

# Agenda OB 77

<b>Vergaderdatum</b>	7-jun-2022		
<b>Tijd</b>	10:00u tot 13:00u (inclusief lunch)		
<b>Locatie</b>	Bij Logius, Wilhelmina van Pruisenweg 52 en Hybride (zie Webex) toegangscode		
<b>Auteur</b>	<a href="#">Joyce Eering   Logius</a>		
<b>Aanwezigen</b>	<a href="#">Sander Boer   Logius</a>	Logius	Voorzitter
	<a href="#">Joyce Eering   Logius</a>	Logius	Secretaris
	<a href="#">Frans de Kok   Logius</a>	Logius	
	<a href="#">Rob Brand   Logius</a>	Logius	
	<a href="#">Bram van Pelt   KPN</a>	KPN	
	<a href="#">Marco Eikenaar   Belastingdienst</a>	Belastingdienst	
	<a href="#">Mark Baas   Reconi</a>	Reconi	
	<a href="#">Hans Milikan   Signicat</a>	Signicat	
	<a href="#">Arien Monster</a>	Gemeente Den Haag	Hybride
	<a href="#">Jacques Urlus   NBA</a>	NBA	
	<a href="#">Jan Geert Koops   Dictu</a>	Dictu	Afgemeld
	<a href="#">Douwe Jan Broersma   Digidentity</a>	Digidentity	
	<a href="#">Bernard Stibbe   VZVZ</a>	VZVZ	Afgemeld

**Mededeling videoconferencing:** Het is mogelijk om de vergadering online via Webex te voeren. Zie in de uitnodiging : vergadernummer en wachtwoord.

## 1. Opening

### 1.1. Vaststellen agenda

## 1.2. Vaststellen notulen/actiepunten OB 75

Het verslag en actiepunten van de vorige meeting [Notulen van OB 75](#)

## 1.3. Mededelingen

# 2. Het Operationeel Beraad

De vergadering vindt plaats bij Logius. Hybride deelname is tevens mogelijk.

# 3. Update vanuit de Refinement Werkgroep

Een overzicht van de status van RFC's en vooruitblik naar de back log. **Woord aan Bram van Pelt.**

# 4. Update vanuit het Intake Team

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

# 5. RFC's ter advies

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

**Samenvatting**

<p><b>Waarom is deze RFC nodig?</b></p>	<p>"Technical Debt" - Bij het schrijven van <a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a> 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><b>Oplossingsrichting</b></p>	<p>In de huidige specificatie tussen HM en MR2 (ketenmachtiging) staan LegalSubjectID en IntermediaryEntityID in &lt;Request&gt;&lt;Subject&gt; element. Echter met de introductie van r1.11 is er destijds besloten om in het &lt;Subject&gt; 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 <a href="https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption">https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption</a>). 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"> <li>• HM-MR1 - IntermediarySubjectID toevoegen aan MR1 response in &lt;Request&gt;&lt;Subject&gt;</li> <li>• HM-MR2 - LegalSubjectID en IntermediaryEntityID uit XACMLAuthzDecisionQuery &lt;Request&gt;&lt;Subject&gt; element halen</li> <li>• HM moeten voor backward compatibiliteit zorgen voor DV</li> <li>• HM moeten met oude en nieuwe MR2-assertions om kunnen gaan zodat MR2 flexibel is met het implementeren van de RFC.</li> </ul>
<p><b>Aanpassing van</b></p>	<p>Specificaties van HM-MR en de bijbehorende processing rules igv Ketenmachtiging</p>
<p><b>Impact op rollen</b></p>	<p>Alle HM en elke MR die ketenmachtigingen verstrekt (MR2).</p> <p>DV die Intermediate.EntityID gebruiken uit de HM-samenvatting of LegalSubjectID halen uit de (in &lt;Advice&gt; 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>

