

Agenda OB 75

Vergaderdatum	5-apr-2022		
Tijd	09:30u tot 12:00u		
Locatie	Online via Webex		
Auteur	Joyce Eering Logius		
Aanwezigen	Sander Boer Logius	Logius	Voorzitter
	Joyce Eering Logius	Logius	Secretaris
	Frans de Kok Logius	Logius	
	Bram van Pelt KPN	KPN	
	Marco Eikenaar Belastingdienst	Belastingdienst	
	Mark Baas Reconi	Reconi	Afgemeld
	Hans Milikan Signicat	Signicat	
	Arjen Monster	Gemeente Den Haag	
	Jacques Urlus NBA	NBA	
	Jan Geert Koops Dictu	Dictu	
	Douwe Jan Broersma Digidentity	Digidentity	
	Bernard Stibbe VZVZ	VZVZ	

Mededeling videoconferencing: Wij zullen de vergadering online via Webex voeren. Als het goed is hebben jullie daarvoor al een uitnodiging ontvangen, inclusief vergadernummer en wachtwoord, en zo niet geef dit dan even aan.

1. Opening

1.1. Vaststellen agenda

1.2. Vaststellen notulen/actiepunten OB 74

Het verslag en actiepunten van de vorige meeting [Notulen van OB 74](#)

1.3. Mededelingen

2. Het Operationeel Beraad

De vergadering (Digitaal, hybride en/of fysiek)

3. Update vanuit de Refinement Werkgroep

Een overzicht van de status van RFCs en vooruitblik naar de backlog. **Woord aan Bram van Pelt.**

4. Update vanuit het Intake Team

Een overzicht van de status van dossiers en vooruitblik naar de backlog (inclusief de link met de Roadmap en EPIC's). **Woord aan Douwe Jan.**

5. RFC's ter advies

5.1. [RFC2352 Registratie van het BSN](#)

Samenvatting

Waarom is deze RFC nodig?	eIDAS-UIT maakt gebruik van het pseudo-ID als uniek identificatienummer van de natuurlijke persoon. De MU kan het pseudo-ID opvragen bij BSNk door o.a. het BSN van de natuurlijke persoon door te geven. Deze RFC behandelt de registratie van het BSN van de natuurlijke persoon voor nieuwe en bestaande middelen.
Oplossingsrichting	Het BSN zal bij de registratie van persoonsgegevens worden uitgevraagd, of kan later worden toegevoegd.
Aanpassing van	Normenkader Betrouwbaarheidsniveaus
Impact op rollen	MU
Impact op aanpalende systemen	
Gerelateerd aan	
Eigenaar	Rob Brand Logius
Implementatietermijn	Direct (administratief)
Testcases van toepassing?	
Motivatie verkorte RFC procedure	

5.2. [RFC2353 Vervanging verwijzing WEH](#)

Samenvatting

Waarom is deze RFC nodig?	Kwaliteit normenkader Het betreft een tekstuele wijziging die nodig is omdat de Wet elektronische handtekeningen waarnaar wordt verwezen, al sinds 2016 niet meer bestaat. Sindsdien is de eIDAS verordening van kracht; Hiernaar moet worden verwezen. Inhoudelijk heeft deze aanpassing geen gevolgen.
Oplossingsrichting	Tekstuele aanpassing van niet van toepassing zijnde passage over de Wet Elektronische Handtekeningen
Aanpassing van	Normenkader betrouwbaarheidsniveaus
Impact op rollen	AD (Laag)

Waarom is deze RFC nodig?	<p>Kwaliteit normenkader</p> <p>Het betreft een tekstuele wijziging die nodig is omdat de Wet elektronische handtekeningen waarnaar wordt verwezen, al sinds 2016 niet meer bestaat. Sindsdien is de eIDAS verordening van kracht; Hiernaar moet worden verwezen.</p> <p>Inhoudelijk heeft deze aanpassing geen gevolgen.</p>
Impact op aanpalende systemen	Niet van toepassing
Gerelateerd aan	Niet van toepassing
Eigenaar	Rob Brand Logius
Implementatietermijn	Direct
Testcases van toepassing?	Niet van toepassing
Motivatie verkorte RFC procedure	De verkorte RFC procedure is hier niet van toepassing

5.3. [RFC2354 VIS-Check op LOA2](#)

