Edukoppeling

Architectuur 1.2.1

Edustandaard

Datum: Juli 2017

Versie: 1.2.1

Status: Definitief

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 onderwijsinstellingen onderling, tussen onderwijsinstellingen en de overheid en tussen onderwijsinstellingen 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[1] 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 ketenpartner is vastgesteld
2. Berichtinhoud is vertrouwelijk en integer
3. Verzending berichten is onweerlegbaar
4. Verkeer tot 1G berichten per jaar

De eerste 3 requirements zijn zaken die met PKI-certificaten uitgevoerd worden. Een kenmerk van Edukoppeling is dat per deelnemer slechts één PKI-certificaat nodig is voor meerdere soorten toepassingen. Het vierde requirement slaat op de aanname dat de hoeveelheid service- en berichtenverkeer de komende jaren sterk zal groeien. Dat er dan ook meer mis kan gaan, is reden om aandacht te besteden aan het ketenbeheer.

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.
- Stappenplan i.o.

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

---

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

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**
1.2.01	WG Edukoppeling	Maart 2015	Initiële versie
1.2.93	WG Edukoppeling	Juni 2015	Concept ter besluitvorming in werkgroep 17-6-2015
1.2.94	WG Edukoppeling	Juni 2015	Concept ter bekrachtiging in standaardisatieraad 2-7-0215
1.2.1	WG Edukoppeling	Juli 2017	Patchversie vastgesteld in werkgroep van 21 juni 2017. Begrippen zijn in een apart document opgenomen.

2. Achtergrond

Relatie met Digikoppeling

Digikoppeling[2] is een transactiestandaard op de zogenaamde pas-toe-of-leg-uit-lijst van de Nederlandse overheid en aanverwante instellingen waaronder ook, dat is alleen weinig bekend, onderwijsinstellingen. Digikoppeling vormt het fundament van de Edukoppeling transactiestandaard. Digikoppeling is echter niet zonder meer te gebruiken in het onderwijsveld:

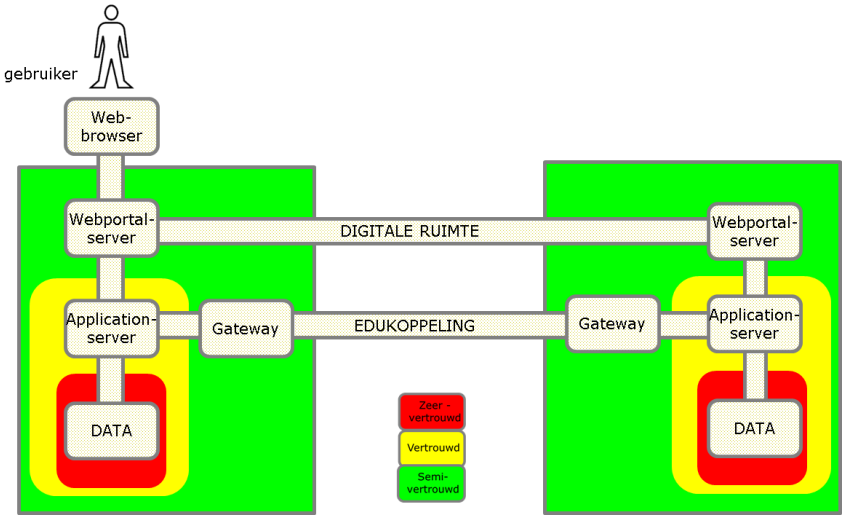
1. Onderwijsinstellingen maken steeds vaker gebruik van SaaS-leveranciers voor de ondersteuning van hun administratieve processen. Deze partijen worden binnen Edukoppeling als formele partij onderkend waardoor de beheerlast (met name rondom certificaatbeheer) voor onderwijsinstellingen beperkt kan blijven.
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 ruggenspraak met de beheerder van Digikoppeling (Logius).

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

Edukoppeling in de onderwijsketen

De ROSA 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. De kleuren geven verschillende beveiligingszones weer. De betekenis van de kleuren is ontleend aan www.noraonline.nl/wiki/beveiligingspatronen.

Edukoppeling dient de communicatie tussen ICT-systemen van verschillende organisaties, specifiek in de vorm van berichtenverkeer. Edukoppeling beschrijft de machine-machine interface.