<b>Waarom is deze RFC nodig?</b>	<i>"Technical Debt"</i> - Bij het schrijven van <a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a> 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.
<b>Impact op aanpalende systemen</b>	nvt
<b>Gerelateerd aan</b>	<a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a>
<b>Eigenaar</b>	<a href="#">Frans de Kok   Logius</a>
<b>Implementatietermijn</b>	<p>Vereist eenvoudig implementatieplan</p> <ul style="list-style-type: none"> <li>• MR2 zal de RFC uiterlijk geïmplementeerd moeten hebben op en nader te bepalen koppelvlakrelease (waarbij het de verplichting van ketenmachtigingen in scope zit).</li> <li>• HM zal de RFC geïmplementeerd moeten hebben voordat of tegelijk met de eerste MR2 die deze RFC implementeert.</li> <li>• 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).</li> </ul>
<b>Testcases van toepassing?</b>	
<b>Motivatie verkorte RFC procedure</b>	

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

### Samenvatting

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

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

#### Samenvatting

<b>Waarom is deze RFC nodig?</b>	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.
<b>Oplossingsrichting</b>	Het BSN zal bij de registratie van persoonsgegevens worden uitgevraagd, of kan later worden toegevoegd.
<b>Aanpassing van</b>	Normenkader Betrouwbaarheidsniveaus
<b>Impact op rollen</b>	MU
<b>Impact op aanpalende systemen</b>	

<b>Waarom is deze RFC nodig?</b>	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.
<b>Gerelateerd aan</b>	
<b>Eigenaar</b>	<a href="#">Rob Brand   Logius</a>
<b>Implementatietermijn</b>	Direct (administratief)
<b>Testcases van toepassing?</b>	
<b>Motivatie verkorte RFC procedure</b>	

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

### Samenvatting

<p><b>Waarom is deze RFC nodig?</b></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><b>Oplossingsrichting</b></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><b>Aanpassing van</b></p>	<p>Normenkader betrouwbaarheidsniveaus</p>
<p><b>Impact op rollen</b></p>	<p>HNP, AD. Voor beide rollen Impact Midden</p>
<p><b>Impact op aanpalende systemen</b></p>	<p>Niet van toepassing</p>
<p><b>Gerelateerd aan</b></p>	<p>Niet van toepassing</p>
<p><b>Eigenaar</b></p>	<p><a href="#">Rob Brand   Logius</a></p>
<p><b>Implementatietermijn</b></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><b>Testcases van toepassing?</b></p>	<p>Niet van toepassing</p>

<p><b>Waarom is deze RFC nodig?</b></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><b>Motivatie verkorte RFC procedure</b></p>	<p>Verkorte RFC procedure niet van toepassing</p>

## 6. RFC's ter bespreking

### 6.1. RFC2357 Toestaan gebruik van Nederlandse rijbewijs model 6I met chip bij Identificatie op Afstand

#### Samenvatting



<b>Waarom is deze RFC nodig?</b>	<p>De huidige <a href="#">Eisen voor Identificatie op Afstand</a> staan het gebruik van rijbewijzen niet toe (zie COL-8.2.3-06). Echter, volgens deze zelfde eisen zou het gebruik van rijbewijzen met een chip mogelijk moeten zijn. Het rijbewijs is in eerste instantie uitgesloten omdat het geen reisdocument is en niet voldoet aan ICAO 9303 part 10 [2]. De betreffende ETSI eis (COL-8.2.3-06) stelt echter dat andere documenten ook ingezet mogen worden, wanneer aangetoond kan worden dat deze vergelijkbaar zijn met een reisdocument in betrouwbaarheid. Met deze RFC willen we het Nederlandse rijbewijs (Model 6I, 14-11-2014) accepteren, waarvoor een onderbouwing is aangeleverd door de Expertgroep normenkaders en onderdeel is van deze RFC.</p> <p>Wanneer andere documenten die niet voldoen aan ICAO 9303 part 10 [2] toegevoegd wensen te worden als geaccepteerd document voor IoA dient dit verzoek ingebracht te worden bij de Expertgroep Normenkaders. De Expertgroep Normenkaders zal beoordelen of het document geaccepteerd kan worden en dit onderbouwen.</p>
<b>Oplossingsrichting</b>	Verwijder het verbod op het gebruik van rijbewijzen.
<b>Aanpassing van</b>	<a href="#">Eisen Identificatie op Afstand</a>
<b>Impact op rollen</b>	MU
<b>Impact op aanpalende systemen</b>	Geen
<b>Gerelateerd aan</b>	<a href="#">RFC2333 vernieuwde eisen Identificatie op Afstand</a>
<b>Eigenaar</b>	<a href="#">Sander Remmerswaal   Digidentity</a>
<b>Implementatietermijn</b>	Direct
<b>Testcases van toepassing?</b>	Deze RFC brengt geen wijzigingen met zich mee op de koppelvlakken en vereist daarmee geen testcases.
<b>Motivatie verkorte RFC procedure</b>	

