edustandaard

Edukoppeling

Architectuur 2.0

M2M gegevensuitwisseling binnen het onderwijs

Edustandaard
Datum: oktober 2020
Versie: 2.0
Status: concept

Inhoudsopgave

1. Leeswijzer

In hoofdstuk 2 wordt de aanleiding, het doel en de doelgroep voor Edukoppeling Architectuur beschreven. In hoofdstuk 3 wordt een algemeen beeld van gegevensuitwisseling toegelicht en in hoofdstuk 4 worden de verschillende Edukoppeling-profielen beschreven. In hoofdstuk 5 zijn een aantal bedrijfstransactiepatronen beschreven en welke profielen hierbij toegepast kunnen worden. In hoofdstuk 6 zijn de relevante bouwstenen op 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 Gebruik ODOC certificaten verwijderd
2.0	WG Edukoppeling	Mei 2020	• Andere indeling • Toegevoegd: REST/SaaS-profiel • Toegevoegd: Profiel voor openbare data (TODO) • Aangepast: Beschrijving OSR bouwsteen • Toegevoegd: Patroon abonneren op wijzigingen middels notificaties • Toegevoegd: de SaaS-profielen kunnen ook gebruikt kunnen worden door onderwijsinstellingen die eigen systemen gebruiken voor M2M gegevensuitwisseling • Aangepast: Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling tussen informatiesystemen van partijen met en binnen de onderwijs • Aangepast: tekst bij Beveiligingspatronen (End-to-End) • Aangepast: Theoretische beschrijving serviceregister (mandatering)

			• Hoofdstuk Foutafhandeling opgenomen • OIN/HRN (aug 2020) • Verschillende tekstuele aanpassingen
2.0	WG Edukoppeling	oktober 2020	Tekstuele aanpassingen

2. Inleiding

2.1. Aanleiding

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

2.2. Doel en doelgroep

Edukoppeling 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.

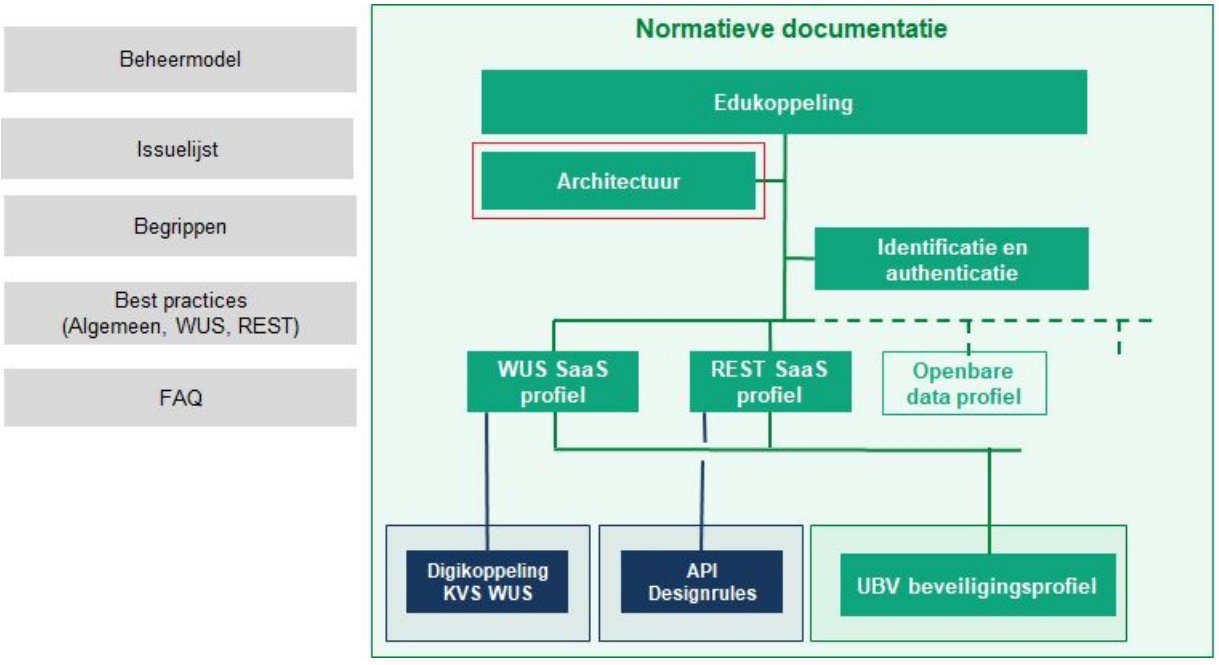
Dit document (en overige Edukoppeling documentatie) is bedoeld voor personen die betrokken zijn bij het ontwikkelen van machine-to-machine (M2M) koppelingen. De documenten beschrijven voor ICT-specialisten hoe de ICT rondom deze koppelingen ingericht moet worden.

2.3. Positionering

Dit Architectuurdocument is één van de normatieve documenten binnen de Edukoppeling-afspraak. Edukoppeling maakt verder ook gebruik van de Edustandaard UBV[2] afspraak. De UBV afspraak bevat een bijlage waarin de transportbeveiligingsvoorschriften voor Edukoppeling zijn opgenomen. Per Edukoppeling profiel wordt dit nog expliciet toegelicht. Verder is het WUS/SaaS-profiel in grote mate afhankelijk van het Digikoppeling/WUS-profiel[3]. Dit is een pas-toe-of-leg-uit standaard van het Forum Standaardisatie met als doelgroep: uitvoeringsorganisaties en zorg- en onderwijsinstellingen. Het volgen van deze standaard geldt als compliance met de Digikoppeling standaard. De werkgroep Edukoppeling bespreekt eventuele afwijkingen met de DIgikoppeling beheerders en zorgt ervoor dat eventuele verschillen worden geminimaliseerd (de ene of de andere kant op).

[1] https://www.wikixl.nl/wiki/rosa/index.php/Hoofdpagina
[2] https://www.edustandaard.nl/standaard_werkgroepen/uniforme-beveiligingsvoorschriften/
[3] https://www.logius.nl/diensten/digikoppeling

Transportbeveiliging is een belangrijk onderdeel van Edukoppeling en is momenteel gebaseerd op Digikoppeling en indirect de NCSC. Binnen Edustandaard is het voornemen om dit los te koppelen met een werkgroep Uniforme Beveiligingsvoorschriften (UBV). De Digikoppeling Beveiligingsstandaarden en -voorschriften worden in UBV in een Edukoppeling profiel opgenomen. Dit profiel bevat de transportbeveiligingseisen van UBV en hebben deels overlap met de Digikoppeling transportbeveiligingseisen. Er worden dus mogelijk Digikoppeling Beveiligingsstandaarden en -voorschriften overschreven. Dit zal alleen zijn om strengere eisen aan transportbeveiliging te stellen. Waar dit relevant is wordt dit gemotiveerd. Naast de transportbeveiligingseisen bevat het UBV Edukoppeling profiel ook een aantal berichtbeveiligingsvoorschriften voor het SaaS/WUS-profiel. Voor dit deel is de Edukoppeling werkgroep verantwoordelijk. De berichtbeveiligingsvoorschriften zijn opgenomen voor de leesbaarheid, zodoende hoeft de gebruiker niet alsnog voor delen het Digikoppeling Beveiligingsstandaarden en –voorschriften document raadplegen.



