edustandaard

Edukoppeling

Architectuur 1.2.2

Edustandaard
Datum: december 2018
Versie: 1.2.2
Status: definitief

Inhoudsopgave

1. Leeswijzer

In hoofdstuk 2 wordt de aanleiding, het doel en de doelgroep voor Edukoppeling Architectuur beschreven. In hoofdstuk 3 wordt de achtergrond van Edukoppeling Transactiestandaard en Architectuur toegelicht. In hoofdstuk 4 wordt aan de hand van transactiepatronen het gebruik van Edukoppeling Transactiestandaard uitgelegd en in hoofdstuk 5 zijn de bouwstenen waaruit Edukoppeling Architectuur bestaat in hoofdlijnen beschreven.

1.1. 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.
1.2.2	WG Edukoppeling	December 2018	#15 Voor TLS, ondertekenen en versleutelen van berichten worden geen ODOC certificaten meer toegepast in productie #24 Digikoppeling 3.0 is vervallen. Alle verwijzingen worden vervangen met een verwijzing naar het Digikoppeling “Overzicht actuele documentatie en compliance” document. #27 Verwijzing naar nieuwste versie Certificeringsschema #28 Overzichtsplaat (figuur 11) aangepast. Doel is end-to-end beveiliging, Edukoppeling is één van de bouwstenen om dit te realiseren. Verder enige tekstuele aanpassingen. #39 Architectuur paragraaf 4.5 (foutafhandeling) samengevoegd met

			paragraaf 3.8 van de transactiestandaard #40 Architectuur paragraaf 5.1 (figuur 11). Compliancevoorzieningen van Digikoppeling en Edukoppeling opnemen. Opmerking in tekst dat de compliancevoorziening voor Edukoppeling nog niet gerealiseerd is.

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, bedrijfkritische gegevens). De Edukoppeling-standaard is gebaseerd op het nationale communicatieprotocol Digikoppeling.
Edukoppeling Transactiestandaard is een belangrijke bouwsteen in de onderwijsreferentiearchitectuur ROSA[1]. Dit document beschrijft de scope, doelen en principes achter de Edukoppeling-infrastructuur, de samenhang met andere ROSA-onderdelen en verklaart de verschillende onderdelen.

2.2. Doel en doelgroep

Edukoppeling is een gedeelde onderwijsvoorziening voor vertrouwelijk machine-machine uitwisseling in het onderwijs en zorgt voor met name technische interoperabiliteit. Die interoperabiliteit draagt bij aan het realiseren van het merendeel van de in ROSA[2] gedefinieerde doelen:

Bovensectorale samenwerking
- Inspelen op beleidswijzigingen
- Terugdringen administratieve lasten

Privacy en beveiliging
- Ketenbrede informatiebeveiliging en privacybescherming

IAA
- Privacy by design

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.

[1] https://www.wikixl.nl/wiki/rosa/index.php/Hoofdpagina
[2] Voor meer informatie over ROSA, zie https://www.wikixl.nl/wiki/rosa/index.php/Doelen_en_principes

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 1.3 (onderdeel van Edukoppeling-specificaties)
- Identificatie en authenticatie 1.0 (onderdeel van Edukoppeling-specificaties)
- Certificeringsschema Informatiebeveiliging en Privacy ROSA[3]
- OnderwijsServiceregister i.o.

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

[3] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

3. Achtergrond

3.1. Relatie met Digikoppeling

Digikoppeling[4] 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 onderwijskundige en 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 doorgaans 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.

