# Concept Verslag ES werkgroep Edukoppeling

Aanwezig: Robert Kars (DUO), Knut Olav Løite (Topicus, VDOD), Gerald Groot Roessink (DUO), Edwin Verwoerd (Iddink, VDOD), Don de Lange (Kennisnet/OSR), Maarten Kok (SBB), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Bureau Edustandaard).

Afwezig: Peter Dam (Cito)

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

**Datum en locatie**
22 januari 2020, 10:00-13.00 uur, Iddink, Asch van Wijckstraat 55, 3811 LP Amersfoort

**Agenda**

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Edukoppeling REST-profiel
4. Architectuurvisie op het OSR (routeringskenmerk / administratiekenmerk)
5. Uniforme beveiligingsvoorschriften Onderwijs
6. Testen services
7. Terugkoppeling Technisch Overleg (TO) Digikoppeling
8. Issuelijst
9. Rondvraag / Sluiting

## 1. Opening, mededelingen, vaststellen agenda

De agenda wordt zonder wijzigingen vastgesteld.

### 1.1. Mededelingen

Er zijn twee nieuwe leden van de werkgroep, Don de Lange (Kennisnet/OSR) en Maarten Kok (SBB).

## 2. Doornemen verslag en actielijst van 25 september 2019

Verslag

Het verslag van 25 september wordt zonder wijzigingen vastgesteld.

Actiepunten

**#80 Code van DUO beschikbaar stellen**

**Afgehandeld**: De code is op github geplaatst door ontwikkelaar zelf.
https://github.com/bloemendaalconsultancy/edukoppeling

**#88 Binnen het onderwijs beveiligingsvoorschriften centraal beheren**
**Afgehandeld**: Dit is gecommuniceerd naar Edustandaard / IBP en binnenkort start de uniforme beveiligingsvoorschriften werkgroep. Bij bespreking van issues wordt besloten of ook issue #22 gesloten kan worden.

**#89 Edukoppeling pushberichten en Digikoppeling voorschrift WB013**
**Afgehandeld**: Er is een reeds een issue (#47) opgenomen waarin wordt voorgesteld om in Edukoppeling aan te geven dat we afwijken op Digikoppeling door pushberichten toe te staan en dat we hiermee ook een andere formulering voor Digikoppeling WB013 moeten opstellen.

**#90 Aankondiging nieuwe versie van Digikoppeling beveiligingsvoorschriften op community platform aankondigen**
**Afgehandeld**: er is een nieuwe versie (1.2) van de Digikoppeling beveiligingsvoorschriften gepubliceerd en dit is op het discussieplatform gemeld. Er wordt nu voor TLS en ciphers verwezen naar NCSC.

**#91 Op het discussieplatform een post plaatsen over het werkings- en toepassingsgebied van het REST**
**Afgehandeld**, maar discussie rond REST loopt nog.

## 3. Edukoppeling REST-profiel Edukoppeling REST-profiel

Er is een conceptversie van het REST-profiel met de werkgroep gedeeld. Deze versie bevat tevens een aantal aandachtspunten, zoals de behoefte van het duidelijk scheiden van de scope, zowel van de afspraken en standaarden als van de Edustandaard-werkgroepen die erover gaan. We constateren dat dit belangrijker wordt omdat er anders verschillende werkgroepen met vergelijkbare vraagstukken bezig zijn. Het betreft met name Edukoppeling, UBV en IAA en daarnaast ook de activiteiten op het vlak van AMIGO. We zien de UBV voorschriften als een basis voor de beveiliging van het transportkanaal. Deze vervangen op termijn de Digikoppeling beveiligingsvoorschriften. Randvoorwaarden bij deze migratie is wel dat deze (zoveel mogelijk) aansluiten op de Digikoppeling beveiligingsvoorschriften. Mochten er wijzigingen in zitten t.o.v. de huidige situatie dan moeten deze ook in de werkgroep besproken worden en zal er een migratiefase gelden.
Vwb AMIGO is er verwarring vanwege de eerdere 0.9 versie van de documentatie van AMIGO waarin het lijkt of er sprake van eigen invulling vwb beveiliging, transactiepatronen etc,, zaken die onderdeel zijn van UBV cq de Edukoppeling-architectuur. Ondertussen is wel duidelijk geworden dat AMIGO zelf geen afspraak is maar een methodiek om afspraken te maken voor een bepaalde toepassingscontext waarbij gebruik wordt gemaakt van de standaarden etc. die reeds in het kader van Edustandaard worden beheerd. AMIGO is de invulling van een aanpak om te kunnen werken onder architectuur en is daarbij ook onderdeel van de ROSA. Aan nieuwe documentatie wordt gewerkt zodat er geen misverstanden over kunnen bestaan (NB Op de website van Edustandaard is daar al een eerste aanzet toe gegeven).

