

Concept Verslag ES werkgroep Edukoppeling

Aanwezig: Robert Kars (DUO), Gerald Groot Roessink (DUO), Edwin Verwoerd (Iddink, VDOD), Don de Lange (Kennisset/OSR), Maarten Kok (SBB), Brian Dommissie (Kennisset, voorzitter), Erwin Reinhoud (Bureau Edustandaard).

Afwezig: Olav Løite (Topicus, VDOD), Peter Dam (Cito),

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

Datum en locatie

18 maart, 10:00-13.00 uur, Telefonisch

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Edukoppeling Architectuur 2.0
4. Edukoppeling REST profiel versie 0.2
5. Testen services
6. Terugkoppeling Technisch Overleg (TO) Digikoppeling
7. Issuelijst
8. Rondvraag / Sluiting

1. Opening, mededelingen, vaststellen agenda

De agenda wordt zonder wijzigingen vastgesteld.

1.1. Mededelingen

De leden wordt gevraagd om REST/SaaS-profiel en Architectuur 2.0 te reviewen en tekstuele aanpassingen in googledoc te verwerken.

2. Doornemen verslag en actielijst van 22 januari 2020

Verslag

Het verslag van 22 januari 2020 wordt zonder wijzigingen vastgesteld.

Actiepunten

<u>92</u>	<u>In overzicht met relevante standaarden aangeven tot welke datum verwacht wordt dat de standaard de status "in gebruik" heeft.</u>	<u>Plannen</u>	<u>Q2 2020</u>	<u>BES</u>	<u>1</u>

93	<u>Het is van belang dat de Edukoppeling werkgroep stakeholder is bij beheer OSR. Dit onder aandacht brengen bij de Architectuurraad en de beheerorganisatie van het OSR (Kennisnet)</u>	<u>Loopt</u>	<u>Q2 2020</u>	<u>BES</u>	<u>1</u>
94	<u>Kan de huidige methodiek o.b.v. BRIN4 vervangen worden met een identiteit van een onderwijsaanbieder (RIO)? Werkwijze beschrijven/bespreken waar BRIN4 stabiele default is en op onderwijsaanbieder niveau indien er meerdere zijn. Heeft impact op documentatie</u>	<u>Plannen</u>	<u>Q2 2020</u>	<u>BES</u>	<u>1</u>

Alle actiepunten zijn gepland voor de komende 3 maanden. Op dit moment ligt de prioriteit bij het REST-profiel en de herziening van de Edukoppeling architectuur.

3. Edukoppeling Architectuur 2.0

3.1. Nieuwe indeling

De focus van de architectuur was tot nu toe Digikoppeling en het WUS-profiel. Met de komst van een REST-profiel moet de architectuur (en overige docs) aangepast worden om het een consistent geheel te maken waarbij we ook de ontwikkelingen rond REST een plaats geven. Hierbij moeten we ook besluiten hoe ver we hierin gaan. Uitgangspunten voor versie 2.0 zijn:

1. Voldoet de nieuwe indeling? Inhoudelijk/tekstueel zal het nog de nodige iteraties vragen.
 - Er wordt besloten dat de nieuwe indeling toegepast kan worden en mogelijkheden biedt om meerdere profielen dan alleen de SaaS context te beschrijven.
 - Het is belangrijk te benoemen in de tekst van het SaaS-profiel (actiepunt #95) dat de SaaS-profielen ook gebruikt kunnen worden door onderwijsinstellingen die eigen systemen gebruiken voor M2M gegevensuitwisseling. Het is dan in de context van het Edukoppeling SaaS-profiel wel wenselijk dat dit ook geregistreerd wordt in het Serviceregister. Ketenpartijen kunnen zo bij de toepassing van het profiel een eenduidige werkwijze toepassen.
 - Er is al de wens om ook een profiel voor openbare data te definiëren in de architectuur. Gerald wil dit oppakken.
 - Maarten geeft aan dat de informatie die White label ontsluit, openbare data is en partijen (SIS leveranciers/Scholen) zich kunnen abonneren op de levering van gegevens (mutaties). Partijen kunnen de data niet wijzigen. Er zijn zo met RIO al verschillende implementaties die de basis voor een openbare data-profiel kunnen vormen. De gegevens van het OSR wordt niet als openbare data beschouwd.
2. Kan de naamgeving voor SaaS-profielen gewijzigd worden in WUS/SaaS-profiel en REST/SaaS-profiel? Beide profielen ondersteunen de huidige rollen van het SaaS-profiel.
 - Er wordt besloten dat de nieuwe naamgeving toegepast kan worden in de documentatie.
3. Voldoen de geformuleerde functionele toepassingsgebieden? Er is een algemeen functioneel toepassingsgebied in de Architectuur opgenomen, een meer specifiek toepassingsgebied geldt per profiel.
 - Er wordt besloten dat de toepassingsgebieden (voorlopig) voldoen.
 - Er wordt wel een opmerking gemaakt over het organisatorisch werkingsgebied. Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling tussen informatiesystemen van partijen **met en binnen de onderwijs**. De tekst zal hierop aangepast worden (actiepunt #96).
4. Net als bij Digikoppeling hanteren we bij de Edukoppeling profielen het uitgangspunt dat de natuurlijke personen (actoren binnen eindorganisatie die handelen) geen rol spelen. We besluiten dit te handhaven.

- Er wordt opgemerkt dat dit op termijn mogelijk gaat veranderen. In de toekomst zal in de architectuur en profielen hier waarschijnlijk rekening mee moeten worden gehouden. Vanuit AVG kan het wenselijk zijn om consent expliciet door de hele keten door te kunnen geven. Het gaat dan met name om use cases die niet in het SaaS-profiel passen, veelal use cases waar de actor namens zichzelf handelt. Standaarden bieden hier meer en meer ondersteuning voor.
5. De beschrijving van het serviceregister (OSR) in de Architectuur is gehandhaafd en gezien de discussie van afgelopen keer wordt gevraagd of er nu voldoende beschreven is.
 - Er wordt aangegeven dat er (tijdelijk) een plaat is opgenomen (figuur 3) om ook het registratieproces te duiden en discussie te voeren welk detailniveau beschreven moet worden.
 - Er wordt aangegeven dat het huidige detailniveau voldoende is (figuur 3 verwijderen). Wel moet er nog een functionaliteit toegevoegd worden, het serviceregister is de authentieke bron voor OINs in het onderwijs (zie discussie OSR).
 6. Het benoemen van zowel profielen en een aantal generieke bedrijfstransacties in de architectuur is gehandhaafd. Een profiel beschrijft een Message Exchange Pattern (MEP) binnen een profiel (enkel req-resp). Een bedrijfstransactie beschrijft de uitwisseling als onderdeel van een proces, er zijn mogelijk meerdere MEPs relevant.
 - Er wordt aangegeven dat het wenselijk is de generieke bedrijfstransacties goed aan te laten sluiten wat men bij AMIGO-aanpak onderkent. Er wordt besloten dat door de analisten die met de AMIGO-methode werken aangegeven moet worden wat ontbreekt. Vanuit BES zal ondersteuning worden gegeven bij een dergelijke analyse om zo gezamenlijk te bepalen of er nu wat ontbreekt (actiepunt #97).

3.2. OSR

In de Edukoppeling architectuur wordt een Onderwijs Service Register als ketenfunctie beschreven. Het serviceregister kent generieke functionaliteit en specifieke functionaliteit voor de SaaS-profielen, het centraal beheer van mandaten. We bespreken de theorie (Edukoppeling), huidige praktijk (de implementatie van het OSR) en een aantal RFC's.

3.2.1. Theorie: OSR functies voor Edukoppeling

Voor Edukoppeling architectuur 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 administratienummers 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).