Samenvatting

<p>Waarom is deze RFC nodig?</p>	<p>Beperking van het aantal fraudegevallen bij aanvraag eHerkenningmiddelen</p> <p>Het belangrijkste argument voor het invoeren van een VIS-check is het feit dat op LoA2/2+ geen vergelijking van de fysieke kenmerken van de aanvrager en de foto op het WID wordt uitgevoerd. Het uitvoeren van een LoA2/2+ VIS-check levert in de praktijk een beperking van het aantal (mogelijke) fraudegevallen op, zo wordt bevestigd door de Deelnemers. Het is niet goed in te schatten hoe groot deze beperking is.</p> <p>De Deelnemers zijn reeds bekend met het uitvoeren van een VIS-check voor LoA3 en de Deelnemers hebben daarom reeds voorzieningen om de VIS-check uit te voeren. De inschatting is daarbij dat het uitvoeren van een VIS-check op LoA2/2+ geen grote impact zal hebben op de procedures van de Deelnemers, maar voor de technische realisatie zal tijd nodig zijn.</p> <p>Aan de VIS-check zijn kosten verbonden. In hoeverre deze kosten een effect hebben op de prijs van een EH2/2+ middel is aan de Deelnemers.</p> <p>Het memo in de bijlage waar deze RFC op is gebaseerd is op 8 februari 2022 in het Tactisch Beraad behandeld, waar positief hierop is gereageerd en verzocht is om deze conceptchange op te stellen voor het Operationeel Beraad.</p>
<p>Oplossingsrichting</p>	<p>Vanaf LOA3 wordt bij de inschrijving al een VIS-check gedaan. Op LOA2 nog niet. Het voorstel strekt ertoe om deze VIS-check ook op LOA2 te doen.</p>
<p>Aanpassing van</p>	<p>Normenkader betrouwbaarheidsniveaus</p>
<p>Impact op rollen</p>	<p>HNP, AD. Voor beide rollen Impact Midden</p>
<p>Impact op aanpalende systemen</p>	<p>Niet van toepassing</p>
<p>Gerelateerd aan</p>	<p>Niet van toepassing</p>
<p>Eigenaar</p>	<p>Rob Brand Logius</p>
<p>Implementatietermijn</p>	<p>Direct (in het normenkader).</p> <p>NB. Voor de technische realisatie zal tijd nodig zijn. De implementatietermijn zal daarom goed afgestemd moeten worden.</p>
<p>Testcases van toepassing?</p>	<p>Niet van toepassing</p>

<p>Waarom is deze RFC nodig?</p>	<p>Beperking van het aantal fraudegevallen bij aanvraag eHerkenningmiddelen</p> <p>Het belangrijkste argument voor het invoeren van een VIS-check is het feit dat op LoA2/2+ geen vergelijking van de fysieke kenmerken van de aanvrager en de foto op het WID wordt uitgevoerd. Het uitvoeren van een LoA2/2+ VIS-check levert in de praktijk een beperking van het aantal (mogelijke) fraudegevallen op, zo wordt bevestigd door de Deelnemers. Het is niet goed in te schatten hoe groot deze beperking is.</p> <p>De Deelnemers zijn reeds bekend met het uitvoeren van een VIS-check voor LoA3 en de Deelnemers hebben daarom reeds voorzieningen om de VIS-check uit te voeren. De inschatting is daarbij dat het uitvoeren van een VIS-check op LoA2/2+ geen grote impact zal hebben op de procedures van de Deelnemers, maar voor de technische realisatie zal tijd nodig zijn.</p> <p>Aan de VIS-check zijn kosten verbonden. In hoeverre deze kosten een effect hebben op de prijs van een EH2/2+ middel is aan de Deelnemers.</p> <p>Het memo in de bijlage waar deze RFC op is gebaseerd is op 8 februari 2022 in het Tactisch Beraad behandeld, waar positief hierop is gereageerd en verzocht is om deze conceptchange op te stellen voor het Operationeel Beraad.</p>
<p>Motivatie verkorte RFC procedure</p>	<p>Verkorte RFC procedure niet van toepassing</p>

6. RFC's ter bespreking

6.1. [RFC2348 Oplossen fouten bij Ketenmachtigingen](#)

