edustandaard

Edukoppeling

Identificatie en authenticatie

Edustandaard

Datum: September 2020

Versie: 1.1

Status: concept

Inhoudsopgave

1 Historie

Versie	Auteur	Datum	Opmerking
0.9	Gerald Groot Roessink	Maart 2018	Conceptversie
1.0	Werkgroep Edukoppeling	September 2018	In lijn gebracht met architectuurdocument. Aangepast op Edustandaard documentformaat.
1.1	Werkgroep Edukoppeling	Aug 2020	• Herstructurering teksten • Benoemen van HRN (OIN voor rechtspersonen / bedrijven) • Header / Payload niet op basis van SOAP beschrijven • Figuur 1 aangepast

2 Inleiding

2.1 Aanleiding

De aanleiding voor de introductie van Edukoppeling in het onderwijsdomein is een steeds groter wordende stroom van geautomatiseerde (machine-machine) processen in het onderwijs. Dit wordt veroorzaakt door vernieuwingen in het onderwijs zelf, in wetgeving, in de beschikbare techniek en de wens om het aantal (technische) koppelvlakafspraken binnen de perken te houden. In toenemende mate lopen de processen over organisaties heen, tussen onderwijsinstellingen onderling, tussen onderwijsinstellingen en overheidsorganisaties en tussen onderwijsinstellingen en bedrijven. En vaak, als er iets nieuws komt, wordt er dan pas nagedacht over de benodigde infrastructuur. Als men niet oppast worden er evenveel infrastructurele oplossingen gerealiseerd als er geautomatiseerde processen zijn. Met Edukoppeling verandert dat. Edukoppeling is een meervoudig inzetbare infrastructuur waarvan de ontwikkeling en het beheer gemeenschappelijk wordt aangepakt.

Edukoppeling is door de bij Edustandaard betrokken partijen geaccepteerd als het communicatieprotocol voor organisaties die werkzaam zijn in het onderwijs met name voor die gegevensuitwisseling waarbij er sprake is van overdracht van vertrouwelijke gegevens waarvoor een hoger risicoprofiel geldt (persoonsgegevens, bedrijfskritische gegevens). De Edukoppeling-standaard is gebaseerd op het nationale communicatieprotocol Digikoppeling[1].

2.2 Doel en doelgroep

Dit document beschrijft de identificatie- en authenticatie-aspecten die binnen Edukoppeling relevant zijn en is onderdeel van de Edukoppeling Architectuur. Het omvat de identificatie van partijen met het zogenaamde Organisatie Identificerend Nummer (OIN). De basis wordt gevormd door het Digikoppeling Identificatie- en authenticatiedocument.

Dit document is bedoeld voor ICT-specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van systeem-naar-systeem koppelingen. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties. De Edukoppeling-documentatie dient naast de Digikoppeling-documentatie gebruikt te worden.

