify the message uniquely within the scope of the sender and receiver for a period of at least 12 months.
@InResponseTo	1	SAML: Unique attribute of the AuthnRequest for which this Response message is the answer.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the Response.
@Destination	1	SAML: URL of the endpoint of the DV on which the message is offered. MUST match the DV's metadata.
@Consent	0..1	Elektronische Toegangsdiensten: MAY be included. When Consent is included, the default value MUST contain urn: oasis:names:tc:SAML:2.0:consent:unspecified.
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM.
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	0..1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloping message. When communicated within a ArtifactResolveResponse the signature on the SAML:Response MAY be omitted, since the parent message already guarantees the integrity.
Extensions	0	Elektronische Toegangsdiensten: MUST NOT be included.
Status	1	Elektronische Toegangsdiensten: MUST contain a StatusCode element with the status of the authentication. See Error handling.
StatusCode	1	SAML: MUST be present in a Status element.
@Value	1	If not 'success' additional information should be provided. (conform Elektronische Toegangsdiensten specifications).
StatusCode	0..1	Only present if top-level StatusCode is not 'success'.
@Value	1	In the event of a cancellation or error, the element MUST be populated with the value AuthnFailed. See Error handling.
StatusMessage	0..1	Only present if top-level StatusCode is not 'success'.
StatusDetail	0	Elektronische Toegangsdiensten: MUST NOT be included.
Assertion	0..1	Elektronische Toegangsdiensten: MUST contain the <Assertion> that is delivered in the response, if the request was processed successfully. See below.
EncryptedAssertion	0	Elektronische Toegangsdiensten: MUST NOT be included.

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    ID="_5e702d5c-de06-11e4-a5a1-080027a35b78"
    InResponseTo="6984066c-de03-11e4-a571-080027a35b78"
    Version="2.0"
    Destination="https://..."
    IssueInstant="2015-04-08T16:30:06Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_5e702d5c-de06-11e4-a5a1-080027a35b78">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion Version="2.0"
        ID="_535162e2-de06-11e4-98a2-080027a35b78"
        IssueInstant="2015-04-08T16:30:05Z">
        <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
        ...
    </saml:Assertion>
</samlp:Response>
```

HM Summary assertion

This paragraph describes a HM summary <Assertion>

Element/@Attribute	0..1	Description
@ID	1	SAML: MUST identify the <Assertion> uniquely within the scope of the Issuer for a period of at least 12 months.
@Version	1	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	1	SAML: Time of issuing of the assertion.
Issuer	1	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM
@NameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPNameQualifier	0	Elektronische Toegangsdiensten: MUST NOT be included.
@Format	0	Elektronische Toegangsdiensten: MUST NOT be included.
@SPProvidedID	0	Elektronische Toegangsdiensten: MUST NOT be included.
Signature	1	Elektronische Toegangsdiensten: MUST contain the Digital signature of the Issuer (HM) for the enveloping Assertion.
Subject	1	Elektronische Toegangsdiensten: MUST be included.
BaseID	0	Elektronische Toegangsdiensten: MUST NOT be included.
NameID	0..1	Rules for processing request requires NameID to contain a TransientID or an ActingEntityID (DV connects to r1.09 or older, for older specifications see https://afsprakenstelsel.etoegang.nl/display/archief/Archief).
EncryptedID	0..1	Elektronische Toegangsdiensten: MUST NOT be included.

SubjectConfirmation	1...2	SAML: Contains the SubjectConfirmation conform the WebSSO profile. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.
Conditions	1	Elektronische Toegangsdiensten: MUST be included.
@NotBefore	1	Elektronische Toegangsdiensten: MUST be included.
@NotOnOrAfter	0..1	Elektronische Toegangsdiensten: MAY be included.
Condition	0	Elektronische Toegangsdiensten: MUST NOT be used.
AudienceRestriction	1	SAML: MUST be included.
Audience	1	Elektronische Toegangsdiensten: Contains the EntityID(s) for all relevant parties that are intended to receive and process this assertion, as per SAML WebSSO profile. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV:<*OIN*>' is to be used.
ProxyRestriction	0	Elektronische Toegangsdiensten: MUST NOT be included.
Advice	0..1	Elektronische Toegangsdiensten: SHOULD be included. See below under processing rules.
AssertionIDRef	0	Elektronische Toegangsdiensten: MUST NOT be included.
AssertionURIRef	0	Elektronische Toegangsdiensten: MUST NOT be included.
Assertion	1	Elektronische Toegangsdiensten: Contains the original <Assertion> elements this assertion is composed of.
EncryptedAssertion	0	Elektronische Toegangsdiensten: MUST NOT be included.
AuthnStatement	1	Elektronische Toegangsdiensten: MUST be included. The AuthenticatingAuthority element MUST be populated with the EntityID of the AD that performed the authentication.
@AuthnInstant	1	Elektronische Toegangsdiensten: MUST contain the time of authentication.
@SessionIndex	0..1	Elektronische Toegangsdiensten: MAY be included.
AuthnContext	1	Elektronische Toegangsdiensten: MUST be included.
AuthnContextClassRef	1	Elektronische Toegangsdiensten: MUST be included. Contains either the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified' (default) or the obtained effective Level of assurance, see below under "rules for processing responses".
AttributeStatement	1	Elektronische Toegangsdiensten: MUST contain an <AttributeStatement> in accordance with the following section and the rules for processing responses.

Example HM Assertion

```
<saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_535162e2-de06-11e4-98a2-080027a35b78">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
```

```
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78" Version="
2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for minimal DV request

```
 <saml:Assertion Version="2.0"
    ID="_535162e2-de06-11e4-98a2-080027a35b78"
    IssueInstant="2015-04-08T16:30:05Z">
    <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        ...
    </ds:Signature>
    <saml:Subject>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:Advice>
        <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78" Version="
2.0">
            <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
    </saml:Advice>
    <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        ...
    </saml:AttributeStatement>
</saml:Assertion>
```