Toelichting: Rob Brand

## 7. Operationele Uitdagingen

In de brainstorm van december 2020 bleek de wens om operationele aspecten en uitdagingen te bespreken, naast de technische RFC's. 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 aandrazen voor op de [Voorraadagenda OB](#). Volgende vergadering is op 5-jul-2022 van **9.30 tot 11.00** en zal **digitaal (Webex)** plaatsvinden.

## Notulen van OB 77

<b>Vergaderdatum</b>	7-jun-2022		
<b>Tijd</b>	10:00u tot 13:00u (inclusief lunch)		
<b>Locatie</b>	Bij Logius, Wilhelmina van Pruisenweg 52 en Hybride (zie Webex) toegangscode		
<b>Auteur</b>	<a href="#">Joyce Eering   Logius</a>		
<b>Aanwezigen</b>	<a href="#">Sander Boer   Logius</a>	Logius	Voorzitter
	<a href="#">Joyce Eering   Logius</a>	Logius	Secretaris
	<a href="#">Frans de Kok   Logius</a>	Logius	
	<a href="#">Rob Brand   Logius</a>	Logius	
	<a href="#">Bram van Pelt   KPN</a>	KPN	

<b>Vergaderdatum</b>	7-jun-2022		
	<a href="#">Marco Eikenaar   Belastingdienst</a>	Belastingdienst	
	<a href="#">Mark Baas   Reconi</a>	Reconi	
	<a href="#">Hans Milikan   Signicat</a>	Signicat	
	<a href="#">Arien Monster</a>	Gemeente Den Haag	
	<a href="#">Jacques Urlus   NBA</a>	NBA	
	<a href="#">Jan Geert Koops   Dictu</a>	Dictu	Afgemeld
	<a href="#">Douwe Jan Broersma   Digidentity</a>	Digidentity	Afgemeld
	<a href="#">Bernard Stibbe   VZVZ</a>	VZVZ	Afgemeld

**Mededeling videoconferencing:** Het is mogelijk om de vergadering online via Webex te voeren. Zie in de uitnodiging : vergadernummer en wachtwoord.

# 1. Opening

Sander heet iedereen welkom.

- Er is een kwetsbaarheid in de externe omgeving van Confluence geconstateerd. Aan de storing wordt gewerkt en zal worden gecommuniceerd zodra het is verholpen en Confluence weer toegankelijk is.
- Rob Brand, Senior Adviseur IV is uitgenodigd voor toelichting op een 3-tal RFC's, welke zijn geagendeerd namens de Expert werkgroep Normenkaders.
- Afgemeld zijn: Jan Geert, Douwe Jan en Bernard.

## 1.1. Vaststellen agenda

- De OB leden hebben de agenda ook in PDF document ontvangen. Op basis hiervan wordt de agenda OB 77 vastgesteld. Het OB is in de maand mei (OB 76) komen te vervallen.

## 1.2. Vaststellen notulen/actiepunten OB 75

- Het verslag van de vorige meeting, maand april [Notulen van OB 75](#) is vastgesteld. Het Operationeel Beraad is in de maand mei (OB 76) komen te vervallen.