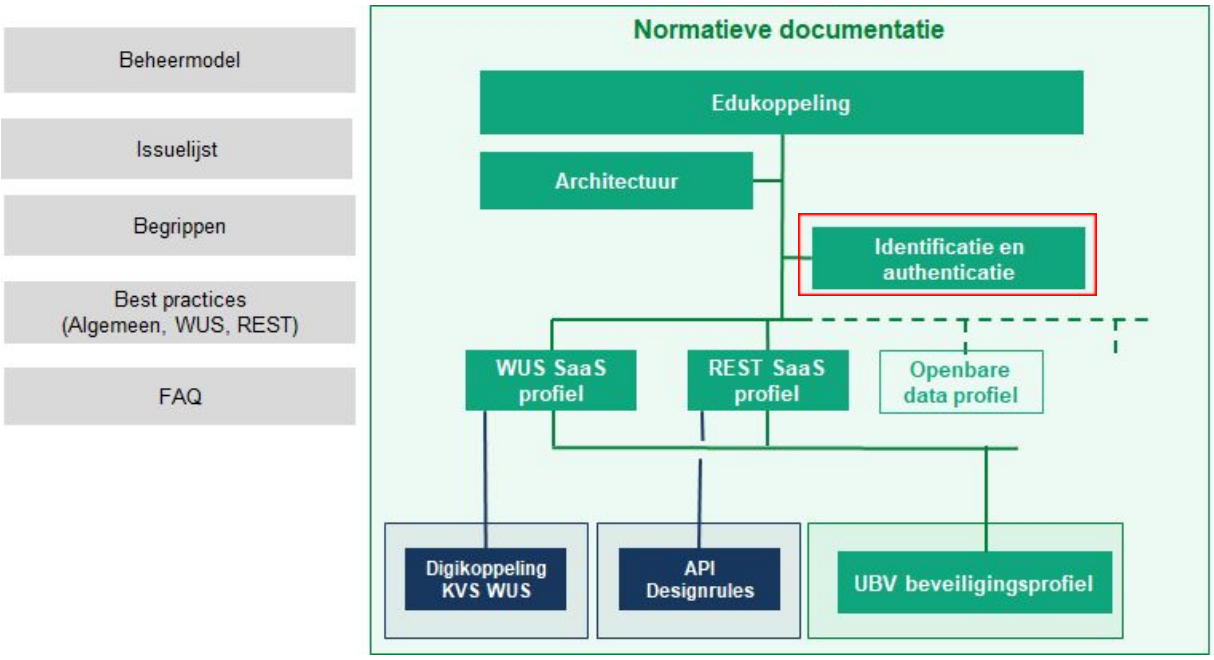
De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerorganisatie Edustandaard[2].

[1] https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/
[2] https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/

2.3 Positionering binnen Edukoppeling Architectuur

Het Edukoppeling Identificatie en Authenticatie document is onderdeel van de Edukoppeling Architectuur.

Het Identificatie en Authenticatiedocument is een aanvulling op het Digikoppeling Identificatie en Authenticatie-document[3] en bevat een aantal principes en voorschriften specifiek voor het onderwijsdomein.



Figuur 1- Positionering van Identificatie en authenticatie binnen Edukoppeling Architectuur

2.4 Kernbegrippen

- *Identificatie*

Identificatie is het kenbaar maken van de identiteit van een subject (een persoon/gebruiker of een proces/systeem). De identiteit op Edukoppeling is uniek en valideerbaar. De identiteit wordt gebruikt om de autorisatie (zie verder) - de toegang tot een service - te beheersen.

- *Authenticatie*

Authenticatie is het proces waarbij nagegaan wordt of een subject daadwerkelijk is wie hij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij opgeeft. Bij de authenticatie wordt bijv. gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken. Het proces van authenticatie is dus onlosmakelijk verbonden met identiteit. Authenticatie levert als het ware de kwaliteit van de identificatie.

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

- *Autorisatie*

Autorisatie is het proces waarin een subject rechten krijgt op het benaderen van een service. De autorisatie wordt toegekend door de service-eigenaar. Het leidende principe (met name bij persoonsgegevens) is doelbinding: je mag alleen zien wat je voor je taak nodig hebt. Bij een collectieve informatievoorziening als deze geldt bovendien: je mag alleen je eigen dingen zien en niet de dingen van je collega-organisatie. De primaire reden voor het vaststellen van de identiteit van een subject is om op basis daarvan vervolgens vast te stellen of dat subject ook gerechtigd is om de gewenste service af te nemen. Die autorisatie (al of niet mede op basis van rollen, machtigingen, vertegenwoordigingen enzovoort) is nadrukkelijk een op de authenticatie volgende, aparte stap. De geauthenticeerde identiteit is dus nodig om autorisatie te kunnen doen. Autorisatie stelt eisen aan authenticatie.

