edustandaard

Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Geert Evers (Cito), Ernst-Jan van Heusevelt (Rovict, VDOD), Robert Kars (DUO), Arjan van Krimpen (Kennisnet, OSO), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet/Bureau Edustandaard).

Afwezig Edwin Verwoerd (Iddink), Herrie Abbink (Educus), Gerald Groot Roessink (DUO), Edmar Kok (DUO), Vertegenwoordiging GEU

Datum en locatie
8 februari 2017, 10:00-13.00 uur, Seats2Meet, Amersfoort

Agenda

1. Opening, mededelingen, vaststellen agenda
    a. Heeft DUO al ervaring opgedaan met Digikoppeling compliancevoorziening?
    b. OSO: SaaS-leveranciers willen gebruikmaken van ODOC-certificaten ipv de PKI overheid certificaten. Toelichting op de impact hiervan.
    c. Start Best Practice Edukoppeling 1.2 op MS WCF platform
2. Doornemen verslag en actielijst
3. Nieuwe conceptversie Edukoppeling (#56):
    a. Edukoppeling Transactiestandaard 1.2.1 (concept)
    b. Edukoppeling Architectuur 1.2.1 (concept)
    c. Edukoppeling - Begrippen (concept)
    d. Edukoppeling Transactiestandaard 1.2.1 - Release Notes
4. Concept Beheermodel &Releasemanagement (#34)
5. Uitwerking OIN (#43), zie: 2016-12-21 identificatie en authenticatie voor Edukoppeling
6. Foutafhandeling bespreken (#42)
7. Rondvraag
8. Sluiting

1. Opening, mededelingen, vaststellen agenda

Mededelingen

Ad 1a
Het betreft hier eigenlijk meer de vraag wat de status is rond het koppelen met de Digikoppeling Compliancevoorziening op basis van een Edukoppeling koppelvlak. Robert meldt dat er nog wordt onderzocht wat de mogelijkheden zijn om deze test uit te voeren. Zodra hierover wat over te melden valt zal dit aan de werkgroep worden teruggekoppeld.

Ad 1b
Een partij die een BRON koppeling heeft op basis van Edukoppeling 1.1 met een ODOC certificaat wilde deze ook op logistieke laag gebruiken voor een koppeling in de OSO keten. De OSO keten ondersteunt momenteel echter nog geen Edukoppeling en dus ook geen ODOC certificaten. Binnen de OSO keten werd de vraag gesteld of er ondanks dat er geen Edukoppeling ondersteund wordt, wel alvast een stap gemaakt kan worden door het kunnen toepassen van ODOC certificaten. Hoewel ODOC technisch identiek is aan PKI-overheid en ook het hele uitgifteproces goed is afgestemd met Logius en geaudit door OCW, zijn er praktische bezwaren geuit binnen de OSO-keten door andere leveranciers. Zij zitten niet direct te wachten op twee certificaten in de keten, omdat dit extra effort voor hen zou kosten, onder andere doordat PKIoverheid certificaten standaard in truststores van verschillende platformen zitten en dit geldt niet voor ODOC certificaten. Deze extra stap vereist mede door de

onbekendheid van ODOC certificaten extra effort bij audits, vereist extra onderzoek/uitleg of eea voldoet aan de beveiligingsrichtlijnen. Er is nu ook onzekerheid rond het lange termijn perspectief, is dit een tijdelijke dienst van DUO of blijft men deze dienst leveren en worden er stappen ondernomen om ook de ODOC hiërarchie standaard in de verschillende platformen op te nemen?
Vanuit de VDOD lijkt het wenselijk dat SaaS-leveranciers die een Edukoppeling koppelvlak ondersteunen dit doen op basis van een PKIoverheid certificaat die zij voor zichzelf aanvragen.
Ter verduidelijking: de huidige toepassing van “schoolcertificaten” ten behoeve van de koppelingen met DUO (BRON, Verzuim), dus nog niet conform het SaaS-model, is/wordt helemaal gebaseerd op ODOC-certificaten (ter vervanging van de oude “schoolcertificaten”). Daar gaat dit issue ook niet over.
Het gaat met name om de m2m koppeling tussen SaaS-leveranciers en andere partijen (DUO, andere SaaS-leveranciers etc.) conform het SaaS-model. Er is hierbij een addertje onder het gras: onderwijsinstellingen die zelf een Edukoppeling koppelvlak ondersteunen (dus niet van een SaaS-dienst gebruikmaken) zullen in principe ODOC certificaten hiervoor mogen gebruiken. Dit heeft wel tot gevolg dat partijen die met deze onderwijsinstelling koppelen alsnog eea moet inrichten om ODOC certificaten te vertrouwen en de benodigde verificatie uit te voeren.