Een ander belangrijk aandachtspunt is dat we duidelijk moeten kunnen aangeven wat het functionele toepassingsgebied van bepaalde standaarden is. Dit maakt het voor de werkgroep duidelijk wat nog ontwikkeld moet worden en voor gebruikers van Edukoppeling inzichtelijk wanneer een profiel toegepast moet worden. Met het ondersteunen van REST-profielen ontstaat er overlap in het functionele toepassingsgebied. Zo is er straks een WUS/SaaS- en een REST/SaaS-profiel die beide hetzelfde toepassingsgebied hebben. Hiermee moeten we de vraag beantwoord worden hoe ketens een keuze gaan maken. We zien de komst van het REST-profiel als de nieuwe standaard die waarschijnlijk bestendiger is dan het WUS-profiel, maar we zien het niet als een migratiefase waarbij nieuwe implementaties een REST-profiel moeten gebruiken. Het is een hybride fase waarin zowel REST als WUS gebruikt kunnen worden. Ketens maken hierin een eigen keuze en het is aan de keten om tot consensus te komen. Wat wel wenselijk is om voor standaarden ook expliciet een einddatum te benoemen (actiepunt #92). Een standaard verloopt na een bepaalde datum, doe hier een uitspraak over. Zowel het WUS/SaaS-profiel als het REST/SaaS-profiel hebben een eigen versie en einddatum (deze kan overigens bijgesteld worden o.b.v. nieuwe inzichten).

Het REST-profiel is opgesteld op basis van documenten van Kennisplatform API's en met name de API Deisgn rules[1]. De principes zijn overgenomen en in het REST-profiel en er is aangegeven welke verplichting voor het betreffende principe geldt in de context van Edukoppeling. We hebben hiermee de keuze om op punten af te wijken van de API Design rules. Deze hebben namelijk een bredere toepassingsgebied dan het Edukoppeling REST/SaaS-profiel. Een aantal van de voorschriften worden tijdens het overleg besproken:

- De API Design rules onderkennen browsers ook als client en hiermee wordt bijvoorbeeld Cross-Origin Resource Sharing (CORS) relevant. In het REST-profiel wordt dit niet van toepassing geacht. Verder zullen we mogelijk bij andere (REST) profielen gebruik maken van principes die we nu binnen het REST SaaS profiel buiten beschouwing laten. Vanuit Forum Standaardisatie loopt er ondertussen een openbare consultatie[2] om de Design Rules op te nemen op de pas-toe-of-leg-uit lijst op te nemen. De verwachting is overigens dat de Design Rules de komende tijd nog wel verder ontwikkeld gaan worden.

- Bij enkele principes is de tekst aangepast en wijkt deze af van verwoording in de API Design rules. We willen in het REST-profiel exact de verwoording van de API Design rules overnemen en dan aangeven of we hier van afwijken en waarom.

- Het REST-profiel ondersteund geen API-keys om de afspraak eenvoudig te houden en er geen noodzaak wordt gezien om deze toe te passen. Men heeft tenslotte via de point to point verbinding op basis van tweezijdige TLS al voldoende informatie over de afnemer. Er wordt aangegeven dat het OSR in het koppelvlak met tweezijdige TLS wel een API-key wil toepassen omdat dienstaanbieders meerdere OIN's hebben. Er is hier wat onduidelijkheid over en dit wordt volgende keer in meer detail besproken.

- Voor OAuth geldt in principe hetzelfde als voor de API-key, we willen het basis REST-profiel eenvoudig houden met hetzelfde functionele toepassingsgebied als WUS. Hiermee is er nog geen noodzaak voor OAuth, maar dit kan op termijn wel een rol gaan spelen bij REST-profielen

- De essentie van de SaaS profielen is het kunnen routeren tussen de rol van verwerker en eindorganisatie. Deze routering is nu nog niet in het REST-profiel uitgewerkt. Er zijn wel een aantal mogelijkheden opgenomen hoe dit ingericht kan worden. Er wordt aangegeven dat Topicus bij Centraal aanmelden de koppeling bijna volledig conform het REST-profiel heeft ingericht. Ook daar is echter nog geen routering ingericht en de mandateringen worden niet centraal (via OSR) vastgelegd. Het SIS haalt de aanmelding op en in de URI zit een kenmerk van de school en in resource zelf zit BRIN van de school. Verder gebruikt Centraal aanmelden OAuth als extra check op OIN

In het REST/SaaS-profiel wordt de term S2S (system-to-system) gebruikt en er wordt besloten de term M2M (machine-to-machine) te gebruiken. Dit sluit beter aan bij het eerdere H2M2M-visiedocument.

