Concept Verslag ES werkgroep Edukoppeling

Aanwezig: Robert Kars (DUO), Gerald Groot Roessink (DUO), Olav Løite (Topicus, VDOD), Pieter Bruring (Kennisnet, OSR), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, Edustandaard).

Afwezig: Peter Dam (Cito), Edwin Verwoerd (Iddink, VDOD), Maarten Kok (SBB)

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

Datum en locatie
29 april, 10:00-12.30 uur, Telefonisch

Agenda

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Edukoppeling Architectuur 2.0
4. Edukoppeling REST profiel versie 0.3
5. Edustandaard Uniforme beveiligingsvoorschriften (UBV)
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 wordt vanuit DUO gemeld dat de RIO API live is voor MBO.

2. Doornemen verslag en actielijst van 18 maart 2020

Verslag
Het verslag van 18 maart 2020 wordt zonder wijzigingen vastgesteld.

Actiepunten
In de nieuwe architectuur wordt een Open Data profiel opgenomen. Dit heeft echter minder prioriteit dan het REST/SaaS-profiel.

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
92	In overzicht met relevante standaarden aangeven tot welke datum verwacht wordt dat de standaard de status “in gebruik’ heeft.	Bespreken na vaststelling REST profiel	Q2 2020	BES	1
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	Afgehandeld, Pieter Bruring is deelnemer namens Kennisnet//OSR	Q2 2020	BES	1
94	Kan de huidige methodiek o.b.v. BRIN4 vervangen worden met een identiteit van een onderwijsaanbieder. Impact documentatie, aansluiting DK/Logius	Plannen	Q3 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.	Afgehandeld	Q2	BES	1
96	Werkgingsgebied in Architectuur aanpassen: met en binnen de onderwijs	Afgehandeld	Q2	BES	1
97	Analyse AMIGO (versie?) om vast te stellen of nu nog wat ontbreekt bij beschrijving bedrijfstransacties in Architectuur	Loopt	Q2	BES/Leden	1
98	In de architectuur bij bouwstenen de functies van het OSR kort te beschrijven (praktijk)	Loopt	Q2	BES/OSR	1
99	Best practice beschrijven van toepassing API-key (REST profiel - OSR)	Plannen	Q2	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	OSR/Kennisnet	1
101	In architectuur opnemen dat binnen Edukoppeling het OIN school (met suffix) onderdeel van mandatering is en kan worden gebruikt voor een autorisatie	Afgehandeld	Q2	BES	1
102	Voorstel van DUO (#100) als advies vanuit Edukoppeling naar beheerder OSR sturen,	Afgehandeld, zie #100	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, review AR over UBV komt nog, partijen leveren zelf input	Afgehandeld	Q2	DUO, Iddink	1

3. Edukoppeling Architectuur 2.0

In de nieuwe conceptversie zijn de volgende punten opgenomen/gewijzigd:

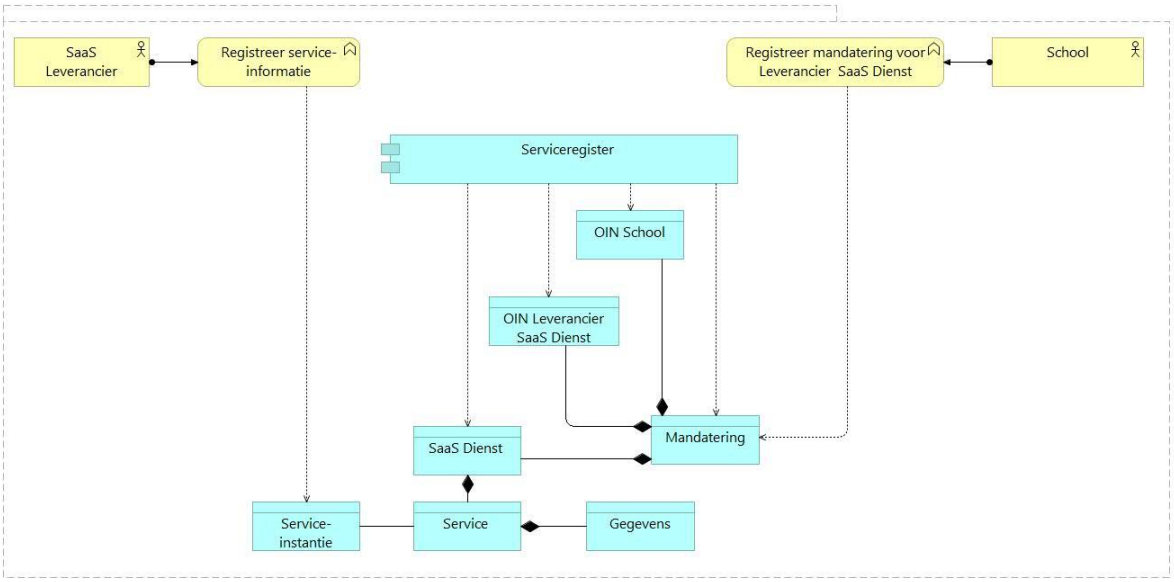
1. Toegevoegd: Patroon abonneren op wijzigingen middels notificaties
2. Toegevoegd: Aangegeven dat de SaaS-profielen ook door onderwijsinstellingen gebruikt kunnen worden die eigen systemen bij ketenuitwisselingen gebruiken.
3. Aangepast: Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling tussen informatiesystemen van partijen **met en binnen de onderwijs**
4. Aangepast: Figuur 3 - Registratie Mandatering in serviceregister

Ad1
Bij de beschrijving van bedrijfstransactiepatronen is het patroon ‘Abonneren op wijzigingen middels notificaties’ toegevoegd. Dit patroon beschrijft o.a. de rollen en een aantal keuzes die bij het werken met een notificatie relevant zijn. Dit is een belangrijke basis om op een standaard manier met notificaties te werken. Hierbij geldt dat de bronhouder/beheerder van de gegevens de abonnees informeert, maar deze bepalen zelf (binnen afgesproken termijn) wanneer zij de gegevens ophalen.

De afnemer moet ook een abonnement kunnen opzeggen.

Er wordt gevraagd of er een plaatje toegevoegd kan worden (actiepunt #105)

Ad4
Een serviceregister is een belangrijk concept binnen Edukoppeling. De vorige keer is het theoretisch model van een serviceregister in de context van de SaaS-profielen al besproken, maar er waren nog wat onduidelijkheden. Om een eenduidig beeld te krijgen wordt er de registratie van een mandatering besproken. Er wordt aangegeven dat we enerzijds een administratief proces hebben, waarbij tekenbevoegden van een school en SaaS-leverancier een overeenkomst ondertekenen. Anderzijds is er een technische implementatie waarbij een school een mandatering voor een SaaS-leverancier in een serviceregister registreert (zie Figuur 1).



Figuur 1 –Registratie mandatering in een serviceregister

De technische implementatie van de registratie van een mandatering willen we eenduidig kunnen koppelen aan de overeenkomst in het administratief proces. Hierbij speelt het begrip 'Dienst' een belangrijke rol. Tot nu toe worden begrippen als Dienst en Service in Edukoppeling min of meer als synoniemen gebruikt. Er wordt voorgesteld om voor beide een definitie op te nemen die het onderscheid duidelijk maakt, een definitie die aansluit bij de ROSA. Hiermee wordt het begrip 'Mandatering' beter geduid en kan in zowel in het administratieve proces als de technische implementatie gesproken worden over een Dienst die bepaalde persoonsgegevens verwerkt. De dienst van de SaaS-leverancier is o.b.v. de mandatering bevoegd om in een bepaalde keten persoonsgegevens uit te wisselen. De Dienst maakt hiervoor gebruik van één of meer Services. De Service definieert de gegevens die uitgewisseld worden. Bij de technische implementatie is de school verantwoordelijk voor de registratie van de mandatering en de SaaS-leverancier is verantwoordelijk voor registratie van (technische) gegevens van de service-instantie die onderdeel is van dienst.

Het Architectuurdocument wordt vastgesteld nadat de volgende wijzigingen nog zijn doorgevoerd:

1. Figuur 1 en een toelichting opnemen. Hierbij moeten ook concrete voorbeelden genoemd worden.
2. Bij de beschrijving van de bouwstenen moet nog een beschrijving van het OSR opgenomen worden. Hiervoor wordt de tekst uit de architectuurscan gebruikt die Kennisnet momenteel opstelt.