Een school heeft typisch de rol van een eindorganisatie en registreert een mandatering. De school kan ook verantwoordelijk zijn voor alle drie de rollen. De LAS-leverancier (Supplier/Administratiepakket leverancier) mag de gegevens verwerken die in de verwerkersovereenkomst met school zijn opgenomen. Het identificerend kenmerk (juridische entiteit) voor een LAS-leverancier is het kvknr (OIN). NB het zou ook het rsin kunnen zijn maar in de praktijk komt die in het onderwijs niet voor als identificerend kenmerk. In technische zin maakt het niet uit welke specifieke service/softwarepakket/applicatie deze gegevens uitwisselt zolang deze maar onder de betreffende juridische entiteit (PKI-o-certificaat met betreffend OIN van verwerker) valt en het proces (gegevens) betreft die is overeengekomen met school.

Tijdens het overleg wordt gesteld dat een serviceregister in de context van Edukoppeling de volgende algemene functies heeft:

- Het serviceregister heeft een telefoonboek-functie voor M2M services (o.a. EK WUS/REST) binnen de onderwijsketen. Een LAS-leverancier heeft typisch de rol van Verwerker en is verantwoordelijk voor het registreren van het Service Endpoint.

- Ten behoeve van het WUS 2W-be-SE profiel kunnen partijen hun publieke PKI-o-certificaat in het serviceregister registreren. De verzender kan deze ophalen en het bericht versleutelen met publieke sleutel van ontvanger.
- Het serviceregister is de authentieke bron van OINs in het onderwijs (niet HR of RIO). Het is belangrijk om eenduidig met identiteiten om te gaan. We zien bijvoorbeeld dat soms een BRIN6 toegepast wordt, dit moet voorkomen worden en hierin speelt een centraal serviceregister een belangrijke rol.

Er wordt opgemerkt dat in praktijk het WUS 2W-be-SE profiel niet gebruikt wordt, in praktijk hoeft een serviceregister (OSR) dit dus niet te ondersteunen totdat partijen hier wel behoefte aan hebben.

Tijdens het overleg wordt gesteld dat een serviceregister in de context van het Edukoppeling SaaS-profiel ook de volgende functies heeft:

- Een eindorganisatie (school) kan een mandatering registreren voor een verwerker (SaaS-leverancier). Hierbij moet in de documenten opgemerkt worden dat een eindorganisatie (school) ook zelf alle drie de rollen kan uitvoeren.
- Bij zowel bij een push als pull gegevensuitwisseling willen partijen de mandatering kunnen verifiëren.

Er wordt besloten om in de architectuur bij bouwstenen de functies van het OSR te beschrijven. Zo houden we in de architectuur een overzicht wat we aan functies voor Edukoppeling nodig achten en wat momenteel in praktijk via het OSR beschikbaar is. Dit wordt samen met beheerder OSR uitgevoerd (actiepunt #98).

3.2.2. Praktijk: Wijzigingsvoorstellen OSR

RFC OSR 3

In de RFC wordt het volgende beschreven:

- Diverse leveranciers van administratiesystemen hebben tijdens een technisch overleg van de dienst Overstapservice Onderwijs (OSO) aangegeven dat zij voor verschillende diensten soms meerdere OIN's gebruiken in verband met de inzet en looptijd van (PKI-overheids-)certificaten en de migratie hiervan.
- In de context van deze wijziging verplaatst de registratie van het OIN van "leveranciersniveau" naar "leverancier-per-dienst-niveau". Het is belangrijk dat wanneer een leverancier voor een nieuwe dienst gebruik wil maken van het OSR er ten minste één OIN wordt doorgegeven ter registratie.
- De OSR implementatiespecialist registreert de OINs als onderdeel van een leveranciersgroep, hiermee wordt aangegeven welke bij elkaar horen. Per dienst kunnen meerdere OIN's worden geregistreerd.
- De mandatering wordt op supplier-/leveranciersgroep geregistreerd, niet op organisatieniveau.