Er is besloten om deze problematiek vast te leggen in het verslag en verder te onderzoeken en nader te beschrijven in een notitie. Deze kan gebruikt worden voor besluitvorming hoe we hier ten aanzien van de standaard zelf en met betrekking tot implementaties mee om willen gaan (actie #0058). Er is een issue geregistreerd (#15) waarin het uiteindelijke besluit zal worden geregistreerd.

Ad 1c
Eerder is door partijen aangegeven dat de implementatie in het MS WCF platform complex is. Dit mede omdat dit platform een aantal basis configuraties biedt die niet goed aansluiten bij wat een Edukoppeling koppelvlak vereist. Er is daarom besloten in het best practice document een beschrijving op te nemen hoe een bepaalde configuratie gebruikt kan worden in combinatie met een aantal specifieke aanvullingen. Dit zal in eerste instantie op basis van één bepaalde versie zijn (in .NET met een Windows Communication Foundation service).

Er wordt aangegeven dat dit een goed begin is, maar dat het beter zou zijn indien er code beschikbaar gesteld wordt waar partijen gebruik van kunnen maken. Momenteel is deze code echter niet beschikbaar en zal vanuit Edustandaard ook niet geleverd kunnen worden. Verder geeft men ook aan dat de ontwikkelingen rond platformen ook niet stil staan, er zijn al weer nieuwe platformen waar partijen gebruik van zullen maken, ook om Edukoppeling implementaties te realiseren. In het vorige overleg is verder ook aangegeven dat er in de Kinderopvang-keten Edukoppeling 1.2 (test)implementaties zijn ontwikkeld op basis van het Python, Java en PHP platform. Het idee is om deze code met de bredere Edukoppeling community te delen maar er wordt nog onderzocht hoe deze code op een goede manier beschikbaar kan worden gesteld. Robert zal zich hier over gaan buigen (#64).

We willen in ieder geval hiermee de problematiek van dit platform/versie kenbaar maken en hopen dat partijen die op basis van dit platform implementeren eventueel code/hints beschikbaar willen stellen om deze ook met de community te delen.

2. Doornemen verslag en actielijst van 14 december 2016

2.1. Doornemen verslag

Er wordt over pagina 5 van het verslag de vraag gesteld of het ook voor het VO/VMBO geldt dat de relatie naar het Bevoegd gezag betrouwbaar geregistreerd is. Er wordt aangegeven dat dit het geval is, maar dat deze relatie ook voor deze sector nu niet standaard via een koppeling beschikbaar wordt gesteld. Er wordt de weder vraag gesteld wat precies het probleem is. Er wordt aangegeven dat er in keten behoefte is om over deze formeel juridische relatie te kunnen beschikken. Er wordt DUO gevraagd te onderzoeken wat de mogelijkheden zijn om de relatie (met Bevoegd gezag/ kvk-nummer of RSIN) zoals in het verslag weergegeven ook digitaal te kunnen ontsluiten (actie #59). Robert wijst erop dat de nu lopende trajecten rondom linked open data wellicht hier een oplossing kunnen bieden.