De conclusie is dat we een basis hebben die in profiel opgenomen kan worden zonder de aandachtspunten. In de nieuwe versie worden alleen de voorschriften opgenomen worden en moet er nog invulling gegeven worden aan o.a. het routeringsvraagstuk.

## 4. Architectuurvisie op het OSR (routeringskenmerk / administratiekenmerk)

Het OSR komt voort uit het H2M2M-visiedocument. Partijen, zoals DUO en Kennisnet (OSO) hebben een eigen serviceregister en het wordt wenselijk geacht om de benodigde functies centraal in te richten. Deze functies kunnen zo onderwijsbreed gestandaardiseerd worden en hebben een nauwe relatie met de Edukoppeling-standaard. Dit laatste geeft ook aan dat het voor Edukoppeling van belang is dat de functies goed aansluiten op de standaard en hiermee zien we ook de Edukoppeling werkgroep als een belangrijke stakeholder bij het beheer

[1] https://docs.geostandaarden.nl/api/API-Designrules/
[2] https://www.forumstandaardisatie.nl/nieuws/openbare-consultatie-rest-api-design-rules-epub-32-en-oauth

van de OSR. Dit is nu nog niet zo georganiseerd. Dit moet onder de aandacht gebracht worden bij de Architectuurraad en de beheerorganisatie van het OSR (Kennisnet). Hiervoor wordt een actiepunt geregistreerd (actiepunt #93). Daarnaast moet in de Edukoppeling Architectuur ook beschreven zijn welke eisen (functies) Edukoppeling aan een ketenfunctie als het OSR stelt.

Voor Edukoppeling zijn de registratie en verificatie van een mandatering belangrijke functies. Een mandatering is op het organisatieniveau (OIN). Verder is in het identificatie- en authenticatiedocument al gesteld dat er ook administraties onderkend moeten kunnen worden. Een SaaS-leverancier en een onderwijsinstelling stellen samen het administratienummer vast. Dit is feitelijk de suffix van het OIN van de onderwijsinstelling (eindorganisatie). Momenteel is er in het OSR een routeringskenmerk opgenomen als onderdeel van het endpoint. Er zijn nu partijen die de mandatering willen kunnen controleren op het niveau van een administratie voordat er mogelijk een endpoint geregistreerd is. De huidige inrichting van het OSR maakt dit niet mogelijk en daarnaast is het ook niet wenselijk om een administratienummer/routeringskenmerk onderdeel te laten zijn van het endpoint. Dit zou een apart te beheren gegeven moeten zijn. Dit samen met het gebruik van een API-key zijn onderwerpen die bij het volgende overleg in meer detail besproken zullen worden. We willen een duidelijk beeld hebben waar de Edukoppelingdocumentatie of OSR-functies aangepast zouden moeten worden.

Er wordt aangegeven dat ondertussen ook het RIO register operationeel is. De invoering verloopt per sector en momenteel zijn de gegevens voor het VO en het MBO beschikbaar en kunnen ontsloten worden. De Edukoppelingdocumentatie zal op verschillende punten aangepast moeten worden aan de toepassing van RIO. De verwachting is dat een onderwijsaanbieder (identifier) dynamischer is dan een onderwijsinstellingserkenning (BRIN4). Moet er om die reden gebruik blijven worden gemaakt van de onderwijsinstellingserkenning omdat partijen hier nu al een bepaalde methodiek voor ontwikkeld hebben waarbij men de BRIN4 als basis gebruikt (default). Het niveau van een onderwijsaanbieder is fijnmaziger en maakt het gebruik van veel suffixen overbodig, zeker als er meerdere onderwijsaanbieders gerelateerd zijn aan een onderwijsinstellingserkenning (BRIN4), iets wat in het MBO meer regel dan uitzondering is en ook in het VO veelvuldig voorkomt. Bovendien zal een onderwijsaanbieder ook weer niet zo dynamisch zijn is de verwachting. Moet dan de instellingserkenning (wat formeel een erkenning is en geen aanduiding van een organisatie) toch gehanteerd blijven worden en mogelijk daaronder de registratie op onderwijsaanbiederniveau gebruikt worden? Er wordt aangegeven dat een onderwijsaanbieder onder een onderwijsbestuur valt, maar een bestuur wordt binnen RIO niet geïdentificeerd op basis van een BRIN4. Het lijkt in ieder geval wenselijk om gebruik te maken van een stabiel en of dat ook de onderwijsaanbieder kan zijn is nog een punt van nader onderzoek. Dit onderwerp zou een volgende keer apart besproken moeten worden om een keuze te maken of de huidige methodiek o.b.v. BRIN4 vervangen kan worden met een identiteit van een onderwijsaanbieder (actiepunt #94).