Met deze wijziging gaat het OSR mandateringen anders registreren dan vanuit Edukoppeling wordt beoogd. Een partij heeft in principe altijd 1 OIN, deze wordt gebruikt in een bepaalde ketenuitwisseling (service) waarvoor ook een mandatering bestaat. Er wordt in de werkgroep wel onderkend dat er reorganisaties/overnames kunnen plaatsvinden, maar dit is een overgang van het ene OIN naar het andere waar de normale procedures gevolgd moeten worden die ook gelden bij een initiële levering van een dienst op basis van een OIN. Een migratiefase moet in de keten eigenlijk procesmatig voorkomen worden. Het is niet wenselijk dat er voor 1 organisatie meerdere OIN's zijn. Een bepaalde verwerker (SaaS-leverancier) heeft altijd 1 OIN en de mandatering is een samenstelling van dit OIN en het OIN van de eindorganisatie (school). De werkgroep stelt dat als een dochteronderneming met een eigen OIN is geregistreerd deze dan ook gebruikt in Edukoppeling en dat tevens de mandatering ook op dat is OIN geregistreerd. Als een dochteronderneming het OIN van de moederorganisatie gebruikt in Edukoppeling dan is de mandatering hierop gebaseerd. Dit betekent dus dat met wijziging van de verantwoordelijke organisatie (OIN) voor een systeem, ook de mandatering en certificaat verandert. We onderkennen wel dat er verschillende afdelingen kunnen zijn binnen organisaties die elk weer eigen systemen hebben, in principe is vanuit Edukoppeling de gedachte dat op basis van de mandatering duidelijk gesteld wordt wie verantwoordelijk is. De moederorganisatie heeft wel een eindverantwoordelijkheid dat er inzicht is waar welke gegevens verwerkt worden (en deze voldoen aan de AVG).

De RFC geeft ook aan dat er duidelijkheid nodig is over de governance van het OSR. Dit werd bij het vorige overleg ook al aangekaart en er is hiervoor ook al een actiepoint geregistreerd. We zien dat deze RFC vanuit OSO-keten is ingediend en deze gebruikt nog geen Edukoppeling. De situatie kan ontstaan dat bij OSR verschillende (redundant/tegenstrijdig) functionele behoeftes belegd worden omdat ketens gegevensuitwisseling nog verschillend ingericht hebben (geen Edukoppeling). Het is wenselijk inzicht te hebben in de governancestructuur en wat de positie van de Edukoppeling werkgroep hierin is.

Conclusie van de werkgroep is: geen meerdere OIN's (en daarmee ook PKI-certificaten) tegelijkertijd toestaan voor 1 leverancier, ook voor de mandatering. Mandatering kan wel overgenomen worden van een leverancier door een moedermaatschappij, maar dan komt er ook een ander OIN en certificaat aan te hangen. Voor de eventuele migratiefase moet er een procesmatige oplossing worden gevonden.

RFC OSR 2 API-key

In de RFC wordt het volgende beschreven:

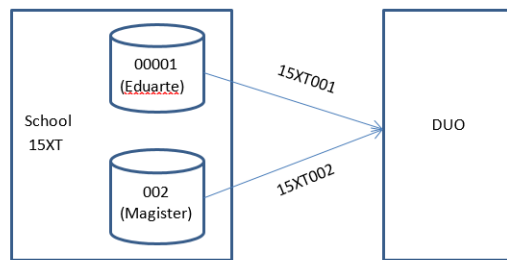
- Het OSR kan verschillende softwarepakketten van één leverancier niet onderscheiden. Met de introductie van de nieuwe functionaliteit dat het OSR moet kunnen omgaan met meerdere OIN's per leverancier is het niet meer houdbaar dat het OSR niet specifiek kan vaststellen van welk softwarepakket/leverancier het verzoek binnenkomt. Het voorstel is om een API-key per softwarepakket voor leveranciers te registreren.
- Bij elk verzoek dat een leverancier doet moeten zij de API-Key meegeven in de header. Zo kunnen we exact onderscheiden welk softwarepakket het verzoek doet en deze registreren in onze logs. De verificatie gebeurt dus op 2 criteria: een geldig certificaat én de API-key.