Samenvatting

<p>Waarom is deze RFC nodig?</p>	<p>"Technical Debt" - Bij het schrijven van RFC2249 Verplicht leveren company name bij ketenmachtigen bleek pagina "Interface specifications HM-MR chain authorization" onduidelijk en incompleet. Er stonden ook twee specificatie onderdelen op die waarvan de tekst met de invoering van r1.11 al aangepast hadden moeten worden en nu niet consistent zijn met de rest van het stelsel, waaronder het koppelvlak tussen HM en MR. Maar ook bleek dat de Leveranciers deze inconsistente specificaties wel letterlijk geïmplementeerd hebben. Omdat het herstel een koppelvlak wijziging tot gevolg heeft was de impact te groot om het herstel in RFC2249 mee te nemen. In de Refinement Werkgroep was de consensus dat deze inconsistenties hersteld moeten worden, maar dan wel via een aparte RFC.</p>
<p>Oplossingsrichting</p>	<p>In de huidige specificatie tussen HM en MR2 (ketenmachtiging) staan LegalSubjectID en IntermediaryEntityID in <Request><Subject> element. Echter met de introductie van r1.11 is er destijds besloten om in het <Subject> element alleen nog maar een TransientID te zetten. En beide elementen staat ook gewoon in de MR1 assertion die toch meegestuurd wordt naar MR2. Die zijn multi-valued en er zitten alleen EncryptedID in. Het versleutelen van attributen en identiteiten was vanaf r1.11 verplicht (zie ook specificaties https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption). En daardoor was het toen ook nodig om meerdere waardes te ondersteunen. De RFC zorgt voor backward compatibiliteit voor DV's op oude koppelvlakken.</p> <p>Deze RFC zal</p> <ul style="list-style-type: none"> • HM-MR1 - IntermediarySubjectID toevoegen aan MR1 response in <Request><Subject> • HM-MR2 - LegalSubjectID en IntermediaryEntityID uit XACMLAuthzDecisionQuery <Request><Subject> element halen • HM moeten voor backward compatibiliteit zorgen voor DV • HM moeten met oude en nieuwe MR2-assertions om kunnen gaan zodat MR2 flexibel is met het implementeren van de RFC.
<p>Aanpassing van</p>	<p>Specificaties van HM-MR en de bijbehorende processing rules igv Ketenmachtiging</p>

Waarom is deze RFC nodig?	<p>"Technical Debt" - Bij het schrijven van RFC2249 Verplicht leveren company name bij ketenmachtigen bleek pagina "Interface specifications HM-MR chain authorization" onduidelijk en incompleet. Er stonden ook twee specificatie onderdelen op die waarvan de tekst met de invoering van r1.11 al aangepast hadden moeten worden en nu niet consistent zijn met de rest van het stelsel, waaronder het koppelvlak tussen HM en MR. Maar ook bleek dat de Leveranciers deze inconsistente specificaties wel letterlijk geïmplementeerd hebben. Omdat het herstel een koppelvlak wijziging tot gevolg heeft was de impact te groot om het herstel in RFC2249 mee te nemen. In de Refinement Werkgroep was de consensus dat deze inconsistenties hersteld moeten worden, maar dan wel via een aparte RFC.</p>
Impact op rollen	<p>Alle HM en elke MR die ketenmachtigen verstrekt (MR2). DV die Intermediate.EntityID gebruiken uit de HM-samenvatting of LegalSubjectID halen uit de (in <Advice> element meegestuurde) originele MR2 assertion. Echter deze RFC zorgt voor 'backwards compatibility' zodat de betreffende DV's zelf het moment kunnen kiezen om naar het nieuwe koppelvlak te gaan.</p>
Impact op aanpalende systemen	nvt
Gerelateerd aan	RFC2249 Verplicht leveren company name bij ketenmachtigen
Eigenaar	Frans de Kok Logius
Implementatietermijn	<p>Vereist eenvoudig implementatieplan</p> <ul style="list-style-type: none"> • MR2 zal de RFC uiterlijk geïmplementeerd moeten hebben op en nader te bepalen koppelvlakrelease (waarbij het de verplichting van ketenmachtigen in scope zit). • HM zal de RFC geïmplementeerd moeten hebben voordat of tegelijk met de eerste MR2 die deze RFC implementeert. • Omdat deze RFC zorgt voor 'backwards compatibility' kunnen DV's zelf het moment kiezen om naar het nieuwe koppelvlak te gaan, vanaf het moment dat het nieuwe koppelvlak beschikbaar komt (en alle MR2 en HM deze al geïmplementeerd hebben).
Testcases van toepassing?	
Motivatie verkorte RFC procedure	

6.2. [RFC2349 Verduidelijking signing Discovery service](#)

