edustandaard

Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Edwin Verwoerd (Iddink), Robert Kars (DUO), Ernst-Jan van Heusevelt (Rovict, VDOD), Erwin Reinhoud (Kennisnet/Bureau Edustandaard), Gerald Groot Roessink (DUO), Arjan van Krimpen (Kennisnet/OSO), Herrie Abbink (Uplearning), Geert Evers (Cito), Brian Dommisse (Kennisnet, voorzitter), Edmar Kok (DUO)

Afwezig: Rob van der Staaij (ThiemeMeulenhoff, GEU)

Datum en locatie
9 september 2015, 09:30-12.00 uur, Seats2Meet, Amersfoort

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst van 17 juni 2015
3. Vaststellen laatste versie documentatie Edukoppeling 1.2
    a. Terugkoppeling formeel standpunt van VDOD
4. Planning uitrol PKI-ODOC certificaten per sector, Edmar Kok, DUO
    a. Voorstel Certificaat per SaaS (endpoint) ipv certificaat per instelling (zie notitie)
5. Voortgang Proefopstelling Edukoppeling OSO, Arjan van Krimpen, Kennisnet
6. Korte terugkoppeling vanuit SION IAA werkgroep mbt voorstel IDM, Erwin Reinhoud, Kennisnet
7. Rondvraag
8. Sluiting

1. Opening, mededelingen, vaststellen agenda

Mededelingen

- Rob van der Staaij heeft zich afgemeld.

2. Doornemen verslag en actielijst

Verslag

- Geen opmerkingen

Stand van zaken rondom realisatie Service Register is vorige keer niet aan bod gekomen, dit wordt de volgende keer op de agenda gezet en zal door Robert Kars worden verzorgd.

Actielijst

#19 - Op het congres van 24 april is hier deels een workshop aan gewijd, verder gaat OSO ook een Edukoppeling proefopstelling uitvoeren. Er wordt tevens aan gedacht om code o.b.v. verschillende platformen te leveren (.NET, Java) die gebruikt kunnen worden bij de realisatie van een Edukoppeling koppelvlak. De komende periode zal er ook gekeken worden wat op dit vlak gedocumenteerd kan worden. Dit hangt samen met vaststellen van specifieke behoeften in het veld.
#20 – Er is nog geen start gemaakt met de checklist voor afweging toepassen Edukoppeling. Dit hangt samen met #19 (inventarisatie behoeften en documenteren). Definities kunnen strakker en meer in lijn met OBK (definitie onderwijsinstelling, school etc). Verder is ner ook behoefte aan ondersteuning bij hoe een bestaand koppelvlak gemigreerd kan worden naar Edukoppeling, bijv. in het kader van UWLR.
#21 - Voorstel IDM, SION IAA werkgroep heeft eerste analyse gedaan en deze wordt onder agendapunt 6 gepresenteerd.
23 –Digikoppeling geeft aan dit ook te onderkennen en gaat hier mee aan de slag, voorlopig wacht Edukoppeling de vorderingen van Digikoppeling af /en kijkt op termijn of deze invulling gevolgd wordt of dat er iets voor de onderwijssector geregeld moet worden. Daarnaast is men binnen de onderwijssector bezig met de ontwikkeling van een Samenwerking Informatiebeveiliging Onderwijsketen platform. De details hierbij zijn nog onbekend. Er wordt navraag gedaan of er reeds informatie gedeeld kan worden. Op termijn moet

binnen WG Edukoppeling besproken worden hoe dit en de ontwikkelingen bij Digikoppeling passen bij de behoefte van de Edukoppeling WG.
#24 - Het GB profiel is relevant binnen het onderwijs. DUO heeft reeds ervaring met dit profiel. De vraag is of we dit binnen het onderwijs willen toepassen gezien de complexiteit. Het GB wordt een agendapunt voor de volgende keer.
#30 - Beleggen afspraken over verantwoordelijkheden bij beheer, geen ontwikkelingen
#31 (nieuw) – In verband met #23 zal een notitie rond Samenwerking Informatiebeveiliging Onderwijsketen met leden van de werkgroep gedeeld worden.
#32 (nieuw)– De besproken analyse IAM onderwijsinstelling medewerker zal gedeeld worden. Hier zal tevens een schatting rond mogelijke tijdspaden opgenomen worden.
#33 (nieuw) –Er is een enkele fout in de tabel met WS-Addressing voorschriften gekomen. Daarnaast zijn binnen de WG een aantal keuzes gemaakt die mogelijk voor incompatibiliteit met versie 1.1 veroorzaken. Er zal een analyse worden gemaakt van de gemaakte wijzigingen, de rationale hierbij en de mogelijke incompatibiliteit met versie 1.1. De analyse backward compatibility tav WS-Addressing header voorschriften zal zo spoedig mogelijk uitgevoerd en gedeeld worden zodat binnen een termijn van enkele weken hier per mail een besluit binnen de werkgroep over genomen kan worden.
#34 (nieuw) – Proces beschrijving rond releasemanagement
#35 (nieuw) – Op Edustandaard site duidelijk aangeven dat daar problemen rond Edukoppeling gemeld kunnen worden