In Edukoppeling wordt een API-key niet nodig geacht. Het bestaande WUS/SaaS-profiel ondersteunt dit niet en bij recente bespreking van het REST/SaaS-profiel werd aangegeven dat men anders dan bij OSR geen functionele behoefte heeft voor een API-key als er met 2-zijdige TLS en een OIN gewerkt wordt. Er wordt tijdens de bespreking wel een nuance aangegeven. We hebben bij OSR RFC 3 al vastgesteld dat een bepaalde organisatie (OIN) het mandaat heeft en verantwoordelijk is voor de verwerking. Bij Edukoppeling zijn afspraken op organisatieniveau, met de API-key komt ook het applicatieniveau in beeld. Het kan voor organisaties handig zijn om bij een uitwisseling ook een pakket te kunnen identificeren. Organisaties groeien en er zijn meerdere afdelingen bij bepaalde processen betrokken. Voor de betrokken ketenpartijen en de organisatie zelf kan het handig zijn om bij een gegevensuitwisseling ook een pakket te kunnen identificeren en loggen. Dit heeft in principe geen impact op de SaaS-profielen en de formele afspraken die hierbij gelden. Het is wel handig dat partijen die hier behoefte aan hebben dit uniform uitvoeren. Er wordt gedacht aan een Edukoppeling best practice. Om dit nader uit te werken wordt een actiepoint (#99) geregistreerd. Een API-key is wel specifiek voor het REST/SaaS-profiel. Of er voor het WUS/SaaS-profiel ook een best practice moet komen moet nog vastgesteld worden.

RFC XXX:

Er is nog geen OSR RFC, maar er is wel een document over het wijzigingsvoorstel. Deze zal nog met leden gedeeld worden (actiepoint #100). Hierin wordt het volgende beschreven:

- In de Edukoppeling architectuur wordt een Service Register beschreven. De functie is centraal beheer van mandaten en services met hun endpoints. Wat er echter niet in staat is wie welke service aan mag roepen, oftewel een centrale autorisatietabel. We willen bespreken of het wenselijk is deze autorisaties ook centraal te beheren en zo ja, hoe.
- 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.



Figuur 1 - DUO wil bij binnenkomende berichten kunnen autoriseren op basis van de mandatering (Edukoppeling I&A administratienummer).

De functionele behoefte is het kunnen autoriseren van binnenkomende berichten en het voorkomen van broadcasten naar verschillende administraties bij uitgaande berichten. Edukoppeling beschrijft in het I&A document het OIN van een school. In dit OIN wordt de suffix gebruikt om een administratienummer op te nemen. In het I&A staat ook beschreven dat dit in de basis de gevraagde functie biedt. Dit is echter niet expliciet in de architectuur beschreven.

Gezien het serviceregister (OSR) de authentieke bron van OINs is, zou impliciet aan deze functionele behoefte invulling kunnen worden gegeven, maar momenteel is in het OSR het routeringskenmerk (administratienummer) onderdeel van het endpoint. In het suffix van het OIN van de school is geen administratienummer opgenomen. DUO gebruikt nog een eigen serviceregister (RAV) en hierin wordt wel een OIN en administratienummer geregistreerd. In de huidige situatie zou DUO met de overgang naar OSR dus deze functionaliteit verliezen.

Er wordt besloten dit in Edukoppeling-architectuur te beschrijven. Het OIN met suffix die onderdeel van mandatering is kan worden gebruikt voor een autorisatie (actiepunt #101). Verder wordt het voorstel van DUO als advies vanuit Edukoppeling naar beheerder OSR gestuurd (actiepunt #102).

4. Edukoppeling REST-SaaS-profiel

Er is er een REST/SaaS-profiel (versie 0.2) opgesteld. Het REST-profiel is opgesteld op basis van documenten van Kennisplatform API's en met name de API Design rules¹. In de 0.2 versie zijn de aandachtspunten die in de 0.1 versie zaten verwijderd. Er worden een aantal generieke voorschriften onderkend (die ook relevant zijn voor het WUS/SaaS-profiel) en een aantal die specifiek zijn voor het REST-profiel.

