Concept Verslag ES werkgroep Edukoppeling

Aanwezig: Robert Kars (DUO), Edwin Verwoerd (Iddink, VDOD), Olav Løite (Topicus), Maarten Kok (SBB), Pieter Bruring (Kennisnet, OSR), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, Edustandaard), Remco de Boer (Archi-XL, toelichting ROSA-scan)

Afwezig: Gerald Groot Roessink (DUO), Peter Dam (Cito)

Agendalid: Ernst-Jan van Heuseveldt (Rovict, VDOD)

Datum en locatie
30 september, 10:00-12.30 uur, Online

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. REST/SaaS-profiel - terugkoppeling openbare consultatie en ROSA-scan
4. PKIo Public en Private Root Certificaten
5. Edustandaard UBV (v0.7) – impact TLS 1.3, ciphers, SNI verplicht voor client, bij voorkeur poort 443, bij voorkeur PKI OCSP stapeling
6. Update Edukoppeling docs – Compliance en overzicht, REST/SaaS, WUS/SaaS, I&A, Best Practices
7. Terugkoppeling TO Digikoppeling
8. Issuelijst
9. Rondvraag / Sluiting

1. Opening, mededelingen, vaststellen agenda

De agenda wordt zonder wijzigingen vastgesteld. Er zijn geen mededelingen.

2. Doornemen verslag en actielijst van 27 mei 2020

Verslag
Het verslag van 27 mei 2020 wordt zonder wijzigingen vastgesteld.

Actiepunten

92	In overzicht met relevante standaarden aangeven tot welke datum verwacht wordt dat de standaard de status “in gebruik’ heeft.	Afgerond
94	Kan de huidige OIN methodiek o.b.v. BRIN4 zoals nu is opgenomen in het I&A document is opgenomen vervangen worden met een identiteit van een onderwijsaanbieder?	Geen wijziging
97	Analyse AMIGO (versie?) om vast te stellen of nu nog wat ontbreekt bij beschrijving bedrijfstransacties in Architectuur	Afgerond
99	Best practice beschrijven van toepassing API-key (REST profiel - OSR)	Geen wijziging
100	Wijzigingsvoorstel OSR dat DUO voor ogen heeft wordt meegenomen in GAP-analyse die binnen het team van OSR opgesteld wordt. Deze zal t.z.t. gedeeld worden met leden	Geen wijziging
103	Er moet met OSR besproken worden of het onderscheiden van profielen (REST/WUS) mogelijk moet zijn. Dit zou dan ook in Architectuur beschreven moeten worden	Geen wijziging
105	Architectuurdocument: Plaatje bij Patroon Abonneren op wijzigingen middels notificaties	Afgerond
106	Advies vragen bij AR over het beheer van poortnummer bij UBV of Edukoppeling. Aansluitend of poort 443 een verplichting moet zijn. Een ander punt voor AR is voorschriften rond berichtbeveiliging in UBV of WUS profiel	Afgerond
107	In de Edukoppeling best practice staat nu nog het gebruik van ODOC certificaten voor testen. Dit moet aangepast worden	Afgerond

3. REST/SaaS-profiel - terugkoppeling openbare consultatie en ROSA-scan

Op het Edukoppeling discussieplatform[1] is half juli een post geplaatst met de vraag aan de leden van het forum om het REST/SaaS-profiel (0.5 versie) en de Architectuur (versie 2.0, juni 2020) te reviewen. De binnengekomen opmerkingen en de ROSA-scan worden besproken.

3.1. Terugkoppeling openbare consultatie

Het ontvangen commentaar richt zich niet alleen op nieuwe zaken die met het REST-profiel geïntroduceerd worden. De terugkoppeling wordt daarom gesplitst in een deel dat over het REST profiel gaat en een deel dat betrekking heeft op de fundamenten van het huidige SaaS-profiel.