Example HM Assertion for Representation

```
Vraag het op bij de BO / Ask BO
```

Example HM Assertion for citizen domain

```
<saml:Assertion Version="2.0"
   ID="_535162e2-de06-11e4-98a2-080027a35b78"
   IssueInstant="2015-04-08T16:30:05Z">
   <saml:Issuer>urn:etoegang:HM:...</saml:Issuer>
   <ds:Signature>
       ...
   </ds:Signature>
   <saml:Subject>
       <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
           <saml:SubjectConfirmationData Recipient="https://..." NotOnOrAfter="2015-04-08T16:40:03Z"
InResponseTo="_6984066c-de03-11e4-a571-080027a35b78"/>
       </saml:SubjectConfirmation>
   </saml:Subject>
   <saml:Conditions NotBefore="2015-04-08T16:29:04Z" NotOnOrAfter="2015-04-08T17:00:04Z">
       <saml:AudienceRestriction>
           <saml:Audience>urn:etoegang:DV:...</saml:Audience>
       </saml:AudienceRestriction>
   </saml:Conditions>
   <saml:Advice>
       <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78" Version="
2.0">
           <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
           <!-- Verbatim copy of AD declaration of identity contents -->
       </saml:Assertion>
       <saml:Assertion IssueInstant="2015-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78" Version="
2.0">
           <saml:Issuer>urn:etoegang:KR:...</saml:Issuer>
           <!-- Verbatim copy of KR declaration of sectoral identity contents -->
       </saml:Assertion>
   </saml:Advice>
   <saml:AuthnStatement AuthnInstant="2015-04-08T16:30:04Z">
       <saml:AuthnContext>
           <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
       </saml:AuthnContext>
   </saml:AuthnStatement>
   <saml:AttributeStatement>
       ...
   </saml:AttributeStatement>
</saml:Assertion>
```

Example - HM Assertion - eIDAS-OUT withService Intermediation

```
<saml2:Assertion ID="_67d2200a8bd8401dc1b7274106731ca6" IssueInstant="2019-02-26T10:35:43.000Z" Version="2.0"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:HM:00000003271247010000:
entities:7611</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_67d2200a8bd8401dc1b7274106731ca6">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
                <ds:DigestValue/>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue/>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:KeyName>f04a58c387f4f8b5f1fa3a614f79f073f3f08953</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" xmlns:saml="urn:oasis:names:
tc:SAML:2.0:assertion">ed3d5655-b6ee-47bf-87d5-fb77302e14b4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" xmlns:saml="urn:oasis:names:tc:
SAML:2.0:assertion">
            <saml:SubjectConfirmationData InResponseTo="_d3fda417414c17b2667995961cf79fc5" NotOnOrAfter="2019-
02-26T10:37:39Z" Recipient="https://brk.eid-tst.ad.nl/brk/HM1CServiceProvider" xmlns:saml="urn:oasis:names:tc:
SAML:2.0:assertion"/>
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml2:Conditions NotBefore="2019-02-26T10:35:43Z" NotOnOrAfter="2019-02-26T10:37:43Z" xmlns:saml2="urn:
oasis:names:tc:SAML:2.0:assertion">
        <saml2:AudienceRestriction>
            <saml2:Audience>urn:etoegang:DV:00000001111111110000:entities:9113</saml2:Audience>
            <saml2:Audience>urn:etoegang:DV:00000002222222220000:entities:9613</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml:AuthnStatement AuthnInstant="2019-04-08T16:30:07Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml2:Advice>
        <saml:Assertion IssueInstant="2019-04-08T16:30:04Z" ID="_8a792d9e-de07-11e4-9db2-080027a35b78" Version="
2.0">
            <saml:Issuer> urn:etoegang:AD:0000000444444444445001:entities:9042</saml:Issuer>
            <!-- Verbatim copy of AD declaration of identity contents -->
        </saml:Assertion>
        <saml:Assertion IssueInstant="2019-04-08T16:30:07Z" ID="dd4dae83-0f35-4695-b24a-29d470a63ea7" Version="
2.0">
            <saml:Issuer> urn:etoegang:MR:0000000555555555001:entities:9042</saml:Issuer>
            <!-- Verbatim copy of MR declaration of identity contents -->
        </saml:Assertion>
    </saml2:Advice>
    <saml2:AuthnStatement AuthnInstant="2019-02-26T10:35:43Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:
assertion">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml2:AuthnContextClassRef>
            <saml2:AuthenticatingAuthority>urn:etoegang:AD:0000000444444444445001:entities:9042</saml2:
AuthenticatingAuthority>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        . . . . .
    </saml2:AttributeStatement>
</saml2:Assertion>
```

Example HM assertion - Attribute Statement - eIDAS-OUT using Service Intermediation

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"
>dafca82e-4806-408e-956e-3a7092643e54</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute Name="urn:etoegang:core:ServiceID">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">urn:
etoegang:DV:00000001111111110000:services:8002</saml2:AttributeValue>
    </saml2:Attribute>
    <saml:Attribute Name="urn:etoegang:core:Representation" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsi="http://www.w3.org
/2001/XMLSchema-instance" xsi:type="xs:boolean">true</saml:AttributeValue>
```

