Edukoppeling

Architectuur

Versie 0.93 (concept)

Edustandaard

Datum: juni 2015

Versie: 0.93

Inhoudsopgave

1. Inleiding

Aanleiding

De aanleiding voor Edukoppeling is een voortdurende stroom van verandering in geautomatiseerde (machine-machine) processen in het onderwijs. Dit wordt veroorzaakt door vernieuwingen in het onderwijs zelf, in wetgeving, in de techniek en de alom aanwezige wens om niet te veel uit te geven. In toenemende mate lopen de processen over organisaties heen, tussen scholen onderling, tussen scholen en de overheid en tussen scholen en bedrijven. En vaak, als er iets nieuws komt, wordt er dan pas nagedacht over de benodigde infrastructuur. Misschien zijn er wel evenveel infrastructurele oplossingen als er geautomatiseerde processen zijn. Met Edukoppeling verandert dat. Edukoppeling is een meervoudig inzetbare infrastructuur waarvan de ontwikkeling en het beheer gemeenschappelijk wordt aangepakt.

Dit document beschrijft de scope, doelen, principes en best-practises achter de Edukoppeling-infrastructuur en verklaart de verschillende onderdelen.

Doel en doelgroep

Edukoppeling is een gedeelde onderwijsvoorziening voor vertrouwelijk machine-machine uitwisseling in het onderwijs. Dit draagt bij aan het realiseren van de volgende onderwijsbreed in ROSA gedefinieerde doelen:

1. Leven lang leren
2. Inspelen op beleidswijzigingen
3. Privacy by design
4. Terugdringen administratieve lasten

Om Edukoppeling een bijdrage aan deze doelen te laten leveren, moet het voldoen aan de volgende algemene requirements:

1. Identiteit van de eindgebruiker is vastgesteld
2. Berichtinhoud is vertrouwelijk en integer
3. Verzending berichten is onweerlegbaar
4. Verkeer tot 1G berichten per jaar

Dit document is bedoeld voor personen die betrokken zijn bij het ontwikkelen van systeem-naar-systeem koppelingen en wordt gebruikt naast een aantal technische beschrijvingen:

- Edukoppeling Transactiestandaard 1.2
- Certificeringsschema 1.1
- Serviceregister i.o.

Deze documenten beschrijven voor ICT-specialisten hoe ICT ingericht kan worden.

Leeswijzer

In hoofdstuk 1 wordt de aanleiding, het doel en de doelgroep voor Edukoppeling beschreven. In hoofdstuk 2 wordt de achtergrond van Edukoppeling toegelicht. In hoofdstuk 3 wordt aan de hand van patronen het gebruik van Edukoppeling uitgelegd en in hoofdstuk 4 zijn de bouwstenen waaruit Edukoppeling bestaat in hoofdlijnen beschreven.

Begrippen

De relevante begrippen zijn opgenomen in bijlage A.

Historie

Versie	**Auteur**	**Datum**	**Opmerking**
0.1	WG Edukoppeling	Maart 2015	Initiële versie
0.93	WG Edukoppeling	Juni 2015	Ter besluitvorming in werkgroep van 17-6-2015

2. Achtergrond

Relatie met Digikoppeling

Digikoppeling[1] is een transactiestandaard op de zogenaamde pas-toe-of-leg-uit-lijst van de Nederlandse overheid en aanverwante instellingen waaronder ook, dat is weinig bekend, onderwijsinstellingen. Digikoppeling vormt het fundament van de Edukoppeling transactiestandaard. Digikoppeling is echter niet zonder meer te gebruiken in het onderwijsveld:

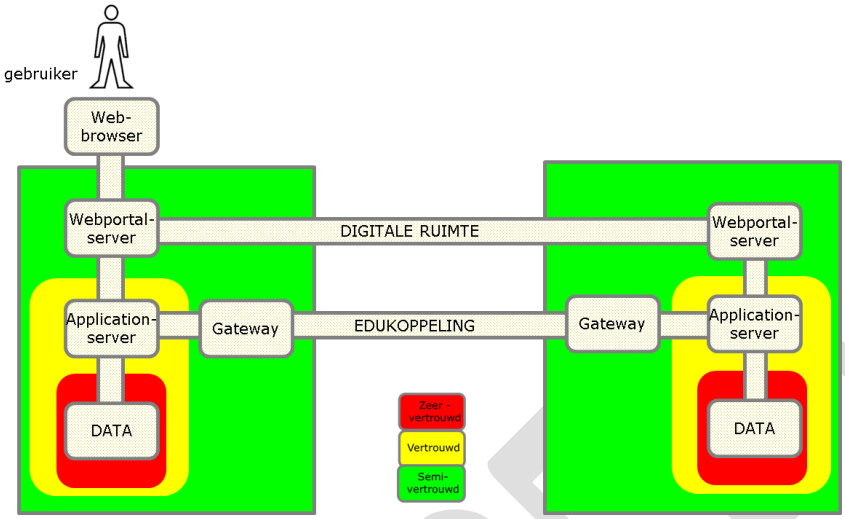
1. Onderwijsinstellingen maken steeds vaker gebruik van SaaS-leveranciers voor de ondersteuning van hun administratieve processen. Deze partijen worden binnen Edukoppeling als formele partij onderkend waardoor de beheerlast (met name rondom certificaatbeheer) voor scholen beperkt kan blijven.
2. Het aantal partijen binnen de onderwijssector is vele malen hoger en meer divers, dan waarvoor Digikoppeling ingezet wordt. Een zo simpel mogelijke en binnen de sector bekende standaard verkleint de kans op fouten en versnelt de implementatietijd. Ook vanwege het aanzienlijke verschil in kennis van diverse ketenpartijen is daarom gekozen voor het toepassen van een kleinere set basistechnologieën. Binnen Edukoppeling worden daarom een aantal Digikoppeling profielen uitgesloten.

De Edukoppeling transactiestandaard vormt een ‘collectieve leg-uit’ voor het onderwijsinstellingen ten aanzien van de pas-toe-of-leg-uit status van Digikoppeling. Van overheidswege worden de onderwijsinstellingen niet gedwongen om beveiligde gegevensuitwisseling op een andere manier dan via de in Edustandaard goedgekeurde versie van Edukoppeling uit te voeren. Andersom worden binnen Edukoppeling geen technologieën geïntroduceerd zonder ruggespraak met de beheerder van Digikoppeling (Logius).

1 Digikoppeling aansluitkit: https://www.logius.nl/ondersteuning/digikoppeling/#c8445

Edukoppeling in de onderwijsketen

De ROSA[2] referentie-architectuur beschrijft voor organisaties in het onderwijs, principes, modellen en standaarden gericht op interoperabiliteit, dat wil zeggen, het vermogen om samen te werken. In figuur 1 worden twee faciliterende infrastructurele onderdelen, de Digitale Ruimte en Edukoppeling, onderscheiden.



Figuur 1 – Basisinfrastructuur onderwijs

In deze figuur zijn schematisch twee organisaties te zien. De basisinfrastructuur faciliteert een servicegerichte samenwerking waarbij de ene organisatie services aanbiedt aan de ander via het internet. In het algemeen gaat het daarbij over vertrouwelijke, privacygevoelige gegevens die beschermd moeten worden. Zonering speelt daarbij een belangrijke rol. De betekenis van de kleuren is ontleend aan www.noraonline.nl/wiki/beveiligingspatronen. Of en in welke mate Edukoppeling vertrouwelijk is, wordt uitgewerkt in hoofdstuk 3.

Edukoppeling dient de communicatie tussen ICT-systemen van verschillende organisaties, specifiek in de vorm van berichtenverkeer. Edukoppeling beschrijft de machine-machine interface, maar ook daarbij zijn mensen impliciet de eindgebruikers, bijvoorbeeld een medewerker die door middel van een webservice inzage krijgt bij een andere organisatie.

En soms zijn mensen expliciet eindgebruiker. De Digitale Ruimte draait om het geven van toestemming aan de gegevensbeheerder om gegevens van de eindgebruiker te leveren aan een andere organisatie. De toestemming in de vorm van een token, wordt door de ontvanger gebruikt in een verzoek de om de gegevens via Edukoppeling op te halen.

2 Voor meer informatie over ROSA, zie http://www.wikixl.nl/wiki/rosa/index.php/Edukoppeling

3. Edukoppeling-infrastructuur

Organisatorisch werkingsgebied

Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling tussen informatiesystemen van partijen binnen de onderwijssector. Onderwijsinstellingen kunnen hierbij deze informatiesystemen lokaal hebben draaien of hebben uitbesteed in de cloud. Onderwijsinstellingen hebben samenwerkingsrelaties met andere onderwijsinstellingen, met de overheid én met private organisaties.

Functioneel toepassingsgebied

Om gegevensuitwisseling te realiseren moeten organisaties op drie niveaus afspraken maken:

1. Over de inhoud en betekenis van berichten (payload en eventuele bijlagen): de structuur, semantiek, waardebereiken enzovoort.

2. Over de logistiek (envelop): transportprotocollen (HTTP), messaging (SOAP), adressering, beveiliging (authenticatie en encryptie) en betrouwbaarheid.

3. Over het transport (netwerk): de protocollen van de TCP/IP stack (TCP voor Transport, IP voor Netwerk) en de infrastructuur, bijvoorbeeld Internet.

