edustandaard

Concept Verslag ES werkgroep Edukoppeling transactiestandaard

Aanwezig: Ernst-Jan van Heusevelt (Rovict/VDOD), Erwin Reinhoud (Kennisnet), Gerald Groot Roessink (DUO), Robert Kars (DUO), Arjan van Krimpen (Kennisnet/OSO), Geert Evers (Cito), Brian Dommisse (Kennisnet, voorzitter), Edwin Verwoerd (Iddink), Herrie Abbink (Uplearning)
Afwezig: Henk Dubbelman (Grafisch Lyceum Rotterdam)

Datum en locatie
1 april 2015, 09:30-12.30 uur, Seats2Meet, Amersfoort

Agenda
1. Opening, mededelingen, vaststellen agenda
    a. Consultatie Digikoppeling 3.0
2. Doornemen verslag en actielijst van 27 januari 2015
3. Aanpassen documentatie Edukoppeling
    a. Edukoppeling Transactiestandaard v1.2 (concept maart 2015)
    b. Edukoppeling Architectuur v0.1 (concept maart 2015)
    c. Terugkoppeling uit VDOD over toepassing certificaten
4. Edukoppeling in de ketenstartarchitectuur Doorontwikkelen BRON
5. Rondvraag
6. Sluiting

1. Opening, mededelingen, vaststellen agenda

Mededelingen
Het toets- en examenplatform Facet gaat Edukoppeling toepassen voor de uitwisseling met scholen.

Consultatie Digikoppeling 3.0
Gerald Groot Roessink geeft toelichting op consultatie DigiKoppeling 3.0:
1. SaaS-problematiek wordt niet in Digikoppeling 3.0 belicht
2. Machtigingsverklaringen voor achterliggende handelende partij wordt steeds relevanter, maar is ook geen onderdeel van Digikoppeling 3.0
3. Digikoppeling heeft nog niet gereageerd op terugkoppeling. Wel worden deze aspecten opgenomen in de roadmap, vanuit Edukoppeling moeten deze dus gevolgd worden en waar mogelijk convergeren.

2. Doornemen verslag en actielijst

Verslag
De volgende opmerking van Ernst-Jan van Heusevelt (pag. 3) kan aangescherpt worden:" Ernst-Jan van Heusevelt geeft aan hij als leverancier de voorkeur heeft voor de uitgifte van PKI-certificaten per instelling.." Ernst-Jan geeft aan dat dit wat hem betreft een vereiste is. Het formele standpunt van het VDOD hierover zal in mei worden gegeven.

Actielijst
#3 – Er is discussie wat de mogelijke nummer-systematiek kan zijn voor onderwijsinstellingen. Er lijkt consensus te zijn dat dit voorlopig een BRIN4 is en optioneel aangevuld met een aanduiding voor een afdeling. Voor de keuze hierbij is het van belang of organisatie(onderdelen) taken hebben in een wettelijk kader en hun bestuurders tekenbevoegd zijn. Het identificerend gegeven wordt opgenomen in het certificaat van de organisatie(onderdeel). Dit zou een keuze zijn die vooruit loopt op de verdere uitwerking van de resultaten van het SION onderwijsinstellingsidentiteit project welke nu bij DUO in ontwikkeling is in het kader van Doorontwikkelen BRON. Verder is onduidelijk in hoeverre de onderwijssector onderkend wordt in de nummer-systematiek van Digikoppeling. Er wordt navraag gedaan bij Digikoppeling of nu prefix 7 formeel gereserveerd is voor het onderwijs (Actie 28: Erwin of Gerald).