Samenvatting

Waarom is deze RFC nodig?	In RFC2304A Discoverydienst wordt beschreven dat gegevens cryptografisch worden ondertekend, maar hier wordt geen duidelijke onderbouwing bij gegeven. Deze RFC licht dit verder toe.
Oplossingsrichting	Aanpassingen van de koppelvlakbeschrijving
Aanpassing van	Discovery Interface MR-MR chain authorisations RFC2304A
Impact op rollen	MR
Impact op aanpalende systemen	Geen
Gerelateerd aan	RFC2304A Discoverydienst
Eigenaar	Bram van Pelt KPN
Implementatietermijn	Administratief
Testcases van toepassing?	Geen nieuwe testcases
Motivatie verkorte RFC procedure	NVT

7. Operationele Uitdagingen

In de brainstorm van december 2020 bleek de wens om operationele aspecten en uitdagingen te bespreken, naast de technische RFCs. Dit agenda onderdeel biedt daar ruimte voor. Het woord aan degenen die iets willen delen.

8. WVTTK

9. Afsluiting

Rondje langs de velden. Deelnemers kunnen hier suggesties aandragen voor op de [Voorraadagenda OB](#). Volgende vergadering is op 3-mei-2022 van **9.30 tot 11.00**

Notulen van OB 75

Vergaderdatum	5-apr-2022		
Tijd	09:30u tot 12:00u		
Locatie	Online via Webex		
Auteur	Joyce Eering Logius		
Aanwezigen	Sander Boer Logius	Logius	Voorzitter
	Joyce Eering Logius	Logius	Secretaris
	Frans de Kok Logius	Logius	
	Bram van Pelt KPN	KPN	
	Marco Eikenaar Belastingdienst	Belastingdienst	
	Mark Baas Reconi	Reconi	Afgemeld
	Hans Milikan Signicat	Signicat	
	Arien Monster	Gemeente Den Haag	
	Jacques Urlus NBA	NBA	Afgemeld
	Jan Geert Koops Dictu	Dictu	
	Douwe Jan Broersma Digidentity	Digidentity	
	Bernard Stibbe VZVZ	VZVZ	

Mededeling videoconferencing: Wij zullen de vergadering online via Webex voeren. Als het goed is hebben jullie daarvoor al een uitnodiging ontvangen, inclusief vergadernummer en wachtwoord, en zo niet geef dit dan even aan.

1. Opening

Sander heet iedereen welkom.

1.1. Vaststellen agenda

De agenda wordt vastgesteld.

- Jacques Urlus en Mark Baas hebben zich afgemeld.

1.2. Vaststellen notulen/actiepunten OB 74

Het verslag van de vorige meeting [Notulen van OB 74](#) is vastgesteld.

1.3. Mededelingen

Sander; In het TB zijn de volgende punten besproken:

- De Belastingdienst legt zich neer bij de uitspraak van de rechter rondom het verplicht inloggen met eHerkenning maar zien geen reden om te stoppen het aanbieden om met eHerkenning in te loggen bij de Belastingdienst
- Het verplicht stellen van de 2-factorauthenticatie is besproken. Hiervoor is een plan beschreven en goedgekeurd om met name de impact hiervan te onderzoeken.
- Er is instemming over de inhoud van release 1.13 24 maart 2022. De te implementeren RFC's zullen komende week worden verwerkt in de Afsprakenstelsel. Afstemming tussen de leveranciers en de Releasemanager zal plaatsvinden ter voorbereiding en over welke changes opgenomen gaan worden in de volgende release.
- Er is geen update over de WDO, onzekerheid blijft of de planning van 1 juli 2022 behaald zal worden.

2. Het Operationeel Beraad

De vergadering, digitaal, hybride en/of fysiek voeren nu de coronamaatregelen zijn opgeheven.

De wijze van vergaderen van het OB wordt besproken. Over het algemeen wordt de huidige (digitaal) wijze, van vergaderen als positief en efficiënt ervaren.

Het OB staat open om het OB periodiek, fysiek/hybride te laten plaatsvinden. Deze zal worden gepland bij Logius, eventueel aansluitend met een lunch. Uitnodiging hiervoor volgt.