```
    </saml:Attribute>
    <!-- igv de service via de Service Catalog vraagt om een ServiceRestriction en de MR-->
    <!-- heeft een service restriction bij de machtiging. Vb restrictie op KvK Vestigingsnr-->
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ActingSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:AttributeValue>
            <!-- # ActingSubjectID - BSN:VP@RVO (PseudoID voor de EB) -->
            <saml:EncrypedID>
                <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04
/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="
#_15531f42aa31bbd4" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>...</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:
00000001111111110000:entities:9613">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
        <saml:AttributeValue>
            <!-- # ActingSubjectID - BSN:VI@RVIG (BSN voor BRP-Attributendienst)-->
            <saml:EncrypedID>
                <xenc:EncryptedData Id="_ed3457856888ad576a0aa751725ce76a6b866" Type="http://www.w3.org/2001/04
/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo>
                        <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"URI="
#_4567788aa31bbd4" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>...</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4" Recipient="urn:etoegang:DV:
00000002222222220000">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo>
                        <ds:KeyName>...</ds:KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>UtEw923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:LegalSubjectID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
        <saml:AttributeValue>
            <!-- # LegalSubjectID - KvK voor de EB)-->
            <saml:EncryptedID>
                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_6bc1c98ef545444da370efd74371ff6f" Type="http://www.w3.org/2001/04/xmlenc#Element">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:RetrievalMethod URI="#_105e787ebce14ea2b6655adb4d736b86" Type="http://www.w3.org
/2001/04/xmlenc#EncryptedKey" />
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>lx922tGEfI9T7WgoduHAZ941XA....</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_105e787ebce14ea2b6655adb4d736b86" Recipient="urn:etoegang:DV:00000001111111110000:entities:9613">
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.
org/2000/09/xmldsig#sha1" />
                    </xenc:EncryptionMethod>
                    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:KeyName>022A8DEA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:
KeyName>
                    </ds:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>gNDIheioi3mgjeyCTviEXDui3.....</xenc:CipherValue>
                    </xenc:CipherData>
                    <xenc:ReferenceList>
                        <xenc:DataReference URI="#_6bc1c98ef545444da370efd74371ff6f" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncryptedID>
        </saml:AttributeValue>
        <! # LegalSubjectID - Geen KvK voor de dienstaanbieder.>
    </saml:Attribute>
    <!-- # CompanyName werkgever voor de EB.-->
    <saml:EncryptedAttribute>
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_67947663adfasdf9410780097b9bf2f04fa8" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000
/09/xmldsig#sha1" />
            </xenc:EncryptionMethod>
            <ds:KeyInfo>
                <ds:KeyName>57890EA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>WYuIOsaf1aNbZdRQPXepQjlw4Tg...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
    <!-- # Optionele Bedrijfs attributen (CompanyName) voor de EB.-->
    <saml:EncryptedAttribute>
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_6974a3dsdf9410780097b9bf2f04fa8" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                <ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/2000
/09/xmldsig#sha1" />
            </xenc:EncryptionMethod>
            <!-- # EB should recognise KeyName.-->
            <ds:KeyInfo>
                <ds:KeyName>57890EA6C6F6CFA466BF18AF714F4CD0611DF3A4CAF23CF67B8BB8F7FC07CAF</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>WYuIOsaf1aNbZdRQPXepQjlw4Tg...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
</saml2:AttributeStatement>
```

AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

Element/@Attribute	0..1	Description
Attribute	0..n	Elektronische Toegangsdiensten: Depending on Rules for processing request: • one or more ActingSubjectID's • one or more LegalSubjectID • one or more EntityConcernedID • ServiceID as multi-valued XACML attribute • exactely one IntermediateEntityID, the identity of Intermediate • one or more ServiceRestrictions, eg ServiceRestriction:Vestigingsnr In case of Ketenmachtiging, MUST contain the attribute IntermediateEntityID.
EncryptedAttribute	0..n	Depending on Rules for processing request • one or more EncryptedAttributes requested by the DV and provided by the AD and/or MR

Example HM AttributeStatement for citizen domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">1ff84f14-df64-11e4-ba1a-080027a35b78</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:AuthorizationRegistryID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:AD:...</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for consumer domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">0013c492-84cd-4c4b-8206-b13007ac2a1c</saml:AttributeValue>
    </saml:Attribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_FirstName" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
            <ds:KeyInfo>
                <ds:Keyname>...</ds:Keyname>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
    <saml:EncryptedAttribute>
        <xenc:EncryptedData Id="_copy_Encrypted_18OrOlder" Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
            <ds:KeyInfo>
                <ds:Keyname>...</ds:Keyname>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>...</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </saml:EncryptedAttribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Example HM AttributeStatement for business domain with multiple entityconcernedtypes

```
<saml:AttributeStatement>
    <saml:Attribute Name="urn:etoegang:core:ServiceID">
        <saml:AttributeValue xsi:type="xs:string">urn:etoegang:DV:...:services:...</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
        <saml:AttributeValue xsi:type="xs:string">dd4dae83-0f35-4695-b24a-29d470a63ea7</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:KvKnr">
        <saml:AttributeValue xsi:type="xs:string">12345678</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:EntityConcernedID:RSIN">
        <saml:AttributeValue xsi:type="xs:string">987654321</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:etoegang:1.9:ServiceRestriction:Vestigingsnr">
        <saml:AttributeValue xsi:type="xs:string">123456789012</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

Rules for processing responses

On a successful authentication the HM MUST generate a 'Summary Assertion' based on the Assertions gathered during the authentication process, using the following processing rules.

- MUST sign the enclosed <Assertion> as well as the <Response> (and/or the enclosing <ArtifactResponse>).
- MUST verify each collected assertion has at minimum the Level of Assurance as requested by the DV. If verification fails, MUST handle the received responses as an unrecoverable error.
- MUST provide an <AuthnContextClassRef>:
    - By default fill the AuthnContextClassRef with the value 'urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified'.
    - When a DV explicitly requests a detailed LoA by including an AuthnContextClassRef in its AuthnRequest (see above): The HM MUST communicate the effective Level of Assurance of the combined assertions. The effective Level of assurance is the minimum of the LoA of the Authentication assertion and (if applicable) the LoA of the Representation authorization assertion(s).

      The MR communicates two Levels of Assurance in its Assertion. A LevelOfAssurance (requested) and a LevelOfAssuranceUsed (actually obtained). The HM MUST use the LevelOfAssuranceUsed from the MR Assertion as the LoA of the Representation authorization.

      .

- HM MUST provide an <Subject> with the following <NameID>
    - *IF* DV connects to r1.13 (or newer) AND non-represenation THEN copy AD-assertion: Subject.NameID.TransientID
    - *IF* DV connects to r1.13 (or newer) AND representation THEN copy MR-assertion: Subject.NameID.TransientID
    - *IF* DV connects to r1.11 (or older) *THEN* copy MR-assertion: XACMLAuthz-Decision.Subject.ActingEntityID
- HM MUST provide an <AttributeStatement> with the following <Attributes> and <EncryptedAttributes>
    - *IF* DV connects to r1.13 (or newer) *THEN*
        - *the HM must copy all relevant information (see Interface specifications DV-HM) from the below sources to the ActingSubjectID attribute:*
            - MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID (EncryptedID)

        - AD-assertion: Response.Assertion.AttributeStatement.ActingSubjectID.
        - copy all relevant AD-assertion: AttributeStatement.EncryptedAttribute
- IF Representation THEN
    - IF DV connects to r1.13 (or newer) THEN
        - copy all relevant EncryptedID from MR-Assertion: XACMLAuthz-Decision.Subject.LegalSubjectID to <LegalSubjectID>
        - copy all relevant EncryptedID from MR-Assertion: XACMLAuthz-Decision.Subject.ActingSubjectID to <ActingSubjectID>
        - copy all relevant MR-assertion: XACMLAuthz-Decision.Resource.EncryptedAttribute
    - *IF* DV connects to r1.11 (or older) *AND* Representation *THEN* copy MR-assertion: XACMLAuthz-Decision.Resource.EntityConcernedID
    - copy MR-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.ServiceID
    - *IF* available copy all MR-assertion: XACMLAuthz-Decision.Resource.ServiceRestrictions
    - *IF* Ketenmachtiging *THEN* copy MR2-Assertion: XACMLAuthz-Decision.Statement.Request.Resource.IntermediateEntityID

- MUST provide an <Advice>, by default filled with verbatim copy of all Assertions – so that original signatures over the assertions remains verifiable – gathered during the authentication process. HM MAY offer their DV to omit this information, if they archive this information and allow for later retrieval.