Er wordt opgemerkt dat nog niet alle ketens de onderwijsinstellingsidentiteit (BRIN4) als identificerend kenmerk kunnen hanteren. Hiermee wordt onderkend dat er nu in bepaalde ketens eea ingericht moet worden om conform Edukoppeling afspraken te kunnen routeren. Hierbij zal een keten dus mogelijk moeten overstappen van het hanteren van BRIN6 naar BRIN 4 voor wat betreft de routeringsmogelijkheden in het Edukoppeling koppelvlak. Indien aanvullende routering noodzakelijk is, bijvoorbeeld Facet examenlocatie dan kan dit altijd nog in de bericht-inhoud (payload) opgenomen worden. Er wordt besloten om vragen/opmerkingen rond identificerende kenmerken van onderwijsentiteiten terug te koppelen aan Gerald via het stuk “20161214 identificatie en authenticatie voor Edukoppeling”, deze zal bij het volgend overleg besproken worden.

Bij DUO worden momenteel waar van toepassing nieuwe koppelingen geïmplementeerd op basis van Edukoppeling 1.2. Hierbij is nu al duidelijk dat er een aantal (kleine) wijzigingen op de standaard wenselijk zijn. Er wordt voorgesteld om de Edukoppeling 1.2.1 versie voorlopig nog even in concept te houden zodat de minor wijzigingen hierin meegenomen kunnen worden. Er wordt derhalve besloten om de Edukoppeling 1.2.1 conceptversie in het volgend overleg opnieuw ter vaststelling voor te leggen.

2.2. Actielijst

#24 Toelichting GB profiel: Blijft nog open staan tot er ruimte is in de agenda (blijft open)
#34 Toelichting releasemanagement: Is een agendapunt (zal worden afgesloten)
#39 Delen van ervaringen bij DAMBO: (blijft open)
#42 Foutafhandeling: Was agendapunt maar is niet besproken (blijft open, volgende keer)
#43 Toelichting OIN: Er is een notitie opgesteld maar nog niet besproken. Commentaar van allen graag zsm richting Gerald zodat dit meegenomen kan worden voor het volgende overleg (blijft open)
#46 Infographic schoolmanagers: Geen prioriteit (afvoeren van de lijst)
#47 Edukoppeling documentatie centraal ontsluiten, via de standaarden pagina zijn alle relevante documenten ook de toelichtende beschikbaar. (kan worden gesloten, wellicht biedt nieuwe site nog meer mogelijkheden)
#49 Notitie SaaS-model: vrijlaten van het toe te passen poortnummer (blijft open)
#50 Onderzoeken problemen vullen WSA:To/From (blijft open)
#52 Best practice document: Volgende keer wordt het eerste concept besproken (blijft open).
#53 Controleer status definitief van Transactiestandaard in documentatie (afgehandeld)
#54 WSA header / Mustunderstand toelichting opnemen in best practices (afgehandeld, wordt onderdeel #52)
#56 Opstellen van minor release 1.2.1 met tekstaanpassingen etc., bevindingen uit implementatie 1.2 bij DUO meteen hierin meenemen als dat kan (blijft derhalve open)
#57 Onderzoeken problematiek met SOAP 1.1 / SOAP 1.2 (blijft open)

3. Nieuwe conceptversie Edukoppeling

De volgende nieuwe conceptversies zijn opgesteld:

a. Edukoppeling - Transactiestandaard 1.2.1
b. Edukoppeling - Architectuur 1.2.1
c. Edukoppeling - Begrippen

In de Transactiestandaard zijn nu expliciet de relevante Digikoppeling stukken opgenomen. Er wordt gevraagd of deze tevens voorzien kunnen worden van een link naar het betreffende document. Daarnaast is ook besloten het Transactiestandaard stuk op een aantal punten aan te passen omdat er bij de implementatie van een 1.2 koppelvlak bij DUO nog eea naar voren is gekomen.

