Streefbeeld

Veilige gegevensuitwisseling binnen de onderwijsketen

September 2017

Inhoud

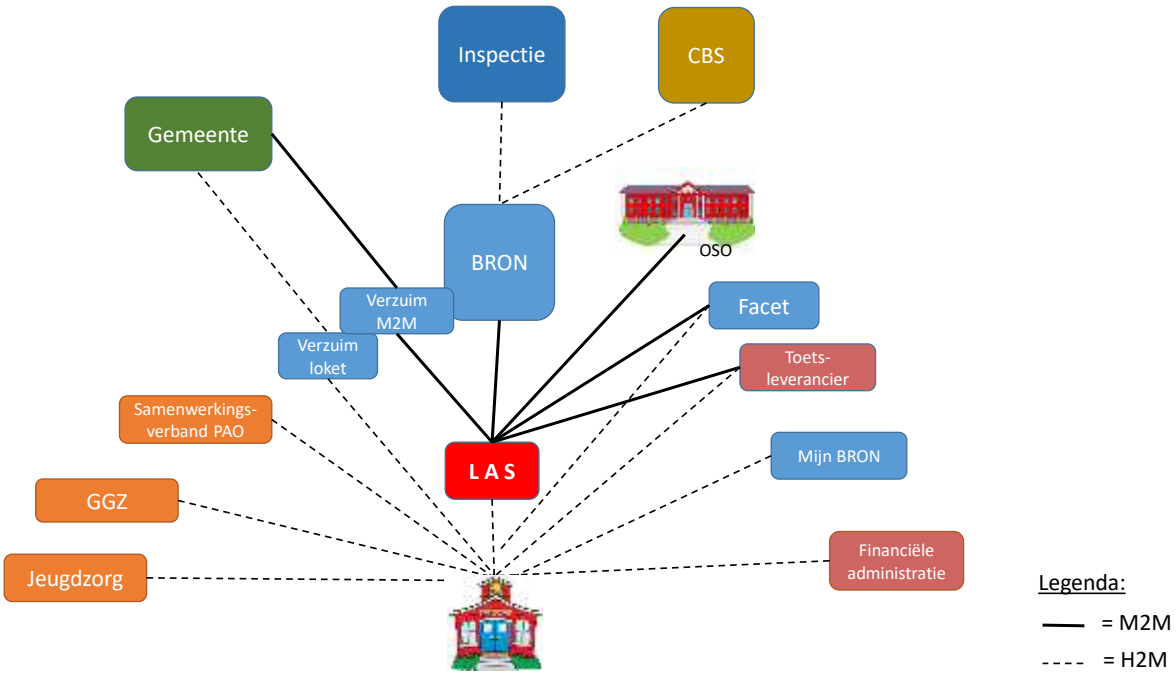
Revisiehistorie

Versie	Auteur	Opmerking
9/3/2016	Kennisnet: Brian Dommisse, Erwin Reinhoud, Arjan van Krimpen VDOD: Ernst -Jan Heuseveldt, Joost van Dijk DUO: Edmar Kok, Gerald Groot Roessink, Meint de Vries, Frank Colstee	Versie besproken en vastgesteld in overleg op 17 maart 2016 met PO-Raad, VO-raad, saMBO-ICT, OCW, DUO, VDOD, Kennisnet
31/7/2017	Brian Dommisse, Erwin Reinhoud (Kennisnet), Paul Kuijt (OCW)	Tekst aangepast op basis inzichten/ontwikkelingen van afgelopen jaar (met name hoofdstuk 2). Begrippen geüniformeerd en in lijn gebracht met o.a. eID/GDI en deze opgenomen in bijlage. Op onderdelen zaken verduidelijkt. Geen wijzigingen die het wezen van het eerder opgestelde streefbeeld veranderen.
26/9/2017	Gerald Groot Roessink	Tekstaanpassingen/-aanvullingen met name rond werking van machtigingen en mandateringen.