NOTE: When copying encrypted XML elements (<EncryptedID>, <EncryptedAttribute>) to create the summary declaration the HM MUST substitute used XML identifiers to point at the EncryptedTypes for a guaranteed unique identifier. This MAY be accomplished by pre- or suffixing the used identifier in the copy.

(Rationale: *@ID* values must uniquely identify the elements which bear them. Identifiers that appear once in the summary assertion and once in the advice assertion(s) will break schema validation of assertions).

All relevant

all <EncryptedID> or <EncryptedAttribute> elements except those encrypted for MR

A receiving DV:

- MUST verify the response matches with the Request responded to.
- MUST validate the signature on the Assertion as well as the Response (and/or the enclosing ArtifactResponse). Message (elements) MUST be signed using a certificate as listed in the SAML metadata of the HM for the purpose of signing for an IDPSSODescriptor of the responding HM. (NB this should correspond to the certificate as published in the network metadata).
- MUST be able to process DeprecatedActingSubjectID to facilitate migration or replacements of identifiers.
- SHOULD verify the structure and contents of the Response.
- SHOULD validate the signature and linking of the Evidence assertions.
- In case the receiving DV is a Dienstbemiddelaar, the Dienstbemiddelaar MUST provide a verbatim copy of the assertion – so that original signatures over the assertions remains verifiable – to the Dienstaanbieder (service supplier).
- IF the DV wants to decrypt urn:etoegang:1.12:EntityConcernedID:PseudoID or urn:etoegang:1.12:EntityConcernedID:BSN the DV must use preinstalled BSNk-keymaterial and software to obtain the actual identifier.
- IF the DV receives a pseudonym THEN the DV SHOULD create a mapping from the obtained Pseudonym to a user account, rather than using the obtained pseudoniem directly as unique key for an account.
- MUST decrypt an Encrypted Pseudonym or Encrypted Identity in the EncryptedID in the Attribute Statement of the Assertion using preinstalled keymaterial and software to obtain the actual identifier.
    - SHOULD create a mapping from the obtained identifier to a user account, rather than using the obtained identifier directly as unique key for an account. This so that a Persistent Pseudonym as well as deprecatedID can be in use at the same time to access an account during migrations.

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied, although considering that the logout message is sent to the AD via the HM. Only supported, is the DV's LogoutRequest where the user chooses to log out from the AD. The DV should never expect a LogoutRequest or a LogoutResponse. The interface for this message is described below.

@ID	SAML: Unique message characteristic
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time the message was created
@Destination	SAML: URL of the HM on which the message is offered.
NameID	Elektronische Toegangsdiensten: MUST contain a NameID element with the transient from the Subject of the concomitant AD assertion. This MUST NOT contain any identifier of the user.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the DV.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the DV for the envelopping message.

RequestKeyMaterial

The DV may request the HM for DV-specific key material which the DV can use to decrypt the EncryptedPseudonym into a DV-specific pseudonym or BSN, as per AUC9 Verstrekken sleutelmateriaal Dienstverleners. The HM can request the keys at the BSNk (see Interface specifications aux HM-BSNk - ProvideDVkeys).

A PKIo-certificate of the DV is required, the PKIo-certificate MUST have a (extended) key usage that allows for keyEncipherment. If the DV may request a BSN, the PKIo-certificate MUST have a Subject.serialNumber containing the organizations OIN.

ProvideKeyMaterial

The Herkenningsmakelaar MUST transfer the PKIo-encrypted key material to the DV unaltered. The HM will receive the DV-keys from the BSNk (see Interface specifications aux HM-BSNk - ProvideDVkeys).

The DV can decrypt the DV-keys using its private key corresponding with the PKIo-certificate used in the request.

snippet.interface specifications HM-AD

XML schema saml protocol extensions

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:etoegang:1.9:samlp-extension"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

    <xs:element name="RequestedAttributes">
          <xs:complexType>
               <xs:sequence>
                    <xs:element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
               </xs:sequence>
          </xs:complexType>
     </xs:element>

</xs:schema>
```

Example message

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:esp="urn:etoegang:1.9:samlp-extension"
    ID="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
    Destination="https://..."
    ForceAuthn="true"
    AssertionConsumerServiceIndex="1"
    AttributeConsumingServiceIndex="4"
    ProviderName="DV Name"
    IssueInstant="2015-04-10T12:30:03Z"
    Version="2.0">
    <saml:Issuer/>urn:etoegang:HM:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference URI="#_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Extensions>
                <saml:Attribute Name="urn:etoegang:core:IntendedAudience">
            <saml:AttributeValue>urn:etoegang:DV:...:entities:...</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceID">
            <saml:AttributeValue>urn:etoegang:DV:...:services:...</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:AttributeValue>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:AttributeValue>
        </saml:Attribute>
        <esp:RequestedAttributes>
```

```
            <md:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" IsRequired="false" />
        </esp:RequestedAttributes>
    </samlp:Extensions>
    <samlp:RequestedAuthnContext Comparison="minimum">
        <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa3</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Rules for processing requests

A requesting HM:

- MUST propagate @ProviderName of the party initiating the Request.

A receiving AD:

- MUST verify a requested service is defined in the Service Catalog and requested accordingly.
- MUST sanitize @ProviderName to remove any script or formatting before displaying.
- In case of Dienstbemiddeling (service intermediation), MUST verify the Dienstbemiddelaar (Service Intermediary) is still authorized by the Dienstaanbieder (Service Supplier) by verifying the authorization status of the mediated service in the Service Catalog.
- The AD MUST determine the branding to be used.
    - If IntendedAudience is eIDAS Berichtenservice, use eIDAS Outbound branding as described in Richtlijnen communicatie eIDAS.
    - Else, base the branding on the information elements listed in the table below.

Domain	LoA in request	EntityConcernedType in service catalog	Branding
Business	1, 2, 2+, 3, 4	urn:etoegang:1.9:EntityConcernedID:KvKnr urn:etoegang:1.9:EntityConcernedID:RSIN urn:etoegang:1.13:EntityConcernedID:PROBASnr urn:etoegang:1.11:EntityConcernedID:eIDASLegalIdentifier	eHerkenning
Business, Consumer	1, 2, 2+, 3, 4	urn:etoegang:1.12:EntityConcernedID:PseudoID urn:etoegang:1.9:EntityConcernedID:Pseudo	eHerkenning
Citizen*	3, 4	urn:etoegang:1.12:EntityConcernedID:BSN	eHerkenning

    * Citizen: r1.12 only EU-citizens via eIDAS BerichtenService
- The AD MUST process the ActingSubjectTypesAllowed list AND the EntityConcernedID:Pseudo.

If one of the criteria is not met, the AD MUST handle this as a non-recoverable error (see Error handling).

Note: When an AD specifies a MR for the HM to use as the next hop, the AD may only specify a MR of the same version.

Response (2)

@ID	SAML: Unique message characteristic.
@InResponseTo	SAML: Unique attribute of the AuthnRequest for which this response message is the answer.
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the HM on which the message is offered. MUST match the HM's metadata.
@Consent	Elektronische Toegangsdiensten: MUST NOT be included.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the AD. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the AD for the enveloped message.
Extensions	Elektronische Toegangsdiensten: MUST NOT be included
Status	Elektronische Toegangsdiensten: MUST be filled conform SAML 2.0 specs when the request is successfully processed. MUST be filled according to Error handling in case of an error or when the request was cancelled.
Assertion	Elektronische Toegangsdiensten: MUST contain an assertion about the authentication (see the next section).

Example AD Response

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    Destination="https://..."
    ID="_62619615-e452-47d3-a44b-93da2d5a76f9"
    InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_62619615-e452-47d3-a44b-93da2d5a76f9">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <samlp:Status>
      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de" IssueInstant="2015-04-10T11:16:28Z" Version="2.0"
>
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:etoegang:AD:...</saml:Issuer>
        ....
    </saml:Assertion>
</samlp:Response>
```