Bij implementaties komt ook naar voren dat partijen (in rol van SaaS-leverancier) nog steeds varianten toe passen die niet geheel binnen het Saa- model passen. Op transportniveau, als logistieke dienstverlener, is de SaaS-leverancier herkenbaar op basis van zijn eigen identiteit in het PKI-certificaat dat gebruikt wordt in de TLS-verbinding en eventueel bij de ondertekening. Een SaaS-leverancier in rol van dienstaanbieder moet het certificaat hierbij conform de daarvoor opgestelde PvE’s gebruiken. Dit betekent bijvoorbeeld dat men niet een certificaat mag gebruiken met een CN die anders is dan de domeinnaam waarop de service beschikbaar is gesteld. Dit probleem lijkt vooralsnog overeen te komen met de subdomein discussie die eerder heeft gespeeld.

Er is toen onderzocht of PKIoverheid het gebruik van wildcards als subdomein wil toestaan. Er is destijds door PKIoverheid aangeven dat dit een beveiligingseis is dat het PvE hierop niet aangepast zal worden. De problematiek die nu speelt zal verder worden toegelicht door Robert en Herrie (actie #60) zodat we duidelijk hebben wat er speelt. Op basis hiervan zal besloten worden wat mogelijke vervolgacties zijn.

Er wordt aangegeven dat de begrippen niet helemaal sporen met nieuwe documenten zoals het Identificatie en authenticatie voor Edukoppeling document. De begrippen zullen nog eens nagelopen worden en de nieuwe versie zal samen met de nieuwe conceptversie van de transactiestandaard opnieuw gedeeld worden.
Er wordt aangegeven dat de versies van Digikoppeling onderdelen die nu in de Transactiestandaard zijn opgenomen dezelfde versies zijn als degene waarvan al eerder de release notes besproken zijn. Er is destijds aangegeven dat de belangrijkste wijzigingen die effect op Edukoppeling hebbende volgende zijn:

- Scheiding van koppelvlakspecificatie en beveiligingsstandaarden. SHA-1 wordt gezien als een zwakke cipher voor signing. Op de “Gangbare Standaarden” lijst van het Forum Standaardisatie wordt naar SHA-2 verwezen. In Digikoppeling beveiligingsstandaarden zijn verwijzingen naar SHA-1 vervangen door SHA-2.
- Verplicht toepassen van TLS 1.2.
- In paragraaf 2.4.2 van koppelvlakspecficatie WUS wordt het type van het wsa:to veld anyURI (in plaats van EndpointReferenceType) om daarmee onderliggende standaarden te volgen.
- Beperking op de toe te passen WSA standaarden. De specificatie van 2006/05 (http://www.w3.org/TR/ws-addr-core/) is verplicht (het alternatief: 2005/08 (http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/) is vervallen).

Er wordt opgemerkt dat deze wijziging wel een GAP oplevert met de Edukoppeling 1.1 versie. Het eerder opgestelde document dat de GAP tussen versie 1.1 en 1.2 beschrijft moet hierop worden aangepast (actie #61).

Er wordt opgemerkt dat de WSA:To in het request nu een wsdl-adres naast het OIN bevat. Dit is een overblijfsel uit 1.1 om ervoor te zorgen dat dit veld compatibel blijft met 1.1. In DK wordt dit veld anders gebruikt, in Edukoppeling lijkt eigenlijk alleen het OIN belangrijk. Is het dan niet veel simpeler en duidelijker dat we hier ook anonymous verplicht stellen? Er moet eerst vastgesteld worden of het bewerken van de WSA velden in request en response op verschillende platformen gevuld kunnen worden (actie #50). Er zijn nu enige implementaties (ook in 1.1 wordt de vulling van deze velden voorgeschreven) en ook de implementaties in de Kinderopvang-keten geven aan dat er geconcludeerd kan worden dat dit geen probleem is. Het issue is reeds geregistreerd (issue #17) maar kan met de verwachte impact niet in de 1.2.1 release meegenomen worden. Deze zal in een komende medior of major release meegenomen worden.