Figuur 1- Positionering van Architectuur binnen Edukoppeling

3. Edukoppeling voor M2M gegevensuitwisseling

3.1. Doel Edukoppeling

Edukoppeling is een bouwsteen voor vertrouwelijke machine-to-machine (M2M) uitwisselingen in het onderwijs en zorgt voor met name technische interoperabiliteit. Die interoperabiliteit draagt bij aan het realiseren van het merendeel van de in ROSA[4] gedefinieerde doelen:

Bovensectorale samenwerking
- Inspelen op beleidswijzigingen
- Terugdringen administratieve lasten

Privacy en beveiliging
- Ketenbrede informatiebeveiliging en privacybescherming

IAA
- Privacy by design

3.2. Organisatorisch werkingsgebied

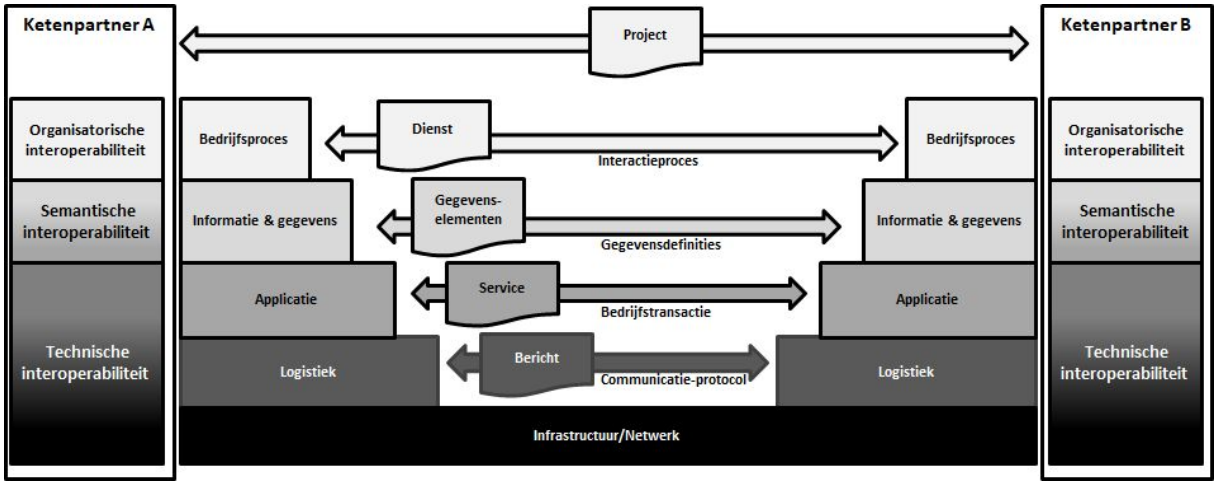
Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling tussen informatiesystemen van onderwijsinstellingen en ketenpartners (onderling, met bedrijven of met de overheid). Onderwijsinstellingen kunnen hierbij deze informatiesystemen lokaal hebben draaien of hebben uitbesteed in de cloud. Onderwijsinstellingen hebben samenwerkingsrelaties met andere onderwijsinstellingen, met de overheid, met gemeenten én met private organisaties.

3.3. Functioneel toepassingsgebied

Met Edukoppeling wordt expliciet aangegeven hoe M2M-gegevensuitwisseling binnen het onderwijs ingericht moet worden. De hoeveelheid gegevensuitwisselingen zal blijven groeien. Er kan dus meer mis gaan als dit niet goed georganiseerd is.

Er worden verschillende profielen onderkend die elk een specifiek toepassingsgebied hebben. Voor alle profielen geldt dat organisaties op drie niveaus afspraken moeten maken:
1. Over de inhoud en betekenis van berichten (payload en eventuele bijlagen): de structuur, semantiek, waardebereik enzovoort.
2. Over de logistiek (envelop): transportprotocollen, messaging, adressering, beveiliging en betrouwbaarheid.
3. Over het transport (netwerk).

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



Figuur 2- Overzicht van de verschillende niveaus die relevant zijn bij gegevensuitwisseling

Edukoppeling richt zich op de applicatie- en logistieke laag. Het is zo opgebouwd dat de verschillende lagen ontkoppeld zijn, maar wel op elkaar aansluiten. Met Edukoppeling streven we naar hergebruik; een ketenpartner kan met één implementatie van een bepaald profiel op een veilige manier een veelheid van toepassingen uitvoeren.

De functionele toepassingsgebieden van Edukoppeling zijn in meer detail gespecificeerd bij de beschrijving van de profielen. Elk profiel wordt gebruikt in een bepaalde context. Zo is het functionele toepassingsgebied van de SaaS-profielen de gegevensuitwisseling waarbij een partij mogelijk een SaaS-leverancier betreft (verwerker) die namens de onderwijsinstelling (eindorganisatie) gemandateerd is voor een bepaalde dienst (en uitwisseling van gegevens middels services).

4. Edukoppeling profielen

4.1. REST vs Digikoppeling

Het landschap van gegevensuitwisseling is aan het veranderen. Hoewel de ontwikkeling van de Digikoppeling ebMS- en WUS-profielen gelijk opging met die van de inrichting van basisregistraties werden deze met name gebruikt om met de berichtuitwisseling de lokale schaduwadministraties bij te houden. Er is ondertussen een ontwikkeling gaande om in plaats van het periodiek up-to-date houden van een lokale schaduwadministratie events uit te wisselen en een centraal register te hanteren (halen bij de bron). De REST API's met een API-gateway vormen hierin de middleware van een nieuwe generatie. REST API's vormen zowel de voorkeurstechnologie voor digitale dienstverlening als voor integratie van systemen. De API is zelf een "product" geworden. API's zijn tegenwoordig in veel organisaties dé communicatievorm met de buitenwereld. Dit is het resultaat van een zichzelf versterkende cirkelbeweging tussen een groeiende vraag naar integratie en technologie die integratie eenvoudiger maakt.

REST is niet gericht op formele validatie en het doorgeven van berichten over een lange keten waarbij onweerlegbaarheid en versleuteling van het bericht van belang zijn[5]. Dergelijke eisen passen beter bij het Digikoppeling WUS- en/of ebMS-profiel. Als we echter een point-to-point uitwisseling beschouwen dan biedt REST vrijwel dezelfde mogelijkheden als WUS. Het Edukoppeling REST/SaaS-profiel heeft een vergelijkbaar functioneel toepassingsgebied als het Edukoppeling WUS/SaaS-profiel. Een aandachtspunt hierbij is dat beide zijn ontstaan vanuit verschillende architectuurprincipes. Zo heeft men het bij REST over resources en niet endpoints waar berichten naar verstuurd worden. Conform de Service Gerichte Architectuur (SGA) van SOAP worden is er een service die via een endpoint aangeboden wordt (vaak via een gateway). De service ondersteunt mogelijk meerdere operaties (meestal irt een bepaalde usecase) met elk zijn eigen berichten.