#4 – Er wordt voorgesteld om dit punt te laten vervallen om niet te veel aanvullende beperkingen op te leggen. Dit aspect is ook onderdeel binnen het ontwerp van het ServiceRegister. Het actiepunt blijft dus voorlopig staan tot vanuit het ontwerp hier invulling aan gegeven kan worden.
#5 – De huidige tekst is het waarom van het niet verplichtstellen van WS-RM voldoende toegelicht en actiepunt kan hiermee gesloten worden.
#9b – De situatiebeschrijving cloudleveranciers is al geleverd en besproken.
#14 – Er wordt voorlopig geen Linkedin groep aangemaakt, via de Edustandaard website kunnen documenten gedeeld worden, dit lijkt voorlopig voldoende.
#16 – Agendapunt
#17 – In huidige documentatie ontbreken standaard foutmeldingen. Idee is om hierbij Digikoppeling te volgen. Er is hier vanuit het Project Utrecht ook richting aan gegeven maar momenteel is onduidelijk wat het standpunt van Digikoppeling in deze is. Er zal navraag gedaan worden bij Digikoppeling.
#18 - Agendapunt
#19 - Op het congres van 24 april is hier deels een workshop aan gewijd.
#20 – Er is nog geen start gemaakt met de checklist voor afweging toepassen Edukoppeling. Deze periode zal hier een begin mee worden gemaakt, maar ook dit zal wat afstemmingsrondes vereisen.
#21 - Voorstel IDM
#22 – Er is nog wat onduidelijkheid of TLS offloading nu ketenbreed acceptabel is en dat ondertekening van het bericht niet noodzakelijk is. Ook hierbij wordt aansluiting gezocht bij wat Digikoppeling stelt. Er is vanuit Logius hierover al per email bevestiging gekomen dat TLS-offloading binnen Digikoppeling toegepast wordt, maar de vraag staat nu uit of Digikoppeling ook (zoals beloofd) wat best practice documentatie hierover kan opstellen.
23 – Er zijn nog geen stappen gemaakt voor een centraal centrum beveiligingsaspecten Edukoppeling. Er wordt op termijn wel met Digikoppeling en SURF overlegd hoe zij hiermee omgaan.
#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 zodat we huidige praktijksituaties en het GB profiel kunnen vergelijken en hier een besluit over kunnen nemen.
#25 - Ernst-Jan van Heusevelt zal binnen de werkgroep de VDOD vertegenwoordigen.
#26 - Formeel standpunt VDOD over PKI-certificaten zal bij het komend VDOD overleg besproken worden.

3. Ketenstartarchitectuur Doorontwikkelen BRON

BRON HO is afgerond. De koppeling tussen Studielink en DUO is Edukoppeling-compliant. Tussen scholen en Studielink (waarschijnlijk) niet. Als we Studielink zien als een soort SaaS-leverancier dan is de gehele keten zeker nog niet Edukoppeling-compliant. De vraag is echter wel of we Studielink wel zo zouden moeten positioneren. Voor Doorontwikkelen BRON is nog geen harde planning bekend, maar voor het MBO zal in ieder geval in 2016 een aantal zaken worden gerealiseerd.

Het heeft de voorkeur om een Edukoppeling als systematiek ook voor het VO toe te passen en dit niet meer via het zakelijk portaal te laten verlopen. Dit is ook met belanghebbende besproken, maar conclusie was dat het juiste moment nog niet daar was. Wanneer dit wel het geval is zal mede bepaald worden door de ervaringen met het MBO in het kader van Doorontwikkelen BRON.

Het PO werkt al via web services, maar nog volgens de ‘oude manier’. Mogelijk gaat dit in 2018 over op de nieuwe systematiek.

Er wordt nog besproken of bij de huidige gegevensuitwisseling binnen het PO de berichten ondertekend worden of niet. Ondertussen is hier navraag over gedaan door Ernst-Jan en wordt gesteld dat deze berichten niet ondertekend worden. Er is dus niet bekend of binnen de PO sector men ervaring heeft met het ondertekenen van berichten. Er wordt voorgesteld dit binnen de onderwijssector te onderzoeken (actiepunt #27).

DUO gaat een deel van de IT opnieuw inrichten en gaat hiermee de koppelvlakken vitaliseren. Er wordt ook in een ServiceRegister voorzien wat mogelijk door de hele sector gebruikt kan gaan worden, de mogelijkheden hiertoe worden met Yenlo, de leverancier die nu voor Facet hiervoor een en ander heeft geregeld, nog besproken. Hiermee zou invulling kunnen worden gegeven aan functionaliteit die ook binnen Edukoppeling gewenst is. In het ServiceRegister kan een machtigingsverklaring geregistreerd worden waarmee een onderwijsinstelling aangeeft welke dienst een bepaalde SaaS-leverancier namens die onderwijsinstelling mag uitvoeren. Voor Facet is deze werkwijze in ontwikkeling en gaat in mei in productie. Met deze werkwijze krijgt het ServiceRegister wel een belangrijke operationele rol waaraan hoge beschikbaarheidseisen gesteld worden. Er moet duidelijk zijn wie verantwoordelijk is voor wat. Om dit en gerelateerde zaken te bespreken wordt het ServiceRegister op de agenda gezet voor het volgend overleg. Robert heeft in april daar een gesprek met Yenlo en zal de uitkomst ervan in dit volgende overleg inbrengen.