Met de komst van het REST-profiel vormt Digikoppeling niet meer de basis, omdat hier nu niets over REST is opgenomen. Alleen voor het WUS/SaaS-profiel wordt er nu aangesloten op Digikoppeling. Dit geldt overigens ook indirect voor de transportbeveiliging voor het REST/SaaS-profiel en WUS/SaaS-profiel, daar wordt UBV leidend, maar blijven we wel op een aantal punten Digikoppeling volgen. Vanuit het TO Digikoppeling is wel aangegeven dat men de komende tijd hieraan gaat werken. De verwachting is dus dat er op termijn ook op dit punt weer op Digikoppeling aangesloten kan worden. Wat hiervan de impact is zal tzt in werkgroep besproken worden.

Helaas was er niet voldoende tijd om alle aspecten van het REST/SaaS-profiel te bespreken. We willen de leden dan ook vragen de keuzes hieronder nog eens goed door te nemen en aan te geven als een alternatief de voorkeur heeft. Daar waar nog geen keuze is gemaakt zullen we proberen via andere kanalen nog tot een besluit te komen.

1. Functioneel toepassingsgebied

Er zijn geen opmerkingen over het functioneel toepassingsgebied en is hiermee vastgesteld.

2. Generieke voorschriften SaaS-profielen

Er zijn geen opmerkingen over de splitsing tussen generieke en specifieke voorschriften WUS en REST. Wel zullen de teksten nog aangepast worden en een aantal paragrafen worden gecombineerd. Dit wordt als onderdeel van de 0.3 versie besproken.

¹ <https://docs.geostandaarden.nl/api/API-Designrules/>

3. Gebruik van de UBV PKI-o beveiligingsvoorschriften

Er wordt aangegeven dat de voorzitter van de UBV werkgroep bij Architectuurraad aangegeven heeft dat het UBV in principe profiel 443 zal vereisen. Er wordt gesteld dat het vereisen van poort 443 onwenselijk is voor de M2M-uitwisseling, dit gaat tegen de huidige Edukoppeling voorschriften in die na uitvoerige discussie zijn opgesteld. Er is in het verleden besloten om niet poort 443 te vereisen om meerdere redenen, en niet alleen omdat dit geen common practice is binnen het onderwijs. Er wordt besloten dat DUO en Iddink de aanvullende argumentatie opleveren zodat deze met UBV besproken kan worden (Actie #104). Het resultaat kan zijn dat het algemene UBV M2M profiel afwijkt van het UBV Edukoppeling profiel.

De UBV-voorschriften zijn nu nog in ontwikkeling en we streven ernaar dat de EK Architectuur en REST/SaaS-profiel voor de zomer door EK werkgroep vastgesteld is en dat dit ook voor het UBV Edukoppeling profiel geldt.

In het REST/SaaS-profiel en WUS/SaaS-profiel zal een verdeling worden gemaakt tussen transportbeveiliging en berichtbeveiliging. Dit is wenselijk omdat de Edukoppeling werkgroep nog verantwoordelijk is voor voorschriften rond het WUS/SaaS-profiel met ondertekening en versleuteling (2W-be-S en 2W-be-SE).

4. Toegepast voor zowel bevestigingen als meldingen opnemen in Architectuur

Voorstel niet besproken, in versie 0.3 willen we het uit profiel verwijderen en opnemen in Architectuur.

5. PKI infrastructuur teksten aanpassen

Voorstel niet besproken, in versie 0.3, verwijzingen naar Digikoppeling verwijderen (DK is nu alleen specifiek voor WUS relevant) en PKI-o is voorschrift transportbeveiliging.

6. Identificatie & Authenticatie

Voorstel niet besproken, in versie 0.3, tekst inkorten, er is ondertussen een Identificatie en Authenticatie document.