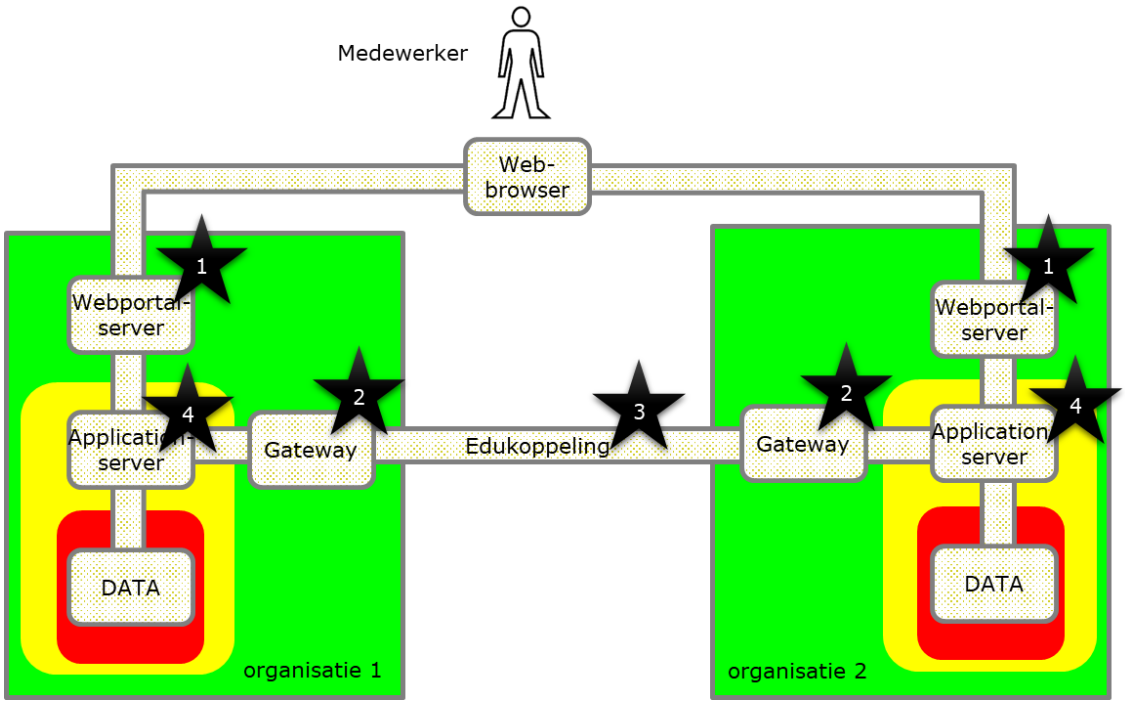
De Edukoppeling Transactiestandaard vormt een ‘collectieve leg-uit’ voor het onderwijsinstellingen ten aanzien van de pas-toe-of-leg-uit status van Digikoppeling. Van overheidswege worden de onderwijsinstellingen niet gedwongen om beveiligde gegevensuitwisseling op een andere manier dan via de in Edustandaard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

3.2. 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 is schematisch een beeld geschetst hoe de basisinfrastructuur ketensamenwerking ondersteund.

[4] Digikoppeling: https://www.logius.nl/diensten/digikoppeling

Edukoppeling Architectuur



Figuur 1 – Schematische weergave ketensamenwerking

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 vooral over vertrouwelijke, privacygevoelige gegevens die beschermd moeten worden. De kleuren geven verschillende beveiligingszones weer. De betekenis van de kleuren is ontleend aan het beschouwingsmodel zonering[5].
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 een medewerker die door middel van een webservice inzage krijgt bij een andere organisatie. In toenemende mate kan dat ook de onderwijsvolger of zijn wettelijke vertegenwoordiger zelf zijn.
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.

In Figuur 1 wordt een schematisch beeld geschetst van deze ketensamenwerking. De school[6] is vertegenwoordigd in deze figuur als de organisatie die mensen in dienst heeft (de medewerker). Deze medewerker heeft bijvoorbeeld toegang tot een administratiesysteem in de cloud en tot bekostigingsgerelateerde informatie van DUO (via het Zakelijk Portaal). We kunnen samenvattend het volgende stellen:

1. In de front-office logt de medewerker van de school met een federatieve sleutel met een beveiligingsniveau waarover in het onderwijs eenduidige afspraken zijn vastgelegd. Dat kan

[5] zie: www.noraonline.nl/wiki/beveiligingspatronen.
[6] Het begrip school wordt in dit gedeelte 'slordig' gebruikt. Het omvat termen als onderwijsinstelling en onderwijsaanbieder.

bijvoorbeeld het beveiligingsniveau substantieel[7] zijn. De authenticatiefederatie is een vertrouwde derde partij die de relatie tussen medewerker en school kan valideren.