## 1.3. Mededelingen

Sander:

- Arjen Monster gaat per 1 september vertrekken bij Gemeente Den Haag en zal niet meer deelnemen aan het OB. Informatie over zijn opvolger wordt t.z.t. bekend gemaakt.
- Er is weinig update over de WDO. De Wet Digitale Overheid is onlangs behandeld in de 2e Kamer en zal op 7 juni 2022 een vervolg afstemming plaatsvinden over de Novelle.
- Er zijn diverse initiatieven rondom de “Wallet” waarbij verschillende collega’s vanuit BZK en Logius betrokken zijn. Welke raakvlakken het zal hebben met eHerkenning is nog niet bekend. Als hier meer duidelijkheid over is zal het worden geagendeerd in het OB.
- Onlangs zijn nieuwe collega’s bij de Beheerorganisatie Stelsel eHerkenning gestart. Kenneth Smit als Informatiebeveiligingsspecialist en Servaas Schram, Sr. Ketenbeheerder .

## 2. Het Operationeel Beraad

De vergadering vindt na een lange periode weer plaats bij Logius. Een aantal leden maken gebruik van hybride deelname. Streven is om één keer in vier maanden fysiek te vergaderen.

## 3. Update vanuit de Refinement Werkgroep

Een overzicht van de status van RFC's en vooruitblik naar de back log. **Woord aan Bram van Pelt.**

- Voortgebracht zijn twee RFC's ter advies aan het OB. Zie agendapunt 5.1. en 5.2. RFC2348 voor het oplossen van fouten bij Ketenmachtiging en RFC2349 Verduidelijking signing Discovery service.
- Machtingsvrij inloggen; In samenwerking met het Intaketeam heeft overleg met de Refiners plaatsgevonden over identificerende attributen omdat momenteel veel vragen zijn omtrent inloggen zonder machtiging en de mogelijkheid voor eventuele uitschakeling van ketenmachtiging. Frans is hierbij betrokken vanuit het Intaketeam. Verwachting is in komende maand weer stappen te maken door afstemming over de te hanteren uitgangspunten en hoe verder hiermee om te gaan. Verwachting is dat een aantal RFC's

gaan volgen rondom de Koppelvlakken omdat het impact gaat hebben op de Dienstencatalogus en ook functionaliteit van eHerkenning kan wijzigen.

- Meldt dat hij het voorzitterschap voor de Refinement werkgroep gaat overdragen. De voorzittersrol komt hiermee beschikbaar en zal een nieuwe voorzitter worden gekozen. Bram blijft wel lid van het OB.
- Heeft de memo welke namens de RWG is opgesteld aan het TB waarin twee oplossingsrichtingen zijn beschreven rondom de rolverdeling voor het schrijven en beoordelen/refinen van RFC's via John Borst laten agenderen. De memo is vooraf besproken met Douwe Jan en Frank Jonker en zal worden behandeld in het aankomende Leverancieroverleg en het TB .
- Het voorstel voor een nieuwe versioning staat op de back-log ter inventarisatie. Hierover heeft een eerste refinement plaatsgevonden. Bram en Frans pakken de actie op voor vervolg uitwerking van de RFC.
- Joyce gaat een gezamenlijk bijeenkomst plannen met het Intaketeam en het Refinement team voor een reflectie moment. De invulling en de vormgeving van de fysieke bijeenkomst zal worden afgestemd met de voorzitters van de werkgroepen Intake en Refinement.

## 4. Update vanuit het Intake Team

Een overzicht van de status van dossiers en vooruitblik naar de back log (inclusief de link met de Roadmap en EPIC's).