De verschillen worden echter nog groter als we de volledige scope van het toepassingsgebied van REST in beschouwing nemen. Het REST-architectuurconcept en RESTful-standaarden zijn vaak gericht op interactie met een gebruiker die een webbrowser of applicatie gebruikt. De huidige aanname bij M2M-uitwisselingen (SaaS-profielen) is dat de natuurlijke personen (achter de eindorganisatie) geen rol spelen. Voor andere mogelijk toekomstige profielen die onderdeel gaan vormen van Edukoppeling wordt de rol van een natuurlijk persoon mogelijk wel relevant (bijvoorbeeld de resource owner binnen een OAuth[6] profiel - Authorization Code Grant). Dit sluit ook aan bij het overheidsconcept *Regie op gegevens* waarbij de betrokkene (degene waarvan de gegevens tussen partijen uitgewisseld worden) meer zeggenschap krijgt over eigen gegevens (inzage en consent wanneer relevant).

4.2. Edukoppeling SaaS-profielen (point-to-point)

Edukoppeling is ontstaan door de behoefte om de steeds toenemende gegevensuitwisseling binnen het onderwijs te standaardiseren. Bij de overheid was dezelfde behoefte ontstaan en hiervoor was de Digikoppeling[7]-standaard ontwikkeld. De basis werd gevormd door ebMS reliable messaging en WUS-profielen. Voor betrouwbare gegevensoverdracht (reliable messaging als onderdeel van het protocol) schrijft Digikoppeling het ebMS-profiel voor. Digikoppeling (ebMS en WUS) staat 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 is echter niet zonder meer te gebruiken in het onderwijsveld:

[5] Dit is mede ook gebaseerd op de huidige status. De verwachting is echter dat op termijn er meer RESTful standaarden komen die formele transacties en berichtbeveiliging ondersteunen. Hiermee zal naar verwachting ook de complexiteit toenemen.

[6] https://tools.ietf.org/html/rfc6749

[7] https://www.logius.nl/diensten/digikoppeling

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 wordt daarom het Digikoppeling ebMS-profiel uitgesloten.

De Digikoppeling-standaard van de landelijke overheid staat model voor het Edukoppeling WUS/SaaS-profiel. 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’.

Met Edukoppeling hoeft er in de onderwijssector geen complexe varianten (zoals ebMS) geïntroduceerd te worden die hetzelfde functionele doel hebben. Edukoppeling biedt een architectuur die een end-to-end reliable interactieproces mogelijk maakt op basis het WUS/SaaS-profiel. Voor hetzelfde functionele toepassingsgebied is er ook een REST/SaaS-profiel, dit profiel is gebaseerd op overheidsbrede afspraken die nog in ontwikkeling zijn (Kennisplatform API’s).

Edukoppeling bestaat uit verschillende documenten en is in beheer bij 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[8] ingericht.

4.2.1. Functioneel toepassingsgebied

Het Edukoppeling SaaS-profiel sluit aan op het functionele toepassingsgebied van Digikoppeling, maar kent zijn eigen specifieke context. Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI. Digikoppeling geeft niet expliciet invulling aan het gebruik van SaaS-diensten en het routeren van en naar een SaaS-dienst en de onderwijsinstelling. Het functionele toepassingsgebied van het Edukoppeling SaaS-profiel is digitale gegevensuitwisseling via een beveiligde point-to-point verbinding waarbij de gegevens gerouteerd kunnen worden tussen een verwerker en eindorganisatie. Dit laatste is geen verplichting indien de eindorganisatie ook de rol van verwerker (en logistieke dienstverlener) heeft. Dit geldt dus voor zowel het REST/SaaS-profiel als het WUS SaaS profiel. Deze hebben hetzelfde functionele toepassingsgebied.

Het Edukoppeling WUS/SaaS-profiel is ontwikkeld op basis van het Digikoppeling WUS-profiel en maakt gebruik van dezelfde standaarden. Daarnaast worden er bij WUS ook profielen met beveiliging

[8] Voor meer info over de Edukoppeling werkgroep, zie https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-edukoppeling/

op berichtniveau ondersteund, waarmee naast point-to-point ook uitwisseling via transparante intermediairs ondersteund wordt. Deze scenario's vallen echter in een ander toepassingsgebied. Het REST-profiel is geheel gebaseerd op RESTful-afspraken en -standaarden. Hoe een en ander concreet ingevuld wordt is beschreven in de betreffende SaaS-profielen.

De Edukoppeling SaaS-profielen (WUS en REST) vormen een 'collectieve leg-uit' voor het onderwijsdomein 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).

4.2.2. Rollen

De Edukoppeling SaaS-profielen onderscheiden drie rollen die relevant zijn bij een M2M-uitwisseling met andere organisaties, dit zijn:

- de eindorganisatie;
- de gegevensverwerker;
- de logistieke dienstverlener.

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 certificeringsschema). In het onderwijs is de verwerker vaak niet dezelfde als de eindorganisatie en wordt de verwerker vaak ingevuld door een SaaS-leverancier (van bijvoorbeeld administratiepakketten).

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. Verder kan het zijn dat een onderwijsinstelling zelf handelt in alle drie de rollen. Wat dit betekent voor de gegevensuitwisseling wordt in de betreffende profielen toegelicht.

4.2.3. Relevante functies van het Serviceregister

Het onderwijsserviceregister (OSR) is een generieke bouwsteen (zie ook: 6.3. Onderwijs Serviceregister) in de Edukoppeling architectuur en heeft o.a. een telefoonboek-functie voor M2M services binnen de onderwijsketen. Een dienstafnemer (onderwijsinstelling of SaaS-leverancier) kan

het register bevragen voor kenmerken en technische details van services. De belangrijkste gegevenselementen (organisatie, mandaten en endpoint) worden onafhankelijk van elkaar onderhouden (zie Figuur 3).

De Edukoppeling architectuur onderkent een serviceregister met een aantal centrale functies, dit zijn:

1. een functie om mandateringen te registeren (eindorganisatie mandateert verwerker) en deze kunnen verifiëren (bij zowel push als pull);
2. een authentieke bron van OIN's die als onderdeel van de Edukoppeling standaard bij gegevensuitwisseling gebruikt worden;
3. een functie om endpoints te registreren en leveren (relevant voor het WUS 2W-be-SE profiel), hierbij kan tevens het profiel (REST/SaaS of WUS/SaaS) aangegeven worden;
4. een functie om publieke PKIo-certificaten te registreren en leveren.