3.1.1. REST/SaaS-profiel

1) Routeringsinformatie in SOAP Header en JSON alleen eisen als er via een Broker gewerkt wordt.
    a. Als de definitie van een broker gelijkgesteld kan worden aan een SaaS-leverancier (of conform Edukoppeling de rol van Verwerker) dan komt deze stelling overeen met de uitgangspunten van het SaaS-profiel. In deze context is het dus wenselijk om routeringsinformatie te standaardiseren.
    b. De opmerking levert wel discussie op hoe om te gaan met de situatie als er niet sprake is van een SaaS-leverancier. Eén of beide partijen kunnen namens zichzelf handelen (bijvoorbeeld een school of ketenpartij). Vanuit standaardisatie van koppelvlakken is het wenselijk om dan ook hetzelfde (SaaS)profiel toe te passen. De partij (school/ketenpartij) geeft dan de eigen identiteit aan op transportniveau (TLS

[1] https://groups.google.com/a/kennisnet.nl/g/edukoppeling/c/Tl9iVL6pFjg

certificaat) en in de betreffende routeringsinformatie. Deze situatie is ook reeds beschreven in de architectuur. Om het profiel in deze situatie uniform te houden moet de betreffende partij zichzelf ook mandateren. Dit lijkt toch te wringen. Om verder te onderzoeken hoe met deze situatie het beste omgegaan kan worden zullen Olav en Robert een advies schrijven (actiepunt #108).

2) Brug tussen XML en JSON ontbreekt. Het grote verschil zit in de namespaces en in de attributen (JSON kent geen attributen). Namespaces hebben natuurlijk geen enkele echte functie. Dus vervallen die bij het gebruik van JSON. Maar voor Attributen moet er wel een conventie bedacht worden.
    a. Dit wordt als een belangrijk punt onderkend, maar de vraag is of dit binnen de scope van Edukoppeling ligt. Edukoppeling stelt geen voorschriften aan de gegevensstructuren en ook niet hoe deze vorm te geven in transport (geen boodschap aan de boodschap). Dergelijke vraagstukken lijken beter binnen AMIGO te passen. Er wordt voorgesteld om de vraag waar regels voor de XML/JSON transformatie belegd kunnen worden aan de AR voor te leggen (actiepunt #109).
    b. Wel onderkent Edukoppeling het gebruik van XML en JSON. Op dit niveau lijkt er wel gesteld te kunnen worden dat JSON wat vrijer is en minder (vaak) strikt gevalideerd wordt. Als gevolg hiervan stellen we dat er een onderscheid kan worden gemaakt in kwaliteit/betrouwbaarheid. Dit met name als partijen een XML-bedrijfsdocument voor het versturen resp. bij ontvangst valideren. Dit lijkt bij toepassing van JSON (nog) wat van ondergeschikt belang te zijn. Bij het vorige punt is er verder ook al gesproken over het meer strikt voorschrijven van de controle van de mandatering door ketenpartijen. In de Architectuur staat nu dat bij zowel push- als pull-gegevensuitwisseling de mandatering tussen eindorganisatie en gegevensverwerker geverifieerd moet kunnen worden in het serviceregister. Met een meer strikt voorschrift (en naleving) in de keten is er een hogere mate van zekerheid dat er rechtmatig gegevens uitgewisseld worden tussen ketenpartijen. Er wordt voorgesteld om deze aandachtspunten de AR voor te leggen (actiepunt #110).

3) Voor het classificeren van de voorschriften is de MoSCoW methode gebruikt. Deze past niet goed en het is beter om de Requirements Notation and Conventions standaard aan te houden (RFC2119).
    a. Dit voorstel is overgenomen en is reeds in de 0.6 versie verwerkt.

4) Bij paragraaf 3.1.2 staat dat het gebruik van internet als MUST geclassificeerd, verderop staat er dat het ook bij private netwerken gebruikt mag worden. Dit is niet consistent.
    a. Dit is aangepast in de 0.6 versie. Het gebruik van internet is nu als ‘MAY’ geclassificeerd.

5) De routeringskenmerken in de HTTP querystring is onwenselijk i.v.m. beperkte lengte hiervan. Daar wil je spaarzaam mee omgaan.
    a. Geen wijziging. De invulling van de routeringskenmerken is uitvoerig in werkgroep besproken met de nodige alternatieve oplossingen. Er is uiteindelijk voor de query string gekozen.

3.1.2. Fundamenten Edukoppeling

Een aantal punten worden kort benoemd die meer betrekking lijken te hebben op de bouwstenen van Edukoppeling en niet direct betrekking hebben op het REST/SaaS-profiel. Omdat de indiener niet aanwezig kon zijn wordt besloten de punten nu niet inhoudelijk te bespreken. Dit voorkomt ook dat het commentaar mogelijk verkeerd geïnterpreteerd. Er wordt besloten om de indiener nog eens voor de volgende werkgroep uit te nodigen zodat eea besproken kan worden. Mocht dat niet lukken dan wordt er een bilateraal overleg gepland.