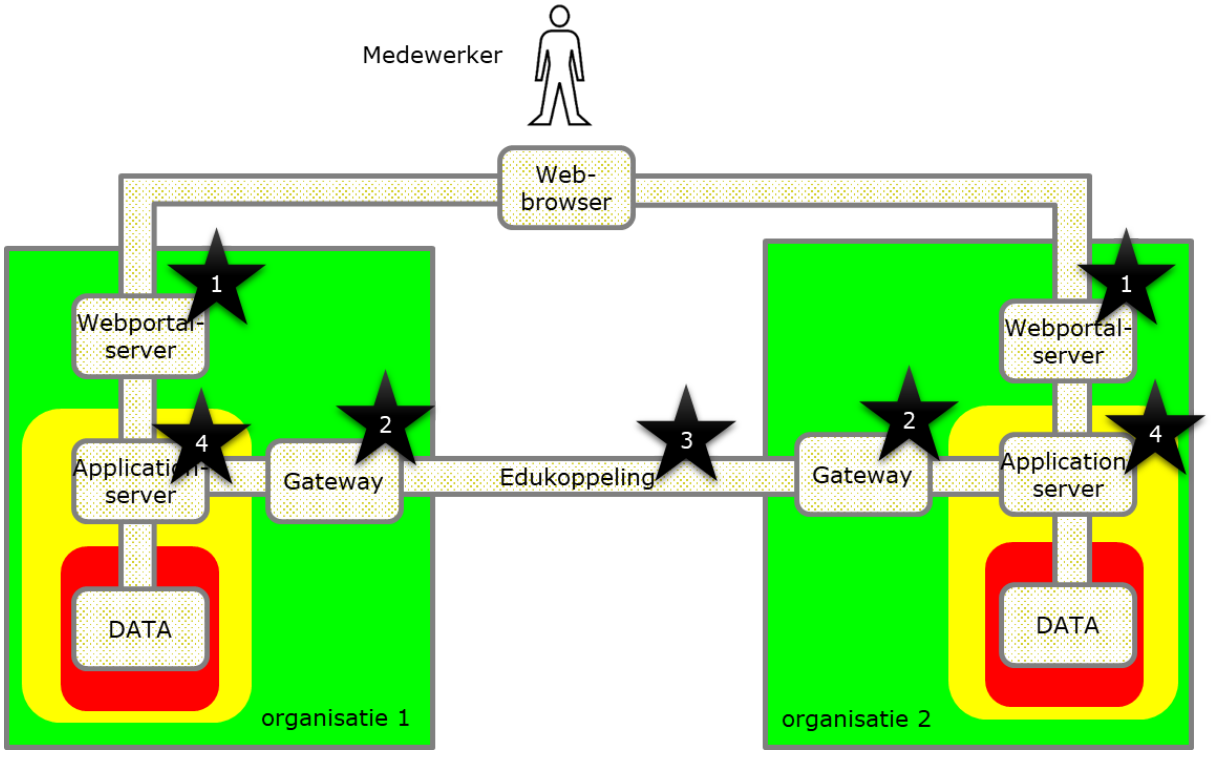
- *Routering*

Routering is kunnen bepalen van het (internet)adres waar een service aangeroepen kan worden. De inrichting van zo'n internetservice wordt in eerste instantie bepaald door de service-eigenaar, maar die dit in de regel uitbesteed aan ander, die in dit geval ook het inrichten van de applicatie in de cloud voor zijn rekening neemt. Dit komt precies, want ook hierbij geldt, het is niet de bedoeling dat privacygevoelige data op een verkeerde locatie wordt bezorgd. Vandaar dat de verantwoordelijke én de bewerker allebei een aandeel hebben in de goede werking van de routering. Als de relatie tussen die twee wordt verbroken, heeft dat per direct gevolgen voor het routeren van het berichtenverkeer.

3 Overzicht SaaS-model

In Figuur 2 is schematisch een beeld geschetst van ketensamenwerking. Deze wordt in meer detail toegelicht in de Edukoppeling Architectuur (hoofdstuk 3). Identificatie en authenticatie in de context van Edukoppeling (SaaS-model) is relevant bij de gegevensuitwisseling in de backoffice (zie ster nummer 2 in de figuur) waarbij expliciet rekening wordt gehouden met een SaaS-leverancier (gegevensverwerker) die in opdracht van de onderwijsinstelling (eindorganisatie) gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke.