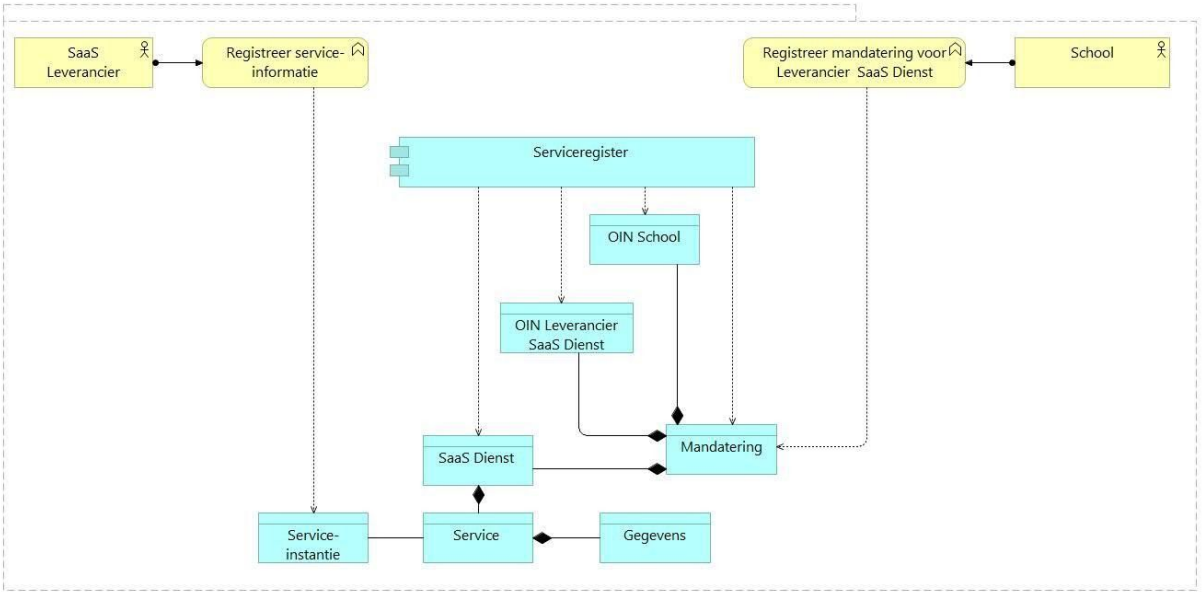
4.2.3.1. Mandatering

Een SaaS-dienst wordt door een SaaS-leverancier (verwerker) aangeboden om de school (eindorganisatie) te ondersteunen bij de uitvoering van bedrijfsfuncties. Een Dienst (zie ROSA[9]) wordt aangeboden in de vorm van één of meerdere services. Deze services bestaan enerzijds uit Grafische User Interfaces (GUIs) voor gebruik door mensen, en anderzijds uit Application Programming Interfaces (APIs) voor gebruik door andere applicaties (M2M communicatie). In de context van Edukoppeling zijn met name de laatste vorm van services (zie ROSA) van belang. Hierbij is het wel van belang dat er onderscheid wordt gemaakt in een abstracte definitie van een Service (schema) en een service instantie (applicatie die de service implementeert)

Er is een administratief proces waarbij tekenbevoegden van een school en SaaS-leverancier in een overeenkomst vastleggen dat de school de SaaS-leverancier mandateert om de dienst te leveren. Hiermee verkrijgt de leverancier doelbinding om namens de school (persoons)gegevens te verwerken in de context van de services die samenhangen met de betreffende dienst. Het is wenselijk om hier ook in technische zin invulling aan te geven, zodat bijvoorbeeld bij M2M-communicatie ketenpartijen kunnen verifiëren of voor de uitwisseling een mandatering bestaat.

Edukoppeling beschrijft hoe in technische zin invulling wordt gegeven aan de registratie van de mandatering en welke functie de mandatering heeft bij de M2M-communicatie. De school wordt geïdentificeerd op basis van een OIN, een SaaS-leverancier/bedrijf op basis van een Handelsregisternummer (HRN). Bij het OIN van de school kan in de suffix het kenmerk van een administratie opgenomen zijn (zie I&A document). De school registreert de mandatering voor een bepaalde dienst van een SaaS-leverancier in een serviceregister en hiermee de services die hiermee samenhangen. De services beschrijven in abstracte vorm welke gegevens met een bepaalde service samenhangen. De SaaS-leverancier registreert gegevens van de eigen service-instanties voor de betreffende services die met de dienst samenhangen (zie Figuur 3). De dienst van de SaaS-Leverancier (die via de GUI door school medewerkers wordt gebruikt) kan binnen de context van de mandatering met de één of meer geregistreerde service-instanties (API's) (persoons)gegevens met ketenpartijen uitwisselen.

[9] https://www.wikixl.nl/wiki/rosa/index.php/Begrippenlijst_ROSA



Figuur 3 – Registratie Mandatering in serviceregister

Een eindorganisatie (school) kan ook zelf alle drie de rollen uitvoeren en is dan door zichzelf gemandateerd. Het OIN van een school bevat mogelijk een suffix. Het OIN van de school identificeert zowel de organisatie (het hoofdnummer) als de administratie (de suffix[10]).

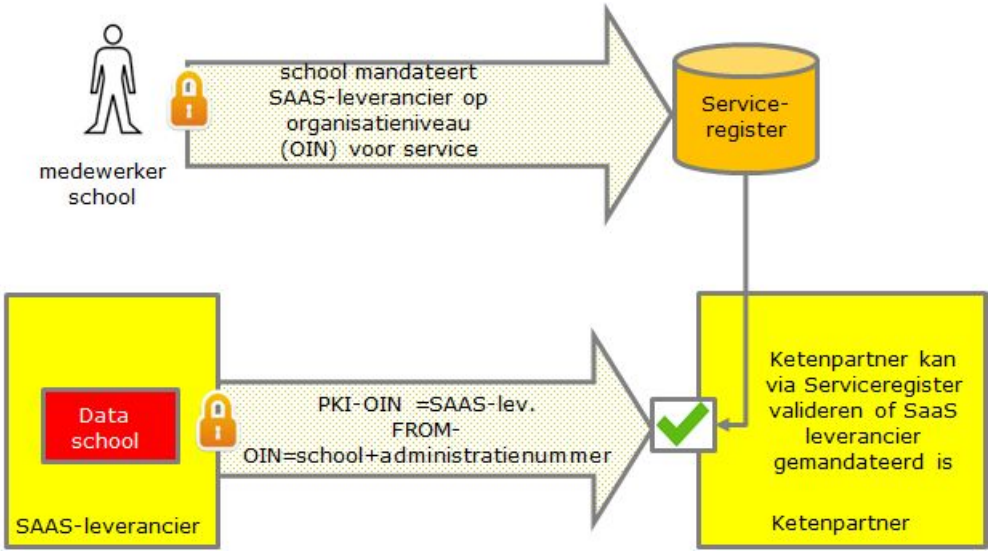
De SaaS-profielen kunnen worden toegepast bij verschillende transactiepatronen waarbij het serviceregister een rol heeft, dit zijn:

- een bevraging (pull);
- een melding (push).

In beide gevallen moet het mogelijk zijn om bij de gegevensuitwisseling de mandatering tussen eindorganisatie en gegevensverwerker te kunnen verifiëren via de gegevens in het Serviceregister.

SaaS-leverancier mandatering bij bevragingen (request-response bedrijfstransactiepatroon)
Indien een SaaS-leverancier een dienstaanbieder bevraagt en er is sprake van vertrouwelijke gegevens die uitgewisseld worden dan wil de ketenpartner (dienstaanbieder) vaststellen of de SaaS-leverancier gemandateerd is om namens de school voor deze dienst te handelen (zie Figuur 4). Dit begint met het mandateren van de SaaS-leverancier door een medewerker van de school. Dit wordt expliciet gemaakt door een registratie hiervan in het serviceregister. Wanneer de SaaS-leverancier de gegevens bij de dienstaanbieder opvraagt, doet hij dit met zijn eigen PKI-certificaat (TLS en mogelijk ondertekening en versleuteling van het bericht) en geeft daarbij aan (middels de zogenaamde ‘FROM’-parameter) namens welke school het vraagbericht opgesteld is. Voor identificatie van de school wordt een OIN gebruikt (zie voor details het *Identificatie en Authenticatie document*). De ketenpartner (dienstaanbieder) verifieert vervolgens of de verwerker namens de eindorganisatie mag aanleveren aan de hand van de vastgelegde mandateringsrelatie in het serviceregister.