Er wordt aangegeven dat als het een bilateraal overleg wordt het wel wenselijk is dat de resultaten met de werkgroep gedeeld worden. In de opmerkingen zitten namelijk een aantal punten die wel vaker bij het bespreken van Edukoppeling naar voren komen, zoals waarom er een PKIo certificaat nodig is. Er wordt aangegeven dat partijen in principe onderling prima met eigen certificaten kunnen werken.

Met Edukoppeling beogen we een mate van standaardisatie te realiseren zodat partijen die in meerdere ketens actief zijn niet zaken als identificatie en authenticatie op verschillende manieren hoeven in te richten. Het is wenselijk één afspraak te hebben op organisatorisch niveau. Daarnaast geeft het gebruik van het OIN ook extra zekerheid rond de identiteit. Zo stelt UBV voorschrift TLS-PKI-01 '*Indien een OIN verplicht en de integriteit daarvan noodzakelijk (niveau 3) is, dient de authenticatie met een certificaat van PKIoverheid plaats te vinden.*'.

Er wordt aangegeven dat deze discussies ook wel spelen bij client-server koppelingen. Er wordt gesteld dat we dit niet echt als M2M verkeer zien en het is ook geen ketenproces. In die context is PKIo (Edukoppeling) niet noodzakelijk.

3.2. ROSA Architectuurscan

Voor het REST/SaaS-profiel is een ROSA Architectuurscan[2] uitgevoerd. Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd.

Voor de volgende punten wordt het advies gegeven om het REST/SaaS-profiel aan te passen:

1) Ontwerpgebied Informatiebeveiliging en privacy (IBP): Eenduidig beschrijven van te nemen maatregelen bij vertrouwelijke gegevens in query parameters. Op pagina 13 staat '*dienen gepseudonimiseerd te zijn*'. Op pagina 18 staat '*kunnen aanvullende beveiligingsmaatregelen toegepast worden, zoals adequaat versleutelen en/of voorkomen ongewenste logging dmv filter*'
    a. In de volgende versie van het REST/SaaS-profiel zal op pagina 13 een vergelijkbare tekst komen als nu op pagina 18 staat.

2) Ontwerpgebied Gegevensuitwisseling in de keten: Gebruik van openbare internet (MUST) en Edukoppeling kan ook toegepast worden in gesloten netwerken. Dit is in tegenspraak met elkaar.
    a. Zie ook het 4e punt bij terugkoppeling openbare consultatie. Deze tekst is in de 0.6 versie reeds aangepast. Het gebruik van internet is nu als 'MAY' geclassificeerd.

3) Ontwerpgebied Gegevensuitwisseling in de keten: De Architectuur definieert foutcategorieën A t/m E. In het profiel worden alleen foutmeldingen voor cat. A (syntaxfouten) gedefinieerd. Hoe passen de andere foutcategorieën op HTTP statuscodes?
    a. De foutafhandeling die in het REST/SaaS-profiel is opgenomen is van hetzelfde niveau als die bij het WUS/SaaS-profiel zijn opgenomen. De nadruk ligt op fouten rond de voorschriften die het profiel introduceert. Concreet betekent dit dat er nu alleen foutmeldingen rond de routeringskenmerken zijn. Fouten (HTTP codes) voor overige foutcategorieën, zoals Service gesloten, Functionele fouten en Prestatie-fouten worden (vooralsnog) niet in de profielen gedefinieerd.
    b. In de volgende versie worden de bestaande bijlagen (Foutafhandeling en OAuth) verwijderd. In het profiel zelf wordt foutafhandeling opgenomen. Er wordt een foutafhandeling flow-specifiek voor het REST/SaaS-profiel (routeringskenmerken) uitgewerkt.

4) Ontwerpgebied Governance: Op pagina 6 wordt XML over REST niet toegestaan, volgens API-24 is het een eigen afweging (COULD). Dit is in tegenspraak met elkaar.
    a. In de volgende versie wordt aangegeven dat bij XML het WUS/SaaS-profiel de voorkeur heeft, maar ketens zijn vrij een eigen keuze te maken (men mag content negotiation ondersteunen).