## 5. Uniforme beveiligingsvoorschriften Onderwijs

De UBV voorschriften zijn met name bedoeld voor transportbeveiliging (TLS / Ciphers). Met de UBV-voorschriften kan de onderwijssector afwijken van de nationale voorschriften (Digikoppeling beveiligingsvoorschriften / NCSC). Er wordt aangegeven dat het belangrijk is dat de UBV-voorschriften aansluiten op de behoeftes van Edukoppeling. Het moet voor gebruikers van Edukoppeling ook duidelijk zijn welke documenten/voorschriften van Digikoppeling blijven gelden en waar UBV impact op heeft en deze overschrijft.

Daarnaast wordt onderkend dat er nu niet bij iedere uitwisseling waarbij sprake is van persoonsgegevens (of gegevens die anderszins dezelfde beveiliging vereisen) een Edukoppeling-implementatie wordt gebruikt. Het dus wenselijk dat er op een hoger niveau dan Edukoppeling dezelfde maatregelen voor transportbeveiliging ingericht worden. Een belangrijke nuance hierbij is echter wel dat deze ketens (op termijn) naar Edukoppeling zouden moeten migreren.

## 6. Testen services

We zijn niet aan dit onderwerp toegekomen en wordt een volgende keer besproken.

## 7. Terugkoppeling Technisch Overleg Digikoppeling

We zijn niet aan dit onderwerp toegekomen en wordt een volgende keer besproken.

## 8. Issuelijst

We zijn niet aan dit onderwerp toegekomen en wordt een volgende keer besproken.

## 9. Rondvraag en sluiting

Er waren geen opmerkingen

## 10. Actielijst

| # | Omschrijving | Status | Einddatum | Actie-houder | Prio |
|---|---|---|---|---|---|
| 80 | Code van DUO beschikbaar gesteld op github https://github.com/bloemendaalconsultancy/edukoppeling | Afgerond | Q3 2019 | BES /DUO | 2 |
| 88 | Advies voor SR opstellen: beveiligingsvoorschriften centraal beheerd door IBP | Afgerond, er wordt een werkgroep uniforme beveiligingsvoorschriften ingericht | Q3 2019 | IBP/Edukoppeling en AR | 1 |
| 89 | Edukoppeling staat pushberichten toe en hierdoor willen we afwijken op WB013 (*Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht*). We willen dit in de volgende release van de Transactiestandaard opnemen | Afgerond, issue aangemaakt (#47) nog bespreken in welke release we dit meenemen | Q4 2019 | BES | 2 |
| 90 | Nieuwe versie Digikoppeling beveiligingsvoorschriften (TLS ciphers) aankondigen op community platform en Edustandaard nieuwsbrief. Voor TLS & ciphers wordt verwezen naar NCSC | Afgerond, melding op platform geplaatst | Q3 2019 | BES | 1 |
| 91 | Op het discussieplatform een post plaatsen over het werkings- en toepassingsgebied van het REST en WUS profiel. Dit is de basis voor het voorstel aan de standaardisatieraad. | Afgerond, maar discussie rond REST loopt nog. | Q3 2019 | DUO (Gerald) | 1 |
| 92 | In overzicht met relevante standaarden aangeven tot welke datum verwacht wordt dat de standaard de status “in gebruik’ heeft. | Plannen | Q2 2020 | BES | 1 |
| 93 | Het is van belang dat de Edukoppeling werkgroep stakeholder | Loopt | Q2 2020 | BES | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | is bij beheer OSR. Dit onder aandacht brengen bij de Architectuurraad en de beheerorganisatie van het OSR (Kennisnet) | | | | |
| 94 | Kan de huidige methodiek o.b.v. BRIN4 vervangen worden met een identiteit van een onderwijsaanbieder. Impact documentatie | Plannen | Q2 2020 | BES | 1 |

**BES = Bureau Edustandaard**
**Grijs = afgehandeld of vervallen**

## 11. 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.<br>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 |
| 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 |