

Notulen van OB 89

Vergaderdatum	4-jul-2023		
Tijd	09:30u tot 11:00u		
Locatie	Teams (zie Teams) toegangscode		
Auteur	Joyce Eering Logius		
Aanwezigen	Kolette Visser	Logius	Voorzitter (tijdelijk)
	Joyce Eering Logius	Logius	Secretaris
	Frans de Kok Logius	Logius	
	Servaas Schrama Logius	Logius	
	Bram van Pelt KPN	KPN	
	Marco Eikenaar Belastingdienst	Belastingdienst	
	Mark Baas Reconi	Reconi	
	René Bonte Reconi	Reconi	
	Marco Bonsink UnifiedPost	UnifiedPost	
	Hans Milikan Signicat	Signicat	
	Jacques Urlus NBA	NBA	
	Jan Geert Koops Dictu	Dictu	
	Douwe Jan Broersma Digidentity	Digidentity	
	Bernard Stibbe VZVZ	VZVZ	Afgemeld

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

1. Opening

- [Kolette Visser](#) heet iedereen welkom.

1.1. Vaststellen agenda

- Agendapunt 5.1 t.a.v. RFC2358 zal bij nader inzien niet worden besproken. Frans de Kok zal een korte update geven over de status en voortgang rondom het aanleveren van de gegevens die in de maandrapportage.
- Bernard Stibbe heeft zich afgemeld.
- De agenda wordt vastgesteld.

1.2. Mededelingen

Kolette:

De omschrijvingen van de aangeboden RFC's waren voor het TB niet duidelijk genoeg waardoor er discussie ontstond met als resultaat dat het TB de RFC's niet wilde goedkeuren. Afgesproken werd om de notitie met omschrijvingen te verduidelijken en vervolgens met een schriftelijke ronde een akkoord op te halen van het TB op de inhoud van release 1.13 22 juni 2023. De reden voor deze schriftelijke ronde was in de komende PI planning en release betreffende RFC's:

- RFC2383: Attributencatalogus niet-natuurlijke personen uitbreiden met TRR en
- RFC2387: Introductie ECTA TRR-BD.

De deadline is 5 juli en de verwachting is dat het TB de aangeboden RFC's goedkeurt.

Belangrijk om goed toe te zien dat een RFC een heldere omschrijving heeft waarom de RFC nodig is.

- In Q2-2023 heeft het Tactisch Beraad een aantal RFC's goedgekeurd. Deze zijn inmiddels verwerkt door de Beheerorganisatie. Binnenkort zal de nieuwe versie: 1.1.3 22 juni 2023 van het Afsprakenstelsel worden gepubliceerd.

1.3. Vaststellen notulen OB 88

- Het verslag van de vorige meeting [Notulen van OB 88](#) zijn vastgesteld.

2. 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 [René Bonte](#) | [Reconi](#).**

Afgelopen periode is gewerkt aan de dossiers:

- I.h.k.v. de inrichting van het Change en release proces verbeteren/vernieuwen wordt samen met o.a. Hans Milikan en Frank Jonker gewerkt aan een nieuwe integrale kwartaalrapportage met planning voor de komende vier kwartalen.
- De notities vanuit de VeHa ETD onder Stelsel Toegang en Beschouwingen Stelsel Toegang Bedrijvendomein v1.0 zijn behandeld in het Petit Comité en verstuurd naar BZK. Er is nog geen reactie hierop ontvangen van BZK.
- Gesprekken vinden regelmatig plaats rondom de Doelarchitectuur Toegang 0.9 met Hans Rob de Reus en vertegenwoordigers van de Leveranciers. Frans de Kok en René zijn aangehaakt bij de besprekingen over de Domein Doelarchitectuur.
- Vanuit de werkgroep TRR is een aantal RFC's voortgebracht voor advies en besluitvorming in het OB en TB. Het dossier TRR zit niet meer in de Intake fase.
- Werkt aan een verzamel RFC voor tekstuele correcties in het AS. Voorstel is om 1 x per kwartaal een verzamel RFC voort te brengen ter besluitvorming in de Governance voor het doorvoeren van tekstuele correcties op het AS.