[2] https://www.edustandaard.nl/standaard_bijeenkomsten/bijeenkomst-werkgroep-edukoppeling-september-2020/

3.3. Conclusie

Er wordt besloten dat het REST/SaaS-profiel met de voorgestelde wijzigingen aan de Architectuurraad aangeboden kan worden ter vaststelling. Voordat deze naar de Architectuurraad verstuurd wordt willen de leden nog wel de versie kunnen reviewen. Het huidige document in de googledrive zal daarom worden aangepast zodat de leden de wijzigingen kunnen volgen. De volgende Architectuurraad is eind oktober en leden kunnen tot 21 oktober opmerkingen/wijzigingen aangeven.

4. PKIo public en private root certificaten

Er wordt stilgestaan bij de ontwikkelingen rond PKIoverheid certificaten. Eerder was al duidelijk geworden dat (bepaalde TSP's) geen public root (G3) certificaten meer leverde. Na navraag bij Logius maakte duidelijk dat sinds begin juli men bezig is met het vervangen van certificaten. Informatie hierover is te vinden op https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen.

In de Edukoppeling community ontstond hiermee de vraag of private root (G1) certificaten toegepast mochten worden voor M2M communicatie. Hoewel zowel private als public root certificaat nu nog mogen worden gebruikt was deze informatie niet nadrukkelijk gedocumenteerd bij Digikoppeling. Recent zijn documenten gepubliceerd waarin dit nadrukkelijk wordt aangegeven:

- https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.3.pdf
- https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Gebruik_en_achtergrond_certificaten_v1.6.pdf
- https://www.logius.nl/sites/default/files/bestanden/website/20200902_Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie.pdf

Zowel private (G1) als public (G3) root certificaten mogen NU dus nog gebruikt worden. Het is wel de verwachting dat op termijn public root certificaten niet meer gebruikt mogen worden voor M2M koppelingen. Er is hierover ook een post geplaatst op het Edukoppeling discussie platform[3]. De ontwikkelingen rond PKIo public root certificaten is ook reeds in het TO Digikoppeling besproken. Het is waarschijnlijk dat er een nieuwe versie (v1.4?) van de Digikoppeling beveiligingsstandaarden en voorschriften komt waarin staat dat alleen PKIoverheid private root certificaten toegepast mogen worden (voorschrift PKI005).

De Edukoppeling documentatie moet nog nagelopen worden waar een vermelding van PKIoverheid public root certificaten staat (actiepunt #111). Verder wordt aangenomen dat alle partijen die een PKIo certificaat hebben door de betreffende TSP worden/zijn benaderd met nadere info. De truststores zullen namelijk ook aangepast moeten worden en zoals altijd moeten certificaten bij gegevensuitwisseling geverifieerd worden (met behulp van CRL of OCSP). Verder informatie rond de ontwikkelingen bij PKIoverheid zijn te vinden op volgende locaties:

- https://logius.nl/diensten/pkioverheid/pkioverheid-update/certificaat-vervangingsplan-veelgestelde-vragen
- https://logius.nl/sites/default/files/bestanden/website/PKIoverheid%20Infographic%201.0%20-%20NL.pdf
- https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2020/september/4/factsheet-pkioverheid-verandert/Factsheet+PKIoverheid+verandert+v1.0.pdf

5. Edustandaard UBV (v0.7)

De Edukoppeling SaaS-profielen verwijzen voor transportbeveiliging naar UBV. UBV is momenteel nog in ontwikkeling. Voor versie 0.7 loopt nu een openbare consultatie:

[3] https://groups.google.com/a/kennisnet.nl/g/edukoppeling/c/yrQDWYdKReM

https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/uniforme-beveiligingsvoorschriften-0-7/

Er wordt aangegeven welke aspecten van het UBV Edukoppeling profiel impact hebben op bestaande Edukoppeling implementaties. Edukoppeling overerft (nu nog) de voorschriften direct van Digikoppeling (NCSC[4]).

De werkgroep vind het wenselijk dat er in het UBV Edukoppeling profiel een duidelijk onderscheid komt tussen voorschriften en adviezen. In de tekst staat soms een voorkeur met mogelijk alternatief en verder worden er verschillende TLS opties genoemd. We willen op voorschriften standaardiseren. Adviezen en opties kunnen bijvoorbeeld als best (current) practice gezien worden en zijn geen onderdeel van de normatieve afspraak. We willen dus het UBV Edukoppeling profiel op een aantal punten aangepast hebben. Er wordt besloten een apart document op te stellen waar we gezamenlijk onze input voor de UBV werkgroep in kunnen opnemen. De basis hiervoor is tijdens dit schrijven reeds gepubliceerd op de google drive (Memo openbare consultatie UBV[5]).