3. Update vanuit de Refinement Werkgroep

Een overzicht van de status van RFCs en vooruitblik naar de backlog. **Woord aan Bram van Pelt.**

- De Refinement werkgroep heeft de twee RFC's voortgebracht ter bespreking in het OB. Zie agendapunt 6.
- Afname in snelheid i.v.m. de tijd en energie welke wordt gestopt in de update van de releases.
- Afstemming met Douwe Jan en Frank Jonker zal plaatsvinden over het voorstel welke is gedaan vanuit de RWG n.a.v. de discussie over het doel en de takenpakket van de RWG. De twee oplossingsrichtingen zijn beschreven in een memo aan het LO.
- Inventarisatie KVK machtigingsvrij inloggen. In de RWG vindt afstemming plaats over voorkeur oplossingsrichting en deze af te geven aan het Intaketeam
- De RFC over versioning binnen de AS staat op de backlog voor refinement.

4. Update vanuit het Intake Team

Een overzicht van de status van dossiers en vooruitblik naar de backlog (inclusief de link met de Roadmap en EPIC's). **Woord aan Douwe Jan.**

- Het duidelijk krijgen, samenhang van de OHW dossiers met het Jaarplan eHerkenning. Op basis hiervan zal de prioriteit van de OHW dossiers in lijn worden gebracht met het JP 2022.
- Het TB heeft aangegeven dat voor het eerstvolgende release de prioriteit ligt rond thema Ketenmachtigingen. Het TB heeft gevraagd om in Q2 een advies op te stellen over de doorontwikkeling van Ketenmachtigingen.
- Gewerkt wordt aan de lange termijn dossiers rondom [BZK - Versnelling BSN-activatie mbv DigiD-onboarding](#). De aansluiting op DigiD en de wens van de KvK om hun dienstverlening via eHerkenning te ontsluiten.
- Met de RVO zijn gesprekken gevoerd over Ketenmachtigen Intermediar portalen. Hans geeft toelichting op zijn voorstel aan RVO 'Alternatief 3' nieuwe functionaliteiten binnen de stelsel ook bruikbaar te laten zijn voor meerdere dienstverleners.
- Deelname aan de "Workshops domein toegang" welke recent heeft plaatsgevonden i.h.k.v. een nieuwe architectuur ontwerp door Hans Rob de Reus. Frans heeft hiervoor een inventarisatie gedaan van de huidige Features eHerkenning en RVO, welke als checklist zal fungeren voor de nieuwe architectuur en heeft tevens Use cases/activiteiten voor 2023 geïnventariseerd waarbij het Intaketeam kan ondersteunen.
- Richard Backx zal gaan vertegenwoordigen in de Intake Werkgroep vanaf april 2022.

5. RFC's ter advies

5.1. [RFC2352 Registratie van het BSN](#)

Samenvatting

Waarom is deze RFC nodig?	eIDAS-UIT maakt gebruik van het pseudo-ID als uniek identificatienummer van de natuurlijke persoon. De MU kan het pseudo-ID opvragen bij BSNk door o.a. het BSN van de natuurlijke persoon door te geven. Deze RFC behandelt de registratie van het BSN van de natuurlijke persoon voor nieuwe en bestaande middelen.
Oplossingsrichting	Het BSN zal bij de registratie van persoonsgegevens worden uitgevraagd, of kan later worden toegevoegd.
Aanpassing van	Normenkader Betrouwbaarheidsniveaus
Impact op rollen	MU
Impact op aanpalende systemen	
Gerelateerd aan	
Eigenaar	Rob Brand Logius
Implementatietermijn	Direct (administratief)
Testcases van toepassing?	
Motivatie verkorte RFC procedure	

Bram:

- Geeft aan dat de RFC's welke ter advies staan geagendeerd volgens het voortbrengingsproces eerst ter bespreking ingebracht moet worden in het OB voorts het ter advies wordt geagendeerd.
- Geeft toelichting op zijn comments rondom de meervoudige identiteitsverklaringen, Burger domein/BSN. Met Rob, eigenaar van de RFC zal afstemming volgen.

Afspraak OB 75: Advies: RFC aanhouden totdat de vragen en opmerkingen zijn besproken en verwerkt. Daarna zal het worden voorgelegd voor advies in het volgende OB.