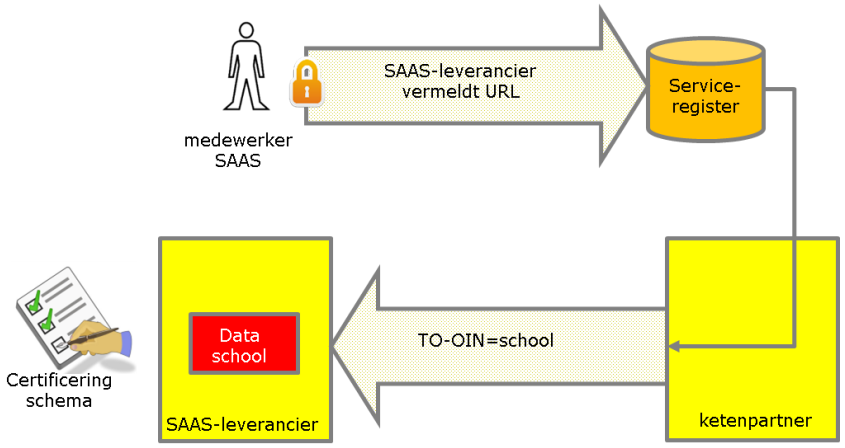
[10] Zie Edukoppeling Identificatie en Authenticatie document



Figuur 4 – SaaS leverancier mandatering bij bevragingen

SaaS-leverancier mandatering bij melding (melding-bevestiging bedrijfstransactiepatroon)
Het patroon melding-bevestiging wordt gebruikt om vertrouwelijke gegevens te versturen. Als de ontvanger een school is die gebruik maakt van SaaS, dan moeten de gegevens 'in het goede bakje' terecht komen (zie Figuur 5). Mogelijk was ook de verzender een SaaS-leverancier en heeft de ontvanger ook nu de mogelijkheid om te valideren of de SaaS-leverancier voor deze uitwisseling gemandateerd is.

De school heeft 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. Tevens wordt de geadresseerde school meegegeven (in de zogenaamde 'TO' -parameter). 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 terechtkomen.



Figuur 5 - SaaS leverancier mandatering bij melding (push)

4.2.3.2. Authentieke bron van OIN's en HRN's

Het serviceregister is de authentieke bron van OIN's binnen het onderwijs. De OIN's worden samengesteld op basis van andere authentieke bronnen zoals BRON (RIO) en HRN's op basis van het Handelsregister. Hoe OIN's en HRN's worden samengesteld staat beschreven in het Edukoppeling Identificatie en Authenticatie document.

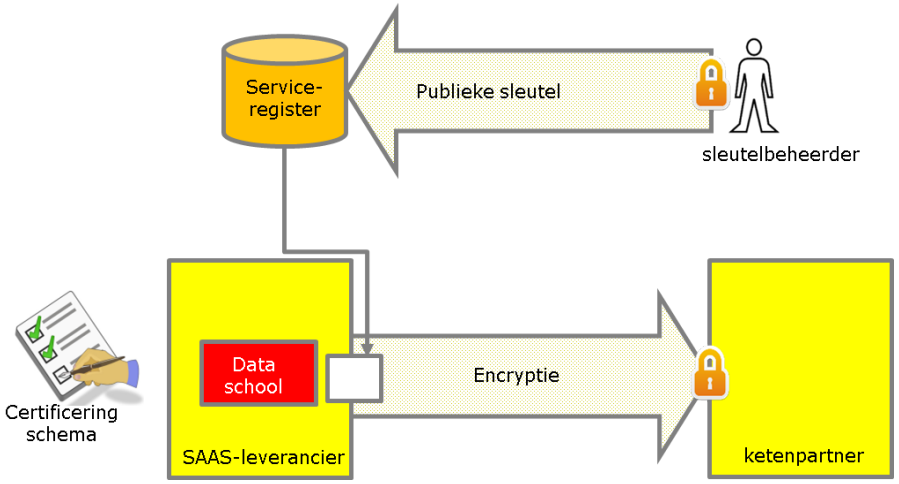
4.2.3.3. Beheer endpoints

Partijen kunnen voor een dienst het endpoint registreren. Partijen die de dienst af moeten nemen kunnen deze bij het serviceregister ophalen. Met de komst van het REST/SaaS-profiel profiel kan een partij kiezen of de gegevens uitgewisseld worden met WUS of REST. Het is serviceregister bevat een profielaanduiding die aangeeft welke van de twee gebruikt moet worden om met het endpoint van de service te communiceren.

4.2.3.4. Beheer publieke certificaten t.b.v. versleutelen berichten

Het transport van vertrouwelijke gegevens vraagt om maatregelen om ervoor te zorgen dat deze niet door onbevoegden kunnen worden ingezien. Het REST/SaaS-profiel en WUS/SaaS-profiel schrijven daarom het gebruik van TLS voor. Daarnaast biedt het WUS/SaaS-profiel de mogelijkheid om berichten te versleutelen wat met name toegepast wordt in het scenario waar er sprake is van een transparante intermediair (bijvoorbeeld een logistieke dienstverlener). Hierbij is het noodzakelijk dat de verzender van het bericht over het publieke certificaat beschikt van de ontvanger.

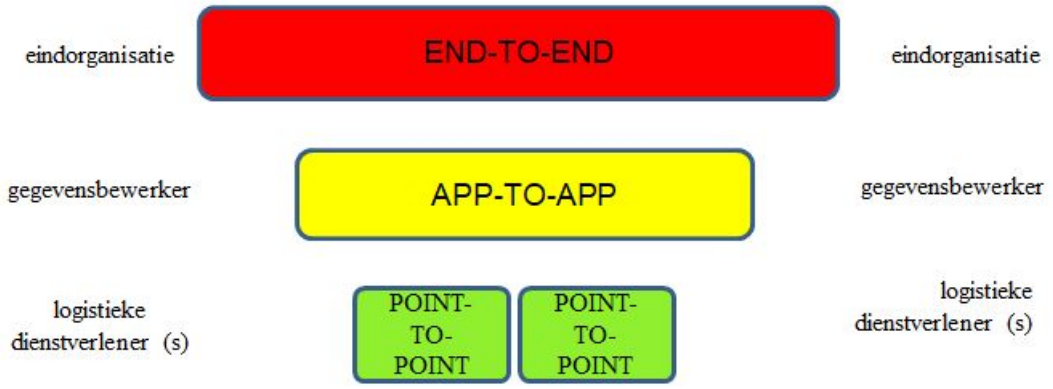
Degene die het bericht encrypt heeft de publieke sleutel nodig van zijn ketenpartner (zie Figuur 6). De ontvanger kan het vervolgens met zijn private sleutel weer decrypten. Iemand anders kan het niet en daarmee is het externe transport vertrouwelijk. Het interne transport binnen een SaaS-leverancier is vertrouwelijk als naar de normen van het certificeringsschema is gekeken en daarop gepaste maatregelen zijn getroffen. De identiteit van een verwerker is opgenomen als OIN/HRN in het PKI-certificaat (PKI-overheid)



Figuur 6 – Versleutelde berichten

4.2.4. Beveiligingspatronen

Op basis van de 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. Naarmate 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 de gegevens tijdens transport niet 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 eerstvolgende schakel.

