

team Stelsendiensten

bezoekadres:
Wilhelmina van Pruisenweg
52
Den Haag

Contactpersoon
Charlotte Adama

charlotte.adama@logius.nl

Datum
21 juni 2016

Kenmerk

verslag

technisch overleg Digikoppeling

Vergaderdatum	21 juni 2016
Deelnemers	E. Spitsbaard (Logius); M. van der Plas (Logius), P. Hering (Logius), H. Romein (DICTU); F. Terpstra (Enable-U), T. Vijlbrief (Kadaster), M. Backer (KING), H. Stekelenburg (KvK), S. Hadiutomo (BKWI), T. Zwaan (BKWI), E. Reinhout (Kennisset); M. van den Brink (Belastingdienst), H. Sinnige (RINIS); G. Groot Roessink (DUO); C. Adama, notulist (Logius)
Status	concept

1. Opening en Mededelingen

- Update doorontwikkeling Digikoppeling portaal: deze wordt getest, de eerste tests zijn positief. In reactie op een eerdere mailing met de vraag om testers; hebben zich tien partijen gemeld die gaan meetesten vanaf eind juni.
Digikoppeling portaal 2.0: wordt aan gewerkt. Een impactanalyse moet gaan leiden tot een uiteindelijk ontwerp. Vanuit het Kadaster is ook iemand aangehaakt bij het project, specifiek voor het beschikbaar stellen van het portaal binnen Diginetwerk.
Het voorstel van Justid voor de CPA Creatievoorziening is vandaag intern (binnen Logius) geaccepteerd en de CPA C zal in de release van oktober in Digikoppeling portaal 2.0 beschikbaar zijn.
- Update project Informatievoorziening Digikoppeling: het projectteam heeft een aantal nieuwe leden. De probleemstelling die in de klankbordgroep is vastgesteld, is nu omgezet in eisen. Er is een eerste aanzet gedaan voor een ontwerp. Emily zal binnenkort de klankbordgroep mailen met een vervolgplanning.
- De beschrijvingen van PKI Overheid certificaten zijn aangepast (SHA1 → SHA2): deze stond nog op de actielijst van het vorige TO DK. Op de Logiuspagina's van PKI overheid zou SHA1 nog genoemd zijn, dit is nu weg.
- Sheila Alting van Geusau-Ghosh, productarchitect Digikoppeling beëindigt haar werkzaamheden voor Digikoppeling per 1-7-2016. Voor OIN blijft ze tot

eind dit jaar nog wel 1 dag in de week aangehaakt. Haar rol wordt overgenomen door Martin van der Plas

2. Verslag en actielijst van 20 april 2016

Het verslag wordt ongewijzigd vastgesteld.

3. Ter informatie: notitie stand van zaken REST

Pieter Hering geeft aan dat de notitie een inleiding is op dit onderwerp. Hij heeft geprobeerd in kaart te brengen wat er allemaal speelt rondom REST. Dit is ook in het GAB besproken. Leden van het TO Digikoppeling geven aan dat dit prettig is.

4. Presentatie REST tov SOAP WSDL

Presentatie door Frank Terpstra, Enable-U, naar aanleiding van een opdracht m.b.t. REST voor het Forum Standaardisatie.

Het Forum heeft veel vragen gekregen over REST: wat is het precies en wanneer gebruik je het?

Voor de inhoud wordt verwezen naar de als bijlage meegezonden presentatie. Hier wordt volstaan met de weergave van de discussie/vragen.

Gevraagd wordt hoe REST tot stand is gekomen en wat het oogmerk is. Belangrijk oogmerk is zoveel mogelijk gebruikers te bedienen, zie ook de presentatie.

Eind jaren 90 is REST bijna gelijktijdig met SOAP ontstaan. Dit is ook de tijd waarin Digikoppeling ontstond. Het omslagpunt in populariteit van REST kwam eigenlijk vlak hierna.