Er zijn meer dossiers [Onderhanden](#) bij het Intake team, daarop zijn enkele planningsaanpassingen gemaakt. Voor een laatste status, zie [Planning eHerkenning - Intake Team - Confluence](#)

3. Update vanuit de Refinement Werkgroep

Een overzicht van de status van RFC's en vooruitblik naar de back log. **Woord aan [Marco Bonsink | UnifiedPost](#)** .

De dossiers waaraan de werkgroep recent heeft gewerkt of nog mee bezig is, zijn:

- Op verzoek van Hans Milikan heeft de RWG feedback en vragen beantwoord rondom de uit te brengen portaal diensten functionaliteit.
- Review en feedback is geleverd op de laatste versie TRR API documentatie aan Eric de Vries en Douwe Jan Broersma.
- Dossier versienummering; RFC2338 wordt volledig gemaakt door Frans de Kok. Na final refinement zal het ter advies worden geagendeerd in het OB.
- RFC2377 t.a.v. onduidelijkheid over het versleutelen van attributen met meerdere certificaten. Op de RFC heeft refinement plaatsgevonden en zijn de comments t.a.v. "Multi Recipients" en is het voorstel om de "tekst (regel)" bij Multi Recipients te verwijderen opnieuw besproken. De RFC staat op de agenda (4.1.) ter advies.
- Review dossier SSO verplichten heeft plaatsgevonden i.s.m. Marco Bonsink en Rene Bonte.
- Refinement heeft plaatsgevonden op twee administratieve RFC's. Deze staan op de agenda van het aankomende OB ter bespreking.
 - [RFC2392 Levering attribuut KvKnr optioneel maken.](#)

- [RFC2358 Nieuw format aanleveren gegevens tbv maandrapportage](#)

4. RFC's ter advies

4.1 [RFC2377 - Duidelijkheid over multi-valued attributen - Change management eToegang - Confluence \(eherkenning.nl\)](#)

Samenvatting

Waarom is deze RFC nodig?

Aanleiding is mantis ticket waaruit blijkt dat klanten van één ETD-Leverancier niet meer in kunnen loggen in het UWV portaal.

De UWV heeft een probleem bij een authenticatie verzoek voor hun 'portaal-dienst' omdat er in het antwoord een versleuteld attribuut zit dat met twee verschillende (UWV) certificaten is versleuteld. UWV verwacht dat de versleuteling maar met één specifiek UWV-certificaat gebeurt, namelijk het certificaat dat in de Dienstcatalogus staat bij de betreffende 'Portaaldienst'.

De meeste ETD-Deelnemers gebruiken inderdaad dat ene certificaat bij de Portaaldienst. Echter één ETD leverancier gebruikt niet het certificaat van de Portaaldienst, maar elk (uniek) certificaat van elke Dienst die in de Portaaldienst zit. Meestal zal elke Dienst in de Portaaldienst hetzelfde certificaat hebben. Maar bij de UWV hebben 2 van de 8 Diensten bij deze Portaaldienst een ander UWV-certificaat.

Volgens specificaties zijn beide manieren van versleuteling met certificaten toegestaan. En het versleutelen van attributen met elk (uniek) certificaat van elke Dienst verdient daarbij misschien wel de voorkeur. Immers in het UWV-Portaal zitten klaarblijkelijk individuele Diensten die op verschillende platformen draaien en daarom geen sleutelmateriaal kunnen delen. En de Diensten op beide platformen moeten mogelijk de waarde van een attribuut kunnen ontsleutelen.

Er zijn nog meer situaties waarin er meerdere waardes kunnen zitten in een versleuteld attribuut:

- Een DV kan zelf (bijv ihkv een infrastructuur- of applicatie-migratie) ook twee certificaten in de dienstcatalogus zetten voor een Dienst. Ook dan wordt elke versleuteling gedaan met beide certificaten.
- Een DV kan zelf bij een certificaat-wissel ok ook tijdelijk twee certificaten in de dienstcatalogus zetten voor een Dienst. Ook dan wordt elke versleuteling gedaan met beide certificaten.
- Igv Dienstbemiddeling kunnen er (versleutelde) waardes in een attribuut zitten die niet eens voor de betreffende Dienstverlener zijn.