Note: the above example only provides the response. The response will be sent via an Artifact binding.

Authentication assertion

Assertion	**@Version**	SAML: Version of the SAML protocol. The value MUST be '2.0'
	@ID	SAML: Unique reference to the assertion
	@IssueInstant	SAML: Time at which the assertion was created
	Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the AD. The attributes NameQualifier, SPNameQualifier, Format and SPProvidedID MUST NOT be included.
	Signature	Elektronische Toegangsdiensten: MUST be included
	Subject	Elektronische Toegangsdiensten: MUST contain a <NameID> with a Transient ID. A SubjectConfirmation element that meets the Web Browser SSO profile MUST be included. Other SubjectConfirmation or SubjectConfirmationData elements MUST NOT be included.
	Conditions	Elektronische Toegangsdiensten: MUST be included. The attributes NotBefore and NotOnOrAfter MAY be included but should be ignored by the receiver.

		An Audience element in the AudienceRestriction element that meets the Web Browser SSO profile MUST be included. Other audience elements MUST include relevant parties: EntityIDs of the requesting DV and the MR/KR/HM (if applicable) to whom the assertion will be targeted. In case of Dienstbemiddeling (service intermediation), both the Dienstaanbieder (service supplier) and Dienstbemiddelaar (service intermediary) are a relevant party and must be listed as audience. For a Dienstaanbieder for whom only the OIN is known, the notation 'urn:etoegang:DV:*<OIN>*' is to be used. Note that for eIDAS Outbound, the eIDAS Berichtenservice has the role of Dienstverlener. So the notation of the EntityID is identical as for the DV (with ROLE "DV" and not "EB"). Other conditions MUST NOT be included.
	Advice	Elektronische Toegangsdiensten: MUST NOT be included
	AuthnStatement	Elektronische Toegangsdiensten: The attribute AuthnInstant MUST contain the time of authentication. The AuthnContext element MUST contain an AuthnContextClassRef element containing the level of assurance at which authentication took place and an AuthenticatingAuthority element containing the OIN format of the KvK number of the AD. In the case of proxying, AuthenticatingAuthority element MUST be populated with a unique identifying attribute for the party that carried out the authentication. Other attributes and elements MUST NOT be included.
	Optional Attribute-Statement	Elektronische Toegangsdiensten: MUST be included if StatusCode is 'Success'. MUST NOT be included otherwise. In case of representation: • ActingSubjectID (EncryptedID@MR) with the internal pseudonym of the acting user MUST be included. • IF an additional ActingSubjectID is requested by the EB in the servicecatalog, the ASTA will be Encrypted for the EB (as an EncryptedID@EB) and MUST contain all identifiers in ASTA-set as described in the service catalogue for the service. • If the ASTA-set can not be delivered by the AD, the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details.

AttributeStatement

The <AttributeStatement> in the summary assertion MUST hold the relevant attribute values obtained in the assertions of the authentication process. The HM MUST NOT add any attributes that are not present in the gathered assertion.

Element /@Attribute	0..1	Description

Attribute	0..n	Depending on Rules for processing request:
		
		• MUST include:
		  • ActingSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier of the acting (natural) person for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).
		  • LegalSubjectID – multi-valued containing one ore more SAML <EncryptedID> (see SAML encryption) as value, each containing an applicable identifier(s) of the ServiceConsumer for a specific Relying Party (eg DienstVerlener, DienstAanbieder, DienstBemiddelaar or MachtigingsRegister).
		  • ServiceID - multi-valued SAML-attribute
		  • ServiceUUID - multi-valued SAML attribute
		• MAY include:
		  • AuthorizationRegistryID (see EntityID).
		
		Other Attribute elements MUST NOT be included.

EncryptedAttribute	0..n	Depending on Rules for processing request • Additional attributes MAY be included here only IF the StatusCode is 'Success'. Other EncryptedAttribute elements MUST NOT be included.

Rules for processing response

A responding AD:

Identifiers:

- MUST include a transient identifier as a <NameID> in Subject; see Linking of Assertions.
- MUST encrypt any other identity according to the rules specified in SAML encryption and added as Attribute in the AttributeStatement.
- MUST ensure that a user consents to authentication for:
  - the ServiceProvider,

        - ServiceName
        - (optional/if applicable) "@ProviderName"
        - Personal attributes and/or BSN of the ActingPerson FOR the Intermediated Service and/or Intermediating Service