5.2. [RFC2353 Vervanging verwijzing WEH](#)

Samenvatting

Waarom is deze RFC nodig?	Kwaliteit normenkader Het betreft een tekstuele wijziging die nodig is omdat de Wet elektronische handtekeningen waarnaar wordt verwezen, al sinds 2016 niet meer bestaat. Sindsdien is de eIDAS verordening van kracht; Hiernaar moet worden verwezen. Inhoudelijk heeft deze aanpassing geen gevolgen.
Oplossingsrichting	Tekstuele aanpassing van niet van toepassing zijnde passage over de Wet Elektronische Handtekeningen
Aanpassing van	Normenkader betrouwbaarheidsniveaus
Impact op rollen	AD (Laag)
Impact op aanpalende systemen	Niet van toepassing
Gerelateerd aan	Niet van toepassing
Eigenaar	Rob Brand Logius
Implementatietermijn	Direct
Testcases van toepassing?	Niet van toepassing
Motivatie verkorte RFC procedure	De verkorte RFC procedure is hier niet van toepassing

- Positief advies naar het TB.

5.3. [RFC2354 VIS-Check op LOA2](#)

Samenvatting

<p>Waarom is deze RFC nodig?</p>	<p>Beperking van het aantal fraudegevallen bij aanvraag eHerkenningmiddelen</p> <p>Het belangrijkste argument voor het invoeren van een VIS-check is het feit dat op LoA2/2+ geen vergelijking van de fysieke kenmerken van de aanvrager en de foto op het WID wordt uitgevoerd. Het uitvoeren van een LoA2/2+ VIS-check levert in de praktijk een beperking van het aantal (mogelijke) fraudegevallen op, zo wordt bevestigd door de Deelnemers. Het is niet goed in te schatten hoe groot deze beperking is.</p> <p>De Deelnemers zijn reeds bekend met het uitvoeren van een VIS-check voor LoA3 en de Deelnemers hebben daarom reeds voorzieningen om de VIS-check uit te voeren. De inschatting is daarbij dat het uitvoeren van een VIS-check op LoA2/2+ geen grote impact zal hebben op de procedures van de Deelnemers, maar voor de technische realisatie zal tijd nodig zijn.</p> <p>Aan de VIS-check zijn kosten verbonden. In hoeverre deze kosten een effect hebben op de prijs van een EH2/2+ middel is aan de Deelnemers.</p> <p>Het memo in de bijlage waar deze RFC op is gebaseerd is op 8 februari 2022 in het Tactisch Beraad behandeld, waar positief hierop is gereageerd en verzocht is om deze conceptchange op te stellen voor het Operationeel Beraad.</p>
<p>Oplossingsrichting</p>	<p>Vanaf LOA3 wordt bij de inschrijving al een VIS-check gedaan. Op LOA2 nog niet. Het voorstel strekt ertoe om deze VIS-check ook op LOA2 te doen.</p>
<p>Aanpassing van</p>	<p>Normenkader betrouwbaarheidsniveaus</p>
<p>Impact op rollen</p>	<p>HNP, AD. Voor beide rollen Impact Midden</p>
<p>Impact op aanpalende systemen</p>	<p>Niet van toepassing</p>
<p>Gerelateerd aan</p>	<p>Niet van toepassing</p>
<p>Eigenaar</p>	<p>Rob Brand Logius</p>
<p>Implementatietermijn</p>	<p>Direct (in het normenkader).</p> <p>NB. Voor de technische realisatie zal tijd nodig zijn. De implementatietermijn zal daarom goed afgestemd moeten worden.</p>
<p>Testcases van toepassing?</p>	<p>Niet van toepassing</p>

<p>Waarom is deze RFC nodig?</p>	<p>Beperking van het aantal fraudegevallen bij aanvraag eHerkenningmiddelen</p> <p>Het belangrijkste argument voor het invoeren van een VIS-check is het feit dat op LoA2/2+ geen vergelijking van de fysieke kenmerken van de aanvrager en de foto op het WID wordt uitgevoerd. Het uitvoeren van een LoA2/2+ VIS-check levert in de praktijk een beperking van het aantal (mogelijke) fraudegevallen op, zo wordt bevestigd door de Deelnemers. Het is niet goed in te schatten hoe groot deze beperking is.</p> <p>De Deelnemers zijn reeds bekend met het uitvoeren van een VIS-check voor LoA3 en de Deelnemers hebben daarom reeds voorzieningen om de VIS-check uit te voeren. De inschatting is daarbij dat het uitvoeren van een VIS-check op LoA2/2+ geen grote impact zal hebben op de procedures van de Deelnemers, maar voor de technische realisatie zal tijd nodig zijn.</p> <p>Aan de VIS-check zijn kosten verbonden. In hoeverre deze kosten een effect hebben op de prijs van een EH2/2+ middel is aan de Deelnemers.</p> <p>Het memo in de bijlage waar deze RFC op is gebaseerd is op 8 februari 2022 in het Tactisch Beraad behandeld, waar positief hierop is gereageerd en verzocht is om deze conceptchange op te stellen voor het Operationeel Beraad.</p>
<p>Motivatie verkorte RFC procedure</p>	<p>Verkorte RFC procedure niet van toepassing</p>

Afspraak OB 75: Het advies is RFC aanhouden totdat de vragen en opmerkingen zijn besproken en verwerkt. Daarna zal het worden voorgelegd voor advies in het volgende OB.