Hans:

- Met de RVO zijn gesprekken gevoerd over de wens voor Intermediar portalen om inzichtelijk te hebben of machtigingen nog actueel zijn. Hans geeft toelichting op het oplossings voorstel en dat RVO hier in 2023 gebruik van wil maken. Het voorstel wordt nader uitgewerkt.
- Heeft een overzicht gemaakt waarin de samenhang van de OHW dossiers verduidelijkt wordt met het Jaarplan eHerkenning. Op basis hiervan wordt de prioriteit van de OHW dossiers in lijn gebracht met het JP 2022.
- Joyce heeft een Kanban Board ingericht met als doelstelling om transparant en Inzichtelijk te hebben aan welke dossier actief wordt gewerkt en door wie en de fase waarin een dossier zich bevindt en wat de voortgang hierop is. Het Kanban bord zal binnenkort in gebruik worden genomen en onderdeel worden van de agenda van het Intake overleg.
- Richard Backx (KPN) heeft zijn deelname overgedragen aan René Bonte (KPN) met ingang van mei 2022.
- Frans heeft gesprekken gevoerd met Enexis t.a.v. API voor machtigingen beheer. De Expert werkgroep NK gaat hiermee aan de slag omdat het normenkader getoetst moet

worden. Het is besproken in het Intakeoverleg waarbij aangegeven is dat het een aangelegenheid is voor een individuele leveranciers. Enexis zal opzoek moeten gaan naar een leverancier voor het specificeren van een koppelvlak en de implementatie.

## **5. RFC's ter advies**

### **5.1. [RFC2348 Oplossen fouten bij Ketenmachtigingen](#)**

#### **Samenvatting**

<p><b>Waarom is deze RFC nodig?</b></p>	<p>"<i>Technical Debt</i>" - Bij het schrijven van <a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a> 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><b>Oplossingsrichting</b></p>	<p>In de huidige specificatie tussen HM en MR2 (ketenmachtiging) staan LegalSubjectID en IntermediaryEntityID in &lt;Request&gt;&lt;Subject&gt; element. Echter met de introductie van r1.11 is er destijds besloten om in het &lt;Subject&gt; 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 <a href="https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption">https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption</a>). 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"> <li>• HM-MR1 - IntermediarySubjectID toevoegen aan MR1 response in &lt;Request&gt;&lt;Subject&gt;</li> <li>• HM-MR2 - LegalSubjectID en IntermediaryEntityID uit XACMLAuthzDecisionQuery &lt;Request&gt;&lt;Subject&gt; element halen</li> <li>• HM moeten voor backward compatibiliteit zorgen voor DV</li> <li>• HM moeten met oude en nieuwe MR2-assertions om kunnen gaan zodat MR2 flexibel is met het implementeren van de RFC.</li> </ul>
<p><b>Aanpassing van</b></p>	<p>Specificaties van HM-MR en de bijbehorende processing rules i.g.v. Ketenmachtiging</p>
<p><b>Impact op rollen</b></p>	<p>Alle HM en elke MR die ketenmachtigingen verstrekt (MR2).</p> <p>DV die Intermediate.EntityID gebruiken uit de HM-samenvatting of LegalSubjectID halen uit de (in &lt;Advice&gt; 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>

<b>Waarom is deze RFC nodig?</b>	" <i>Technical Debt</i> " - Bij het schrijven van <a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a> 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.
<b>Impact op aanpalende systemen</b>	n.v.t.
<b>Gerelateerd aan</b>	<a href="#">RFC2249 Verplicht leveren company name bij ketenmachtigen</a>
<b>Eigenaar</b>	<a href="#">Frans de Kok   Logius</a>
<b>Implementatietermijn</b>	Vereist eenvoudig implementatieplan <ul style="list-style-type: none"> <li>• MR2 zal de RFC uiterlijk geïmplementeerd moeten hebben op en nader te bepalen koppelvlakrelease (waarbij het de verplichting van ketenmachtigingen in scope zit).</li> <li>• HM zal de RFC geïmplementeerd moeten hebben voordat of tegelijk met de eerste MR2 die deze RFC implementeert.</li> <li>• 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).</li> </ul>
<b>Testcases van toepassing?</b>	
<b>Motivatie verkorte RFC procedure</b>	

Frans geeft toelichting op de RFC en op de antwoorden n.a.v. de opmerkingen en vragen uit het OB 75\_april 2022. Hierin is eveneens toegevoegd de verduidelijking dat het een koppelvlak wijziging betreft naar dienstverleners. Tenslotte zijn tevens ter verduidelijking een paar tekstuele aanpassingen gedaan i.s.m. de Refinement werkgroep.