SOAP is geschikt om specifieke berichten met een bekende groep gebruikers uit te wisselen. Er wordt op dit moment nog gewerkt aan standaarden voor REST, bijv. authenticatie. Verwacht wordt dat REST SOAP/WSDL niet op elk gebied zal vervangen. Nieuwe applicaties, vooral op het gebied van mobiele raadpleegfunctionaliteit, krijgen in de regel eerder een REST API dan een SOAP/WSDL interface. Bestaande applicaties blijven op SOAP/WSDL.

Van belang is om inzichtelijk te maken wat de markt wil en waar de markt mee bezig is.

De nieuwe situatie is dat er veel verschillende kanalen bij zijn gekomen die internet gebruiken en op verschillende manieren bediend willen worden (zoals smart cities, mobile devices, smart watches etc.).

Bij SOAP WSDL is de logistieke laag (waarmee je o.a. kunt valideren etc.) erg dik. Bij REST zit dit er niet in. Doordat dit een veel kleiner en compacter bericht is wordt met REST een veel hogere performance behaald.

REST is vooral sterk in gegevensuitwisseling naar applicaties en een groot publiek waarvan je niet hoeft te weten wie ze zijn. SOAP heeft nog steeds meer functionaliteiten met betrekking tot het faciliteren van ketenprocessen. Het gaat erom dat het de programmeurs gemakkelijker gemaakt wordt. Wat je ziet met REST is dat er vaak een dominante partij is. De vraag is hoe een standaardisatie-instituut een dominante partij zou kunnen worden.

Naar aanleiding van het onderzoek is een drietal aanbevelingen gedaan: a.) een handreiking RESTful APIs (hoe kun je hier als overheid mee omgaan), b.) toetsen op standaarden (om inzicht te krijgen in REST standaarden), c.) implementatie analyse (om meer inzicht te krijgen in de gebruiksvriendelijkheid). Deze laatste aanbeveling is niet overgenomen, de andere twee wel.

Paul Dam is in opdracht van het Bureau Forum Standaardisatie bezig met het organiseren van een sessie op 7 juli.

Gevraagd wordt wat de frequentie is waarmee we in de gaten kunnen houden wat de ontwikkelingen zijn m.b.t. REST. Lancelot Schellevis, heeft op 21 juni een presentatie gegeven aan de Regieraad Interconnectiviteit. Behalve het verspreiden van de kennis hierover zijn er nog geen plannen gemaakt.

5. Uitkomsten WS-RM onderzoek

Toelichting door Pieter Hering, Logius:

In de afnemersraad werd de vraag gesteld wat er met WS-RM wordt gedaan, omdat de indruk was dat hier weinig gebruik van wordt gemaakt en er daardoor weinig leveranciers zijn die dit aanbieden. Uit de afnemersraad kwam het verzoek om te onderzoeken wat de huidige stand van zaken is van de implementatie van WS-RM. Aan één van de leveranciers van Logius is gevraagd om dit onderzoek uit te voeren, namelijk Deloitte. Uit het onderzoek kwam naar voren dat WS-RM weinig tot niet wordt gebruikt.

De opdrachtgever van Logius (Binnenlandse Zaken) gaat navragen wat de status is bij de BRO en BRP. Zij hebben namelijk expliciet aangegeven WS-RM nodig te hebben en te willen aanbieden. Dit wordt in de afnemersraad op de agenda gezet. Hierna komt dit bij de Regieraad gegevens: wat te doen met het WS-RM deel binnen Digikoppeling 3.0.

De vraag is ook of dit op de pas-toe-leg-uit-lijst moet komen en of dit verplicht gesteld moet worden.

Henk Romein geeft aan dat bij DICTU ook een WS-RM implementatie is conform Digikoppeling. Probleem daarbij was dat de Digikoppeling standaard van relatief hoge versies van onderliggende software uit gaat.