2. In de backoffice worden gegevens uitgewisseld conform de Edukoppeling standaard. De SaaS-leverancier is de partij die de uitwisseling feitelijk uitvoert in opdracht van de eindorganisatie (bijv. een school). De SaaS-leverancier beveiligt het verkeer (tweezijdig TLS) met een PKI-Overheidscertificaat met zijn eigen identiteit (OIN).
3. In een collectief serviceregister wordt bijgehouden (dat doet een namens het bestuur van de school gedelegeerde medewerker) of een organisatie is gemandateerd als bewerker van de uitgewisselde gegevens. Deze regelt het bijbehorende serviceverkeer namens de school.
4. Voor de beoordeling van de correcte werking van (cloud)systemen zijn normen beschikbaar. Dit is toegesneden op het uitwisselen met Edukoppeling.

[7] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502

4. Edukoppeling-infrastructuur

4.1. 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.

4.2. 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.

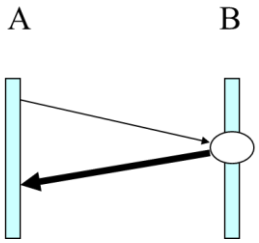
Edukoppeling richt zich alleen op de logistieke laag en is ontkoppeld van de andere lagen. Daardoor kan een ketenpartner met één implementatie op een veilige manier een veelheid van toepassingen uitvoeren.

4.3. 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.

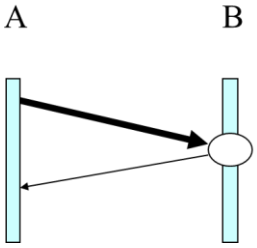


Figuur 2 – Patroon request-response

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.

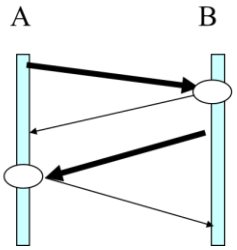


Figuur 3 – Patroon melding-bevestiging

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).

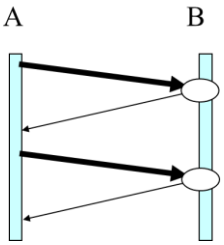


Figuur 4 – Asynchrone uitwisseling

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:

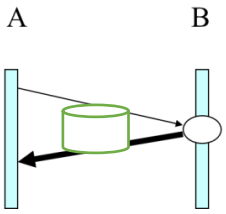


Figuur 5 – Antipatroon polling

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. Het basispatroon binnen Digikoppeling is dat de beoogde ontvanger aansluitend het grote bericht ophaalt.



Figuur 6 – Patroon grote berichten (zonder metabericht)

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

4.4. 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. Een onderwijsinstelling en DUO zijn voorbeelden van een

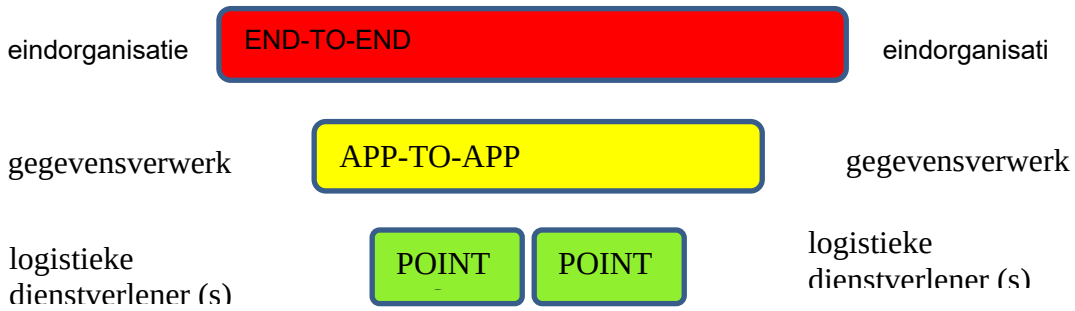
eindorganisatie. De eindorganisatie is degene die verantwoordelijk is voor bescherming van de privacy.

Rol: Gegevensverwerker
De gegevensverwerker 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 verwerkersovereenkomst noodzakelijk is (zie bouwsteen certificeringschema). In het onderwijs is de verwerker 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 AVG moet voldoen aan de regels die gelden voor een verwerker.