4. Aanpassen documentatie Edukoppeling (Transactiestandaard en Archtiectuur)

Een aantal weken vooraf aan het overleg is de nieuwe conceptversie van de Transactiestandaard en een eerste concept van een Architectuur document aan de deelnemers ter review aangeboden. Idee hierbij was dat er nog tijdig commentaar besproken en verwerkt kon worden. Er bleek echter nog onvoldoende tijd om ruim vooraf aan het overleg terugkoppeling te geven en deze te bespreken. Er is dan ook besloten om deze punten te inventariseren en tijdens het overleg te bespreken. Een volledige lijst met opmerkingen is in de bijlage opgenomen. De onderwerpen die besproken zijn volgen hieronder:

- Duidelijke formulering scope / use cases ontbreekt
  Het is nu onduidelijk wanneer de standaard precies toegepast moet worden welke voordelen het gebruik biedt. In de Digikoppeling standaard is hierover eea opgenomen, maar er blijkt dus duidelijk behoefte aan meer richtlijnen. Hiertoe is dan ook actiepunt 20 voor opgesteld (checklist opstellen voor afweging toepassen Edukoppeling).
- Onderscheid tussen optionele en verplichte onderdelen
  Men mist nu een MoSCoW indicatie voor de verschillende onderdelen. Er kan in de documentatie gekozen worden om dit sterker aan te zetten, de opzet tot nu toe is in principe dat alles verplicht is. Alleen na de discussie rond TLS-offloading is er voor gekozen om zowel het Best Effort profiel (2W-be) als het Best Effort profiel met ondertekening (2W-be-S) te ondersteunen.
- Op welk niveau vindt identificatie plaats en hoe organiseren we dat en welke identiteit wordt in het certificaat opgenomen? Dit was al bij actiepunt 3 besproken. Er lijkt consensus te zijn dat dit voorlopig een BRIN4 is en optioneel aangevuld met een aanduiding voor een afdeling.
- Hoe governance is geregeld is niet opgenomen in de documentatie. Er is een paragraaf ‘Beheer’ opgenomen waarin ook Edustandaard benoemd wordt. Men wil dit dus duidelijker naar voren laten komen en wellicht aanvullen met hoe actief toezicht geregeld wordt.
- End-2-end beveiliging kan niet als optie gezien worden, maar is integraal onderdeel van de standaard. Hiermee wordt gesteld dat voor alle Edukoppeling toepassingen e-2-e beveiliging gewenst is. Door e-2-e beveiliging als integraal onderdeel te zien van de standaard zal dat in de specificatie ook moeten worden opgenomen en niet in het architectuurdocument.
- Meer uitleggen
  Robert en Gerald constateren dat we meer moeten uitleggen over hoe de standaard te gebruiken. Dat is nu nog summier en de verwachting is dat we vanuit partijen die er mee aan de slag gaan vooral veel vragen hierover krijgen.

De werkgroep constateert dat het verwerken van de opmerkingen in de documenten zeer gewenst is, ook met het oog op verdere bespreking met de achterban. Met name Ernst-Jan wijst erop dat hij graag een aangepaste versie van de documenten, dan wel deze versie plus een reactie op de ingebrachte opmerkingen, zou willen krijgen voor de ALV van de VDOD waarin dit wordt geagendeerd. Die bijeenkomst is op 22 mei. Zie ook actiepunt #26.

5. Rondvraag

Geen bijzonderheden.

6. Sluiting

Afgesproken wordt dat de volgende werkgroepbijeenkomst op 17 juni zal plaatsvinden van 9.30-12.30 (incl. lunch) wederom in Amersfoort.

Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
0003	Voorstel nummer-systematiek t.b.v. logistieke punten en achterliggende handelende partij	n.t.b.	n.t.b.	BES	n.t.b.
0004	Voorstel voor identificerende kenmerken van berichten (upi)	In uitvoering bij SR project	Begin januari 2015	BES	n.t.b.
0005	Tekstvoorstel niet verplichtstellen WS-RM	afgehandeld	November 2014 (input voor 0016)	Gerald/Robert	1
0009b	Situatiebeschrijving cloudleveranciers	afgehandeld	Begin januari 2015	Herrie	n.t.b.
0014	Aanmaken Linkedin groep	afgehandeld	Begin januari 2015	BES	n.t.b.
0015	Uitnodigen Studielink	afgehandeld	15 september 2014	Brian	n.t.b.
0016	Documentatie Edukoppeling herzien met zaken die zijn behandeld onder punt 4	In uitvoering	Mei 2015	Erwin, Robert, Gerald	1
0017	Standaard foutmeldingen (volgen Digikoppeling)	In uitvoering	n.t.b.	BES	n.t.b.
0018	Beschrijven samenhang Edukoppeling aspecten (Architectuur)	In uitvoering	n.t.b.	Erwin	1.
0019	Ondersteuning implementaties	n.t.b.	n.t.b.	n.t.b.	n.t.b.
0020	Checklist opstellen voor afweging toepassen Edukoppeling	In uitvoering	ntb	Kennisnet/Erwin	2.
0021	Voorstel IDM	n.t.b.	n.t.b.	DUO/Robert?	1.
0022	Navraag Digikoppeling TLS offloading	In uitvoering	n.t.b.	BES/Erwin	1
0023	Onderzoek centraal centrum beveiligingsaspecten Edukoppeling	In uitvoering	n.t.b.	BES	n.t.b.
0024	Toelichting GB profiel	In uitvoering	ntb	BES/Erwin	2.
0025	Formele vertegenwoordiging VDOD (*Ernst-Jan van Heusevelt is gedelegeerde vanuit VDOD)*	afgehandeld	Maart 2015	Ernst-Jan van Heusevelt	1
0026	Formeel standpunt VDOD over PKI-certificaten	In uitvoering	ntb	Ernst-Jan van Heusevelt	1
0027	Onderzoeken in hoeverre binnen de onderwijssector men bekend is met het ondertekenen van berichten bij s2s koppelingen	n.t.b.	n.t.b.		n.t.b.
0028	Navragen over nummersystematiek voor onderwijs in OIN (Logius)	In uitvoering	Volgend overleg in juni 2015	Erwin / Gerald	1