- *App-to-app*
  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. 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).

- *End-to-end*
  Omdat onderwijsinstellingen vaak met SaaS-oplossingen werken heeft een ketenpartner zekerheid nodig van welke onderwijsinstelling gegevens afkomstig zijn of dat deze gegevens nergens anders terecht komen dan waar ze voor bedoeld waren. Het Edukoppeling SaaS-profiel is een inrichtingsvorm om End-to-End beveiliging te organiseren en bouwt voort op de point-to-point verbinding. Dit betekent dat, bovenop TLS en PKI, extra maatregelen nodig zijn om de keten 'achter de voordeur' te sluiten. De eerste maatregel is een routeringsmechanisme voor het kunnen 'routeren achter de voordeur'. Bij berichtuitwisseling wordt er in de logistieke laag een FROM- en TO-parameter opgenomen. Hierin staat het OIN van zender respectievelijk ontvanger. De tweede maatregel is het vastleggen (en kunnen verifiëren) van de mandateringsrelatie tussen eindorganisatie en gegevensverwerker in een servicregister. De derde maatregel is het certificeringsschema

dat de aandacht vestigt op de beveiligingsmaatregelen die een dienstverlener bij cloud-computing heeft ingericht zodat onder andere de bovengenoemde zekerheid kan worden gegarandeerd.

Bij de Edukoppeling SaaS-profielen spelen tot nu toe 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[11]. In de huidige profielen wordt geen relatie gelegd tussen een natuurlijke personen en een uitwisselingsbericht.

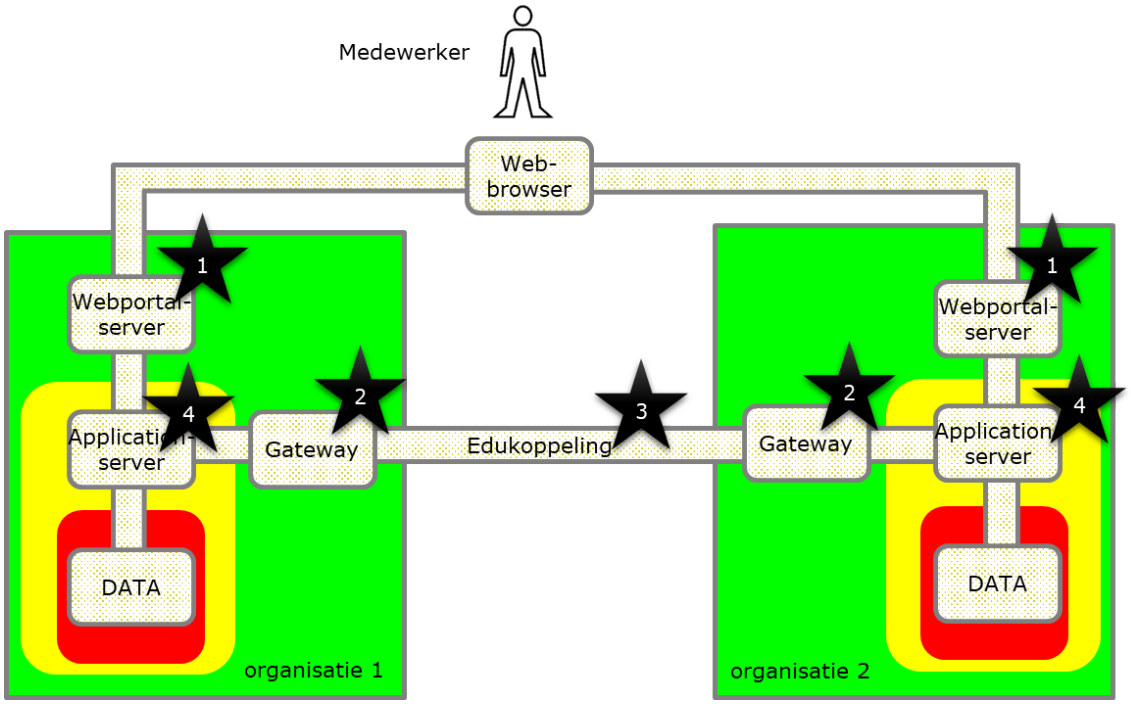
4.2.5. Praktijkscenario's

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. Verder kan een onderwijsinstelling bij gegevensuitwisseling gebruik maken van het Edukoppeling SaaS-profiel zodat ketenpartijen dit bij gegevensuitwisseling ook kunnen valideren (onderwijsinstelling heeft zichzelf gemandateerd).
2. *Cloud installatie van software (Niet Transparante Intermediair)*
   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[12].
3. *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.

De ROSA referentiearchitectuur beschrijft voor organisaties in het onderwijs, principes, modellen en standaarden gericht op interoperabiliteit, dat wil zeggen, het vermogen om samen te werken. In Figuur 8 is schematisch een beeld geschetst hoe de basisinfrastructuur ketensamenwerking ondersteunt.

[11] 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.
[12] 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.



Figuur 8 – 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[13].
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 natuurlijk 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 8 wordt een schematisch beeld geschetst van deze ketensamenwerking. De school[14] 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 sleutel met een beveiligingsniveau waarover in het onderwijs eenduidige afspraken zijn vastgelegd. Dat kan bijvoorbeeld het beveiligingsniveau substantieel[15] zijn.
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

[13] zie: www.noraonline.nl/wiki/beveiligingspatronen.
[14] Het begrip school wordt in dit gedeelte 'slordig' gebruikt. Het omvat termen als onderwijsinstelling en onderwijsaanbieder.
[15] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32015R1502

eindorganisatie (bijv. een school). De SaaS-leverancier beveiligt het verkeer (tweezijdig TLS) met een PKI-Overheidscertificaat met zijn eigen identiteit (HRN).

3. In een collectief serviceregister wordt bijgehouden (door 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.

4.3. Edukoppeling openbare data profiel (TODO)

4.3.1. Functioneel toepassingsgebied

4.3.2. Rollen

4.3.3. Beveiligingspatronen

4.3.4. Praktijksituaties

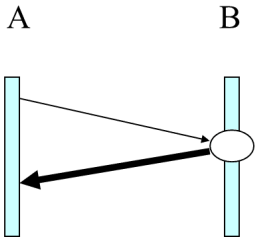
5. Bedrijfstransactiepatronen

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

5.1. Patroon: Request-response (bevraging)

Een bevraging is (volgens Digikoppeling[16]) een vraag waar direct een reactie op wordt verwacht. Hierbij is snelheid van afleveren belangrijk. Als een service niet beschikbaar is, dan hoeft de vraag niet als onderdeel van het protocol opnieuw worden aangeboden (best effort).