<p>Oplossingsrichting</p>	<p>Een DV moet er rekening mee houden dat een <i>Attribuut</i> (of <i>Identificerend Kenmerk</i>) versleuteld kan worden met meerdere certificaten, optioneel zelfs voor meerdere <i>Recipients</i> (ontvangende partijen), zie https://afsprakenstelsel.etoegang.nl/display/as/SAML+encryption. Bij het ontsleutelen zal de DV moeten kijken naar zijn eigen <i>EntityID</i> in '<i>Recipient</i>' én naar de '<i>KeyName</i>' die hoort bij het DV-certificaat (en bijbehorende private-key) waar de DV het attribuut mee kan ontsleutelen. In het AS wordt gerefereerd naar https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html#sec-eg-EncryptedKey waar staat dat je naar deze <i>KeyName</i> moet kijken maar in het AS staan niet expliciet dat er voor de zelfde <i>Recipient</i> meerdere (<i>EncryptedKeys</i> met verschillende) <i>KeyNames</i> gebruikt kunnen worden. Dit zou veel duidelijker kunnen.</p> <p>De Dienstverleners moeten zorgen dat de specificaties goed geïmplementeerd worden. En de Makelaars moeten hun klanten daarbij helpen. In dit soort situaties waarin een Dienstverlener de specificaties onvolledig implementeren en daarmee Gebruikers buiten kunnen sluiten van een specifieke ETD-Leverancier heeft de Makelaar een extra verantwoordelijkheid. Liefst heeft de Makelaar al tijdens het aansluiten zeker gesteld dat de Dienstverlener om kan gaan dat dit kan voorkomen.</p> <p>De Makelaars zijn verantwoordelijk om te zorgen dat Gebruikers van een specifieke ETD Leverancier niet uitgesloten worden doordat deze (binnen de specificaties) meerdere waardes in de attributen mee stuurt.</p>
<p>Aanpassing van</p>	<p>Specificaties - processing rules</p>
<p>Impact op rollen</p>	<p>HM en DV</p>
<p>Impact op aanpalende systemen</p>	
<p>Gerelateerd aan</p>	<p>Mantis ticket https://issues.eherkenning.nl/view.php?id=11202</p>
<p>Eigenaar</p>	<p>Mada Miesen KPN</p>
<p>Implementatietermijn</p>	<p>Wat betreft de technische specificaties is het een administratieve verduidelijking en kan deze RFC direct verwerkt worden. Echter een implementatie termijn zou moeten beginnen met een inventarisatie door Makelaars, die daarna een plan moeten bedenken om hun klanten daarbij helpen.</p>
<p>Testcases van toepassing?</p>	<p>Helaas zijn er geen Testcases voor DV (onboarding) in het afsprakenstelsel.</p>
<p>Motivatie verkorte RFC procedure</p>	

Toelichting: [Frans de Kok | Logius](#) is bij nader inzien gestart met een herstel RFC. Zie [RFC2398 Herstel 'DeprecatedActingSubjectID' - Change management eToegang - Confluence \(eherkenning.nl\)](#) opgesteld. Deze volgt t.z.t. op de agenda ter bespreking.

Opmerkingen:

- Jan Geert: Is niet eens met de wijziging zoals beschreven in de RFC en wil de verplichting voor DV's om de "multiple recipients" en "multiple certificaten" (attributen) te ondersteunen verwijderd hebben. Dit geeft wederom enige discussie.
- De HM's geven een positief advies op de RFC aan het TB. Handreiking door Hans Milikan. Hij zal een overleg met de makelaars organiseren waarbij gesproken zal worden over hoe in de toekomst dit probleem te voorkomen.

