edustandaard

Agenda ES-werkgroep Edukoppeling transactiestandaard

Leden: Edwin Verwoerd (Iddink), Gerald Groot Roessink (DUO), Robert Kars (DUO), Herrie Abbink (Educus), Peter Dam (Cito), Arjan van Krimpen (Kennisnet/OSO), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet)
Agendalid: Ernst-Jan van Heuseveldt (Rovict, VDOD)

Datum en locatie
24 januari 2018, 10.00-13.00 uur (incl. lunch)
Locatie: Seats2Meet, boven station Amersfoort

1. Opening, mededelingen, vaststellen agenda

2. Doornemen verslag en actielijst van 21 september 2017

3. Ontwikkelingen rond Digikoppeling
    a. Versie 3.0 teruggetrokken
    b. Geen gebundelde versie meer (2.0)
    c. OIN in WSA:To en WSA:From
    d. Roadmap
    e. Foutcodes opgenomen in Best Practice
    f. Nieuwe versie Compliance voorziening

4. Beveiligingsvoorschriften:
    a. Toegestane ciphersuites
    b. Controle CN server certificaat

5. Identificatie en authenticatie document (actiepunt #43)

6. Review Ontwerp Serviceregister (*PvE Onderwijs Serviceregister*)

7. Doornemen issuelijst (*Issuelijst (versie 20180117) behorend bij Afspraak Edukoppeling*)

8. Rondvraag

9. Sluiting

Alle bijlagen (apart en als ZIP) zijn te vinden op:
https://www.edustandaard.nl/standaard_bijeenkomsten/bijeenkomst-werkgroep-edukoppeling/

Ad3
Er zijn verschillende ontwikkelingen bij Digikoppeling.

Versie 3.0 teruggetrokken
We hebben dit al eerder besproken, DK 3.0 komt te vervallen en er komt geen verzoek om Digikoppeling 3.0 op de 'pas-toe-of-leg-uit' lijst op te nemen van Forum Standaardisatie[1]. Het verschil tussen Digikoppeling 2.0 en 3.0 was de toevoeging van koppelvlak WS-RM aan Digikoppeling 3.0. Logius geeft aan dat de 3.0 versie en documenten van de Logius site[2] verwijderd zullen worden. Eventuele verwijzingen naar de 3.0 versie moeten ook uit de Edukoppeling-documentatie verwijderd worden (issue #24).

Geen gebundelde versie meer
Met het vervallen van DK3.0 is er geen bundeling van documenten onder een bepaalde versie, maar worden de documenten onder een eigen versie gepubliceerd. We hadden hiervoor al een Edukoppeling structuurdocument

[1] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
[2] https://www.logius.nl/diensten/digikoppeling/detailinformatie/

opgesteld waarin naar relevante Digikoppeling documenten verwezen wordt. Dit document komt ook te vervallen nu Digikoppeling zoals verwacht hiervoor een eigen document heeft opgesteld (Digikoppeling Overzicht Actuele Documentatie en Compliance[3]). Voor een aantal DK documenten is er een nieuwe versie gepubliceerd. Op basis van de release notes moet duidelijk worden of er wijzigingen met impact voor EK zijn (issue #24).

OIN in WSA:To en WSA:From
Met het vervallen van 3.0, vervalt tevens onze aansluiting met Digikoppeling rond de opname van het OIN in de WSA:To en WSA:From. In het afgelopen Technische Overleg Digikoppeling (d.d. 11-01-2018) is er een wijzigingsvoorstel ingediend om in een volgende release van Digikoppeling WUS weer optioneel het OIN in de WSA:To en WSA:From op te nemen. Hiermee blijft Edukoppeling ook op dit punt aangesloten op de Digikoppeling standaard, EK blijft opname van OIN in de WSA:To en WSA:From verplicht stellen. We verwachten dat dit voorstel geaccepteerd zal worden en zal dan waarschijnlijk rond de zomer in de nieuwe DK Koppelvlakstandaard WUS opgenomen worden. Een volgende stap is om ook in de DK WUS Best practices gegevensuitwisselingspatronen met intermediairs op te nemen. Onderdeel hiervan is dan tevens het SaaS model dat mogelijk wel meer generiek beschreven zal worden. Dit heeft ook een relatie met issue #17, willen we het WSA:To veld nog steeds vullen met anonymous of aansluiten op de verwachtte generieke vulling van DK die hierin waarschijnlijk het endpoint van de web service opneemt.