Uiteindelijk is er altijd een natuurlijke persoon die als gebruiker optreedt, bijvoorbeeld medewerker die door middel van een webservice inzage krijgt bij een andere organisatie. In toenemende mate is dat de onderwijsvolger of zijn wettelijke vertegenwoordiger zelf. De Digitale Ruimte draait om het geven van toestemming om data te leveren aan een andere organisatie. In dat geval wordt de toestemming in de vorm van een token door de ontvangende partij meegegeven in een verzoek over Edukoppeling op te halen.

In de zonering zijn de ‘voorkant’ en ‘achterkant’ ontkoppeld. De gebruiker, bijvoorbeeld de leerling of leerkracht of administratieve kracht, heeft een authenticatiemiddel waarmee zijn identiteit en de onderwijsinstelling/dataset wordt vastgesteld. Denk daarbij aan wachtwoorden, tokens of een E-identiteitskaart. Het IAA-stelsel dat daarbij hoort maakt geen onderdeel uit van deze documentatie. Bij uitwisseling via Edukoppeling speelt alleen de identiteit van de onderwijsinstelling/dataset een rol. Dat is onder andere gebaseerd op PKI-certificaten en wordt verder uitgewerkt in hoofdstuk 3.

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 is ontkoppeld van de andere lagen. Daardoor kan een ketenpartner met één implementatie op een veilige manier een veelheid van toepassingen uitvoeren.

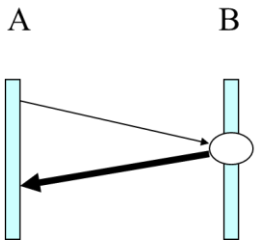
Uitwisselingspatronen

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.

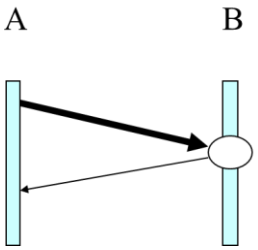


Figuur 2 – Patroon request-response

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. Dit wordt bijvoorbeeld toegepast voor een notificatiebericht.

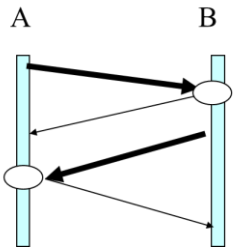


Figuur 3 – Patroon melding-bevestiging

In dit patroon gaan de systemen van de ontvanger iets doen. Belangrijk is de schadelijke effecten te voorkomen als een bericht twee keer wordt verzonden (door een time-out) of als meldingen in de verkeerde volgorde binnenkomen. Digikoppeling lost dat op met het patroon Gegarandeerde aflevering. Edukoppeling ondersteunt dat niet. 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).

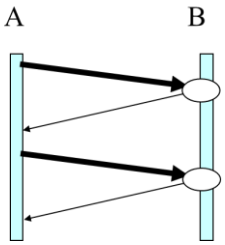


Figuur 4 – Asynchrone uitwisseling

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 uitgevoerd:

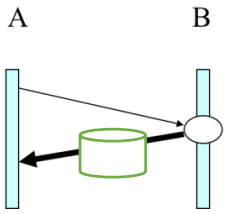


Figuur 5 – Antipatroon polling

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 een relatief dure oplossing. Uitgangspunt is dat alle deelnemers aan Edukoppeling zowel webservices kunnen aanroepen als 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:

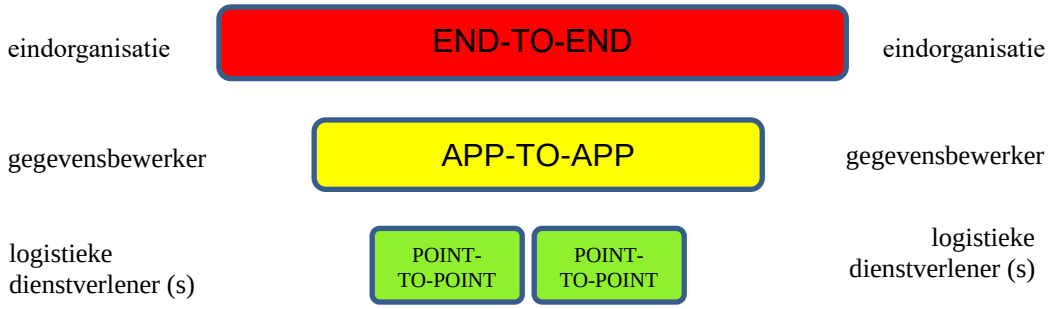
Rol: Eindorganisatie
De eindorganisatie is de organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie. Deze is gebonden aan een (vaak collectief gemaakte) uitwisselingsovereenkomst of gegevensleveringsovereenkomst, o.i.d. Zijn hebben niet een opdrachtrelatie. De eindorganisatie is degene die verantwoordelijk is voor bescherming van de privacy. Bijvoorbeeld: onderwijsinstelling wisselt uit met DUO en onderwijsinstelling wisselt uit met onderwijsinstelling.