Afspraak OB 89: Positief advies. Voortbrengen voor besluitvorming in het TB.

5. RFC's ter bespreking

5.1 [RFC2358 Nieuw format aanleveren gegevens tbv maandrapportage](#)

Samenvatting

Waarom is deze RFC nodig?	In de huidige situatie worden te verwerken gegevens in diverse en afwijkende formaten aangeleverd. Dit hindert de verwerking ervan. Door over te gaan op één format wordt de verwerking eenvoudiger, waardoor sneller kan worden gerapporteerd. Daarnaast is dit een voorbereiding op de overgang naar Power BI, waar de rapportage in de toekomst in zal worden verwerkt.
Oplossingsrichting	Om de verwerking van de maandrapportage kwalitatief te verbeteren vragen we van alle deelnemers om een door ons gespecificeerd format te gaan gebruiken voor het aanleveren van de gegevens die in de maandrapportage worden verwerkt. Het voorgestelde format is bijgevoegd in deze RFC.
Aanpassing van	Operationeel handboek
Impact op rollen	geen impact op DV's, wel op AD, MR, HM
Impact op aanpalende systemen	Geen impact

Waarom is deze RFC nodig?	In de huidige situatie worden te verwerken gegevens in diverse en afwijkende formaten aangeleverd. Dit hindert de verwerking ervan. Door over te gaan op één format wordt de verwerking eenvoudiger, waardoor sneller kan worden gerapporteerd. Daarnaast is dit een voorbereiding op de overgang naar Power BI, waar de rapportage in de toekomst in zal worden verwerkt.
Gerelateerd aan	<i>Maandrapportage XML Aggregator;</i> Aanlevering Maandrapportages ; <i>Afstemming met Hendricus Wind en Frans de Kok.</i>
Eigenaar	Servaas Schrama Logius
Implementatietermijn	Direct
Testcases van toepassing?	Niet nodig
Motivatie verkorte RFC procedure	Het stelsel heeft baat bij snel in werking treden van deze RFC, in de vorm van snellere verwerking van gegevens in de rapportage, alsmede de verbetering in de kwaliteit van de rapportage.

[Frans de Kok | Logius](#) Deze RFC staat onterecht ter bespreking. Frans, geeft een korte toelichting op de voortgang en laatste ontwikkelingen t.a.v. de volgende punten:

- Nieuw format JSON is voorgelegd aan de RWG en is feedback gevraagd op de specificaties aanleveren van gegevens.
- De twee methodes voor het transporten van de gegevens wordt momenteel besproken en zal t.z.t. worden beschreven en worden toegevoegd in deze RFC.
- Het aanleveren van Delta gegevens is niet meer nodig. De gegevens van de oude maand zal worden herschreven door de nieuwe aangeleverde gegevens.
- Hans vraagt aandacht voor de link in de servicerapportage (gegevens van de MR en de DC) en om hier nader naar te kijken.

Afspraak OB 89: De RFC zal na afstemming in de Intake werkgroep en final refinement (RWG) t.z.t. worden voortgebracht naar het OB ter bespreking.

5.2 [RFC2382 Aanpassing woord authenticatiemiddel incl. nieuwe definitie in Gebruiksvoorwaarden](#)

Samenvatting

Waarom is deze RFC nodig?	<p>In het normenkader zijn de woorden "token" en "authenticatiemiddel" vervangen door het woord "middel". Tevens is in de begrippenlijst het woord "middel" uitgelegd waarbij de huidige definitie uit de eIDAS verordening van een Elektronisch identificatiemiddel (nader te noemen "middel") is overgenomen. Zie RFC2371.</p> <p>Echter in het AS waaronder de gebruiksvoorwaarden komt het woord "authenticatiemiddel" nog steeds voor waardoor er weer ruis ontstaan in de gebruikte begrippen. Om niet nogmaals onduidelijkheid te creëren wordt met deze RFC ook het woord "authenticatiemiddel" vervangen door het woord "middel" inclusief de aanpassing van de definitie.</p>
Oplossingsrichting	Met deze RFC wordt de onduidelijkheid rondom het woord "authenticatiemiddel" weggenomen, omdat deze door één nieuwe term vervangen wordt zoals ook in het Normenkader is gebeurd. De definitie van "authenticatiemiddel" zal aangepast worden naar de definitie uit de eIDAS verordening van een Elektronisch identificatiemiddel (nader te noemen "middel").
Aanpassing van	AS / Gebruiksvoorwaarden
Impact op rollen	geen impact
Impact op aanpalende systemen	geen impact
Gerelateerd aan	RFC2371
Eigenaar	Kolette Visser
Implementatietermijn	Direct (administratief)
Testcases van toepassing?	nvt
Motivatie verkorte RFC procedure	Het betreft een verduidelijking en daarmee alleen een tekstuele aanpassing.