1. Inleiding

Leerling- en personeelsgegevens worden binnen en buiten het onderwijs gebruikt in een groot aantal toepassingen van verschillende publieke en private partijen: softwareleveranciers van leerling- cq studentadministratiesystemen (LAS/SIS), leveranciers van financiële en personeelsadministratiesystemen, DUO, Inspectie, Kennisnet, Samenwerkingsverbanden Passend Onderwijs, Facet, educatieve uitgeverijen, toetsleveranciers, Gemeente, Jeugdzorg, GGZ. Die gegevens zijn te raadplegen, te uploaden of te downloaden via zogeheten digitale loketten of portals ofwel door in te loggen op een administratiesysteem. Voor al deze systemen en toepassingen moet de gebruiker zich vaak apart aanmelden.
Dit geldt ook voor de andere organisaties in het onderwijsveld die gebruik maken van gegevens (Gemeenten, samenwerkingsverbanden e.d.). Het gaat hier om de **H2M** (Human-to-Machine) interface: de voorkant (front-office) van het werksysteem waarmee een medewerker/professional toegang krijgt tot de benodigde data (en niet meer).
Bij het inloggen bij een bepaalde dienst of toepassing (portal of loket of administratiesysteem) is er gezien de privacy-gevoeligheid van de gegevens vaak extra zekerheid vereist en wordt multi-factor authenticatie toegepast bijvoorbeeld door toepassing van een token naast de gebruikersnaam en wachtwoord. Een toepassing kan hier vaak zelfstandig invulling aan geven. Om te voorkomen dat medewerkers van scholen bij iedere toepassing apart en op verschillende manieren (met verschillende tokens, wachtwoorden o.i.d) moeten inloggen zou een onderwijssector brede aanpak voor H2M wenselijk zijn.

Een groot deel van de verwerking van gegevens vindt plaats bij de leverancier van een administratiesysteem (LAS, SIS of anders) dat in de "cloud" draait. Hiervoor heeft de school een bewerkersovereenkomst gesloten met de softwareleverancier. De medewerkers van de school gebruiken het systeem om hun gegevens te bewerken of te delen met andere partijen. Vanuit een administratiesysteem worden gegevens dus vaak ook rechtstreeks (dus zonder of naast de tussenkomst van een loket) uitgewisseld met BRON, Verzuimregister, OWP, Facet en met andere scholen in het kader van OSO.
Dit gebeurt beveiligd via een **M2M** (Machine-to-Machine) koppeling, maar nog wel vaak ieder op zijn eigen manier. In het plaatje wordt de veelheid van toepassingen waarmee een gebruiker geconfronteerd kan worden gevisualiseerd. Als voorbeeld van een administratiesysteem is de LAS genoemd. Merk op dat voor het H2M-deel toegang tot de LAS (of ander administratiesysteem) in feite niet afwijkt van toegang tot een extern portaal of loket.



De school is eindverantwoordelijk voor privacy en beveiliging van de leerlinggegevens. Dit is bevestigd in de 'kamerbrief over privacy en informatiebeveiliging' (3 juli 2015).

We staan aan de vooravond van een opschaling van M2M verwerking en dat zal belangrijke gevolgen hebben voor alle betrokken partijen.
Het risico bestaat dat los van elkaar verschillende oplossingen worden uitgewerkt of in stand worden gehouden voor de afzonderlijke domeinen en sectoren alsmede voor de afzonderlijke processen en toepassingen. Een ander risico is dat ontwikkelingen over elkaar heen buitelen: dat vanuit de urgentie moet worden gekozen voor een korte termijn oplossing, die daarna dan moet worden gevolgd door een andere, betere oplossing.
Beide risico's kunnen leiden tot (blijvende) onnodig hoge kosten en lasten voor alle betrokken partijen.

Om de risico's te beperken wordt bij alle partijen in de keten de noodzaak gevoeld om voor zowel M2M als H2M te komen tot een integrale oplossing (streefbeeld) voor alle domeinen en sectoren in het onderwijsveld voor de lange termijn waarbij er op de korte termijn wel al stappen gezet gaan worden om het streefbeeld te bereiken.
Bij alle betrokkenen bestaat bovendien de overtuiging dat nu actie nodig is, gezien de urgentie van een aantal vraagstukken. Korte termijn en lange termijn lopen in tijd in elkaar over. Voor de knelpunten op de korte termijn is haast geboden, bijvoorbeeld om grote onnodige uitgaven te voorkomen gericht op het in standhouden van een reeds verouderde infrastructuur.