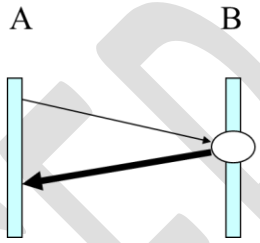
Edukoppeling richt zich alleen op de logistieke laag en zorgt voor ontkoppeling van de andere lagen. Daardoor kan een ketenpartner met één implementatie op een veilige manier een veelheid van toepassingen uitvoeren.

Uitwisselingspatronen

Met Edukoppeling worden een aantal uitwisselingspatronen of message exchange patterns (mep's) ondersteund.

Patroon: Request-response

Het patroon request-reponse is het basale patroon waarbij een serviceprovider (B) een webservice inricht, bijvoorbeeld voor het bevragen van een gegevensbron, waarbij de levering aan de servicerequester (A) volgt binnen dezelfde sessie. Die wordt ook wel een synchrone uitwisseling genoemd. Dit patroon wordt typisch toegepast in een situatie waarbij een gebruiker op het resultaat zit te wachten. Dit mag vanzelfsprekend niet te lang duren. Technisch is er een time-out (bijvoorbeeld 20 seconden) verbonden aan een request-reponse interactie. De boodschap aan de gebruiker luidt dan: "probeer het later nog eens". Daarna wordt de transactie geacht niet te hebben plaats gevonden.

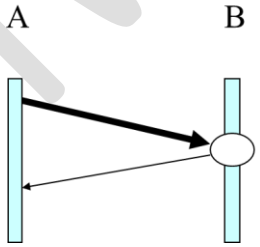


Figuur 2 – Patroon request-response

Dit patroon komt ook voor in Digikoppeling

Patroon: Melding-bevestiging

Het patroon melding-bevestiging lijkt op het vorige patroon. Het verschil is, dat de informatiestroom nu andersom loopt. De informatie wordt gestuurd door A en de ontvangst wordt synchroon door B bevestigd.

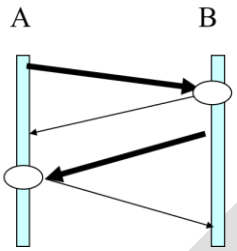


Figuur 3 – Patroon melding-bevestiging

In dit patroon kan er iets veranderen in de systemen van de ontvanger. Belangrijk is de eventuele schadelijke effecten te voorkomen als een bericht twee keer wordt verzonden (door een time-out) of als meldingen in de verkeerde volgorde binnenkomen bij B. Digikoppeling lost dat op met het patroon Gegarandeerde aflevering, maar dat wordt niet ondersteund door Edukoppeling. Wel geldt bij dit patroon de voorwaarde dat berichten 'idempotent' zijn, dat wil zeggen dat altijd de laatste stand wordt gebruikt (meld gebeurtenis, niet mutaties).

Patroon: Asynchrone uitwisseling

Een asynchrone uitwisseling is twee keer het patroon melding-bevestiging in verschillende richtingen. Eerst wordt een melding gestuurd (A) en de ontvangst bevestigd (B). Op een later tijdstip, als de melding is verwerkt wordt een terugmelding gestuurd (B) en wordt de ontvangst daarvan bevestigd (A).

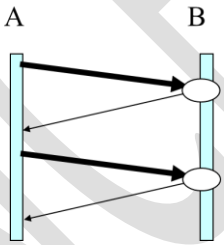


Figuur 4 – Asynchrone uitwisseling

Meestal wil A zekerheid hebben dat een melding door B is verwerkt en bewaakt A of er een terugmelding is ontvangen en geen meldingen zijn verdwenen.

Antipatroon: Polling

Asynchrone uitwisseling kan ook als volgt worden weergegeven:

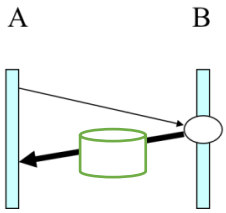


Figuur 5 – Antipatroon polling

Het voordeel hiervan is er maar één partij services hoeft aan te bieden (B). Per saldo is het daarmee sneller te realiseren dan het vorige patroon. Het nadeel is echter dat A voortdurend webservicecalls afvuurt aan B om te vragen of er het eerste bericht al is verwerkt. Dit wordt pollen genoemd. Dat vraagt veel hardwarecapaciteit en daardoor is het toch een relatief dure oplossing. Alle deelnemers aan Edukoppeling kunnen in principe service aanbieden. Toepassing van dit antipatroon is niet nodig en wordt afgeraden.