**OB 77:** Positief advies naar het TB met de aanvulling van het implementatietermijn tot een nader te bepalen datum.



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

### Samenvatting

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

Bram geeft toelichting op de RFC en op de antwoorden welke hierin zijn opgenomen n.a.v. de opmerkingen en vragen uit het OB 75\_april 2022.

**OB 77:** Positief advies naar het TB.

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

### Samenvatting

<b>Waarom is deze RFC nodig?</b>	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.
<b>Oplossingsrichting</b>	Het BSN zal bij de registratie van persoonsgegevens worden uitgevraagd, of kan later worden toegevoegd.
<b>Aanpassing van</b>	Normenkader Betrouwbaarheidsniveaus
<b>Impact op rollen</b>	MU
<b>Impact op aanpalende systemen</b>	
<b>Gerelateerd aan</b>	
<b>Eigenaar</b>	<a href="#">Rob Brand   Logius</a>
<b>Implementatietermijn</b>	Direct (administratief)
<b>Testcases van toepassing?</b>	
<b>Motivatie verkorte RFC procedure</b>	

Rob geeft toelichting op de voorgestelde wijziging. N.a.v. de discussie over het implementatietermijn bij registratie BSN wordt vastgesteld dat de implementatietermijn op “Direct “ blijft staan. Het gaat hier namelijk om een verduidelijking van de bestaande werkwijze en blijft de implementatietermijn dus op “Direct “ staan.

Algemene opmerking aan de Expertgroep Normenkader en het verzoek om bij het schrijven van de RFC, goed te kijken naar de leesbaarheid en duidelijke taal van de teksten.

**Afspraak:** Aanhouden totdat de storing met Confluence is verholpen en de antwoorden op de vragen en opmerkingen geraadpleegd kunnen worden in Confluence. Het advies van het OB zal vervolgens worden opgehaald middels een schriftelijke ronde.

**OB 77:** Positief advies naar het TB. Vastgesteld op 16 juni 2022 na een schriftelijk uitvraag.

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

### Samenvatting

<p><b>Waarom is deze RFC nodig?</b></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><b>Oplossingsrichting</b></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><b>Aanpassing van</b></p>	<p>Normenkader betrouwbaarheidsniveaus</p>
<p><b>Impact op rollen</b></p>	<p>HNP, AD. Voor beide rollen Impact Midden</p>
<p><b>Impact op aanpalende systemen</b></p>	<p>Niet van toepassing</p>
<p><b>Gerelateerd aan</b></p>	<p>Niet van toepassing</p>
<p><b>Eigenaar</b></p>	<p><a href="#">Rob Brand   Logius</a></p>
<p><b>Implementatietermijn</b></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><b>Testcases van toepassing?</b></p>	<p>Niet van toepassing</p>

<p><b>Waarom is deze RFC nodig?</b></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><b>Motivatie verkorte RFC procedure</b></p>	<p>Verkorte RFC procedure niet van toepassing</p>

Rob geeft toelichting op de voorgestelde wijziging. Op advies van de leden wordt de implementatiedatum van de VIS check veranderd in "nader door het leveranciersoverleg te bepalen".

**Afspraak:** Aanhouden totdat de storing met Confluence is verholpen en de antwoorden op de vragen en opmerkingen geraadpleegd kunnen worden in Confluence. Het advies van het OB zal vervolgens worden opgehaald middels een schriftelijke ronde.