BES = Bureau Edustandaard

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

Bijlage A: Terugkoppeling tav documenten versie 1.2 maart 2015

1. Duidelijke formulering scope / use cases ontbreekt
2. Onderscheidt tussen optionele en verplichte onderdelen
3. Verwijderen van definities die al in Digikoppeling zijn opgenomen
4. PKI-Onderwijscertificaten
    a. Gaat DUO deze uitgeven en worden deze onderdeel van de transactiestandaard?
    b. Wanneer worden deze wel/niet toegepast?
    c. Naam (PKI-ODOC)?
    d. Plan van eisen (waar wijken deze af van PKI-overheid), wordt het Subject.serial gebruikt voor identiteit?
    e. Wie stelt vast (en waar) dat het PKI Onderwijscertificaat gelijkwaardig is aan PKI Overheidscertificaat? De school, DUO, de leverancier?
    f. Komen de identiteiten voor certs uit een centraal beheerd register? Kunnen deze certs voor koppelingen bij allerlei processen gebruikt worden (niet alleen DUO)?
    g. Op welk niveau vindt identificatie plaats en hoe organiseren we dat en welke identiteit wordt in het certificaat opgenomen?
5. Certificeringsschema /IdM
    a. Certificeringsschema is procedureel, vraag is of het IdM deel van e-2-e beveiliging hiermee geborgd is, of dat er aanvullende voorschriften nodig zijn, waar gaan we deze beleggen?
    b. Kunnen we bestaande (nationale) infra gebruiken (e-herkenning), of het gebruiken we PKIcerts om een omgeving/instelling te kenmerken (PKI-certificaten per school ‘aan de voorkant’)?
6. Termen als Digi of Edukoppeling zijn in sommige tekstdelen producten en in een andere delen lijkt het erop dat de afsprakenset wordt bedoeld.
7. Edukoppeling ondersteunt twee scenario’s maar dit komt niet sterk genoeg naar voren
    a. school verantwoordelijk, leverancier in bewerkersrol
    b. school verantwoordelijke en koppelt zelf
8. Pagina 5, figuur 1 en transactiestandaard paragraaf 3.3, er zijn meerdere vormen van identificatie die moeten eerst worden uitgeschreven in het architectuurdocument en niet opeens in het Transactiestandaard specificatiedocument naar voren komen.
9. Pagina 13, End tot End beveiliging, de beschrijving van de problematiek en oplossing is niet conform de laatste bespreking (onderdeel onderzoek hoe dit binnen onderwijs te regelen).
10. ServiceRegister als Machtigingsregister, is dit al operationeel op deze manier? Kunnen allerlei partijen voor onderlinge gegevensuitwisseling (niet met DUO) hier gebruik van maken? Is dit een keuze en blijft als alternatief het gebruik van proxy-certificaten?
11. Pagina 3 (aanleiding), intro punt 1 en 2 ontbreekt en zijn niet voldoende onderbouwd.
12. Pagina 5, de bouwstenen van de Edukoppeling Architectuur komen niet sterk genoeg naar voren.
13. In hoofdstuk 4 staat benoemd de principes waarvan wordt afgeweken t.o.v. de Digikoppeling standaard. In het document worden de principes om af te gaan wijken niet in de vorm genoemd (of verwezen) zoals dat bij ROSA is gedaan.
14. Algemeen, er ontbreekt nog steeds een logische architectuurbeschrijving als hoofdstructuur
15. Er ontbreekt uitleg hoe de TLS te offloaden en daaruit het OIN te halen (actiepunt 22).
16. Hoe gaan we om met foutmeldingen (actiepunt 17).
17. Bij paragraaf Scope van Edukoppeling, de term ‘partijen’ vervangen door ‘organisaties’.
18. Hoe governance is geregeld is niet opgenomen in de documentatie

19. End-2-end beveiliging kan niet als optie gezien worden, maar is integraal onderdeel van de standaard.