→ Actie: Pieter zal navragen welke leveranciers in het onderzoek van Deloitte ondervraagd zijn.

Een oproep voor de volgende keer: zijn er nog meer organisaties die iets met WS-RM gaan doen?

6. Presentatie nieuwe compliancevoorziening

Live demo door Martin van der Plas, Logius van het Digikoppeling portaal 1.0 op de ontwikkelomgeving van ICTU. Dit is volledig op open source gebaseerd.

Er is een DART tool ontwikkeld voor de beheerders van Logius om WUS/WSRM berichten naar onszelf te kunnen sturen en er wordt gebruik gemaakt van de reeds bestaande ebMS console om ebMS berichten te kunnen sturen.

De rapportages van de tests zijn terug te vinden in het Digikoppeling portaal. Op dit moment wordt deze nog getest op de acceptatieomgeving. Zodra deze operationeel is kunnen we hier nog meer laten zien. In het Digikoppeling portaal kun je ook de WSDL's downloaden, die je kunt overnemen en in je eigen applicatie kunt laten inlezen om berichtenverkeer met WS-RM uit te wisselen.

Vanaf de Compliance voorziening kun je twee kanten op testen: berichten sturen aan de Compliance voorziening of de Compliancevoorziening vragen om berichten te versturen naar je eigen applicatie.

Voor de demo wordt DART gebruikt om berichten naar de Compliance voorziening te sturen. Bij de resultaten in DART wordt alleen getoond of een test wel/niet geslaagd is. Verdere informatie over de test is terug te vinden in de rapportages in het Digikoppeling portaal. Als je doorklikt in het testresultaat zie je de groepen uit de standaard waarop is getest en als je verder doorklikt, kom je bij de validatie per regel uit de standaard. Hier staan de details van welke eisen er in de standaard beschreven staan en hoe dit in de praktijk in de code wordt getest. Hier is exact te zien wat wij doen aan validaties.

De omgeving is straks in eerste instantie alleen via het internet bereikbaar. In de volgende release (2.0 verwachte datum oktober) ook via Diginetwerk.

Op het moment dat je bent ingelogd kun je ook je profiel aanpassen:

1. het OIN nummer van de organisatie.
2. de endpoints.
3. certificaten: Het uploaden van de certificaten kan met de public key. Je kunt ze decrypten met je private key. Het certificaat kun je gebruiken

voor encrypted messages naar jezelf.

Gevraagd wordt of het mogelijk is om te kunnen groeperen op de testen die uitgevoerd zijn; bijvoorbeeld op datum. Dit is in deze versie nog niet het geval.

Gevraagd wordt of het mogelijk is om een rapportage uit te draaien die gedeeld kan worden met leveranciers om aan te geven dat je compliant bent. Dit staat op de back-log. Emily geeft aan dat dit waarschijnlijk niet in release 2.0 van oktober wordt meegenomen, maar waarschijnlijk wel in de release daarop.

Het zou ook interessant zijn als aangegeven zou worden welke profielen je nodig hebt voor bepaalde basisregistraties.

Basic Security Profile 1.1. zit hierin. De eerste release wordt eind juli / begin augustus waarschijnlijk live gebracht.

Hele expliciete vragen m.b.t. dit onderwerp kunnen nog nagemaïld worden.

7. Bespreking "binnengekomen vraag DUO"

Toelichting Gerald Groot-Roessink: een groot deel van het onderwijs werkt in de cloud, hier kijkt Digikoppeling niet naar. DUO volgt Digikoppeling, nu hebben zij last van één van de regels: de zogenaamde 'wildcard' regel. Een SAAS leverancier in de cloud gebruikt endpoints voor elke school apart. Zij hebben een groot aantal scholen in hun bestand staan. Zij hebben voor elke school een subdomein geregistreerd. In de huidige situatie gebruiken zij hier geen PKI-overheid certificaten voor.