Hierbij is het gewenst om de korte termijn oplossingen in relatie tot het **streefbeeld** te bezien. Vanuit de huidige situatie kan er zo een **roadmap** opgesteld worden die in de tijd convergeert naar de gewenste situatie voor de sector, het streefbeeld.

Om bovenstaande redenen is door de sectorraden PO en VO en MBO (vanuit het SION-programma), Kennisnet, VDOD en DUO eind 2015 een werkgroep ingesteld met vertegenwoordigers van die partijen. Eerste stap was het opstellen van een startdocument, waarin een streefbeeld wordt bepaald.
Bij het ontwikkelen van het streefbeeld zijn een aantal kaders in acht genomen, deze komen met name uit de ROSA[1] en zijn uitgewerkt in de Bijlage: Architectuurvisie H2M2M. Met het toepassen van de kaders die ROSA stelt ligt het streefbeeld in lijn met de kaders van de sectoren PO, VO en MBO.
De sector HO is niet expliciet meegenomen, vanwege de wat andere structuur[2], hoewel de hier genoemde principes ook daar grotendeels van toepassing zijn.

Meer specifieke uitgangspunten met betrekking tot de informatiebeveiliging door ketenpartijen zijn de volgende[3]:
- Ketenbrede waarborging van vertrouwelijkheid en integriteit.
- Ketenbrede waarborging van betrouwbaarheid en controleerbaarheid.

De specifieke eisen die hierbij horen zijn de volgende:
- Gegevens worden in opdracht van de scholen (op basis van mandaat) veilig tussen de systemen van de SaaS leveranciers en andere partijen uitgewisseld. Die opdracht is te verifiëren door betrokken partijen.
- Scholen weten welke personen in hun organisatie de uitwisseling hebben geactiveerd (machtigen) en andere betrokken partijen kunnen dit verifiëren.

[1] https://www.wikixl.nl/wiki/rosa/index.php/Doelen_en_principes
[2] Met name de positie van Studielink in de gegevensuitwisseling
[3] Zie https://www.edustandaard.nl/fileadmin/edustandaard/Bestanden/Bijeenkomsten/Standaardisatieraad/02-07-2015_Bijlage_VI_-_ROSA_Katern_Privacy_en_informatiebeveiliging_v1.0.pdf

2. Achtergrond

Inleiding

Bij het realiseren van een verwerking van leerlinggegevens die voldoet aan de eisen van privacy en informatiebeveiliging, gaat het dus om twee hoofdonderwerpen.
De wijze van machine-to-machine koppeling (**M2M**) is vooral een technische verantwoordelijkheid van de ketenpartijen (Kennisnet, DUO, softwareleveranciers)[4]. De scholen zijn primair verantwoordelijk voor een veilige human-to-machine interface **(H2M)** met de systemen waar zij mee werken.

M2M

Bij onderwijsinstellingen die voor het LAS gebruik maken van een SaaS-oplossing vindt een groot deel van de verwerking van de gegevens plaats in het systeem van de SaaS-leverancier en die heeft technische koppelingen ingericht om gegevens met andere partijen uit te wisselen. In deze situatie is de onderwijsinstelling de eindorganisatie en de SaaS-leverancier de gegevensbewerker en logistieke dienstverlener (zie Edukoppeling[5]). Deze situatie wordt in dit document verder aangeduid als het SaaS-model.
De verwerking van de gegevens gebeurt onder verantwoordelijkheid van de school en betreft zowel gegevens waarvoor een wettelijke grondslag bestaat, als andere gegevens. Voor gegevensbewerkingen waarvoor geen wettelijke grondslag bestaat, heeft de school uitdrukkelijke toestemming van de leerling c.q. zijn/haar ouders (of anders de wettelijke vertegenwoordiger) nodig.
Voor de verwerking in een administratiesysteem heeft de school een bewerkersovereenkomst afgesloten met de softwareleverancier. In 2015 zijn in het kader van het Doorbraakproject convenanten opgesteld voor zowel gegevensverwerking in het funderend onderwijs en MBO door educatieve uitgevers als door leerlingadministratiesystemen (LAS), waarmee met name de privacy nog beter geborgd is. Bewerkersovereenkomsten en privacy-bijsluiters kunnen hiervan afgeleid worden.
Dit zijn allemaal instrumenten waarmee de school haar verantwoordelijk voor een deel kan invullen, maar het zijn in principe "papieren" instrumenten. Controle op naleving ervan is in de dagelijkse praktijk ondoenlijk. De vraag is hoe scholen zoveel mogelijk geholpen kunnen worden bij het in die dagelijkse praktijk "afdwingen" (privacy by design) van het juist omgaan met de persoonsgegevens.