7. Gebruik Onderwijs Serviceregister

Er is besloten dat de documentatie over OSR in Architectuur volstaat (SaaS-profiel). Wel moet de eerder aangegeven beschrijving rond autorisatie/broadcasten opgenomen worden. Ook komt er met het REST-profiel de mogelijkheid dat (gemandateerde) partijen met een bepaald profiel, of 2 verschillende profielen, gegevens uitwisselen. Er moet met OSR besproken worden of het onderscheiden van profielen mogelijk moet zijn. Dit zou dan ook in Architectuur beschreven moeten worden (actiepunt #103)

8. Routing o.b.v. (HTTP header/JWT)

Voorstel niet besproken, in versie 0.3, wordt een voorstel uitgewerkt als er geen input van leden komt. Er is hierover ook een oproep geplaatst op het discussieplatform.

9. API-03: Only apply default HTTP operations

Voorstel niet besproken, in versie 0.3 sluiten we aan op WUS en vereisen een POST. GET is onwenselijk als input query vertrouwelijke gegevens bevat (ivm logging op server etc.)

10. API-12: Allow access to an API only if an API key is provided, voor REST SaaS-profiel geldt dat een API-key niet gebruikt wordt

Voorstel niet besproken, in versie 0.3 wordt een API-Key toegestaan (Could: op basis van nog te beschrijven best practice).

11. API-14: OAuth 2.0 can be used for authorisationidentificatie & Authenticatie

Voorstel niet besproken, in versie 0.3 geen Oauth toegestaan (Won't)

5. Testen services

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

6. Terugkoppeling Technisch Overleg Digikoppeling

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

7. Issuelijst

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

8. Rondvraag en sluiting

Er waren geen opmerkingen. De volgende bijeenkomst zal eind april, begin mei worden.

9. 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 (<i>Indien WS-Security wordt toegepast, is het controleren van de signature door de ontvangende partij verplicht</i>). 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	Plannen	Q2 2020	BES	1

	datum verwacht wordt dat de standaard de status "in gebruik" heeft.				
93	Het is van belang dat de Edukoppeling werkgroep stakeholder is bij beheer OSR. Dit onder aandacht brengen bij de Architectuurraad en de beheerorganisatie van het OSR (Kennisnet)	Loopt	Q2 2020	BES	1
94	Kan de huidige methodiek o.b.v. BRIN4 vervangen worden met een identiteit van een onderwijsaanbieder. Impact documentatie	Plannen	Q2 2020	BES	1
95	In architectuur aangeven dat de SaaS-profielen ook gebruikt kunnen worden door onderwijsinstellingen die de eigen systemen gebruiken voor M2M gegevensuitwisseling.	Plannen	Q2	BES	1
96	Werkingsgebied in Architectuur aanpassen: met en binnen de onderwijs	Plannen	Q2	BES	1
97	Analyse AMIGO (versie?) om vast te stellen of nu nog wat ontbreekt bij beschrijving bedrijfstransacties in Architectuur	Plannen	Q2	BES/Leden	1
98	In de architectuur bij bouwstenen de functies van het OSR kort te beschrijven (praktijk)	Plannen	Q2	BES/OSR	1
99	Best practice beschrijven van toepassing APY-key (REST profiel - OSR)	Plannen	Q2	BES/OSR	2
100	DUO deelt met leden het wijzigingsvoorstel voor OSR	Plannen	Q2	DUO	1
101	In architectuur opnemen dat binnen Edukoppeling het OIN school (met suffix) onderdeel van mandatering is en kan worden gebruikt voor een autorisatie (vaststellen dat WS-A/REST headr oin suffix overeenkomt met suffix mandatering	Plannen	Q2	BES	1
102	Voorstel van DUO (#100) als advies vanuit Edukoppeling naar beheerder OSR sturen	Plannen	Q2	BES	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
104	Argumentatie inbrengen in UBV werkgroep tegen het verplicht stellen van poort 443 voor M2M verkeer	Maandag 30 maart is de eerstvolgende werkgroep UBV	Q2	DUO, Iddink	1

BES = Bureau Edustandaard

Grijs = afgehandeld of vervallen

10. 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 uitsluitel 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 routing 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