Op basis van deze drie rollen zijn drie beveiligingsniveaus 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 (vertrouwelijke) 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). 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 dit beveiligingsniveau samen met de volgende (end-to-end). In Edukoppeling is het expliciet gemaakt vanwege de toepassing van Software-as-a-Service (SaaS).
  Om te voorkomen dat berichten in de keten door derden aangepast kunnen worden, worden deze door de verwerker ondertekend (gesigned) met een eigen PKI-overheid certificaat. Berichten worden versleuteld (ge-encrypt) als er partijen in de keten zijn die het bericht niet mogen inzien. Voor het versleutelen is het publieke certificaat van de ontvangende partij nodig.

De identiteit van een verwerker is opgenomen als Organisatie Identificatie Nummer (OIN) in het PKI-certificaat (PKI-overheid)

- *End-to-end*
  Omdat onderwijsinstellingen 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 van WS-adressing staat het OIN van zender respectievelijk ontvanger. De tweede maatregel is het vastleggen (en kunnen verifiëren) van de mandateringsrelatie tussen eindorganisatie en gegevensverwerker. De derde maatregel is het certificeringsschema dat aantoont dat de aandacht vestigt op beveiliging die een dienstverlener bij cloud-computing heeft ingericht.

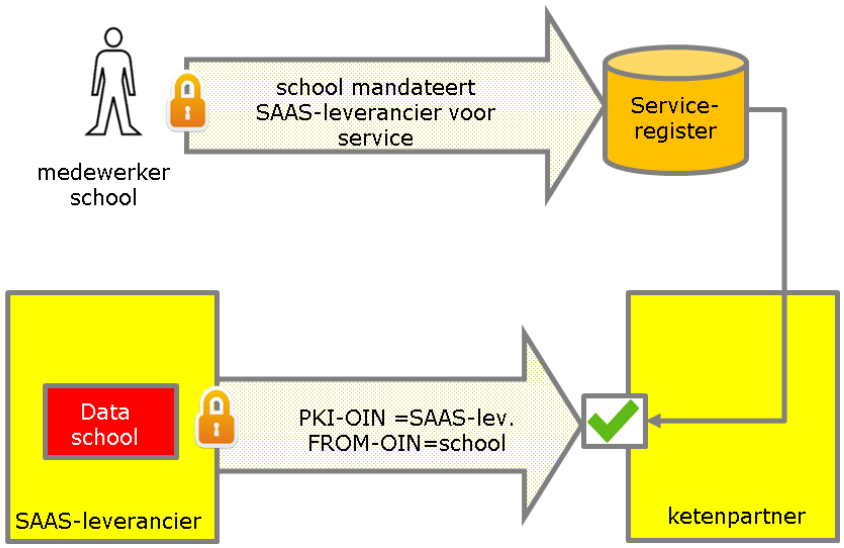
In Edukoppeling spelen de natuurlijke personen achter de eindorganisatie, geen rol. In werkelijkheid zijn dat de leerlingen, leerkrachten of ondersteunend personeel die toegang hebben tot een gegevensverwerkend systeem[8]. In Edukoppeling wordt geen relatie gelegd tussen een natuurlijke personen en een uitwisselingsbericht.

[8] 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.

4.4.1. 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)



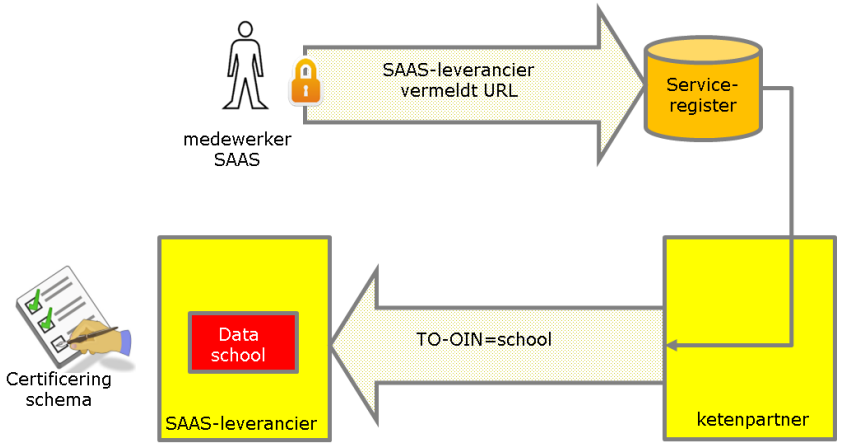
Figuur 8 – Identificatie van de servicerequester

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 een service aanroept, *signt* hij het bericht met zijn eigen PKI-certificaat en zet in de FROM-parameter namens welke school het bericht opgesteld 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.