3. Vaststellen laatste versie documentatie Edukoppeling 1.2

a) Terugkoppeling formeel standpunt van VDOD

In de Standaardisatieraad van 2 juli. 2015 is het volgende besluit genomen: *De Standaardisatieraad gaat akkoord met Edukoppeling 1.2, met het voorbehoud van een terugkoppeling op een aantal besproken punten, waaronder het oordeel van de leveranciers. Dit wordt geagendeerd voor de volgende vergadering. Dan kan tevens een terugkoppeling gegeven worden van de eerste ervaringen met de testopstelling bij OSO.*

Een van die besproken punten was de formele acceptatie van de VDOD, dat op 2 juli nog niet ingenomen kon worden omdat de laatste wijzigingen in de 1.2 versie pas eind juni na de werkgroep van 17-6 beschikbaar konden komen. Inmiddels heeft men tot eind augustus de tijd gehad en Ernst-Jan van Heusevelt kan namens de VDOD melden dat de leden van de VDOD zijn geconsulteerd en er geen bezwaren zijn om de voorliggende conceptversie te accepteren als de transactiestandaard voor berichtuitwisseling.

Er wordt door Robert Kars de vraag gesteld of hiermee ook de voorkeur voor ondertekenen van berichten toegepast gaat worden. Omdat dit nu nog niet als bindend voorschrift opgenomen is, zullen de verschillende projecten hier zelfstandig de afweging maken. Op termijn, als er ervaring is opgebouwd met het ondertekenen van berichten bij de verschillende partijen, kan de stap gemaakt worden om dit als bindend voorschrift op te nemen. Dit is dus wel de stip op de horizon waarnaar we streven.

Er wordt door Gerald Groot Roessink opgemerkt dat technici bij DUO opgemerkt hebben dat 1.2 op een of twee punten incompatibel lijkt te zijn met de 1.1 versie. Dit zit in de invulling van de WS-Addressing velden. Hoewel de inhoud van deze velden zowel in een voorbereidend subwerkgroepje als in de werkgroep is besproken, is dit niet eerder geconstateerd. DUO heeft de 1.1 versie eerder al geïmplementeerd in het MBO-veld (Digitaal Aanmelden en bij de nieuwe BRON-uitwisseling) en zou graag zien dat 1.2 backwards compatible is. Herrie Abbink onderschrijft dit als leverancier waar die uitwisseling al een jaar draait. Die eis van backwards compatibiliteit is overigens niet eerder expliciet uitgesproken en er is ook niet expliciet daarop getoetst.
Er wordt voorgesteld dat de incompatibiliteit wordt geanalyseerd en dat hierover een notitie wordt opgesteld waarin tevens een voorstel wordt gedaan om de specificatie indien nodig aan te passen. Deze notitie wordt gedeeld met de Werkgroep (actiepunt #33). Als het voorstel wordt geaccepteerd, wordt de specificatie conform hiermee aangepast en dit is dan de versie van de standaard die als definitief wordt gepubliceerd. De werkgroep verwacht op voorhand niet dat deze aanpassing impact zal hebben op het doorlopen vaststellingsproces.

Ernst-Jan van Heusevelt vraagt hoe er nu omgegaan wordt met toekomstige wijzigingen. Tevens moet er duidelijkheid rond releasemanagement komen, bijv. wanneer wordt 1.2 geïntroduceerd en 1.1 uitgefaseerd (actiepunt #34). Dit wordt zeker relevant als een bepaalde versie van de standaard niet meer backwards compatible is met een vorige versie. Wellicht moet er dan ook besloten worden om het versienummer te wijzigen (bijv. niet meer 1.2 maar 2.0, als dat nu ook al het geval zou zijn)..

Vervolgens wordt gevraagd hoe er überhaupt met problemen en issues uit het veld omgegaan wordt. In principe is de Edustandaard site het kanaal voor partijen om melding te maken van problemen bij het toepassen van een standaard (zie: https://www.edustandaard.nl/participeren/standaard-indienen/hoe-wijzig-ik-een-bestaande-afspraak/). Wijzigingsverzoeken kunnen daar worden ingediend. Op de pagina van Edukoppeling zelf zal een issue-/RFC-lijst worden bijgehouden. Dit is ook de praktijk bij andere standaarden. Naast meldingen via site kunnen werkgroepleden natuurlijk ook direct melding maken van problemen bij de voorzitter van de werkgroep. Er wordt door werkgroepleden aangegeven dat dit tot nu toe niet duidelijk was en er wordt voorgesteld dit explicieter te maken op de Edustandaard site (actiepunt #35).