- MUST ensure only to provide a BSN to receipients on the BSN AutorisationList otherwise respond with a non-recoverable error. See Error handling for more details
- MUST determine appropriate identity(s) according to Determine appropriate ECTA and Identifiers:
- In case of no representation:
    - An AD MUST include all appropriate (ECTA) identifiers of the acting user for the DV in ActingSubjectID, as described in the service catalogue for the service
    - If an AD can not provide any of these requested ECTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Representation
    - An AD MUST include the internal pseudonym of the acting user for the MR in ActingSubjectID
    - If additional ASTA-identifiers are requested by the EB (in the ServiceCatalog) then an AD MUST include all appropriate ASTA-identifiers of the acting user for the DV* in ActingSubjectID, as described in the service catalogue for the service
        - ActingSubjectID MUST contain an EncryptedID encrypted only for the receiving DA/DB that requested the specific ASTA. The recipient of the ASTA for the DA and DB SHOULD be taken from the IntendedAudience element in the request.
            - In case of a DA for whom only the OIN is known, the notation 'urn:etoegang:DV:<*OIN*>' is to be used as recipient.
    - If an AD can not provide any of these requested ASTA-identifiers the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- In case of Service Intermediation
    - An AD MUST ensure ServiceProvider is authorised to use service intermediation as stated on the list AllowedForServiceIntermediation IF the AD does not want to use the service catalog to determine that the ServiceProvider is authorised to intermediate the intermediated service
    - If the AD does configure the AllowedForServiceIntermediation list locally, An the AD MUST use the ServiceCatalog to determine that the ensure ServiceProvider is authorised to intermediate the intermediated service as stated in the ServiceCatalog
    - An AD MUST add ASTA- and ECTA-identifiers for the intermediated service as stated in the ServiceCatalog using the same above processing rules as for the DV
- IF non-representation AND NOT service intermediation THEN MUST include the appropriate identity(s) of the user for the Dienstverlener (DV) as an <EncryptedID> in ActingSubjectID
- IF non-representation AND service intermediation THEN MUST include the appropriate identity(s) of the user for both Dienstverleners (DienstBemiddelaar (DB) and Dienstaanbieder (DA)) as an <EncryptedID> in ActingSubjectID

Reference implementation processing rules for Identities

- DV.ServiceProviderID = ServiceCatalog(request.ServiceUUID).ServiceProviderID
- DV.IntermediatedService = ServiceCatalog(request.ServiceUUID).IntermediatedService
- DV.ASTA-sets = ServiceCatalog(DV.ServiceUUID).ActingSubjectTypeAllowed
- DV.ECTA-sets = ServiceCatalog(DV.ServiceUUID).EntityConcernedTypeAllowed
- IF non-representation THEN
    - Determine approperiate.Identities (DV.ECTA-sets, DV.ServiceProviderID, DV.Type)
    - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- IF representation THEN
    - MUST include Internal pseudonym of the user for the appropriate MachtigingRegister as an EncryptedID@MR in ActingSubjectID
    - IF DV.ASTA-sets THEN
        - Determine appropriate.Identities (DV.ASTA-sets, DV.ServiceProviderID, DV.Type)
        - MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DV in ActingSubjectID
- **# ico Service Intermediation via service-catalog, DB authorization must be checked in service catalog**
- **IF DV.IntermediatedService AND DV.ServiceProviderID IS IN Config(AllowedForServiceIntermediation) THEN**
    - **DA.ServiceUUID = DV.IntermediatedService**
    - **DA.ServiceProviderID = ServiceCatalog(DA.ServiceUUID).ServiceProviderID**
    - **DA.@intermediationAllowed = ServiceCatalog(DA.ServiceUUID).@intermediationAllowed**
    - **DA.ServiceIntermediationAllowed = ServiceCatalog(DA.ServiceUUID).ServiceIntermediationAllowed**
    - **DA.ASTA-sets = ServiceCatalog(DA.ServiceUUID).ActingSubjectTypeAllowed**
    - **DA.ECTA-sets = ServiceCatalog(DA.ServiceUUID).EntityConcernedTypeAllowed**
    - **IF DA.@intermediationAllowed = “generalAvailable” OR (DA.@intermediationAllowed = “requiresApproval” AND DV.ServiceProviderID IS IN DA.ServiceIntermediationAllowed) THEN**
        - **IF non-representation THEN**
            - **Determine approperiate.Identities (DA.ECTA-sets, DA.ServiceProviderID)**
            - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**
        - **IF representation AND DA.ASTA-sets THEN**
            - **Determine appropriate.Identities (DA.ASTA-sets, DA.ServiceProviderID)**
                - **MUST include all appropriate.Identities (Type and Value) as an EncryptedID@DA in ActingSubjectID**

Determine appropriate.Identities for (ECTA- or ASTA-) Sets for Recepient (DV of DA)

DetermineAppropriateIdentifiers (sets, Recipient.ServiceProviderID)

- GROUP ecta/acta-sets BY setNumber in sets
- ORDER sets ASSENDING BY setNumer
- FOR EACH set IN sets
    - # check IF all IdentityTypes in set can and may be provided for het user
    - FOR EACH IdentifierType IN set
        - IF IdentifierType=BSN AND Recipient.ServiceProviderID NOT on the BSN AutorisationList THEN respond with a unrecoverable error (Attributes not supported). See Error handling for more details.

            - IF IdentifierType can not be provided for this user THEN next set
        - # all IdentifierTypes are checked, current Set = *appropriate* set
        - # Add the Identifiers of the user for all IdentifierTypes (Identificerende kenmerken) in the *appropriate set to appropriate.Identities*
        - FOR EACH IdentifierType IN set
            - appropriate.Identities[IdentifierType] = IdentifierValue of IdentifierType for the user and Receipient combination
        - RETURN appropriate.Identities
- # No appropriate Set can be provides for this user - start error handling
- respond with a recoverable error (Attributes not supported). See Error handling for more details.

Note: At this moment the use of ASTA-sets and Service Intermediarion is limited to the EB for eIDAS Outgoing.

Attributes:

- MUST include additional attributes as an AttributeStatement.EncryptedAttribute that are requested by the DV (Dienstaanbieder /DienstBemiddelaar) as specified in the Service catalog and consented by the user.
- IF required attributes cannot be provided (because of consent of not available) MUST act according to UC on not providing Attributes (see Attributen niet leverbaar of niet toegestaan) : stop the authentication flow and start error flow.
- MUST encrypt attributes according to the rules specified in 3. SAML encryption and added as an Encrypted Attribute in the AttributeStatement.
- MUST ensure user consent according to rules of the Attribute Policy (see Attributenbeleid)
- MUST ensure that only attributes are provided that are listed for the requested service in the service catalog
- If additional required atributes are requested by the DV (in the HM-request) then an AD MUST include these Attributes
- If an AD can not provide a requested required atttributes the AD MUST respond with a recoverable error (Attributes not supported). See Error handling for more details
- If additional optional atributes are requested by the DV (in the HM-request) then an AD SHOULD include these Attribute

Reference Implementation of Processing Rules for Attributes

- IF Request.RequestedAttributes THEN
    - FOR EACH attribute IN Request.RequestedAttributes
        - attribute.isRequired = **ServiceCatalog(DV.ServiceUUID).RequestedAttribute[attribute].isRequired**
        - IF attribute available AND user-consent THEN MUST
            - include attribute as EncryptedAttribute@DV with a unique Encrypted_DATA_ID that is the same as the attribute name in the attribute catalogue (e.g. urn:etoegang:1.9:attribute:FirstName).
        - ELSE IF attribute.isRequired THEN respond with a recoverable error). See Error handling for more details.