Het patroon request-response 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-response interactie. De boodschap aan de gebruiker luidt dan: "probeer het later nog eens". Daarna wordt de transactie geacht niet te hebben plaatsgevonden.

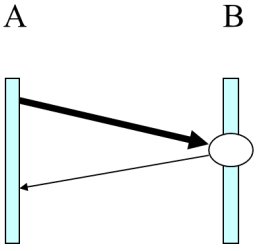


Figuur 9 – Patroon request-response

Dit patroon komt ook voor in Digikoppeling.

5.2. 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.



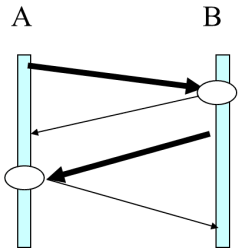
Figuur 10 – Patroon melding-bevestiging

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).

[16] https://www.forumstandaardisatie.nl/standaard/digikoppeling

5.3. 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).

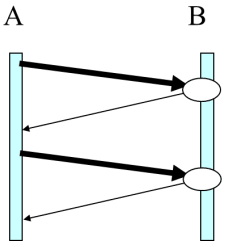


Figuur 11 – Asynchrone uitwisseling

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.

5.4. Antipatroon: Polling

Asynchrone uitwisseling kan ook als volgt worden uitgevoerd:

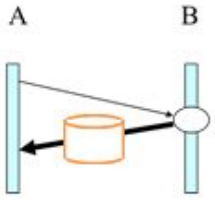


Figuur 12 – Antipatroon polling

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 webservice calls 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.

5.5. 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 13 – Patroon grote berichten (zonder metabericht)

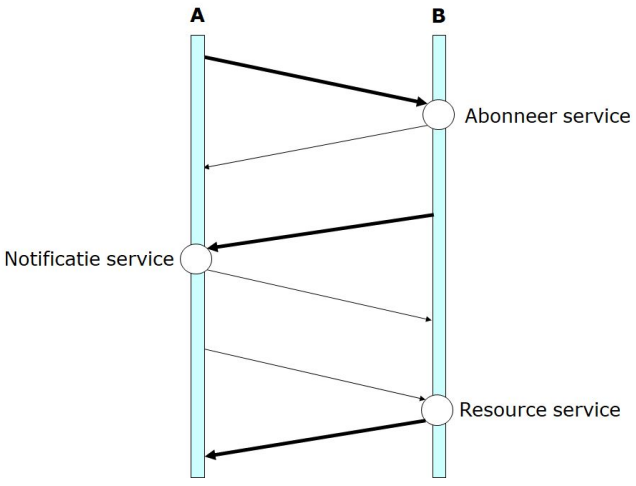
Grote berichten kunnen als attachment ook aan een gewoon bericht worden toegevoegd. Dat is waarschijnlijk eenvoudiger te realiseren, maar vanaf de genoemde grenswaarde weegt dat voordeel niet meer op tegen de toegenomen kans op transportfouten.

5.6. Patroon: Abonneren op wijzigingen middels notificaties

Zoals de inleiding al genoemd, is er een verandering op gang gekomen van het synchroniseren van administraties naar het direct bevragen bij de bron. Dit kan in eerste instantie prima met bovenstaande patronen ingevuld worden. Wie echter welke rol daarbij voert is niet altijd duidelijk: “Haal jij de gegevens bij mij op, of stuur ik gegevens naar jou door?”. En is een notificatiebericht alleen een notificatie of heeft het ook inhoud?
En hoe wordt ik op de hoogte gehouden als er iets verandert in een voor mij belangrijke administratie?

Om te voorkomen dat deze discussie elke keer opnieuw gevoerd worden, hanteren we binnen Edukoppeling de volgende uitgangspunten:

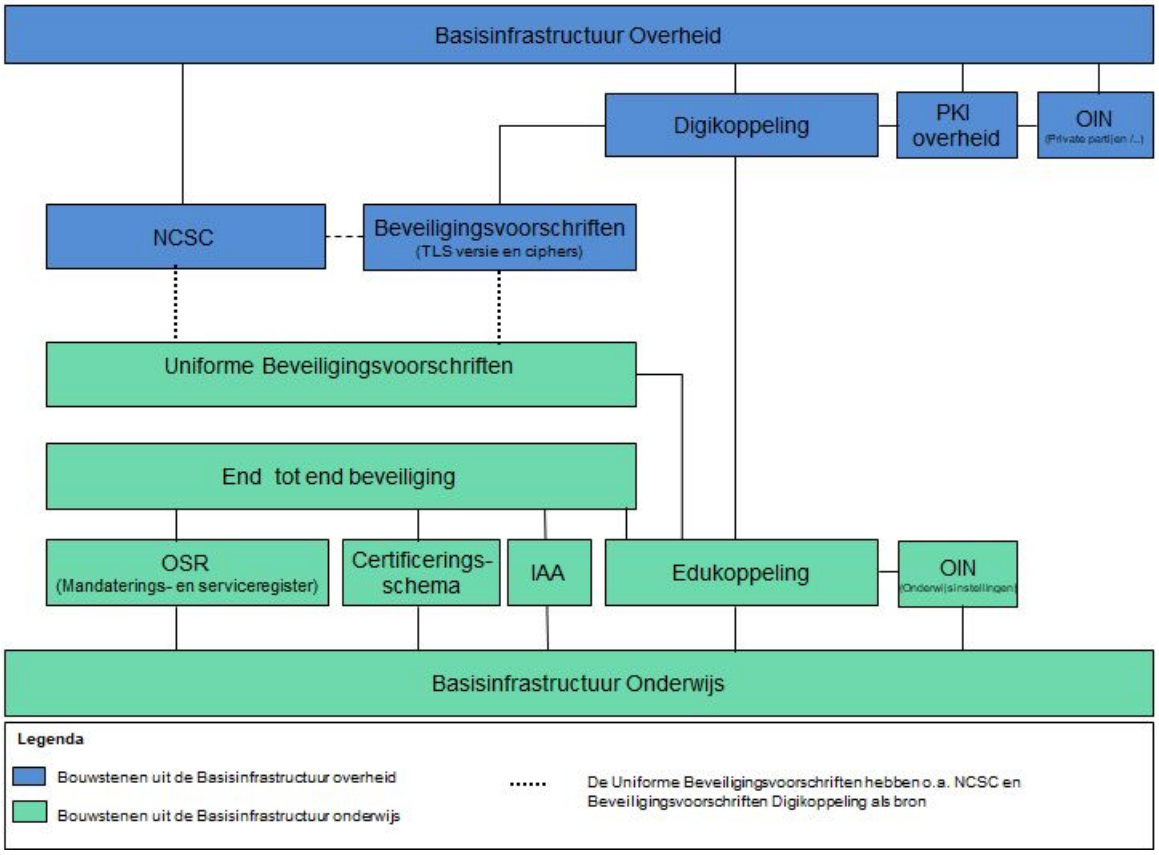
- Elke resource, elk object (verderop: gegevens) kent een beheerder; de organisatie die het gegeven in beheer heeft, en 1 of meer afnemers; de organisaties die deze resources gebruiken. In 1:n koppelvlakken is de centrale dienstverlener de houder van de gegevens, en zijn de gekoppelde organisaties de afnemers. In 1:1 situaties wordt een van beide partijen aangewezen als beheerder.
- Updates op gegevens bij de beheerder worden geïnitieerd door de afnemer middels het patroon ‘Melding - bevestiging’ of ‘ Asynchrone uitwisseling’.
- Ophalen van de actuele stand van zaken wordt altijd middels het request -response patroon gerealiseerd, niet door een melding vanuit de beheerder.
- Wanneer een partij geïnteresseerd is in wijzigingen in een gegeven bij de beheerder kan hij dat kenbaar maken middels een abonnementenservice. Dit is een service die de beheerder moet leveren aan zijn afnemers.
- Bij een wijziging op een gegeven worden alle abonnees hiervan in kennis gesteld middels een notificatiebericht. Dus is altijd een “Melding - Bevestiging” met daarin alleen het unieke resourceID waarmee de abonnee, op het moment dat het hem uitkomt, de actuele stand kan ophalen. De gegevens zelf worden niet direct teruggeleverd. Hiermee wordt een maximale ontkoppeling gegarandeerd, ook bij wijzigingen in de toekomst.