6. Rondvraag en sluiting

Helaas zijn niet alle agendapunten besproken. De aangepaste Edukoppeling documentatie, de terugkoppeling vanuit TO DK en Issuelijst worden een volgende keer besproken. Omdat we de laatste versie van de REST/SaaS-profiel nog formeel willen aftikken voor de Architectuurraad van 29 oktober, komen we op woensdag 21 oktober nog een keertje bijeen. Dan kunnen we ook de niet behandelde agendapunten behandelen.

7. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
94	Kan de huidige OIN methodiek o.b.v. BRIN4 zoals nu is opgenomen in het I&A document is opgenomen vervangen worden met een identiteit van een onderwijsaanbieder zoals nu in RIO is opgenomen?	Plannen	Q3 2020	BES	2
99	Best practice beschrijven van toepassing API-key (REST profiel - OSR)	Plannen	Q3	BES/OSR	2
100	Wijzigingsvoorstel OSR dat DUO voor ogen heeft wordt meegenomen in GAP analyse die binnen het team van OSR opgesteld wordt. Deze zal tzt gedeeld worden met leden	Loopt	Q2	Kennisnet/OSR	1
103	Er moet met OSR besproken worden of het onderscheiden van profielen (REST/WUS) mogelijk moet zijn. Dit zou dan ook in Architectuur beschreven moeten worden	Plannen	Q2	BES/OSR	1
108	Advies schrijven hoe om te gaan met de situatie als één of beide partijen namens zichzelf handelen. Wordt dan het SaaS	Plannen	Q3	Olav/Robert	1

[4] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls/ICT-beveiligingsrichtlijnen-voor-Transport-Layer-Security-v2.pdf
[5] https://docs.google.com/document/d/1r_JeVmbcNQRqFodJUJG3kPbw7HblisiAdOIiO8ZJit0/edit

	profiel toegepast of een (lite) variant				
109	AR vragen waar regels voor XML/JSON transformatie belegd kunnen worden	Plannen	Q3	BES	1
110	AR informeren dat er tussen XML en JSON een onderscheidt gemaakt kan worden in kwaliteit/betrouwbaarheid. Wenselijk om striktere voorschriften voor validatie van XML (en JSON) en mandatering wenselijk zijn. Deze moeten dan ook wel nageleefd (kunnen) worden	Plannen	Q3	BES	1
111	De Edukoppeling documentatie moet nagelopen worden waar een vermelding van PKIoverheid public root certificaten staat	Plannen	Q3	BES	1

BES = Bureau Edustandaard
Grijs = afgehandeld of vervallen

1) 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 Heuseveldt 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
9	Minor release 1.2.1 vastgesteld, stukken (Transactiestandaard, Architectuur, Begrippen) kunnen worden gepubliceerd.	21-6-2017
10	De laatste versie van de Best Practices document (0.2) kan worden gepubliceerd. Daarna van tijd tot tijd aanvullen/aanpassen op basis van input uit implementaties etc.	21-6-2017
11	Alle bestanden relevant voor een bepaald overleg worden op de site in een zip ontsloten	27-09-2017

12	Er kunnen onderwerpen geagendeerd worden die niet direct verband houden met de standaard zelf maar wel met de context van de standaard	27-09-2017
13	Er komt in 2019 een nieuwe medior versie van de standaard (1.3) waarin verduidelijkingen in documentatie worden opgenomen en zaken in lijn worden gebracht met wat nu al in implementaties de praktijk is op basis van eerdere afspraken/afstemming hierover. In 2018 worden de wijzigingen via release notes en conceptversie aangekondigd.	16-05-2018
14	Er wordt geen gelaagd versiebeheermodel (op het niveau van de set en de individuele documenten) meer toegepast. Versionering wordt nu enkel toegepast op het niveau van beschrijvende documenten. Er wordt een ‘Compliance en overzicht’ document opgesteld met een tabel waarin de verschillende vigerende versies van de documenten opgenomen worden. Als voor een bepaald document een nieuwe versie komt dan wordt de oude versie opgenomen in een tabel met voorgaande versies. Voor ketens die een bepaald REST of WUS profiel implementeren is het wel raadzaam om in het programma van eisen niet alleen de versie van de transactiestandaard op te nemen maar ook de versie van de andere normatieve documenten (inclusief de relevante Digikoppeling documenten).	1-05-2019