Roadmap Digikoppeling
Er is een Digikoppeling roadmap 2018-2020 (zie bijlage). Het is gericht op het voorbereiden van de tactische keuzes voor doorontwikkeling van de Digikoppeling standaard én voorzieningen in de komende jaren. Hierbij is rekening gehouden met de vele ontwikkelingen die spelen rond Digikoppeling zoals het digitaal stelsel Omgevingswet, Generieke Gemeentelijke Infrastructuur, het toenemende gebruik van op REST gebaseerde webservices, het vernieuwde OIN beleid en de behoefte met betrekking tot het aanbieden van de informatie over Digikoppeling. Het goede nieuws is dat hierin tevens een aantal punten opgenomen zijn die we vanuit Edukoppeling al als aandachtspunt hadden geïdentificeerd. Zo zal er door een externe partij onderzoek worden gedaan naar problematiek rond signing. We verwachten dat er in Q2-3 resultaten beschikbaar komen. Deze zullen hopelijk bijdragen aan het meer interoperabel kunnen definiëren van aspecten die met signing en wellicht encryptie samenhangen. Het plan is om goed werkende voorbeelden en uitwerkingen op basis van bijvoorbeeld in Java en .net als Best Practices te publiceren. Daarnaast zal In 2018 er ook stappen worden gezet om de informatie over te zetten naar een nieuwe omgeving. Voor de gebruikers is het nu lastig om overzicht te hebben en houden over het gebruik van de standaard en welke versie nu geldig is. Afhankelijk van de uitkomsten kan Edukoppeling hierop aansluiten.

Foutcodes opgenomen in Best Practice
Eind vorig jaar is er een wijzigingsvoorstel ingediend om foutcodes weer in de Digikoppeling Best Practices op te nemen (issue #16). In de nieuwe versie van de DK BP[4] zijn de foutcodes opgenomen. Alle foutcodes in de transactiestandaard worden nu in de DK BP beschreven, behalve de foutmeldingen die samenhangen met het verplicht gebruik van OIN in WSA:To en WSA:From (foutcode 20, 21 en 22). Er kan nu binnen de werkgroep besproken worden hoe we hiermee om willen gaan: foutcodes handhaven zoals het nu is (als voorschrift voor web service die deze moeten kunnen terugkoppelen) of opnemen in EK BP en voor alle foutcodes naar DK BP verwijzen en enkel foutcode 20, 21 en 22 opnemen.

Nieuwe versie Compliance voorziening
Er is een nieuwe versie van de compliancevoorziening. Deze heeft een aantal eerder geconstateerde problemen rond de WUS WSDL opgelost.

Ad4
Toegestane ciphersuites
De OSO keten heeft het gebruik van de TLS cipher TLS_RSA_WITH_AES_256_GCM_SHA384 uitgesloten. Digikoppeling en dus Edukoppeling staan het gebruik van deze cipher nog wel toe.

De bronnen die OSO heeft gehanteerd voor dit besluit zijn de cipher lijst die Mozilla heeft samengesteld voor modern compatibility: https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility, alsmede het researchwerk van Qualys die oa de gerenomeerde SSLTEST hebben gebouwd, hun documentatie staat op: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices. Hierbij wordt uitgegaan van zo min mogelijk backwards compatibility en een juist zo sterk mogelijke versleuteling van de verbindingen. Dit heeft alles te maken met de bijzondere persoonsgegevens die OSO verwerkt. Doel is om de datastreams niet alleen nu maar ook in de toekomst veilig te houden. De reden waarom je alleen nog maar ciphers die forward secrecy ondersteunen is te lezen op bijv: https://wiki.mozilla.org/Security/Server_Side_TLS#Forward_Secrecy of zelfs in de NCSC factsheet over TLS.