Het OB doet een verzoek aan de Expert werkgroep NK voor een explicieter beschrijving van de check/controlle voor buitenlandse paspoorten, identiteiten - en reisdocumenten. Frans zal het afstemmen met Rob.

- Raadplegen register/dataset. Lijst ontbreekt voor buitenlandse identiteiten- en reisdocumenten.

6. RFC's ter bespreking

6.1. RFC2348 Oplossen fouten bij Ketenmachtigingen

Samenvatting

Waarom is deze RFC nodig?	<p>"Technical Debt" - Bij het schrijven van RFC2249 Verplicht leveren company name bij ketenmachtigen bleek pagina "Interface specifications HM-MR chain authorization" onduidelijk en incompleet. Er stonden ook twee specificatie onderdelen op die waarvan de tekst met de invoering van r1.11 al aangepast hadden moeten worden en nu niet consistent zijn met de rest van het stelsel, waaronder het koppelvlak tussen HM en MR. Maar ook bleek dat de Leveranciers deze inconsistente specificaties wel letterlijk geïmplementeerd hebben. Omdat het herstel een koppelvlak wijziging tot gevolg heeft was de impact te groot om het herstel in RFC2249 mee te nemen. In de Refinement Werkgroep was de consensus dat deze inconsistenties hersteld moeten worden, maar dan wel via een aparte RFC.</p>
Oplossingsrichting	<p>In de huidige specificatie tussen HM en MR2 (ketenmachtiging) staan LegalSubjectID en IntermediaryEntityID in <Request><Subject> element. Echter met de introductie van r1.11 is er destijds besloten om in het <Subject> element alleen nog maar een TransientID te zetten. En beide elementen staat ook gewoon in de MR1 assertion die toch meegestuurd wordt naar MR2. Die zijn multi-valued en er zitten alleen EncryptedID in. Het versleutelen van attributen en identiteiten was vanaf r1.11 verplicht (zie ook specificaties https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption). En daardoor was het toen ook nodig om meerdere waardes te ondersteunen. De RFC zorgt voor backward compatibiliteit voor DV's op oude koppelvlakken.</p> <p>Deze RFC zal</p> <ul style="list-style-type: none">• HM-MR1 - IntermediarySubjectID toevoegen aan MR1 response in <Request><Subject>• HM-MR2 - LegalSubjectID en IntermediaryEntityID uit XACMLAuthzDecisionQuery <Request><Subject> element halen• HM moeten voor backward compatibiliteit zorgen voor DV• HM moeten met oude en nieuwe MR2-assertions om kunnen gaan zodat MR2 flexibel is met het implementeren van de RFC.
Aanpassing van	Specificaties van HM-MR en de bijbehorende processing rules igv Ketenmachtiging