Nu willen zij edu-koppeling gaan toepassen. De DK standaard volgt de richtlijnen van PKIoverheid, die stellen dat een service certificaat niet met een wildcard mag werken. Dit is een belemmering om met name bij deze partij de standaard toe te passen. Dit gaat nog verder: aan de serverkant hangt ook het portaal (front end). Hiervoor kunnen zij dus ook niet een eigen certificaat gebruiken met een wildcard want dan lopen zij op het front end spaak omdat het certificaat dan niet vertrouwd wordt.

De vraag is nu: waarom staat er een wildcard regeling in het Programma van Eisen van PKI overheid? Het is toch geen rare oplossing om als SAAS domein voor al je leveranciers een subdomein te registreren?

Digikoppeling volgt dus het programma van eisen van PKI overheid. Pieter heeft deze vraag bij hen neergelegd en zij hebben hiervoor een onderbouwing gegeven. Wij kunnen hier nu zelf heel weinig beslissen. De uitleg van PKI overheid zit bij deze notitie.

Je kunt een PKI overheid certificaat niet met wildcard aanvragen.

Martin geeft aan dat KPN hetzelfde probleem heeft maar hiervoor voor elke klant een apart certificaat aankoopt.

→ Emily of Pieter laten iemand van PKI overheid contact opnemen met Gerald Groot-Roessink. De afspraken die hieruit komen worden terug gelegd in dit overleg.

8. Bespreking ontvangen vragen van Kennisnet

a. Onderzoek naar ondertekenen van berichten (profiel 2W-BE-S)
Digikoppeling WUS:

De vraag is: wat is de status van de WSI organisatie? Veel voorschriften zijn gebaseerd op wat de WSI heeft voorgeschreven en de laatste versies dateren van 2010.

Kennisnet wil het ondertekenen toepassen maar loopt nu tegen een probleem aan.

Vanuit de standaard: zijn de voorschriften die zijn opgenomen valide? In Microsoft moet gehackt worden om het conform standaard op te leveren.

→ Actie: Pieter/Martin zullen onderzoeken of signing toepasbaar is bij het gebruik van verschillende adapters. De leveranciers worden hierbij betrokken Als workaroud onderzoekt DUO (Gerald Groot Roessink) het Windows Communication Foundation van Microsoft.

b. Verplicht gebruik van poort 443 voor communicatie over HTTPS:

Kennisnet ziet in de Digikoppeling omgeving dat andere partijen gebruik maken van andere poortnummers.

Martin geeft aan dat altijd gebruik gemaakt wordt van poort 443.

Erwin Reinhoud geeft echter aan dat in de onderwijssector toch wel veel gebruik gemaakt wordt van andere poortnummers. Als de daadwerkelijke praktijk bij implementaties is dat er andere poortnummers gebruikt worden, dan is de vraag of poort 443 gehanteerd moet blijven worden.

Uit ervaring is gebleken dat het heel erg onhandig is om verschillende poortnummers te gebruiken.

--> Actie: Logius zal onderbouwen waarom wij gebruik maken van één poort: 443.

Uitkomsten en vervolgacties komen op de agenda in september.

9. Stand van zaken OIN beleid

Dit onderwerp komt niet ter sprake in verband met de tijd.

Korte toevoeging Pieter Hering: het OIN beleid wordt a.s. donderdag in de Regieraad Gegevens besproken.

10. Ter kennisgeving: Ervaringen met Digikoppeling, Diginetwerk en PKI Overheid

Dit onderwerp komt niet ter sprake in verband met de tijd.

11. Format aanmelden agendapunten TO

Emily geeft aan een aantal vragen via de mail te hebben gekregen die Pieter vervolgens in een notitie heeft gezet. Naar aanleiding hiervan is een format ontwikkeld. In dit format kunnen de leden van het TO agendapunten aanbieden.

→ Actie: Format als word bestand meesturen.

12. Rondvraag

Geen.

CONCEPT