Patroon: Grote berichten

Bij hele grote berichten (>20 MB) schrijft Digikoppeling voor dat deze apart worden gedownload, nadat de tijdelijke opslaglocatie door middel van een metabericht is opgevraagd door of gemeld aan de beoogde ontvanger. In Edukoppeling is dat metabericht voor de opslaglocatie een request-respons patroon of een melding-bevestiging patroon (zie hierboven).



Figuur 6 – Patroon grote berichten (zonder metabericht)

Grote berichten kunnen als attachement aan een gewoon bericht worden toegevoegd. Dat is waarschijnlijk eenvoudiger te realiseren, maar vanaf de genoemde grenswaarde weegt voordeel niet meer op tegen de toegenomen kans op transportfouten.

Beveiligingspatroon

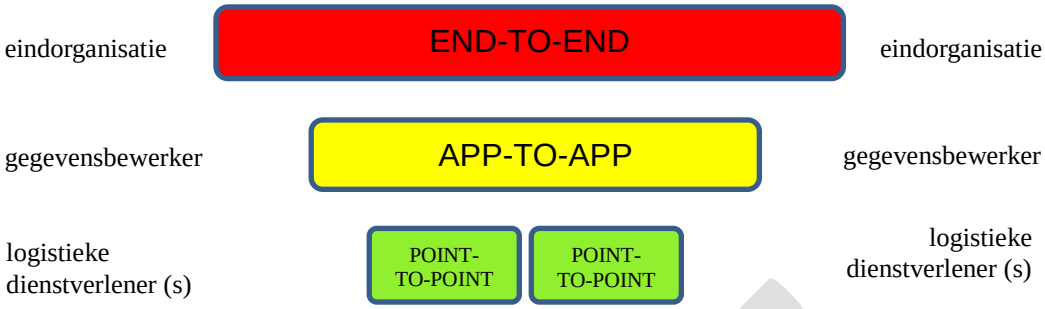
Edukoppeling onderscheidt drie rollen die binnen één organisatie worden uitgevoerd in machine-machine uitwisseling met andere organisaties. Vanwege cloud-computing in het onderwijs is dat er één meer dan in Digikoppeling:

Rol: Eindorganisatie
De eindorganisatie is de organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie. Deze is gebonden aan een (vaak collectief gemaakt) programma van eisen, uitwisselingsovereenkomst, gegevensleveringsovereenkomst o.i.d. Dit is niet een opdrachtrelatie. De eindorganisatie is degene die verantwoordelijk is voor bescherming van de privacy. Bijvoorbeelden: school wisselt uit met DUO of school wisselt uit met school.

Rol: Gegevensbewerker
De gegevensbewerker is een organisatie die in opdracht van de eindorganisatie gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke. In deze functie heeft deze organisatie toegang tot de (privacygevoelige) gegevens. De zorgplicht ligt echter nog steeds bij de eindgebruiker waardoor een bewerkersovereenkomst noodzakelijk is (zie bouwsteen certificeringschema). In het onderwijs is de bewerker vaak niet dezelfde als de eindgebruiker.

Rol: Logistieke dienstverlener
Een logistieke dienstverlener is een organisatie die interoperabiliteitsfuncties uitvoert zoals, identificatie, authenticatie, autorisatie, routering, monitoring. Privacy by design houdt in dat deze partij werkt met ‘gesloten envelop’ en de gegevens niet kan inzien of wijzigen. Er zijn in het onderwijs enkele gevallen waarbij een aparte logistieke dienstverlener die niet samenvalt met de gegevensbewerker, actief is.

Op basis van deze drie rollen zijn drie beveiligingsniveau's bij externe koppelingen te onderscheiden (zie figuur 7).



Figuur 7 – Beveiligingspatroon externe koppeling

Bij het beveiligen van externe verbindingen wordt een risico-analytische benadering gevolgd. Naar mate de ketens ingewikkelder worden, er meer gegevens over gaan en het belang van de uitwisseling groter wordt ('legal transactions') zijn meer maatregelen noodzakelijk. In het algemeen kunnen we daar het volgende over zeggen:

- *Point-to-point*

  Een beveiligde point-to-point verbinding bestaat uit een tweezijdige TLS-tunnel. Hierbij wordt gebruik gemaakt van PKI- certificaten om het verkeer tussen twee opeenvolgende servers in de keten te beschermen. Hierdoor kan een derde tijdens transport niet de gegevens inzien. Het certificaat moet vertrouwd zijn (geldig PKI-overheid of PKI-ODOC). De identiteit van de PKI-houder speelt op dit niveau geen rol. Als de keten uit meerdere schakels bestaat geeft een point-to-point verbinding slechts gedeeltelijke bescherming.