Bij de realisatie van het streefbeeld inzake M2M moet per onderwerp en domein rekening gehouden worden met de stand van zaken per domein/keten voor wat betreft de overgang naar M2M en de urgentie van het beschikbaar komen van oplossingen in bepaalde sectoren enerzijds *(de vraagkant),* en de fase van ontwikkeling van oplossingen en standaarden anderzijds *(de aanbodkant)*.

[4] het komt ook nog voor dat scholen een eigen ICT-infrastructuur hebben met een eigen "endpoint" waarmee de M2M wordt geregeld. In het HO en Mbo zal dat eerder voorkomen dan bij het funderend onderwijs.
[5] Edukoppeling: https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/

Vraagkant

Vanuit DUO, SBB en Kennisnet zijn er momenteel 6 koppelvlakken met de scholen in het PO, VO en MBO. Deze staan links in de tabel.

Koppelvlakken M2M en DUO/Kennisnet	PO	VO	MBO
BRON	M2M met door DUO verstrekt (school)certificaat (wordt vernieuwd in 2017) per aanleverpunt. In nieuwe BRON wordt dit gerealiseerd op basis van Edukoppeling 1.2 (planning 2020)	Geen M2M. Batchgewijs via ZP. In nieuwe BRON wordt dit gerealiseerd op basis van Edukoppeling 1.2. Realisatie gestart in 2017.	Tot aan 2017 nog geen M2M; Batchgewijs via ZP. In nieuwe BRON wordt dit gerealiseerd op basis van Edukoppeling. Voor Inwinnen is dat begin 2017 in productie (op basis van Edukoppeling 1.1, nog niet de laatste versie), andere processen volgen.
Verzuim	nog geen	- M2M overheidscertificaat per school - via loket	- met eigen overheids-certificaat per school - via loket
Examens Facet	nog geen	M2M via Edukoppeling (1.1, nog niet de laatste versie)	M2M via Edukoppeling (1.1, nog niet de laatste versie)
OSO	M2M met PKIoverheid-certificaat per SaaS	M2M met PKIoverheid-certificaat per SaaS	geen
DAMBO	Nvt	Nvt	Edukoppeling (oude versie 0.93) met certificaat per SaaS
BPV-keten (met SBB)	nvt	nvt	Alle koppelingen tussen scholen en SBB op basis van Edukoppeling 1.1 (nog niet de laatste versie)
UWLR (uitwisseling leerlinggegevens en resultaten)	Staat als wijzigingsverzoek op de standaard geregistreerd, nog geen concrete planning	Idem	idem
Eindtoets PO	Staat op de roadmap voor schooljaar 2018/19	nvt	nvt

Voor elk van deze onderdelen zijn er knelpunten die in meer of mindere mate dringend om een oplossing vragen.

- Voor de **sector PO** geldt dat de schoolcertificaten (ODOC) in de bestaande M2M koppeling verouderd waren en dringend vervangen moesten worden. Vanuit de PO-sector was het een dwingende wens om over te stappen op SaaS-certificaten en de relatie school-LAS-leverancier op een andere minder arbeidsintensieve manier te regelen. Dat is in 2016/17 niet gelukt en is toch gekozen voor het vervangen van de oude schoolcertificaten door nieuwe. Die operatie zal in Q3 2017 zijn afgerond. Alle betrokkenen willen dat een nieuwe vervangingsronde over 3 jaar vermeden wordt en er een M2M aanpak is geïmplementeerd gebaseerd op het streefbeeld. Dit is aangegeven in het Admin-k overleg tussen OCW, de PO-Raad, VO-raad, DUO, Kennisnet en de VDOD.