Toelichting: [Kolette Visser](#)

Opmerking: ontvangt compliment voor de goede search en replace en fijn dat de term "middel" uniform gehanteerd gaat worden. Verzoek om het woord "middel" te linken naar de "begrippenlijst".

Afspraak OB 89: Positief, volgende keer in het OB 90 ter advies agenderen.

5.3 [RFC2392 Levering attribuut KvKnr optioneel maken](#)

Samenvatting

Waarom is deze RFC nodig?	Volgens de Attributencatalogus niet-natuurlijke personen is de registratie van het attribuut KvKnr (door een MachtigingsRegister) verplicht voor elke niet-natuurlijke persoon. Echter als een niet-natuurlijke persoon geregistreerd wordt op basis van het PROBAS of TRR register, is het attribuut KvK-nr niet beschikbaar omdat een (niet-natuurlijke) persoon in deze registers geen KvK-nr heeft.
Oplossingsrichting	Maak de registratie van attribuut KvK-nr voor niet-natuurlijke personen optioneel in de attribuut catalogus niet-natuurlijke personen.
Aanpassing van	Attributencatalogus niet-natuurlijke personen
Impact op rollen	MR
Impact op aanpalende systemen	-
Gerelateerd aan	
Eigenaar	Frans de Kok Logius
Implementatietermijn	Direct (administratief)
Testcases van toepassing?	
Motivatie verkorte RFC procedure	RFC2392 is heel kleine aanpassing die onvermijdelijk is (PROBAS en TRR hebben geen KvK-nr dus KvK-nr kan voor deze groepen niet geregistreerd worden). Het is een administratieve correctie op de TRR/PROBAS RFC's die al goedgekeurd zijn. De RFC wordt nog wel via email ter informatie aangeboden aan de Refinement Werkgroep.

Toelichting: [Frans de Kok | Logius](#)

- Interne controle door de BO (vinkjes) nog niet volledig.

Afspraak OB 89: Positief, volgende keer in het OB 90 ter advies agenderen.

6. Operationele Uitdagingen/WVTTK

Dit agenda onderdeel biedt ruimte om operationele aspecten en uitdagingen te bespreken, naast de technische RFC's. Rondje langs de velden. Het woord aan degenen die iets willen delen.

Frans:

- Aankondiging is gedaan door het Aggregator Team dat controles weer uitgevoerd gaan worden. Deze actie is ingang gezet i.v.m. achterstallig onderhoud op controles, vooral t.a.v. certificaten waarbij veel controles uitgezet werden. De backlog met de planning voor het opleveren en aanzetten controles is beschikbaar. Er gaat gestart worden met testen in de pre-productie.

Douwe Jan:

- Geeft aan niet tevreden te zijn over de aanpak en afhandeling van de Mantis-melding door UWV. Hij herhaalt de opmerking uit het vorige OB over de te lange doorlooptijd van de analysefase en het vinden van een oplossing/antwoord. Hij zal een voorstel doen om de aanpak en voortgang te evalueren.

7. Afsluiting

Het OB in de maand augustus komt te vervallen i.v.m. de zomervakanties. De volgende vergadering is op 5-sep-2023 van 9.30 tot 11.00 en zal digitaal (Teams) plaatsvinden.