Logius (beheerder Digikoppeling) geeft aan dat ze actief meldingen van het NCSC krijgen op het gebied van acute beveiligingsrisico's, het is echter nu onduidelijk of dit ook geldt voor het gebruik van ciphers. Dit wordt momenteel uitgezocht. Het issue is reeds bij Logius gemeld en de OSO keten / Onderwijssector kan ook als bron

[3] https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/digikoppeling_2.0/Digikoppeling_Overzicht_Actuele_Documentatie_en_Compliance_v1.0.pdf
[4] https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/digikoppeling_2.0/Digikoppeling_Best_Practices_WUS_v1.10.pdf

beschouwd worden voor de aanscherping van beveiligingsvoorschriften[5]. Er loopt dus nu eea rond dit punt en naar verwachting zal tijdens het overleg of kort daarna er meer duidelijkheid komen hoe Logius hiermee omgaat. Vooralsnog is de verwachting dus dat Digikoppeling de OSO keten hierin gaat volgen, hierbij wel mogelijk de nuance dat de betreffende cipher een uitfaseertraject in gaat om partijen de tijd te geven voordat deze geheel uitgesloten wordt.

Ad5 en 6
Het Identificatie en authenticatie document is na interne review in onze werkgroep op donderdag 21 september in een workshop in het kader van Doorontwikkelen BRON vo gebruikt als input om samen het BRON-team en de LAS-leveranciers in het vo te bekijken of het als basis kan dienen voor de soms complexe routerings- en adresseringsvraagstukken. In ieder geval is duidelijk geworden dat routerings- en adresseringsvraagstukken overal spelen en dat met afspraken rondom de adressering van organisaties en organisatieonderdelen ihkv OIN niet altijd de gewenste granulariteit wordt behaald, nu niet met BRIN en ook later niet met RIO. Ieder proces/voorziening heeft hier nu eigen oplossingen voor bedacht die niet met elkaar overeenkomen. Een issue wat hiermee samenhangt is het nader specificeren van de vulling van het OIN voor onderwijsinstellingen (issue #20).
Voor BRON is een keuze gemaakt tav de wijze waarop routeringsinformatie kan worden vastgelegd en doorgegeven nl. door gebruik te maken van het suffix in het OIN en door het aanleggen van een eerste opzet van wat later door moet groeien naar een serviceregister. We kunnen in de Best practices e.d. hier aandacht aan besteden.

De uitkomsten van de bovengenoemde workshop hebben geleid tot aanpassingen in het IAA-document (Gerald heeft beloofd een nieuwe versie hiervan nog voor de komende werkgroep op te leveren).

Het punt van preciezere adressering is eerder al onderkend in het streefbeeld H2M2M en daar is als streefbeeld geschetst dat we een uniforme set van requirements en specificaties moeten gaan bewerkstelligen voor wat genoemd is een serviceregister waarin we die gewenste granulariteit op een eenduidige wijze kunnen vastleggen. Diverse decentrale serviceregisters die nu in gebruik of in wording zijn zouden uiteindelijk conform die set ingericht moeten worden, uiteraard via migraties op momenten dat die mogelijk zijn.
In het kader van het project Vroegtijdig Aanmelden MBO is een Serviceregister als basisinfrastructuur-component ook onderkend. Er is opdracht gegeven tot het opstellen van een ontwerp waarbij zoveel mogelijk rekening wordt gehouden met de hierboven geschetste bredere toepassing. In de laatste Architectuurraad van Edustandaard is deze aanpak onderschreven en is toegezegd om vanuit Edustandaard mee te werken aan de kwaliteitsborging.

Hoewel dit het ontwerp dus niet direct een verantwoordelijkheid is voor de werkgroep Edukoppeling, is ons door de projectcoördinator Wiebe Buising gevraagd om mee te denken over die set van specificaties en requirements zodat die zo goed mogelijk aansluiten op de standaard Edukoppeling.
Naast de professionele review van onze werkgroep wordt er ook een ROSA-scan uitgevoerd door Bureau Edustandaard op het ontwerp, die zal worden geagendeerd in de Architectuurraad van 15 februari.

Er is een begeleidingsgroep vanuit OCW ingesteld die het ontwerp moet valideren. De uitkomsten van de ROSA-scan en het reviewcommentaar vanuit de Edukoppeling-werkgroep zijn kwaliteitsinstrumenten die helpen bij het opstellen van het ontwerp en het valideren ervan.

NB sommige werkgroepleden hebben dubbele en zelfs driedubbele petten op tav dit onderwerp (ze zijn ook betrokken bij begeleidingsgroep en/of architectuurraad). De review die we hier willen doen is vooral gericht op de consequenties die het ontwerp van het serviceregister mogelijk heeft voor de Edukoppeling-standaard.

[5] https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/digikoppeling_2.0/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.1.pdf