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 eindorganisatie waardoor een bewerkersovereenkomst noodzakelijk is (zie bouwsteen certificeringschema). In het onderwijs is de bewerker vaak niet dezelfde als de eindorganisatie.

Rol: Logistieke dienstverlener
Een logistieke dienstverlener is een organisatie die faciliteert bij de verzending en ontvangst van berichten. Een logistieke dienstverlener heeft wel of niet tijdelijk data onder zijn hoede. Een ketenvoorziening als serviceregister of traffic centra bevat wel gegevens over de uit te wisselen data, maar niet de data zelf. Deze worden hier verder niet beschouwd. Er zijn echter ook logistieke dienstverleners die wel data zien passeren. De regel daarbij is dat die logistieke dienstverleners met een ‘gesloten envelop’ werken (principe privacy by design).

Nota bene, het is mogelijk dat een logistieke dienstverlener desalniettemin in het kader van de WBP moet voldoen aan de regels die gelden voor een bewerker.

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 geldt het volgende:

- *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 niet de gegevens tijdens transport 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 bescherming tot de eerst volgende schakel.

- *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 PKI-certificaat gebruikt om het bericht te signen en het certificaat van de andere gegevensbewerker om te encrypten. Daarmee wordt het extern transport volledig beschermd.

- *End-to-end*

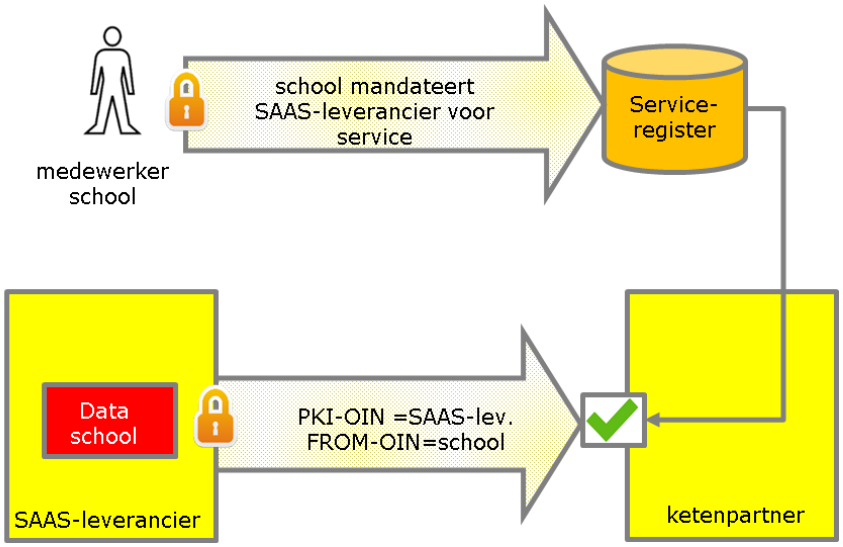
  Omdat onderwijsinstelling vaak met SAAS-oplossingen werken heeft een ketenpartner zekerheid nodig van welke onderwijsinstelling gegevens afkomstig zijn of nergens anders terecht komen. Dit betekent dat, bovenop PKI, extra maatregelen nodig zijn om de keten 'achter de voordeur' te sluiten. De eerste maatregel 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 eindorganisatie en gegevensbewerker. De derde maatregel is het certificeringsschema dat aantoont dat de aandacht vestigt op beveiliging bij cloud-computing.

In Edukoppeling 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[3]. In Edukoppeling wordt geen relatie gelegd tussen een natuurlijke personen en een uitwisselingsbericht.