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)

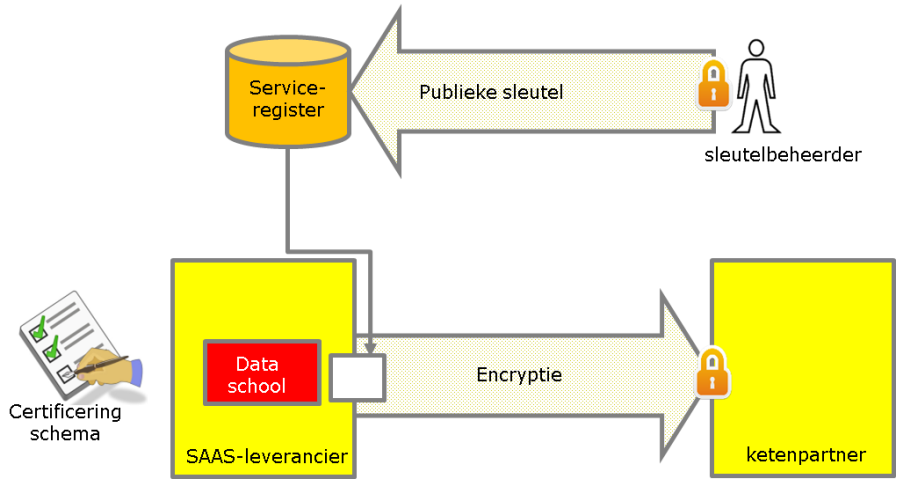


Figuur 9 – Identificatie van serviceaanbieder

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 dienstverlener geregeld heeft 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 bericht *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 certificeringsschema is gekeken en daarop gepaste maatregelen zijn getroffen.

4.4.2. Praktijksituaties

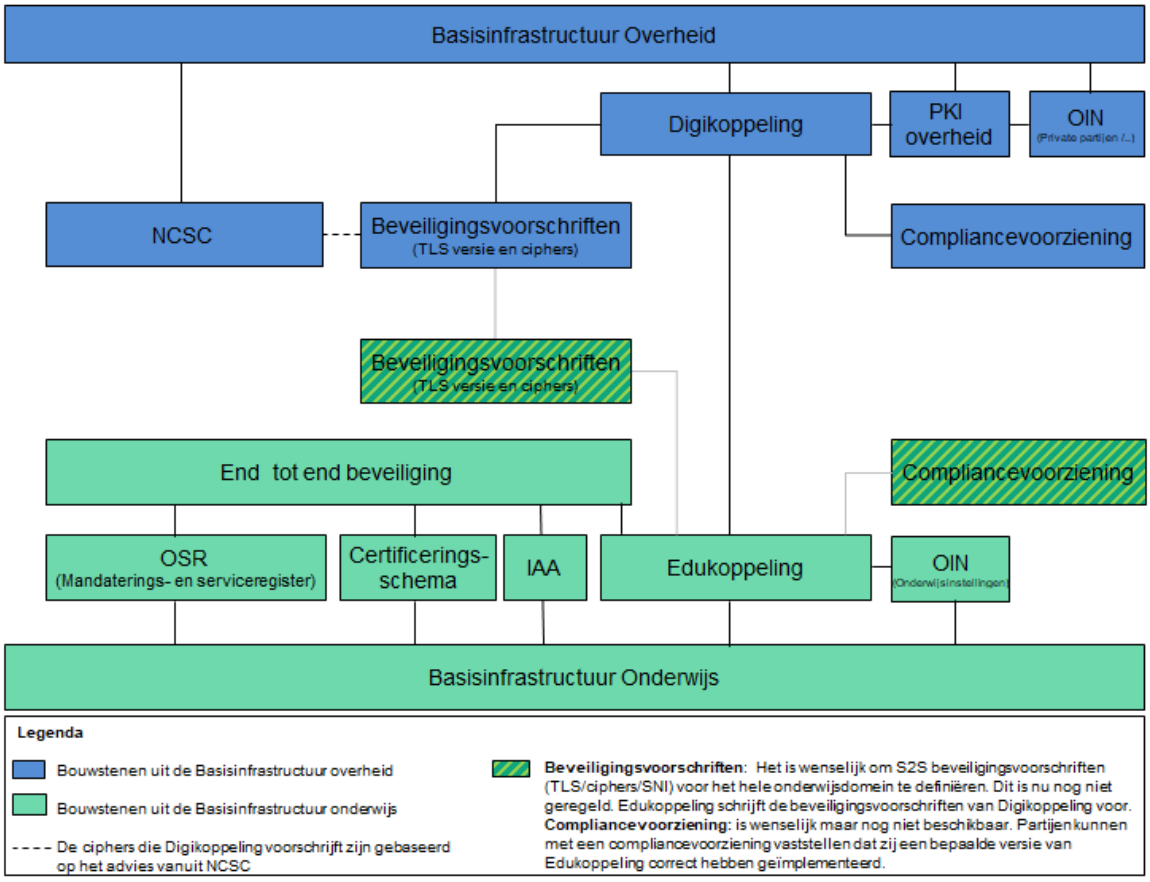
In de praktijk kunnen de hierboven onderscheiden rollen samenvallen. Dit levert verschillende situaties op:

1. *Lokale installatie*
   Als de verwerkende software lokaal is geïnstalleerd bij een onderwijsinstelling, 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[9].
3. *Niet-transparante intermediair*
   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.

[9] 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.

5. Bouwstenen

Edukoppeling is opgebouwd uit een aantal landelijke bouwstenen waarbij de kern wordt gevormd door Digikoppeling. Om binnen het onderwijs bij gegevensuitwisseling end-to-end beveiliging te realiseren wordt gebruik gemaakt van bouwstenen uit de Basisinfrastructuur Overheid en Onderwijs. (zie figuur 11).



Figuur 11 – Overzicht van bouwstenen om end-to-end beveiliging te realiseren

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.

5.1. Edukoppeling Transactiestandaard

De Digikoppeling standaard van de landelijke overheid staat model voor Edukoppeling Transactiestandaard. 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, een gewenste terugkoppeling die in het onderwijs sterk speelt in samenwerkingsrelaties. Dit betekent dat er alsnog op applicatieniveau 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[10] 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 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. Dit heet E-delivery. In Nederland loopt een traject voor een Nationaal Accesss Point (NAP) dat het landelijke standaard (Digikoppeling) vertaalt naar E-delivery en vice versa. Mocht dat succesvol zijn, dan kan dit ook werken met Edukoppeling.

De Edukoppeling Transactiestandaard 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[11] ingericht.

Logius, de beheerder van Digikoppeling biedt een dienst aan om compliancetesten uit te voeren. Deze toetst of partijen hun software (berichten) conform de eisen van de Digikoppeling Koppelvlakstandaarden hebben ontwikkeld en geïmplementeerd. Een dergelijke voorziening voor Edukoppeling is wenselijk maar nog niet beschikbaar. Partijen kunnen zo vaststellen dat zij een bepaalde versie van Edukoppeling correct hebben geïmplementeerd.

5.2. Organisatie Identificatie Nummer (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[12]. 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 gegevensverwerker aan te duiden. Meer details zijn uitgewerkt in de Edukoppeling Transactiestandaard en in het document Edukoppeling Identificatie en Authenticatie.