- *App-to-app*

  In Digikoppeling valt deze beveiligingsniveau samen met de volgende. In Edukoppeling is het expliciet gemaakt vanwege de toepassing van software-as-a-service (SAAS). De identiteit van de bewerker wordt met zekerheid vastgesteld door het signen met een PKI-certificaat (PKI-overheid of PKI-ODOC) waarin het Organisatie Identificatie Nummer (OIN) van de gegevensbewerker is opgenomen. Bovendien wordt dit certificaat gebruikt om het bericht te encrypten. Daarmee wordt het extern transport volledig beschermd.

- *End-to-end*

  De centrale vraag bij SAAS is hoe weet de ketenpartner van welke school gegevens afkomstig zijn of welke zekerheden zijn er dat gegevens bij de bedoelde school terecht komen en nergens anders? De eerste maatregel is WS-addressing voor het kunnen 'routeren achter de voordeur'. In de from- en to-parameter staat het OIN van zender respectievelijk ontvanger. De tweede maatregel is het vastleggen van de mandateringsrelatie tussen eindgebruiker en gegevensbewerker. Dit geeft de ketenpartner zekerheid dat wordt gehandeld conform de wil van de eindgebruiker. De derde maatregel is dat door middel van het certificeringsschema de interne keten eindgebruiker - gegevensbewerker is beschermd.

In deze opzet spelen de natuurlijke personen achter de eindorganisatie, geen rol. In werkelijkheid zijn er leerlingen, leerkrachten of ondersteunend personeel die toegang hebben tot een

gegevensverwerkend systeem hetzij lokaal of in de cloud[3]. Edukoppeling legt nooit een relatie tussen deze natuurlijke personen en het service- en berichtenverkeer dat zo'n systeem via Edukoppeling met andere organisaties heeft.

Best-practises

In de praktijk kunnen de hierboven onderscheiden rollen samenvallen. Dit levert verschillende situaties op:

1. Lokale installatie
   Als de verwerkende software lokaal is geïnstalleerd, dan vallen alle drie de rollen samen. De school werkt in dit geval met een eigen PKI-certificaat en er is geen certificeringsschema nodig. Doorgaans kan met een TLS-tunnel het externe verkeer afdoende worden beschermd. Signing en encryptie kunnen achterwege blijven. Vanwege de eenduidigheid van Edukoppeling wordt in deze situatie wel met ws-addressing gewerkt en een impliciete mandateringsrelatie (zie bouwsteen serviceregister).

2. Cloud installatie van software
   In veel gevallen maken scholen gebruik van gegevensverwerkende software in de cloud. Er wordt gebruik gemaakt van ws-addressing en de expliciet vastgelegde mandateringsrelatie wordt gecheckt met het PKI-certificaat van de cloud-leverancier[4]. Deze heeft een assessment doorlopen aan de hand van het certificeringsschema.

3. Cloud installatie van infrastructuur
   Edukoppeling ondersteunt de situatie waarbij het ontvangen en verzenden van berichten apart van de gegevensverwerkende software in de cloud wordt uitbesteed. Deze logistieke dienstverleners hebben geen bemoeienis van de data. In dit geval zijn signing en encryptie door de gegevensverwerker noodzakelijke voorwaarden

Beheerpatroon

Uitgangspunt voor ketenbeheer is dat er bij de uitwisseling van gegevens soms dingen fout gaan en dat dat niet erg is mits er maatregelen zijn getroffen om die fouten te detecteren en te herstellen. In Edukoppeling worden vijf typen fouten onderscheiden:

Cat.	Typering	Omschrijving	Verwerking
A	Syntax fouten	Fouten in de syntax van bericht (WSA, XSD). (Zie lijst Transactiestandaard)	In gateway verzender (feed forward controle). En in gateway ontvanger voor feedback naar verzender met soap-fault. Actie beheerder.
B	Service gesloten	Vanwege onderhoud, aanroep buiten window, overload, oid	In gateway ontvanger. Soap-fault naar verzender. Automatische herhaling tot een instelbaar

[3] Toegang voor de menselijke gebruikers wordt geregeld in het IAA-stelsel. Dit omvat het verschaffen van een authenticatiemiddel en het aanleveren van een gepaste, aan een organisatie/dataset gekoppelde, identiteit.
[4] De identiteit van het PKI-houder wordt behalve met de signing zoals beschreven in Digikoppeling ook wel vastgesteld met behulp van de zogenaamde, niet in Digikoppeling gedocumenteerde, TLS-offloading. Signing is breder toepasbaar en heeft de voorkeur boven TLS offloading.