Figuur 14 - Patroon Abonneren op wijzigingen

6. 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.



Figuur 15 - 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. De bouwstenen waar Edukoppeling gebruik van maakt worden in dit hoofdstuk toegelicht.

6.1. Organisatie Identificatie Nummer (OIN/HRN)

Elke partij die via Edukoppeling de gegevensuitwisseling inricht of laat inrichten, wordt geïdentificeerd op basis van het unieke Organisatie Identificatie Nummer (OIN) ook wel HRN indien het een bedrijf betreft, zie nummersystematiek Digikoppeling[17]. 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 de logistieke laag van een bericht om de eindorganisatie aan te duiden en in PKI-certificaten om de verwerker aan te duiden. Meer details zijn uitgewerkt in de *Edukoppeling Transactiestandaard* en in het document *Edukoppeling Identificatie en Authenticatie*.

6.2. PKIoverheid

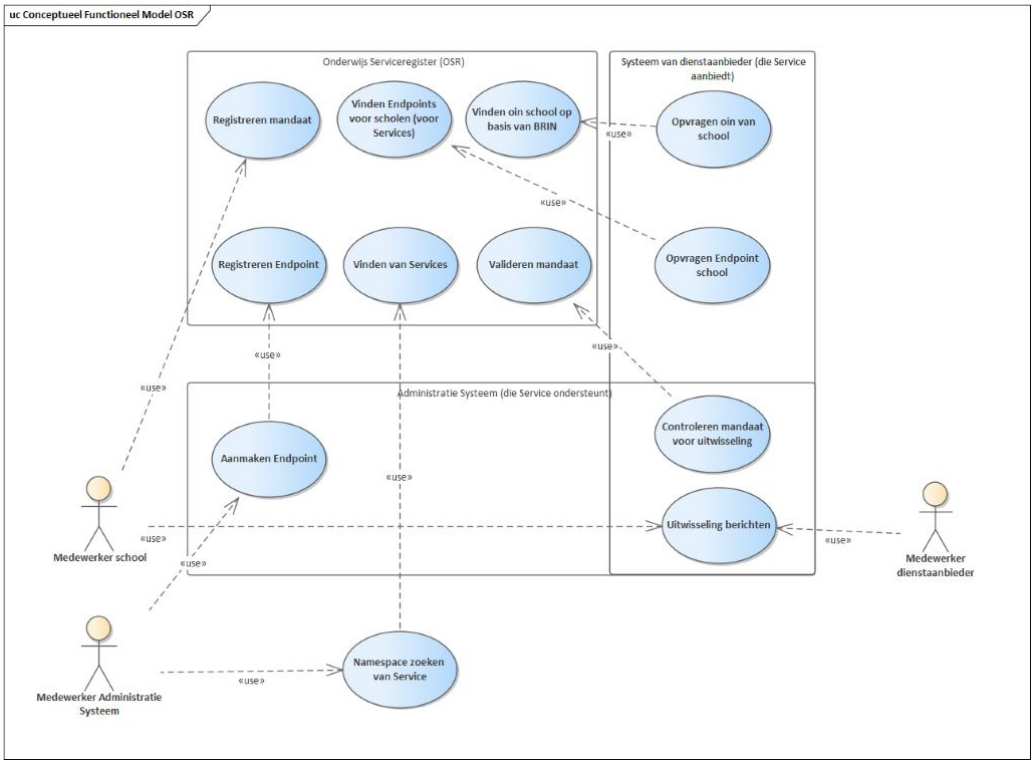
Conform Digikoppeling wordt voor authenticatie gebruik gemaakt van Public Key Infrastructure (PKI) certificaten. De PKI-certificaten kunnen worden gebruikt voor ondertekening en versleuteling zoals dit

[17] Digikoppeling nummersystematiek: https://www.logius.nl/standaarden/digikoppeling/architectuur-en-koppelvlakstandaarden/ Digikoppeling Gebruik en achtergrond certificaten

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 identificerend gegeven dat voor deze aanvrager in het certificaat opgenomen moet worden. Voor Edukoppeling worden conform Digikoppeling private root (G1) PKIoverheid-certificaten gebruikt[18].[19]

6.3. Onderwijs serviceregister (OSR[20])

Een implementatie van een serviceregister is het Onderwijs Serviceregister. Met het Onderwijs Serviceregister (OSR) kunnen medewerkers van scholen middels het portal centraal mandaten registreren voor SaaS-leveranciers. SaaS-leveranciers beheren de technische afleveradressen (endpoints). Daarnaast gebruiken zowel administratie systemen als systemen van dienstaanbieders OSR functionaliteiten, waarbij beide systemen mandaten kunnen valideren. Figuur 16 is een overzicht van de functies van het OSR.



Figuur 16 - Conceptueel functioneel model OSR

6.4. Certificeringsschema informatiebeveiliging en privacy ROSA

In 2015 is voor het eerst het certificeringsschema[21] geregistreerd bij Edustandaard. Het Certificeringsschema is gerelateerd aan Edukoppeling. 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

[18] https://www.pkioverheid.nl/

[19] Let op: Niet alle PKIoverheidcertificaten bevatten een OIN. Het moeten certificaten zijn die geschikt zijn voor Digikoppeling (zie ook voorgaande voetnoot).

[20] https://www.kennisnet.nl/onderwijs-serviceregister/

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

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.
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.

6.5. 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 2020), 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[22]. In de huidige situatie hebben partijen en ketens het IAA onderdeel van end-to-end beveiliging verschillend ingericht.

6.6. Compliancevoorziening

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.

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

7. Foutafhandeling

7.1. Foutcategorieën

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. Zie lijst in verschillende profielen	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. Automatische herhaling tot een instelbaar maximum. Daarna actie beheerder.
C	Service reageert niet (tijdig)	Er volgt geen synchrone response binnen de afgesproken time-out (beschreven in uitwisselovereenkomst)	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 uitwisselovereenkomst)	In applicatie ontvanger. Indien herstelbaar fout 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.