Waarom is deze RFC nodig?	<p>"Technical Debt" - Bij het schrijven van RFC2249 Verplicht leveren company name bij ketenmachtigen bleek pagina "Interface specifications HM-MR chain authorization" onduidelijk en incompleet. Er stonden ook twee specificatie onderdelen op die waarvan de tekst met de invoering van r1.11 al aangepast hadden moeten worden en nu niet consistent zijn met de rest van het stelsel, waaronder het koppelvlak tussen HM en MR. Maar ook bleek dat de Leveranciers deze inconsistente specificaties wel letterlijk geïmplementeerd hebben. Omdat het herstel een koppelvlak wijziging tot gevolg heeft was de impact te groot om het herstel in RFC2249 mee te nemen. In de Refinement Werkgroep was de consensus dat deze inconsistenties hersteld moeten worden, maar dan wel via een aparte RFC.</p>
Impact op rollen	<p>Alle HM en elke MR die ketenmachtigen verstrekt (MR2). DV die Intermediate.EntityID gebruiken uit de HM-samenvatting of LegalSubjectID halen uit de (in <Advice> element meegestuurde) originele MR2 assertion. Echter deze RFC zorgt voor 'backwards compatibility' zodat de betreffende DV's zelf het moment kunnen kiezen om naar het nieuwe koppelvlak te gaan.</p>
Impact op aanpalende systemen	nvt
Gerelateerd aan	RFC2249 Verplicht leveren company name bij ketenmachtigen
Eigenaar	Frans de Kok Logius
Implementatietermijn	<p>Vereist eenvoudig implementatieplan</p> <ul style="list-style-type: none"> • MR2 zal de RFC uiterlijk geïmplementeerd moeten hebben op en nader te bepalen koppelvlakrelease (waarbij het de verplichting van ketenmachtigen in scope zit). • HM zal de RFC geïmplementeerd moeten hebben voordat of tegelijk met de eerste MR2 die deze RFC implementeert. • Omdat deze RFC zorgt voor 'backward compatibility' kunnen DV's zelf het moment kiezen om naar het nieuwe koppelvlak te gaan, vanaf het moment dat het nieuwe koppelvlak beschikbaar komt (en alle MR2 en HM deze al geïmplementeerd hebben).
Testcases van toepassing?	
Motivatie verkorte RFC procedure	

Frans: De RFC wordt toegelicht. Hierop worden de volgende opmerkingen en aanvullingen gedaan:

- Op aangeven van Marco wordt de titel van de RFC gewijzigd in “oplossen” van fouten bij KM i.p.v. “verbeteren”. *Is reeds aangepast, Done!*
- Beschrijving van de Processing rules heeft nog verduidelijking. Hierin wordt tevens de versioning regel rondom de Koppelvlakversie meegenomen. Uitgangspunt van het stelsel is namelijk om twee oude koppelvlak releases aan te blijven bieden. Als n.a.v. deze RFC een nieuwe koppelvlak erbij komt zou het mogelijk betekenen dat koppelvlak 1.9 komt te vervallen, waar veel dienstverleners op zitten.
- Marco vraagt de RFC te verduidelijken op de vraag of een koppeling met de dienstverleners aangepast moet worden.

Afspraak OB 75: Frans gaat de genoemde punten oppakken en de RFC updaten. In het volgende OB zal het ter advies worden geagendeerd.

6.2. [RFC2349 Verduidelijking signing Discovery service](#)

Samenvatting

Waarom is deze RFC nodig?	In RFC2304A Discoverydienst wordt beschreven dat gegevens crypto grafisch worden ondertekend, maar hier wordt geen duidelijke onderbouwing bij gegeven. Deze RFC licht dit verder toe.
Oplossingsrichting	Aanpassingen van de koppelvlakbeschrijving
Aanpassing van	Discovery Interface MR-MR chain authorisations RFC2304A
Impact op rollen	MR
Impact op aanpalende systemen	Geen
Gerelateerd aan	RFC2304A Discoverydienst
Eigenaar	Bram van Pelt KPN
Implementatietermijn	Administratief
Testcases van toepassing?	Geen nieuwe testcases
Motivatie verkorte RFC procedure	NVT

Bram geeft toelichting op de RFC. De Soap signing handtekening standard moet nog verder uitgewerkt te worden.

Afspraak OB 75: Bram gaat de RFC updaten en verder finetunen in de Refinement werkgroep. In het volgende OB zal het ter advies worden geagendeerd.

7. Operationele Uitdagingen

In de brainstorm van december 2020 bleek de wens om operationele aspecten en uitdagingen te bespreken, naast de technische RFCs. Dit agenda onderdeel biedt daar ruimte voor. Het woord aan degenen die iets willen delen.

- Hans geeft een update over de voortgang en planning van de aankomende release. Deze verloopt voorspoedig.
- Hans gaat de mogelijkheid na voor een demo over de Discovery dienst in het OB.
- Douwe Jan, idem voor een demo rondom PROBAS registratie.
- Bernard Stibbe zal de status POC MedMij pilot nagaan en het terugkoppelen. En hij gaat in één van de komende bijeenkomsten een toelichting geven hoe dienstverleners (denk aan ziekenhuizen) in het medmij domein aan worden gesloten.

8. WVTTK

Geen.

9. Afsluiting

Rondje langs de velden. Deelnemers kunnen hier suggesties aandragen voor op de [Voorraadagenda OB](#). Volgende vergadering is op 3-mei-2022 van **9.30 tot 11.00**