		(Zie lijst Transactiestandaard)	maximum. Daarna actie beheerder.
C	Service reageert niet (tijdig)	Er volgt geen synchrone response binnen de afgesproken time-out (beschreven in programma van eisen)	In gateway verzender. Automatische herhaling tot een instelbaar maximum. Daarna signaal naar beheerder.
D	Functionele fouten	Fouten bij het verwerken van een bericht. (beschreven in programma van eisen)	In applicatie ontvanger. Indien herstelbaar soap-fault naar verzender en actie beheerder. Anders actie beheerder van de ontvanger.
E	Prestatie-fouten	Overschrijding van prestatie-drempelwaarden (beschreven in programma van eisen)	Wordt gemonitord door serviceverlener en /of de serviceaanvrager.

Best-practises

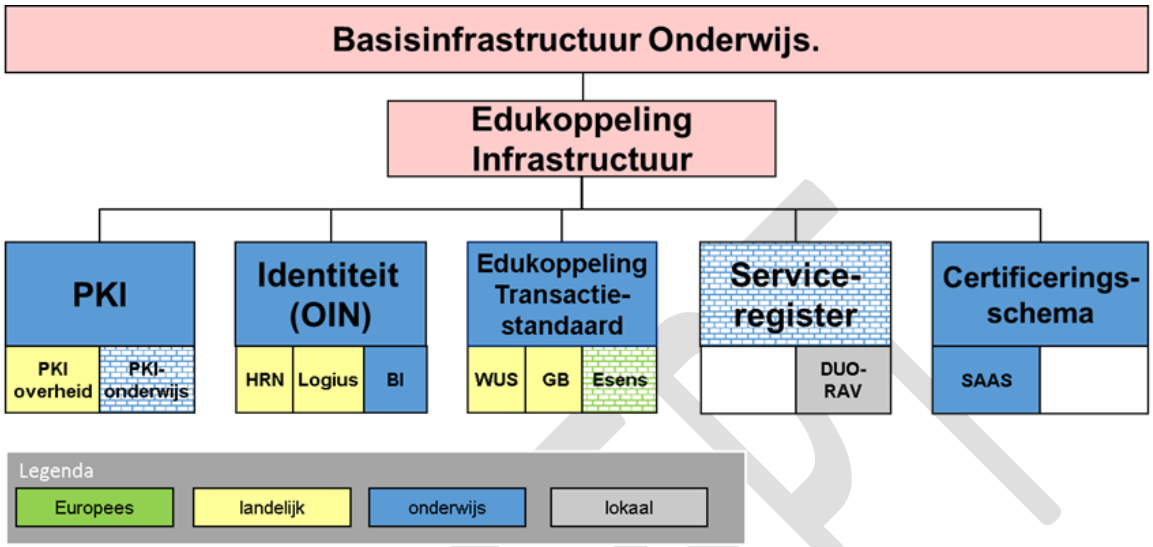
Een gateway is stateless. De gateway heeft als functie om zo snel en zo veel mogelijk berichtenverkeer af te handelen. Hij houdt daarom niet de verwerkingsstatus bij van de verschillende berichten die zijn ontvangen of verstuurd. Dat wordt zonodig applicatieniveau gedaan.

Foutmeldingen zijn toegankelijk voor de beheerders en die hebben de taak om foutmeldingen regelmatig te onderzoeken, eventueel door samenspraak met de beheerder van de ketenpartner. De gateway biedt naast de aangeboden service ook een lege “pingservice“.Deze kan worden gebruikt bij opstartproblemen en bij het analyseren van fouten.

Een veelvoorkomende maatregel als er geen of niet tijdig een verwachte reactie komt van de ketenpartner, is het herzenden van een bericht. Berichten moeten dan idempotent zijn. Dubbele verzending of ontvangst in verkeerde volgorde leidt bij idempotente berichten tot hetzelfde resultaat.

4. Bouwstenen

Edukoppeling is opgebouwd uit een aantal bouwstenen die zo mogelijk zijn gebaseerd op landelijke bouwstenen (zie figuur 8).



Figuur 8 – Edukoppeling Architectuur

De bouwstenen voor de Edukoppeling Architectuur worden gevormd door zaken die essentieel zijn om beveiligde en betrouwbare gegevensuitwisseling mogelijk te maken. Deze bouwstenen worden in dit hoofdstuk toegelicht.

Transactiestandaard

De Digikoppeling standaard van de landelijke overheid staat model voor Edukoppeling. Maar er zijn wel zaken die specifiek zijn:

- Profielen voor gegarandeerde aflevering worden uitgesloten
  Binnen de Edukoppeling community wordt geen toegevoegde waarde aan deze profielen gehecht of zelfs een negatieve waarde. Dat een bericht gegarandeerd is afgeleverd, wil nog niet zeggen dat het ook gegarandeerd is verwerkt. Dit betekent dat er alsnog op applicatie niveau maatregelen moeten worden genomen.
- De profielen zijn aangepast voor cloud-computing
  In het onderwijs heeft cloud computing op grote schaal ingang gevonden. Dit betekent dat de SAAS-leverancier moet kunnen ‘routeren achter de voordeur’. Daartoe zijn de ws-addressing afspraken van Digikoppeling (de soap-envelop) uitgebreid. Overigens in overleg met Logius, de beheerder van Digikoppeling.