5.3. PKIoverheid

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 TSP’s. Een TSP is verantwoordelijk voor het controleren van de identiteit van de aanvrager en het opnemen van het

[10] De WS-* familie bestaat onder meer uit de standaarden WSDL, UDDI en SOAP. Daarom wordt deze familie wel aangeduid met WUS.
[11] Voor meer info over de Edukoppeling werkgroep, zie https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-edukoppeling/
[12] Digikoppeling nummersystematiek: https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/ Digikoppeling Gebruik en achtergrond certificaten

identificerend gegeven dat voor deze aanvrager in het certificaat opgenomen moet worden. Voor Edukoppeling worden conform Digikoppeling PKIoverheid certificaten gebruikt[13].[14]

5.4. Onderwijs Service Register

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 Onderwijs Service Register 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 onder meer gebaseerd op eerder werk in de Routerings en Autorisatie Voorziening (RAV) in gebruik bij DUO.

5.5. Certificeringsschema

In 2015 is voor het eerst het certificeringsschema[15] geregistreerd bij Edustandaard. Het Certificeringsschema is gerelateerd aan de Edukoppeling Transactiestandaard. Waar Edukoppeling gaat over de verbinding tussen organisaties, gaat het Certificeringsschema over informatiebeveiliging en privacy bínnen die organisaties. Met het Certificeringsschema kunnen binnen het onderwijsdomein organisaties die ict-diensten leveren worden getoetst op basis van een gezamenlijk opgesteld ‘normenkader’ dat wordt doorontwikkeld en beheerd binnen Edustandaard. Organisaties worden daarom niet meermalen getoetst op verschillende normenkaders en kunnen eenvoudig aantonen dat ze informatiebeveiliging en privacy op orde hebben.

Onderwijsinstellingen kunnen eenvoudig nagaan of een dienstverlener voldoet aan de gestelde maatregelen.

De maatregelen in het toetsingskader zijn niet uitputtend. Er zijn altijd meer maatregelen die een organisatie kan treffen. In zo’n situatie dienen de maatregelen die relevant zijn voor die externe leverancier doorgezet te worden naar die externe leverancier en door de organisatie getoetst/gecontroleerd te worden.

---

[13] https://www.pkioverheid.nl/
[14] Let op: Niet alle PKIoverheidcertificaten bevatten een OIN. Het moeten certificaten zijn die geschikt zijn voor Digikoppeling (zie ook voorgaande voetnoot).
[15] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

Voldoen aan het certificeringsschema is als randvoorwaarde gesteld om via Edukoppeling vertrouwelijke gegevens uit te wisselen. Ketenpartijen kunnen hier dan ook expliciet naar vragen aan hun ketenpartners die met ze willen koppelen.

In het certificeringsschema wordt in het kader van de end-to-end-security bij SaaS-leveranciers onder meer aandacht besteed aan de benodigde maatregelen dat de klant-omgeving van de ene onderwijsinstelling is gescheiden van de ander. Dit is een verlengstuk van de technische maatregelen in Edukoppeling.
Er zijn binnen Edustandaard afspraken gemaakt over de governance van het certificeringsschema. Op basis van risicoanalyse kan het schema periodiek worden aangescherpt/uitgebreid. De toetsingsprocedure zal op termijn worden aangescherpt van een *self-assessment* naar een *third party* mededeling.

5.6. Identificatie, Authenticatie en Autorisatie (IAA)

Bij gegevensuitwisseling tussen systemen is er veelal ook een persoon betrokken die het proces initieert en wordt hiermee onderdeel van de te organiseren end-to-end beveiliging. In principe schrijft het Certificeringsschema binnen de categorie vertrouwelijkheid al de te nemen maatregelen voor Logische toegang. Deze maatregelen (richtlijnen, procedures, systemen en beheersingsprocessen) moeten er voor zorgen dat alleen bevoegden toegang tot informatiesystemen verkrijgen.

De toegang is gerelateerd aan de aspecten identificatie, authenticatie en autorisatie. Het certificeringsschema gaat niet in detail op deze aspecten in. Het Toekomstbeeld Toegang wel. Dit toekomstbeeld, wat momenteel nog in ontwikkeling is (verwachte oplevering halverwege 2019), definieert de IAA-bouwstenen die gebruikt kunnen worden om volledige end-to-end beveiliging te realiseren. Meer informatie over het Toekomstbeeld Toegang is te vinden op de ROSA wiki[16]. In de huidige situatie hebben partijen en ketens het IAA onderdeel van end-to-end beveiliging verschillend ingericht.

[16] https://www.wikixl.nl/wiki/rosa/index.php/Werkgroep_IAA