LevelOfAssurance:

- An AD MUST include the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied.
- MUST include the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied. An AD MUST NOT include a level for which it is not certified.

Determine appropriate ECTA and Identifiers:

- all the EntityConcernedTypes in an Identifier Set of EntityConcernedTypes with the same set number in the Service catalog.
- IF no set numbers are used, only one EntityConcernedType is allowed THEN handle this EntityConcernedType as if it was in 1 set.
- all the EntityConcernedTypes in the identifier set with the lowest possible set number the AD/MR can provide for this response. LegalSubject.
- IF AD/MR can't provide for any Identifier Set THEN start Error Handling
- Determine the response.EntityConcernedTypes and the corresponding response.LegalSubject.Identifiers for the selected identifier set.
- For ECTA=BSN the applicable service provider MUST be listed on the BSN Autorisation List OTHERWISE start Error Handling

Example attribute after decryption

```
<saml:Attribute Name="urn:etoegang:1.9:attribute:FirstName"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:attrext="urn:oasis:names:tc:SAML:attributes:ext"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
    attrext:OriginalIssuer="urn:etoegang:1.9:attribute-sourceid:NLWID"
    attrext:LastModified="2015-03-31T12:00:00Z">
    <saml:AttributeValue xsi:type="xs:string">...</saml:AttributeValue>
</saml:Attribute>
```

Example AD Assertion - representation

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:EncrypedID>
            <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                Type="http://www.w3.org/2001/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                        URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                Recipient="urn:etoegang:MR:...">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                </xenc:EncryptionMethod>
                <ds:KeyInfo>
                    <ds:KeyName>...</ds:KeyName>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                </xenc:CipherData>
                <xenc:ReferenceList>
                    <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                </xenc:ReferenceList>
            </xenc:EncryptedKey>
        </saml:EncrypedID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
```

```
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:MR:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>true</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:MR:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>...</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>yRy923JJlgAi2MTgx1qohLiDBgi...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>

 </saml:AttributeStatement>

</saml:Assertion>
```

Example AD Assertion - citizen domain

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
```

```
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-961e-
cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:KR:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:KR:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>...</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
```

```
                        <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                    </xenc:ReferenceList>
                </xenc:EncryptedKey>
            </saml:EncrypedID>
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

Example AD Assertion - consumer domain

```
<?xml version="1.0" encoding="UTF-8"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="_f0ba7712-50e4-4d30-8bb5-e63a771507de"
    IssueInstant="2015-04-10T11:16:28Z"
    Version="2.0">

    <saml:Issuer>urn:etoegang:AD:...</saml:Issuer>
    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_f0ba7712-50e4-4d30-8bb5-e63a771507de">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>...</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyName>...</ds:KeyName>
        </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">d6730e65-500a-44e2-961e-
cca53e7c60a4</saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData InResponseTo="_4b5af9ca-33ef-400f-9c97-398ab0c8e9c7"
                NotOnOrAfter="2015-04-10T11:18:28Z" Recipient="https://..." />
        </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2015-04-10T11:16:28Z" NotOnOrAfter="2015-04-10T11:18:28Z">
        <saml:AudienceRestriction>
            <saml:Audience>urn:etoegang:HM:...</saml:Audience>
            <saml:Audience>urn:etoegang:DV:...</saml:Audience>
        </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2015-04-10T11:16:28Z">
        <saml:AuthnContext>
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:loa4</saml:AuthnContextClassRef>
            <saml:AuthenticatingAuthority>...</saml:AuthenticatingAuthority>
        </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
        <saml:Attribute Name="urn:etoegang:core:Representation">
            <saml:AttributeValue>false</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ServiceUUID">
            <saml:Attribute>bf83ccef-6c9d-443f-ac11-9df0a0a9d299</saml:Attribute>
        </saml:Attribute>
        <saml:Attribute Name="urn:etoegang:core:ActingSubjectID">
            <saml:AttributeValue>
                <saml:EncrypedID>
```

```
                    <xenc:EncryptedData Id="_cd52e15a16e2a0aa751725ce76a6b866"
                        Type="http://www.w3.org/2001/04/xmlenc#Element">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"
                                URI="#_15531f77a9f1e0b5e0cce442aa31bbd4" />
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                    <xenc:EncryptedKey Id="_15531f77a9f1e0b5e0cce442aa31bbd4"
                        Recipient="urn:etoegang:DV:...">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                        </xenc:EncryptionMethod>
                        <ds:KeyInfo>
                            <ds:KeyName>...</ds:KeyName>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>...</xenc:CipherValue>
                        </xenc:CipherData>
                        <xenc:ReferenceList>
                            <xenc:DataReference URI="#_cd52e15a16e2a0aa751725ce76a6b866" />
                        </xenc:ReferenceList>
                    </xenc:EncryptedKey>
                </saml:EncrypedID>
            </saml:AttributeValue>
        </saml:Attribute>

        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_FirstName" Type="http://www.w3.org/2001
/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
                    ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>
        <saml:EncryptedAttribute>
            <xenc:EncryptedData Id="Encrypted_urn_etoegang_1.9_attribute_18OrOlder" Type="http://www.w3.org/2001
/04/xmlenc#Element">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
                <ds:KeyInfo>
                    <ds:Keyname>...</ds:Keyname>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>...</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
            <xenc:EncryptedKey>
                 ...
            </xenc:EncryptedKey>
        </saml:EncryptedAttribute>