De onderstaande begrippen worden opgenomen in de begrippenlijst.

Begrip	Definitie	Bron
Dienst	Verzameling samenhangende (digitale) activiteiten en functionaliteiten die een dienstaanbieder beschikbaar stelt aan een opdrachtgever	ROSA
Dienstaanbieder	Partij die (digitale) diensten levert. In de context van het onderwijs kan dit een externe, private of publieke partij zijn, maar het kan ook een onderwijsinstelling zijn	ROSA
Dienstafnemer	Partij die (digitale) diensten afneemt	ROSA
Service	Functionaliteit voor de uitwisseling van berichten in het kader van een dienst.	ROSA

Serviceaanbieder	De partij die een service beschikbaar stelt aan serviceafnemers	ROSA
Serviceafnemer	De partij die een service van een serviceaanbieder afneemt	ROSA
Serviceregister	Dit register is een catalogus van informatiediensten. Afnemers kunnen zich oriënteren op beschikbare services. Het serviceregister helpt bij het formaliseren van de noodzakelijke overeenkomsten bij gebruik.	ROSA

4. Edukoppeling REST-SaaS-profiel

Ook voor het REST/SaaS-profiel is een nieuwe conceptversie opgesteld. Vorige keer is niet het hele document besproken, maar er zijn wel een aantal zaken gewijzigd, het betreft het volgende:

1. Volgorde en niveau van compliance van overheidsbrede voorschriften aangepast
2. Keuze routering obv HTTP header
3. Opdeling voorschriften beveiliging in deel Transportbeveiliging (beheer UBV) en Berichtbeveiliging (beheer EK)
4. Verschillende tekstuele aanvullingen / wijzigingen.

Ad1
Het Edukoppeling REST/SaaS-profiel is opgesteld op basis van documenten van Kennisplatform API's en met name de API Design rules[1]. Er wordt toegelicht dat deze documenten en de principes hierin een veel bredere scope hebben dan voor het Edukoppeling REST/SaaS-profiel beoogd wordt. In de huidige versie van het REST/SaaS-profiel worden voor de traceerbaarheid wel alle principes uit de documenten overgenomen. Per principe is er vervolgens o.b.v. de MoSCoW methodiek aangegeven in welke mate het principe relevant is voor het profiel. De vraag is nu hoe directief we hierin willen zijn, willen we een open profiel (o.b.v. Could) waarbij we ruime keuze vrijheid laten voor keten implementaties, of willen we een strikt profiel (o.b.v. Won't) waarbij we heel duidelijk aangeven dat bepaalde zaken niet toegestaan zijn.

Er wordt voorgesteld om bij zaken die duidelijk buiten het functioneel toepassingsgebied liggen strikt voor te schrijven dat deze niet binnen het profiel toegepast worden. Er wordt als voorbeeld een aantal standaarden genoemd die niet van toepassing zijn (Won't):

1. CORS
2. GEO informatie / CRS;
3. Oauth;
4. en omdat er nog een WUS profiel is sluiten we voor het REST profiel XML uit (principe API-22: JSON first).

Zowel over het uitsluiten van OAuth als XML is er wat discussie. Er zijn al implementaties met een OAuth profiel en men vindt het wenselijk deze compliant te laten zijn met Edukoppeling REST/SaaS-profiel. Ook al staan er in het REST/SaaS-profiel geen inhoudelijke voorschriften rond OAuth wordt besloten dat de toepassing van Oauth mogelijk moet zijn (Could). We kunnen ervaringen uit ketens ook gebruiken voor een toekomst profiel met OAuth.

Ook rond het uitsluiten van XML is wat discussie, het REST profiel kan tenslotte hier prima mee overweg. We hebben echter nu met Edukoppeling de situatie dat er ook al een WUS

[1] https://docs.geostandaarden.nl/api/API-Designrules/

profiel is dat XML gebruikt. Zonder uitspraak vanuit de standaard kunnen ketenpartijen een verschil van mening hebben wat toegepast moet worden. Er wordt besloten om XML toe te staan (Could), maar dat er wel aangegeven wordt dat bij XML het de voorkeur heeft om het WUS/SaaS-profiel te gebruiken.