Streefbeelden bij SAAS

Identificatie van de servicerequester

Alvorens een vertrouwelijke service te leveren (request-response patroon) heeft de ketenpartner een sterke identiteit van de eindorganisatie, de school, nodig (zie figuur 8)



Figuur 8 – Identificatie van de servicerequester

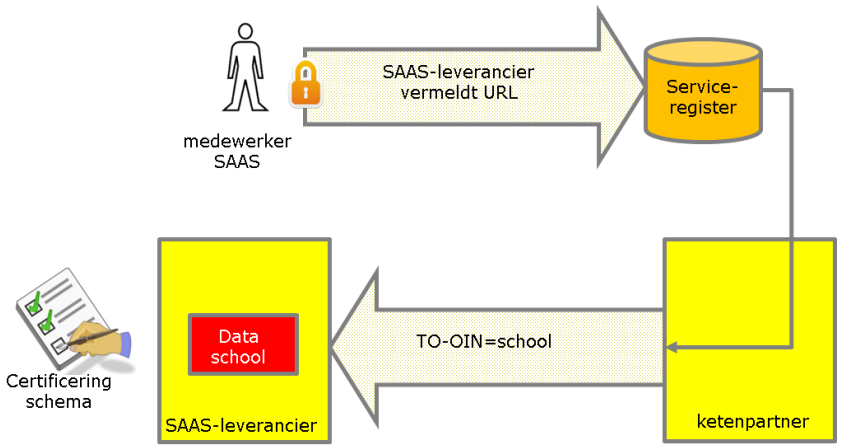
Dit begint met het mandateren van de SAAS-leverancier door een medewerker van de school. Dit wordt expliciet gemaakt door een formulier of op een beveiligde site en geregistreerd. Wanneer de SAAS-leverancier namens een school een service aanroept, signt hij het bericht met zijn eigen PKI-certificaat en zet in de from-parameter voor welke school het is. De ketenpartner controleert dit aan de hand van de vastgelegde mandateringsrelatie.

In figuur 8 heeft de SAAS-leverancier het bericht gesigned. Daarmee ligt niet alleen vast wie dat is, maar ook dat dit de partij is die onweerlegbaar het bericht heeft verzonden en dat het bericht tijdens transport integer is gebleven.

[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.

Identificatie van serviceaanbieder

Het patroon melding-bevestiging wordt gebruikt om vertrouwelijke gegevens te versturen. Als dat een school is die gebruik maakt van SAAS, dan moet dat ‘in het goede bakje’ terecht komen (zie figuur 9)

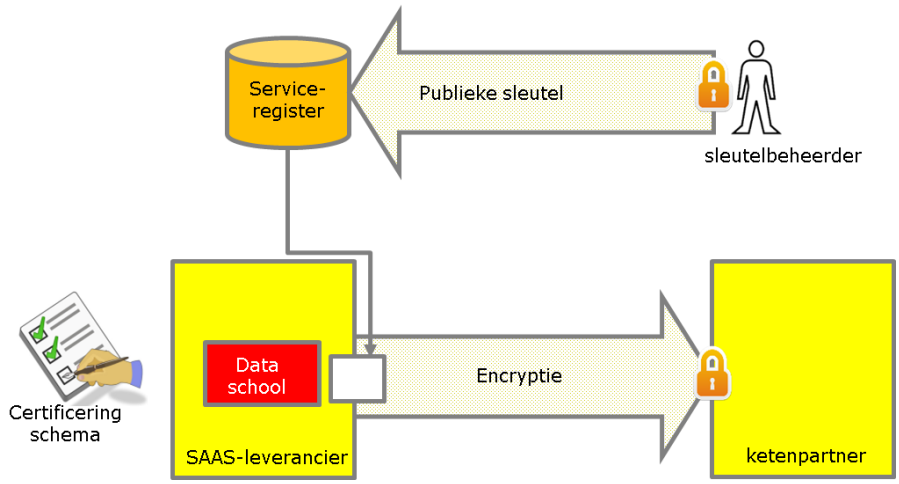


Figuur 9 – Identificatie van serviceaanbieder

In figuur 8 heeft de school de SAAS-leverancier gemandateerd. Wat er aan toe moet worden gevoegd is op welk internetadres of URL de gegevens afgeleverd moeten worden. Dit wordt gebruikt om de gegevens te versturen en tevens wordt de geadresseerde school in de TO-parameter gezet. Hiermee kan de SAAS-leverancier ‘routeren achter de voordeur’. Het certificeringsschema geeft de verzender zekerheid dat de gegevens bij de goede school terecht komen.

Berichten vertrouwelijk

Het transport van vertrouwelijke gegevens vraagt om maatregelen om ervoor te zorgen dat de ze niet door onbevoegden kunnen worden ingezien (zie figuur 10).



Figuur 10 – Berichten vertrouwelijk

Degene die het berichte encrypt heeft de publieke sleutel nodig van zijn ketenpartner. De ontvanger kan het vervolgens met zijn private sleutel weer decrypten. Iemand anders kan het niet en daarmee is het externe transport vertrouwelijk. Het interne transport binnen een SAAS-leverancier is vertrouwelijk als naar de normen van het certifceringsschema is gekeken.