4. Planning uitrol PKI-ODOC certificaten per sector

a) Voorstel Certificaat per SaaS (endpoint) ipv certificaat per instelling

Er wordt een notitie toegelicht (PKI PO versie 20150907) waarin wordt beschreven hoe er met PKI certificaten in het PO omgegaan kan worden.

In de notitie wordt de huidige situatie beschreven en een tweetal alternatieven. Omdat de huidige situatie niet voldoet aan de benodigde beveiligingseisen (o.a. door verouderde certificaten) moet er overgestapt worden naar één van de alternatieven.

Er wordt door vertegenwoordigers van de leveranciers aangegeven dat het 2e alternatief, ‘Hanteer één certificaat per SAAS-leverancier’, niet voldoet. Er wordt onderkend dat het gebruik van één certificaat per SaaS leverancier gewenst is, maar dit betreft dan een certificaat waarmee de connectie wordt opgezet en beveiligd en waarmee de leverancier wordt geïdentificeerd, SaaS leveranciers gebruiken nu echter een schoolcertificaat van de school ook om de identiteit van de handelende partij aan een bepaalde school te kunnen koppelen. Als die geschrapt wordt en er komt niets voor in de plaats dan wordt hiermee de verantwoordelijkheid naar de SaaS-leverancier verschoven zonder dat die iets in handen heeft om (juridisch) te kunnen waarborgen/checken dat de school goed in zijn rol zit. Als je niet iets hiervoor regelt maar wel de PKI-ODOC per school schrapt dan is het voor de VDOD-leden onbespreekbaar nu. Er moet geregeld wordt dat de ID van school herkenbaar moet zijn.

Hiermee ontstaat vanzelf het nu gewenste alternatief, namelijk het gebruik van een SaaS leverancier certificaat voor de uitwisseling (S2S) en gebruik van het schoolcertifcaat ter ondersteuning van IDM van de handelende partij en zijn/haar relatie met een bepaalde onderwijsinstelling (H2H/H2S). Dit hangt dus samen met agendapunt 5 en wordt gezien als een mogelijke korte termijn oplossing van het IDM vraagstuk.
Het zou wenselijk zijn om ruim voor de datum dat de nieuwe certificaten aflopen er een alternatief is ontwikkeld waarbij in de lijn van informatiebeveiliging op het gebied van identificatie voor de school/gebruiker een verbeterslag is gemaakt. Of er dan een andere identificatiewijze komt die minder een intensief/kostbaar distributieproces vergt zoals nu met de certificaten het geval is, is iets wat onderzocht moet worden vanuit het perspectief van alle actoren.

Robert Kars merkt op dat het twee lagen zijn:

- Certificaat van school is bedoeld om relatie school-SaaS aan te geven
- In Edukoppeling wordt altijd het certificaat van SaaS-leverancier gebruikt waarmee de connectie wordt opgezet en de leverancier wordt geïdentificeerd.

Eerste laag willen we op termijn kunnen vervangen, maar de tweede blijft dan onveranderd. Daarbovenop willen we de relatie van de eindgebruiker met de school namens wie die optreedt kunnen verifiëren en daarmee een echte e2e beveiliging realiseren.

Sowieso zijn alle aanwezigen het erover eens dat het PKI-ODOC certificaat ruim toepasbaar moet zijn voor alle onderwijsuitwisselprocessen dus niet alleen voor de communicatie met DUO maar ook voor OSO, UWLR-achtige uitwisselingen, Vensters etc.

5. Terugkoppeling vanuit SION IAA werkgroep mbt voorstel IDM

De verschillende geïdentificeerde varianten van het IDM vraagstuk worden kort toegelicht. Geen van de oplossingen is geschikt voor korte termijn. Voor allen geldt dat er eea nog gerealiseerd moet worden. Men zou graag in een korte notitie terug zien hoe eea zich tot elkaar verhoud (actiepunt #33).

Eén van de mogelijke alternatieven is het toepassen van de Kennisnet Federatie en een IdP. Maar de huidige situatie voldoet niet aan het vereiste betrouwbaarheidsniveau. Hiervoor kunnen wel verschillende stappen worden genomen. Er wordt de mogelijkheid geopperd om de tokens die men t.b.v. toegang tot het Zakelijkportaal wil gaan uitgeven gebruikt kunnen worden om deze situatie te verbeteren. Daarnaast zal er dan nog eea gedaan moeten worden om betrouwbaar deze identiteit te kunnen koppelen aan bepaalde onderwijsinstelling.