**OB 77:** Positief advies naar het TB. Vastgesteld op 16 juni 2022 na een schriftelijk uitvraag.

## 6. RFC's ter bespreking

## 6.1. RFC2357 Toestaan gebruik van Nederlandse rijbewijs model 6I met chip bij Identificatie op Afstand

### Samenvatting

<b>Waarom is deze RFC nodig?</b>	<p>De huidige <a href="#">Eisen voor Identificatie op Afstand</a> staan het gebruik van rijbewijzen niet toe (zie COL-8.2.3-06). Echter, volgens deze zelfde eisen zou het gebruik van rijbewijzen met een chip mogelijk moeten zijn. Het rijbewijs is in eerste instantie uitgesloten omdat het geen reisdocument is en niet voldoet aan ICAO 9303 part 10 [2]. De betreffende ETSI eis (COL-8.2.3-06) stelt echter dat andere documenten ook ingezet mogen worden, wanneer aangetoond kan worden dat deze vergelijkbaar zijn met een reisdocument in betrouwbaarheid. Met deze RFC willen we het Nederlandse rijbewijs (Model 6I, 14-11-2014) accepteren, waarvoor een onderbouwing is aangeleverd door de Expertgroep normenkaders en onderdeel is van deze RFC.</p> <p>Wanneer andere documenten die niet voldoen aan ICAO 9303 part 10 [2] toegevoegd wensen te worden als geaccepteerd document voor IoA dient dit verzoek ingebracht te worden bij de Expertgroep Normenkaders. De Expertgroep Normenkaders zal beoordelen of het document geaccepteerd kan worden en dit onderbouwen.</p>
<b>Oplossingsrichting</b>	Verwijder het verbod op het gebruik van rijbewijzen.
<b>Aanpassing van</b>	<a href="#">Eisen Identificatie op Afstand</a>
<b>Impact op rollen</b>	MU
<b>Impact op aanpalende systemen</b>	Geen
<b>Gerelateerd aan</b>	<a href="#">RFC2333 vernieuwde eisen Identificatie op Afstand</a>
<b>Eigenaar</b>	<a href="#">Sander Remmerswaal   Digidentity</a>
<b>Implementatietermijn</b>	Direct
<b>Testcases van toepassing?</b>	Deze RFC brengt geen wijzigingen met zich mee op de koppelvlakken en vereist daarmee geen testcases.
<b>Motivatie verkorte RFC procedure</b>	

Rob: De RFC wordt toegelicht en besproken.

Afspraak OB 77:

Rob zal de vraag “Wat te doen wanneer andere documenten die niet voldoen aan ICAO 9303 part 10 [2] en toegevoegd wensen te worden als geaccepteerd document voor IoA” meenemen naar de Expertgroep Normenkaders en verder uitzoeken. De uitkomst hierover zal hij opnemen in de RFC. De RFC zal in het volgende OB, 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 RFC's. Dit agenda onderdeel biedt daar ruimte voor. Het woord aan degenen die iets willen delen.

Bram:

- BSNk wijzigt van P1 sleutelnummer en staat gepland op 20 juni voor de productie. Hij heeft vernomen dat BSNk alleen versie P2 gaat ondersteunen en versie P1 gaan uitfaseren. Het is niet duidelijk in hoeverre dit bericht klopt en welke problemen en impact het tot gevolg zal hebben. Hans heeft overleg met BSNk tijdens een RKO planning en zal het hierin meenemen en terugkoppeling geven aan.

Sander:

- De insteek voor het stelsel Peppol (de internationale standaard voor het verzenden, ontvangen en verwerken van elektronische facturen) is dat deze moet voldoen op substantieel niveau. Momenteel wordt nagedacht over hoe eHerkenning hierbij kan helpen. Het biedt wellicht een kans voor de OB leden om hieraan bij te dragen en de samenwerking op te zoeken.

## 8. WVTTK

- Namens het OB bedankt Sander, Arjen Monster voor zijn bijdrage en fijne samenwerking en wenst hem succes toe!

## 9. Afsluiting

Rondje langs de velden. Deelnemers kunnen hier suggesties aandrazen voor op de [Voorraadagenda OB](#). Volgende vergadering is op 5-jul-2022 van **9.30 tot 11.00** en zal **digitaal (Webex) plaatsvinden**.