In de discussie wordt duidelijk dat de aanduiding *Won't* niet duidelijk aangeeft dat een bepaald principe/standaard niet toegepast wordt en dus uitgesloten is om eventuele onnodige interoperabiliteitsproblemen, complexiteit en andere discussies te voorkomen. Momenteel geldt voor Won't de volgende definitie: '*Deze eisen zijn (op termijn) wel gewenst maar voor dit profiel is besloten deze functionaliteit niet verder uit te werken)'.* De MoSCoW methode heeft met name betrekking op het prioriteren van requirements en is niet bedoeld als maatstaf hoe strikt een voorschrift opgevolgd moet worden of dat iets juist niet mag. Vooralsnog betreft deze onduidelijkheid met name m.b.t. 'Won't' en de definitie hiervan zal aangepast worden. Voorschriften met deze aanduiding dienen niet toegepast te worden in de context van het REST/SaaS-profiel.

Ad2
In het REST/SaaS-profiel willen we expliciet maken hoe een verwerker kan routeren naar een bepaalde eindorganisatie en inzichtelijk is van welke eindorganisatie het bericht afkomstig is. Dit zonder dat we eisen stellen aan de inhoud (payload van het bericht). Bij WUS gebruiken we daar de WS-Addressing header voor.

Het vorige overleg zijn we er niet aan toegekomen om een keuze te maken uit de verschillende opties. In de 0.3 versie is nu de keuze gemaakt om dit via HTTP headers op te nemen. We zien het gebruik van HTTP headers om OIN door te geven ook al bij TLS offloading. Het huidige voorstel maakt gebruik van twee nieuwe HTTP headers die voor zowel het request als de resonse een TO en FROM parameter definiëren.

Er is wat discussie omdat leden het gebruik van HTTP headers onwenselijk vinden. Bij bestaande implementaties wordt er verder voor dergelijke informatie gebruik gemaakt van query parameters of het path om naar de school te verwijzen. Er wordt voorgesteld om hiervan gebruik te maken. Er wordt besloten dat er met verschillende leden wordt besproken wat een passende invulling voor het routeringsvraagstuk kan zijn. Deze wordt in de volgende release meegenomen.

5. Edustandaard Uniforme beveiligingsvoorschriften (UBV)

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

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. De volgende bijeenkomst wordt voor eind mei gepland.

10. Actielijst

#	Omschrijving	Status	Einddatum	Actie-houder	Prio
92	In overzicht met relevante standaarden aangeven tot welke datum verwacht wordt dat de standaard de status “in gebruik’ heeft.	Bespreken na vaststelling REST profiel	Q2 2020	BES	1
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)	Afgehandeld	Q2 2020	BES	1
94	Kan de huidige methodiek o.b.v. BRIN4 vervangen worden met een identiteit van een onderwijsaanbieder. Impact documentatie	Plannen	Q3 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.	Afgehandeld	Q2	BES	1
96	Werkgingsgebied in Architectuur aanpassen: met en binnen de onderwijs	Afgehandeld	Q2	BES	1
97	Analyse AMIGO (versie?) om vast te stellen of nu nog wat ontbreekt bij beschrijving bedrijfstransacties in Architectuur	Loopt	Q2	BES/Leden	1
98	In de architectuur bij bouwstenen de functies van het OSR kort te beschrijven (praktijk)	Loopt	Q2	BES/OSR	1
99	Best practice beschrijven van toepassing API-key (REST profiel - OSR)	Plannen	Q2	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
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-	Afgehandeld	Q2	BES	1

	A/REST headr oin suffix overeenkomt met suffix mandatering				
102	Voorstel van DUO (zie #100) als advies vanuit Edukoppeling naar beheerder OSR sturen	Afgehandeld	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	Afgehandeld	Q2	DUO, Iddink	1
105	Architectuurdocument: Plaatje bij Patroon Abonneren op wijzigingen middels notificaties	Plannen	Q2	DUO/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. 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