Het is duidelijk dat er nu geen goede alternatieven beschikbaar zijn. Vandaar dat de ideeën bij agendapunt 4 mogelijk als beste korte termijn oplossing beschouwd kunnen worden. Er moet de komende tijd verder onderzocht worden wat een robuuste generieke lange termijn oplossing kan zijn (actiepunt #21). Omdat de certificaten in 3 jaar verlopen moet de nieuwe oplossing voor die tijd beschikbaar zijn.

6. Voortgang Proefopstelling Edukoppeling OSO

Kennisnet is gestart met het project ‘proefopstelling OSO op Edukoppeling’. Arjan geeft hier een presentatie over. Het karakter van de proefopstelling is ‘technisch’; Er gaat uitgezocht worden hoe de OSO infrastructuur moet worden aangepast om op basis van Edukoppeling te werken. Organisatorische zaken als het vervangen van de huidige certificaten door SAAS en/of school certificaten zijn niet in scope van de proefopstelling.
Ook de koppeling met de back office valt buiten de scope. In OSO wordt OfficeHeart gebruikt voor het beheer van aanleverpunten (door scholen) en het uitleveren van PKI-certificaten. In de proefopstelling worden aparte aanleverpunten met een eigen registratie toegepast; certificaten zullen het PKI-ODOC formaat volgen en bij voorkeur ook ‘echt’ zijn.

7. Rondvraag

Nu duidelijk is geworden dat de uitrol van certificaten zowel per leverancier als per school noodzakelijk blijven, vraagt Edmar Kok aan de werkgroepleden of ze mee willen denken met het opstellen van de business case voor dit uitgifteproces. Afgesproken wordt dat Edmar de business case die DUO nu al heeft gemaakt wordt gedeeld met de werkgroep (via Brian Dommisse te distribueren) en dat zij daarop aanvullingen en aanpassingen voorstellen. Bij voorkeur zsm omdat de besluitvorming en de uitgifte zelf nog dit jaar moet worden afgerond cq opgestart (actiepunt #36).

8. Sluiting

Er wordt nog een datumprikker gestuurd voor datum van volgend overleg.

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
0016	Documentatie Edukoppeling herzien met zaken die zijn behandeld onder punt 3	Afgehandeld	juni 2015	Erwin, Robert, Herrie, Arjan	1
0018	Beschrijven samenhang Edukoppeling aspecten (Architectuur)	Afgehandeld	juni 2015	BES/DUO	1
0019	Ondersteuning implementaties	Punt voor discussie in SR, geldt voor meer standaarden	n.t.b.	Brian	n.t.b.
0020	Checklist opstellen voor afweging toepassen Edukoppeling	In uitvoering	n.t.b.	BES	2.
0021	Voorstel IDM medewerker onderwijsinstelling bij gebruik SaaS dienst	In uitvoering, wordt deels belegd bij werkgroep IAA-architectuur	2015/2016	SION IAA WG/ Edukoppeling WG	2
0023	Onderzoek centraal centrum beveiligingsaspecten Edukoppeling	In uitvoering	Loopt	BES	2
0024	Toelichting GB profiel	In uitvoering	Okt/nov 2015	BES/Erwin	1.
0026	Formeel standpunt VDOD over PKI-certificaten	Afgehandeld	Juni/juli 2015	Ernst-Jan van Heusevelt	1
0028	Navragen over nummersystematiek voor onderwijs in OIN (Logius)	afgehandeld	in juni 2015	Erwin / Gerald	1
0029	Rol 2, gegevensbewerker, definitie aanpassen aan juridische context	Afgehandeld, in documentatie verwerkt	Juni 2015	BES	1
0030	Beleggen afspraken over verantwoordelijkheden bij beheer	Nog op te starten	n.t.b.	n.t.b.	2
0031	Delen van notitie platform Samenwerking Informatiebeveiliging Onderwijsketen	loopt	September 2015	BES	1
0032	Delen van notitie Analyse IAM onderwijsinstelling medewerker	loopt	September 2015	BES	1
0033	Delen analyse backward compatibility tav WS-Addressing header voorschriften en specificatie aanpassen	loopt	Eind september 2015	BES/DUO	1
0034	Procesbeschrijving rond releasemanagement	ntb	ntb	BES	
0035	Op Edustandaard site duidelijk aangeven dat daar problemen rond Edukoppeling gemeld kunnen worden.	ntb	ntb	BES	
0036	Business case uitrol PKI-ODOC delen met Werkgroep. Aanvullingen/aanpassingen op BC leveren	Wordt opgestart Volgt daarna	Half september Eind september	Edmar Kok (DUO) Werkgroepleden Edukoppeling	1

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