Primair bestaat Edukoppeling uit een aangevuld Digikoppeling-WUS[5] profiel. Een tweede Digikoppeling profiel wat binnen de onderwijssector toegepast kan worden is het Grote Berichten (GB) profiel. Dit kan worden toegepast bij gegevensuitwisseling van grote (>20Mb) samengestelde informatieproducten. Hierbij gelden vooralsnog geen aanvullende voorschriften. De basis van dit

5 De WS-* familie bestaat onder meer uit de standaarden WSDL, UDDI en SOAP. Daarom wordt deze familie wel aangeduid met WUS.

profiel is dat de verzender van een groot bericht een metabericht verzendt of ontvangt en de ontvanger het bericht van het aangegeven internetadres geautomatiseerd downloadt.

Ook Europa wordt service- en berichtenverkeer gestandaardiseerd onder de noemer Esens. Vooralsnog is met Europa in Edukoppeling geen rekening gehouden.

De Edukoppeling Transactiestandaard (TS) is uitgewerkt in een apart document en in beheer genomen door Edustandaard. Edustandaard is een open platform waar partijen binnen het onderwijsveld bij elkaar komen om afspraken te maken. Hier vindt tevens de doorontwikkeling van de standaard plaats. Hiertoe is een werkgroep Edukoppeling[6] ingericht.

Identiteit

Elke partij die via Edukoppeling de gegevensuitwisseling inricht of laat inrichten, wordt geïdentificeerd op basis van het unieke Organisatie Identificatie Nummer (OIN), zie nummersystematiek Digikoppeling[7]. De identiteit is gebaseerd op het Nieuw Handelsregister (bij bedrijven of bevoegd gezagen), op Logius (bij overheidsinstellingen) of op de Basislijst Instellingen (opvolger van BRIN). Het OIN wordt gebruikt in ws-addressing om de eindorganisatie aan te duiden en in PKI-certificaten om de gegevensbewerker aan te duiden. Meer details zijn uitgewerkt in de Edukoppeling Transactiestandaard (TS).

PKI

Conform Digikoppeling wordt voor authenticatie gebruik gemaakt van Public Key Infrastructure (PKI) certificaten. De PKI-certificaten kunnen worden gebruikt voor ondertekening en versleuteling zoals dit ook in Digikoppeling wordt toegepast. Deze certificaten worden uitgegeven door CSP's. Een CSP 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. Voor Edukoppeling kunnen twee soorten certificaten toegepast worden, dit zijn:

1. PKI-Overheidscertificaten – Digikoppeling (PKIO)[8]
2. PKI-OCW Digitale Onderwijscertifcaten (ODOC)

Technisch werken deze certificaten op dezelfde manier. Het werkingsgebied is verschillend. PKIO certificaten kunnen door iedereen worden aangevraagd en ODOC certificaten zijn alleen beschikbaar voor organisaties die in het onderwijs werkzaam zijn. ODOC certificaten. Meer details zijn uitgewerkt in de Edukoppeling Transactiestandaard (TS).

6 Voor meer info over de Edukoppeling werkgroep, zie http://www.edustandaard.nl/participeren/werkgroepen/werkgroep/werkgroep-edukoppeling/

7 Digikoppeling nummersystematiek: http://www.logius.nl/fileadmin/logius/product/digikoppeling/algemeen/Gebruik_en_Achtergrond_Digikoppeling_Certificaten_v1.2.1.pdf

8 Let op: Niet alle PKI-overheidscertificaten bevatten een OIN. Het moeten certificaten zijn die geschikt zijn voor Digikoppeling (zie ook voorgaande voetnoot).

Serviceregister

Een algemene indeling, afkomstig uit de UDDI-standaard, van een serviceregister is in drie soorten "pagina's":

- White pages beschrijven organisaties die web services beschikbaar stellen. Deze informatie maakt het mogelijk web services te vinden op basis van (kenmerken van) de organisatie die ze beschikbaar stelt.
- Yellow pages beschrijven de business services die beschikbaar zijn, ingedeeld volgens nader te bepalen taxonomieën. Deze informatie maakt het mogelijk om services te vinden op basis van een inhoudelijke categorisering.
- Green pages beschrijven de technische interfaces waarlangs de services benaderd kunnen worden. Deze informatie maakt het mogelijk services daadwerkelijk aan te roepen.