Hiermee wordt het van belang dat beide (gegevensverwerker en eindorganisatie) geïdentificeerd kunnen worden. De SaaS-leverancier beveiligt het verkeer (tweezijdig TLS) met een PKI-Overheidscertificaat met hierin de eigen identiteit (HRN). Bij Digikoppeling hanteert men een andere naam voor OIN's van rechtspersonen (bedrijven). Voor bedrijven die in het handelsregister staan wordt het organisatie identificerend nummer een HRN (Handels Register Nummer) genoemd. Deze certificaten worden uitgegeven door Trust Service Providers (TSP). Een TSP is verantwoordelijk voor het controleren van de identiteit van de aanvrager en het opnemen van het identificerend gegeven dat voor deze aanvrager in het certificaat opgenomen moet worden. Zie ook de toelichting over de toepassing van een PKI-infrastructuur in hoofdstuk 2 van de Transactiestandaard.



Figuur 2- Schematische weergave ketensamenwerking

In het volgende hoofdstuk wordt ingegaan op de identificatie van de onderwijsinstelling (eindorganisatie).

4 Logistieke identiteit

In dit hoofdstuk wordt behandeld hoe met identiteiten binnen Edukoppeling wordt omgegaan.

4.1 Header vs Body

Principe 1. Functie en logistiek zijn zoveel mogelijk gescheiden in respectievelijk body en header.

(of anders gezegd: Edukoppeling heeft geen boodschap aan de boodschap)

Een SaaS-leverancier kan diensten leveren aan meerdere scholen tegelijkertijd. Om die reden is in de Edukoppeling standaard afgesproken dat het zogenaamde Organisatie Identificerende Nummer (OIN) van de verzender en ontvanger van de school is opgenomen. Op basis hiervan kan de SaaS-leverancier achter de voordeur routeren.
Functionele aspecten waar de verwerkende applicatie iets mee moet, zitten per definitie in de body van het bericht. Bijvoorbeeld: als je leerlingen wilt kunnen tellen per school (zie verderop), dan wordt daarover in de body gecommuniceerd
Door deze strikte scheiding kan een ketenpartner “gelaagd” werken: een applicatie werkt met body (payload) en een gateway werkt met de header (adressering). Dat is relevant als een organisatie een complex applicatielandschap heeft. De scheiding in lagen is in het geval van DUO bijvoorbeeld ook scheiding in beveiligingszones.

4.2 Identiteit school

Het OIN is volgens de definities van Digikoppeling een identiteit van 20 karakters. In deze systematiek is ruimte voor BRIN4 (=het ID van een onderwijsinstellingserkenning). Het volgende schema is ontleend aan Digikoppeling.

Prefix	Identificerend nummer	Bron
00000001	RSIN	Handelsregister
00000002	Fi-nummer	Het fiscaal nummer wordt verstrekt door de Belastingdienst aan de organisatie zelf10 (alleen voor organisaties die niet in het Handelsregister staan).
00000003	KvK nummer	Handelsregister11
00000004	subnummer	subOIN register
00000005	Onderdelen van de Staat der Nederlanden	nog aan te wijzen
00000006	Onderdelen van het Rijk	nog aan te wijzen
00000007	BRIN nummer	De Basisregistratie Instellingen (BRIN) is een register van onderwijsinstellingen dat door DUO wordt beheerd in opdracht van het Ministerie van OCW.
00000008	Buitenlandse nummers	Buitenlandse nummers
00000009	Nog niet in gebruik	
00000099	Test OIN’s	Elke organisatie mag een test OIN gebruiken mits voorzien van deze prefix.

Figuur 4 – OIN/HRN Nummersystematiek [4]

[4] Zie pagina 17 Digikoppeling Identificatie en Authenticatie
https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/

Het Register Instellingen en Opleidingen (RIO) is de opvolger van het register BRIN. Dit zal op termijn leiden tot een andere invulling van het OIN.

Principe 2. Het OIN kan worden gevalideerd bij een nationaal of sectoraal register (met als consequentie: het OIN biedt rechtszekerheid in het economisch verkeer)

Overheidsorganisaties en bevoegd gezagen kunnen op Edukoppeling opereren met een OIN dat is ontleend aan het handelsregister. In de onderwijspraktijk en -wetgeving is het gebruikelijk dat “kleinere eenheden” zelfstandig opereren. Daarvoor kennen we nu het register BRIN dat is gekoppeld aan het handelsregister. Volgens bovenstaand schema mag daar ook een OIN op worden gebaseerd.