4. Concept Beheermodel (actiepunt #34)

Het documenteren van het releasemanagement is eerder ter sprake gekomen en is ook als een issue geregistreerd (#14). Op basis van de zaken die in het vorig overleg zijn besproken is een beheermodel voor Edukoppeling opgesteld dat in grote mate overeenkomt hoe dit bij Digikoppeling geregeld is.

De verschillende elementen die hierbij van belang zijn worden toegelicht. Er wordt aangegeven dat hoewel er vorige keer besloten is om niet de status “Teruggetrokken” te onderkennen het misschien toch handig is dit wel te doen om extra beheer van deze afwijking te voorkomen. Alle deelnemers stemmen hiermee in en het document zal hierop aangepast worden (actie #62). De Edustandaard site moet deze verschillende statussen van de versie duidelijk kunnen communiceren.

Het document kan met de aangegeven aanpassingen gepubliceerd worden.

5. Foutafhandeling bespreken (actiepunt #42)

Dit onderwerp is deze keer niet aan bod gekomen en wordt doorgeschoven naar het volgende overleg van april 2017. Wel wordt er nog een issue besproken dat DUO bij de implementatie van een Edukoppeling 1.2 koppelvlak is tegengekomen. Er wordt besloten om betrokkenen bij DUO een voorstel te laten uitwerken hoe het beste met

foutafhandeling en betreffende codes omgegaan kan worden (actie #63 / issue #16). Na overleg met BES zal dit voorstel met werkgroep gedeeld worden. Na consensus zal dit vervolgens in de nieuwe 1.2.1 conceptversie van de Transactiestandaard verwerkt worden.

6. Rondvraag

Geen.

7. Sluiting

Er zijn een aantal nieuwe overleggen gepland. De volgende bijeenkomst is op 12 april van 10:00 tot 13:00.

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
0024	Toelichting GB profiel	In uitvoering	2017	BES/Erwin	2
0034	Afspraken rond releasemanagement: voorstellen besproken in werkgroep 14-12-2016, deze nu uitwerken in notitie	Afgehandeld	Q1, 2017	BES	1
0039	Delen van informatie rond DAMBO implementatie met ondertekenen van berichten	Geen prioriteit op dit moment, implementaties BRON en BPV hebben voorrang	2017	BES/ Educus (Herrie)	3
0042	Edukoppeling foutmeldingen agenderen en in WG bespreken	Loopt	12 april 2017	WG	1
0043	Verduidelijking toepassing OIN nu en in de toekomst conform het nieuwe RIO model.	Notitie niet besproken op 8-2, leden werkgroep reageren schriftelijk, behandeling op 12 april	12 april 2017	Gerald	1
0046	Edukoppeling infographic voor schoolmanagers.	Afgevoerd, geen prio op dit moment	2017	?	3
0047	Centraal beschikbaar stellen van relevante Edukoppeling documentatie. Nu staat documentatie bij verschillende overleggen op Edustandaard site.	Afgehandeld. Alle relevante documenten zijn nu op de centrale standaardenpagina te vinden. Als nieuwe site andere, betere mogelijkheden biedt dan worden die benut.	Q1 2017, afhankelijk van nieuwe Edustandaard site	BES / Brian	2
0049	Nav reactie Digikoppeling over gebruik poort 443 wordt een aanvullend voorschrift geformuleerd voor Edukoppeling hoe om te gaan met vrij laten van het toe te passen poortnummer	Loopt	Q1 2017	VDOD/ DUO Ernst-Jan / Gerald	2
0050	Onderzoeken of platformen het zetten van WSA:From en WSA:To velden in synchrone response berichten ondersteunen	Loopt	Q1 2017	BES	3
0052	Opstellen van (“Best Practices”) document met aanvullende informatie die helpt bij implementeren van de standaard	Loopt	april 2017	BES, Robert	2
0053	Controleer status definitief van Transactiestandaard in documentatie	Afgehandeld	januari 2017	BES	1