Een serviceregister dient kortweg om 1) informatie over de ketenpartners, zoals het publieke gedeelte van een PKI-certificaat, 2) Informatie over de collectief afgesproken services en 3) informatie over wie welke services namens wie aanroept/aanbiedt.

In relatie tot Edukoppeling wordt het serviceregister van belang om de mandateringsrelatie vast te leggen. Deze laatste informatie wordt gebruikt in combinatie met PKI en WS-addressing om per onderwijsinstelling de juiste webservice aan te roepen en om een inkomende servicerequest te autoriseren. Het serviceregister voor de hele sector is nog in ontwikkeling. Het is gebaseerd op eerder werk in de Routerings en Autorisatie Voorziening (RAV) in gebruik bij DUO.

Certificeringsschema

In 2014 is het initiële certificeringsschema geregistreerd bij Edustandaard voor end-to-end-security bij cloud leveranciers en biedt procedurele zekerheid dat de klant omgeving van de ene onderwijsinstelling is gescheiden van de ander. Dit is een verlengstuk van de technische maatregelen in Edukoppeling. Zie:
http://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema-rosa-1/1.1/.

Het schema bestaat uit een set normen die afkomstig zijn uit de zogenaamde Cloud Control Matrix en is tegen de beveiligingsnormen ISO 27001 en 27002 en privacy wetgeving aangehouden. Met dit resultaat kunnen cloud-leveranciers:

- Periodiek een audit doorlopen aan de hand van de opgestelde normen;
- Een standaard bewerkersovereenkomst met de onderwijsinstelling afsluiten

Organisaties die de resultaten hebben overlegd en waar nodig maatregelen kunnen laten zien, worden opgenomen in het certificeringsregister. Het streefbeeld zoals ook verwoord in het P&S-katern van de ROSA is dat dit een formeel aspect wordt van wettelijke taken waarbij een SAAS-leverancier is betrokken. Opname in het register waarborgt voor onderwijsinstelling dat privacy en security bij uitbesteding voldoen aan het normenkader.

Er zijn binnen Edustandaard afspraken gemaakt over de governance van het certificeringsschema. Op basis van risico-analyse kan het schema periodiek worden aangescherpt/uitgebreid. De toetsingsprocedure zal worden aangescherpt van een selfassessment naar een third party mededeling.

Bijlage A: Begrippenlijst

Deze begrippenlijst is aanvullend op de begrippenlijst van Digikoppeling.

Onderwijsinstelling

De onderwijsgerelateerde organisatie met het aanbieden van onderwijs als doel. Deze wordt geïdentificeerd met BRIN4.

Authenticatie

Het valideren van de identiteit van een organisatie die deelneemt aan Edukoppeling verkeer (‘ben jij wie je zegt dat je bent?’).

Autorisatie

Het bepalen of de service afnemer toestemming heeft voor de gevraagde dienst (‘mag jij wat je vraagt?’) of wat de het toegestane gegevensbereik voor de service afnemer is van de (‘waar mag je bij?’)

BRIN

Basisregister Instellingen. Register beheert door DUO met daarin alle bekostigde en aangewezen onderwijsinstellingen en gelieerde vestigingen. BRIN staat ook voor de identificatiecode van een instellingen van 4 posities.

Cloudleverancier

Leverancier van software 'in de cloud'. Zie ook SaaS.

Digikoppeling

Digikoppeling faciliteert gegevensuitwisselingen tussen overheidsorganisaties door standaardisatie van koppelvlakken (een overeengekomen set middelen en afspraken). Zie ook https://www.logius.nl/ondersteuning/digikoppeling/#c8445

Edustandaard

Edustandaard is een platform waar alle partijen binnen het onderwijsveld bij elkaar komen om afspraken te maken. Deze afspraken gaan bijvoorbeeld over het vindbaar maken van digitaal leermateriaal door middel van vastgestelde begrippen, of over het overbrengen van leerlinggegevens van het ene systeem naar het andere. Zie ook http://www.edustandaard.nl/.

Identificatie

Het relateren van een organisatie aan een registratie bij een identititeitsprovider. In het onderwijs is dat in veel gevallen BRIN, maar ook het NHR en Logius worden gebruikt.

ROSA

Referentie Onderwijssector Architectuur. Is de verbijzondering van de NORA voor de sector onderwijs. Voorheen: Referentie Architectuur Onderwijs (RAO).

SaaS

Software as a Service. Is een vorm van Cloud Computing. Veel toegepast in het onderwijs. De leerling, leraar of administratief personeel logt remote in op het systeem van de cloud- of SaaS-leverancier.