4.3 Administraties[5]

Zoals in de inleiding gezegd, veel scholen hebben een administratie in de cloud. In het verleden is wel gewerkt met de aanname dat scholen administraties bijhouden per vestiging(serkenning), maar dat wringt. Scholen hebben hun eigen afwegingen waarom ze één of meer contracten met SaaS-leverancier afsluiten of zelf met verschillende SaaS-leveranciers. Ook samenwerking van scholen kan invloed hebben op de administratieve indeling. Omdat scholen ook samen een administratie kunnen voeren, krijgt dit een eigen identiteit dat onafhankelijk is van de identiteit van deze samenwerkende scholen.

Principe 3. Een school bepaalt zonder restricties welke administratieve indeling hij hanteert. (ergo: dit kan niet worden gebaseerd op criteria als geografie, onderwijsniveau of leerjaar, wet)

Volgens dit principe registreren scholen welke administraties ze voeren. Deze registratie wordt gebruikt om een OIN op te baseren dat wordt gebruikt in de SOAP-header van Edukoppeling.
Dit heeft de volgende praktische consequenties:

1. Bij een uitwisseling waarbij het eerste contact uitgaat van de school, BRON is daarvan een voorbeeld, wordt door de ketenpartner(s) per keten per leerling/student de identiteit van de administratie onthouden. Dat is nodig om in latere instantie een bericht de andere kant op te kunnen sturen over die leerling/student.
2. Als het eerste contact uitgaat van een andere partij dan de school, bijvoorbeeld een nieuwe school wil met gebruikmaking van functionaliteit in zijn administratiesysteem via de digitale weg een dossier opvragen bij de oude school, en de oude school heeft niet zoiets als een servicebus waarbinnen deze oude school aanvragen van buitenaf zelf routeert (dit is namelijk niet gebruikelijk in het onderwijs), dan is er een lijst nodig met de door de oude school gevoerde administraties en de services die door deze administraties worden ondersteund. De aanvraag kan dan worden gericht aan de administratie die de service “dossier opvragen” ondersteunt. Dit zal een openbare lijst worden, onderdeel van bijvoorbeeld het Onderwijs serviceregister (OSR). Aanbevolen wordt om bij een administratie een vrije invulling te geven van de populatie leerlingen/studenten.

[5] In de praktijk wordt ook de term aanleverpunt gebruikt. Die wordt hier niet overgenomen omdat dit éénrichtingsverkeer suggereert. Behalve dat, is deze term ook anders qua definitie en gebruik bij verschillende services in het onderwijs, wat verwarring in de hand werkt.

4.4 Opbouw van het OIN voor scholen

Partijen worden uniek geïdentificeerd aan de hand van een Organisatie Identificerend Nummer (OIN). Het OIN bestaat altijd uit 20 posities en bestaat uit een aantal vaste onderdelen: “de prefix”, “hoofdnummer” en “suffix”.

Voorschrift: Op basis van de OIN-systematiek (Figuur 4) is het OIN voor een school als volgt: ‘00000007’(prefix) + de onderwijsinstellingserkenning-ID (3 voorloopnullen, BRIN4 = 4 posities + 00, hoofdnummer) + het administratienummer (3 posities, suffix).

Het OIN voor het afgeleide administratiepunt komt er als volgt uit te zien: “0000000700025MB00003”. Het administratienummer mag in principe door de school ism de SaaS-leverancier zelf worden bepaald.

Principe 4. Dit administratienummer is uniek per BRIN-ID binnen de keten.

(ergo: het kan worden hergebruikt voor verschillende processen die een beroep doen op dezelfde administratie)

Elk administratiepunt binnen dezelfde instelling zal dan in gezamenlijk overleg een andere suffix gebruiken in het OIN om de uitwisseling met DUO en eventuele andere ketenpartners mogelijk te maken. Het OIN identificeert zowel de organisatie (het hoofdnummer) als de administratie (de suffix). Dit is terug te vinden in de technisch/logistieke laag van de berichtuitwisseling, de zogenaamde WS-Addressing:To en WS-Addressing:From headers (zie Transactiestandaard).