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 bij een onderwijsinsteling, dan vallen alle drie de rollen samen. De onderwijsinstelling werkt in dit geval met een eigen PKI-certificaat en er is geen certificeringsschema nodig. Een TLS-tunnel biedt ook bescherming bij het externe verkeer tegen inkijk door derden, tenzij het verkeer over servers van derden loopt.

2. Cloud installatie van software
   In veel gevallen maken onderwijsinstellingen gebruik van gegevensverwerkende software in de cloud. Hierbij horen de identificerende maatregelen bij servicerequester en – aanbieder uit de vorige paragraaf[4].

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 (Zie lijst Transactiestandaard)	In gateway ontvanger. Soap-fault naar verzender. Automatische herhaling tot een instelbaar maximum. Daarna actie beheerder.
C	Service reageert niet (tijdig)	Er volgt geen synchrone response binnen de afgesproken time-out	In gateway verzender. Automatische herhaling tot een instelbaar maximum. Daarna signaal naar beheerder.

[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.

		(beschreven uitwisselovereenkomst)	
D	Functionele fouten	Fouten bij het verwerken van een bericht. (beschreven iniuitwisselovereenkomst)	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 uitwisselovereenkomst)	Wordt gemonitord door serviceverlener en /of de serviceaanvrager.

Best-practises

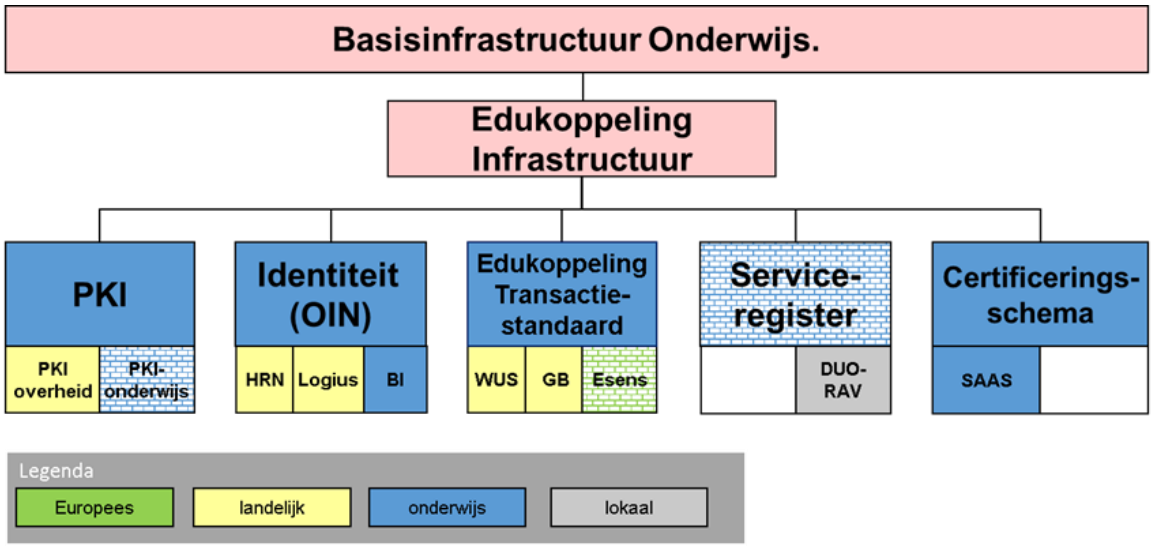
Een gateway is stateless. De gateway heeft als functie om zo snel en zo veel mogelijk berichtenverkeer af te handelen. Hij houdt daarom niet de verwerkingsstatus bij van de verschillende berichten die zijn ontvangen of verstuurd. Dat wordt zonodig applicatieniveau gedaan.

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 11).



Figuur 11 – 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.

Nota bene: Logius, de beheerder van Digikoppeling heeft een Compliance-voorziening voor Digikoppeling-3. De werkt ook voor Edukoppeling.

Identiteit (OIN)

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:

https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-2017/

De vorige versie van het Certificeringsschema (versie 1.1) bestaat voornamelijk uit een set maatregelen gebaseerd op de Cloud control matrix van de Cloud Security Alliance. De nieuwe versie (vastgesteld op 13 juli 2017) is gebaseerd op ISO 27001 en ISO 27002 en uitgebreid met beschrijvingen over het proces, toezicht, et cetera. Met dit resultaat kunnen SaaS-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.