    </saml:AttributeStatement>
</saml:Assertion>
```

LogoutRequest

For single logout, the Single Logout Profile that is part of the SAML 2.0 Web Browser SSO Profile is applied on the understanding that the logout message is sent to the AD through the HM. The interface for this message is described below.

@ID	SAML: Unique message attribute
@Version	SAML: Version of the SAML protocol. The value MUST be '2.0'.
@IssueInstant	SAML: Time at which the message was created.
@Destination	SAML: URL of the AD on which the message is offered.
NameID	Elektronische Toegangsdiensten: MUST contain a NameID element, this MUST NOT contain the Internal pseudonym or Specific pseudonym of the user.
Issuer	Elektronische Toegangsdiensten: MUST contain the EntityID of the HM.
Signature	Elektronische Toegangsdiensten: MUST contain the Digital signature of the HM for the enveloped message.

snippet.issues

Mantis

snippet.loa-rule.ad

The AD MUST communicate the Level of Assurance at which the authentication was realized. This realization is the minimum of the Level of Assurance of the registration process of the authenticated user and the Level of Assurance of the authentication mechanism applied. An AD MUST NOT communicate a level for which it is not certified.

snippet.loa-rule.hm

The HM MUST communicate the effective Level of Assurance of the combined assertions. The effective Level of assurance is the minimum of the LoA of the Authentication assertion and (if applicable) the LoA of the Representation authorization assertion(s).

⚠ The MR communicates two Levels of Assurance in its Assertion. A LevelOfAssurance (requested) and a LevelOfAssuranceUsed (actually obtained). The HM MUST use the LevelOfAssuranceUsed from the MR Assertion as the LoA of the Representation authorization.

snippet.loa-rule.mr

The MR MUST communicate the Level of Assurance of the registered authorization. A MR MUST NOT communicate a level for which it is not certified.

- In case of a chain of authorizations, the MR MUST communicatie the minimum of the LoA of all Representation authorizations in the applicable chain (so far).
- In case of a request for a portal service, a MR MUST communicate the Level of Assurance as the minimum Level of Assurance of all applicable service authorizations chosen by the user.

snippet.ondergetekende

Bedrijf

Naam:	
Handelsnaam:	
KvK nummer:	

Contactpersoon

Naam:	
Functie:	
E-mailadres:	
Telefoonnummer:	

snippet.ondertekening

Datum:	
Plaats:	
Naam:	
Handtekening:	

Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen. Als PDF of Word document mag deze ook digitaal ondertekend worden.

snippet.optionele.functionaliteit

	Herkennings makelaar	Middelen uitgever	Authenticatie dienst	Machtigingen register
eHerkenning				
Bedrijven (G2B, B2B)	O			
Consumenten (B2C)		O	O	
Aanvullende features				
Gevalideerde attributen		O	O	O
Single sign-on			O	

snippet.primaire.componenten

Componenten noodzakelijk voor het authenticeren, autoriseren en ondertekenen in de productieomgeving *Waaronder cookieservers en endpoints voor dienstencatalogus en metadata*
Ondersteunende diensten voor de productieomgeving in beheer bij de beheerorganisatie *Mantis, dienstencatalogus- en metadata-aggregator*
eHerkenning website

snippet.saas

Sluit u als (SaaS-)leverancier aan namens een Dienstverlener (DV)? Er is sprake van Dienstbemiddeling in de volgende gevallen:

1. U wilt gebruikmaken van uw eigen SSL-certificaat;
2. U kunt geen gebruikmaken van het SSL-certificaat van de dienstverlener;
3. Hetzelfde portaal/dezelfde aansluiting wordt namens meer dan één dienstverlener aangeboden.

snippet.samlbindingspdf

http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

snippet.secundaire.componenten

Ondersteunende diensten voor het productienetwerk in beheer bij de beheerorganisatie *Confluence, managementrapportage*
Ondersteunende diensten voor het testnetwerk *Waaronder de simulator, dienstencatalogus- en metadata-aggregator, pre-productiesystemen van deelnemers*

snippet.servicerestriction

⚠ Een beperking tot een vestiging betekent dat de vertegenwoordiger alleen bevoegd is om de desbetreffende vestiging te vertegenwoordigen.

Indien een dienstverlener een beperking op subdossier- of vestigingsnummer accepteert

- MOET deze ook transacties accepteren zonder deze beperking
- MOET deze een aangeleverde beperking respecteren. Het negeren ervan kan dit als gevolg hebben dat er geen rechtsgeldige rechtshandeling tot stand is gekomen
- MAG dit subdossier- of vestigingsnummer niet gebruikt worden als bepaling van de locatie, maar alleen om de grenzen van de vertegenwoordigingsbevoegdheid vast te stellen

snippet.startingpoint.happy

- Start the module: DV create SAML2.0 AuthnRequest HM
- Use the values shown in the happy flow, unless stated otherwise

snippet.testen.betrouwbaarheidniveaus

An HM is required to test each AD/MR with only one Level of Assurance. It is therefore not needed to repeat this test for each LoA the AD/MR offers.

snippet.tls

Voor normen voor veilige SSL/TLS verbindingen wordt verwezen naar Secure connection, gebaseerd op het NCSC Whitepaper "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)".

snippet.uitfaseren.eh1

EH1 vervalt per 1-7-2021

Met ingang van 1 juli 2021 komt het gebruik van het betrouwbaarheidsniveau eH1 te vervallen en moeten de middelen en machtigingen minimaal voldoen aan de normen van het betrouwbaarheidsniveau eH2.

snippet.url.ac

https://extranet.eherkenning.nl/1.11/attribuutcatalogus.xml

snippet.url.ac.prod

https://extranet.eherkenning.nl/1.11/attribuutcatalogus.xml

snippet.url.ac.test

https://extranet.eherkenning.nl/1.11/test/attribuutcatalogus.xml

snippet.url.dc.prod

https://aggregator.etoegang.nl/1.13/servicecatalog.xml

snippet.url.dc.test

https://aggregator.etoegang.nl/test/1.13/servicecatalog.xml

snippet.url.managementrapportage

https://rapportage.etoegang.nl/reportUpload.php

snippet.url.metadata.prod

https://aggregator.etoegang.nl/1.13/networkmetadata.xml

snippet.url.metadata.test

https://aggregator.etoegang.nl/test/1.13/networkmetadata.xml

snippet.url.simulator

https://simulator.etoegang.nl

snippet.url.sso

*.sso.eherkenning.nl

snippet.url.website

www.eherkenning.nl

snippet.urnprefix

urn:etoegang:

snippet.wachtwoord

Het wachtwoord:

- MOET ten minste 8 letters bevatten;
- MOET ten minste 1 kleine letter bevatten [a-z];
- MOET ten minste 1 hoofdletter bevatten [A-Z];
- MOET ten minste 1 cijfer bevatten [0-9];
- MOET ten minste 1 bijzonder teken bevatten [- _ ! $ % & ' . = / \ : < > | ? @ [ ] ^ ` { } ~];
- MAG NIET de gebruikersnaam bevatten;
- MAG NIET gelijk zijn aan een van de 5 eerder gebruikte wachtwoorden.

snippet.wiki

Confluence