In principe is het mogelijk dat deze werkwijze op termijn migreert van de uit 4 karakters bestaande onderwijsinstellingserkenning-ID (cq de BRIN4) naar de uit 7 karakters bestaande ID van een onderwijsaanbieder, het onderwijskundige object dat staat voor de schoolorganisatie (dus niet het bestuur) in RIO. Hiervoor zullen de ontwikkeling en vulling van het project RIO nauwgezet worden gevolgd.

Bovenstaande opbouw beschrijft een OIN voor een school op basis van een BRIN4. OINs kunnen op meerdere manieren worden opgebouwd. De prefix zal dan verschillen. Een OIN voor een private partij heeft als hoofdnummer het KvK-nummer en zal de volgende prefix bevatten: “00000003”. De suffix[6] zal altijd “0000” bevatten. Een softwareleverancier zal het OIN bijvoorbeeld kunnen gebruiken voor de uitwisseling. Zij beschikken immers niet over een BRIN4. Voor DUO geldt het volgende OIN 00000001800866472000 (hoofdnummer is het RSIN uit het handelsregister).

4.5 Identiteit rechtspersoon

De SaaS-leveranciers hebben in het SaaS-model ook een OIN gebaseerd op het handelsregister (dit wordt een HRN genoemd). Dit komt NIET terug in de header van het bericht, maar WEL in het PKIoverheid-certificaat voor het beveiligen van het verkeer én in het Onderwijs serviceregister (OSR) voor het valideren van de bewerkersrelatie met de school.

[6] Zie pagina 18 Digikoppeling Identificatie en Authenticatie: https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/

4.6 Centrale OIN Registratie

Logius heeft een website met toegang tot alle OIN nummers. Dit heet de Centrale OIN Registratie (COR)[7]. Dit is een service voor overheidsorganisaties die gaan uitwisselen met andere overheidsorganisatie. Het OIN van DUO is bijvoorbeeld op die manier al te bevragen. Logius heeft aan DUO gevraagd om hierin ook de onderwijsinstellingen te betrekken.

4.7 Ontwikkelingen

In het onderwijs zien we meer en meer, al of niet formele, samenwerkingsverbanden tussen scholen cq besturen. Vwb de identificatie is het soms lastig om te bepalen hoe deze samenwerkingsverbanden gezien moeten worden. Nu zie je nog dat een van de scholen in zo'n samenwerking de administratie voert richting BRON (inschrijvingen etc.) en dat onderling tussen de besturen een verrekening plaatsvindt. Grote impact op de vulling van het OIN heeft dit dus dan niet, voor de overheid is er maar 1 partij met wie ze communiceren.
Het wordt lastiger als het samenwerkingsverband samen een gemeenschappelijke administratie gaat voeren van waaruit gegevensuitwisseling plaatsvindt. BRIN als identificerend kenmerk houdt dan alleen nog maar stand als beide scholen vallen onder dezelfde instellingserkenning. Bij een samenwerkingsverband tussen twee besturen is dat niet meer aan de orde.

In RIO is het mogelijk om zo'n samenwerkingsverband als Onderwijsaanbieder te beschouwen die een relatie kan hebben met twee besturen en met twee juridische entiteiten (erkenningen). Hoe dat uitwerkt in de gegevensuitwisseling en voor de juiste vulling van het OIN is nog niet uitgekristalliseerd. De ontwikkeling wat betekent dat (op termijn) voor deze afspraak zal nauwgezet gevolgd worden.

4.8 Afronding

De Edukoppeling-standaard heeft expliciete voorschriften over hoe partijen elkaar kunnen herkennen in het machine-machine berichtenverkeer. Deze afspraken zijn tot stand gekomen onder paraplu van de nationale standaard Digikoppeling. Edukoppeling is verder uitgewerkt vanuit het aspect cloud-computing.

Het verwachte resultaat is een openbare en enkelvoudige 'adressenlijst' (Onderwijs serviceregister, OSR) die iedereen kan gebruiken die digitaal wil communiceren met een organisatie in het onderwijsveld. Initieel kan deze lijst worden gebaseerd op specifieke lijstjes van BRON, OSO en anderen. Nadat deze bijeen zijn gevoegd, ligt het onderhoud van een belangrijk deel bij de scholen.

[7] Zie: http://portaal.digikoppeling.nl/registers/