0054	WSA header / Mustunderstand toelichting opnemen in best practices	Afgehandeld	januari 2017	BES	1
0056	Opstellen van minor release 1.2.1 met tekstaanpassingen etc.	loopt	April 2017	BES	1
0057	Onderzoeken problematiek met SOAP 1.1 en mogelijkheden om SOAP 1.2 binnen Edukoppeling/Digikoppeling toe te kunnen passen	loopt	Q2 2017	BES	2
0058	Opstellen notitie over toepassing ODOC certificaten voor zowel onderwijsinstellingen als SaaS leveranciers	loopt	Q2 2017	BES	2
0059	DUO onderzoekt of de relatie tussen onderwijsidentiteit digitaal ontsloten kan worden	loopt	Q2 2017	DUO	2
0060	Gebruik van PKI certificaten in SaaS-model	loopt	Q2 2017	Robert/Herrie	2
0061	Beschrijving van GAP tussen Edukoppeling versie 1.1 en 1.2 aanpassen op wijzigingen die de laatst vastgestelde Digikoppeling versie heeft	loopt	Q2 2017	BES	2
0062	Beheermodel aanpassen: De status “Teruggetrokken” opnemen. Daarna beheermodel publiceren op Edustandaard	loopt	maart 2017	BES	1
0063	Voorstel uitwerken hoe het beste met foutafhandeling en betreffende codes omgegaan kan worden	loopt	Q2 2017	DUO	1
064	Onderzoeken of voorbeeldcode van testimplementaties Kinderopvang (Python, Java en PHP) kunnen worden gepubliceerd	op te starten	Q2 2017	Robert Kars (DUO)	2

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen

Besluiten

#	**Omschrijving**	**datum**
1	Toepassingsgebied van de WUS wordt verbreed naar meldingen. WS-RM gaan we daarmee dus niet opnemen in de standaard als comply or explain-standaard (voor ebMS was dit al besloten). Mocht in het onderwijs WS-RM (of ebMS) toch nodig zijn voor bepaalde uitwisselingen, dan is het advies om dat eerst met de Edukoppeling WG te bespreken.	01-10-2014
2	Foutafhandeling: kijken wat het TO Digikoppeling gaat overnemen van project Utrecht en daarop foutafhandeling Edukoppeling baseren .	01-10-2014
3	Certificeringsschema: als onderwerp wel in de werkgroep Edukoppeling aan de orde laten komen om input te kunnen leveren, maar niet om het inhoudelijk het schema in zijn geheel te behandelen en te onderhouden. NB er wordt een aparte werkgroep binnen Edustandaard hiervoor opgericht die ook breder kijkt naar andere IB-aspecten.	01-10-2014

4	Voorleggen aan Architectuurraad of REST een kandidaat is om in Edustandaard te worden opgenomen. Daarbij ook laten bepalen waar (in welke werkgroep) dit het best belegd kan worden.	01-10-2014
5	Edukoppeling 1.2 wordt door de werkgroep geadviseerd om te gebruiken bij alle nieuw op te zetten uitwisselingen. Als het advies wordt overgenomen door de Standaardisatieraad op 2 juli dan is Edukoppeling 1.2 de voorgeschreven transactiestandaard. NB Standaardisatieraad heeft advies overgenomen vooruitlopend de formele acceptatie van de VDOD waarover op 2 juli nog geen uitsluitsel kon worden gegeven.	17-06-2015
6	In de werkgroep van 9-9-2015 heeft Ernst-Jan van Heusevelt namens de VDOD aangegeven dat de leden instemmen met Edukoppeling 1.2 als de te hanteren Transactiestandaard.	09-09-2015
7	Berichten moet kunnen worden geleverd op basis van een OIN gebaseerd op BRIN in de routeringsinformatie (WSA headers), een verdere verfijning in het OIN voor een automatische routering achter voordeur is niet gewenst,	14-12-2016
8	Van Beheermodel/Releasemanagement v0.3 kan een definitieve versie gemaakt worden en gepubliceerd met aanpassing die in de bijeenkomst van 8-2-2017 zijn aangegeven	8-2-2017