- Voor het proces **Verzuim** geldt dat voor alle sectoren de overgang van loket naar M2M voor 2016 op de agenda staat in verband met de kwaliteit van de verzuimregistratie en wettelijke aanpassingen. Zeker voor PO, waarvoor de regeling nu nog niet bestaat, is er een sterke wens vanuit de sectorraad om dit meteen via Edukoppeling te gaan regelen. En als dat niet meteen kan dan in ieder geval wel de schoolcertificaten vervangen door SaaS-certificaten. Gezien het feit dat dit samenhangt met het bovenstaande is dit ook nog niet gerealiseerd.
- Voor het VO wordt sinds maart 2017 in het kader van Doorontwikkelen BRON gewerkt aan een M2M oplossing voor alle processen op basis van Edukoppeling 1.2.
- **Facet** maakt voor het aanleveren van planningen in het VO en het MBO gebruik van M2M koppeling, op basis van de SaaS-variant van Edukoppeling.
- Voor **BRON MBO** is in het kader van Doorontwikkelen BRON gewerkt aan een M2M oplossing op basis van Edukoppeling. Dit is voor het proces 'Inwinnen' begin 2017 live gegaan.
- Digitaal Aanmelden MBO **(DAMBO**) heeft een voor-versie van Edukoppeling geïmplementeerd, die vervangen zou moeten worden door de nieuwe versie. Gezien de ontwikkelingen in het MBO richting een centrale aanmeldfaciliteit is dit voorlopig in de ijskast gezet.
- In de BPV-keten zijn alle uitwisselingen tussen scholen en SBB op basis van Edukoppeling in de loop van 2016 live gegaan.De certificaten voor de uitwisseling tussen scholen onderling in het kader van **OSO** waren verouderd. Een vervanging van die certificaten zou begin 2017 noodzakelijk zijn geweest. OSO werkt ook niet met schoolcertificaten maar met aanleverpunt certificaten. Voor iedere unieke combinatie van school-systeem werd een certificaat gebruikt (er waren dus scholen met meerdere certificaten). In 2016 is besloten om die certificaten volledig te gaan schrappen en te vervangen door PKIoverheid-certificaten per bewerker (SaaS-leverancier)[6]. De relatie school/systeem-bewerker wordt vastgelegd in een OSO-register dat wordt gebruikt om te controleren of een uitwisseling namens een school is toegestaan.

Per overheidssector geldt dat in principe één technisch koppelvlak met DUO voldoende is om alle verschillende domeinen te koppelen.

Aanbodkant

Voor de PO-sector zijn voor M2M gemeenschappelijke en geïntegreerde oplossingen uitgewerkt. Twee oplossingen springen er uit:
- de uitgifte door DUO gedurende 2017 van onderwijscertificaat (onderwijssector breed) die aan de nieuwste beveiligingseisen (conform PKI-Overheid) voldoet;
- de ontwikkeling van de Edukoppeling Transactiestandaard door de desbetreffende Edustandaard-werkgroep Edukoppeling[7].

Er waren in principe twee mogelijke oplossingen beschikbaar die voldeden aan de beveiligingseisen (waarbij ook het bestaande beveiligingsprobleem voor PO-certificaten en OSO-certificaten wordt opgelost):
- Het ***SaaS-model***, waarbij alle scholen/instellingen die gebruik maken van de SaaS-dienst van een softwareleverancier en deze ook de rol van logistieke dienstverlener heeft en dus op basis van het eigen PKI certificaat[8] een beveiligde verbinding opzet met de externe partij waarmee namens de onderwijsinstelling gegevens uitgewisseld worden.
- Het ***traditionele model***, waarbij per school één (school)certificaat moet worden geïnstalleerd voor de gegevensuitwisseling met DUO[9].

In het traditionele geval dient gebruik gemaakt te worden van het nieuwe ODOC-certificaat. Deze nieuwe certificaten worden verstrekt met behulp van een token via het Zakelijk Portaal bij DUO. Bij het SaaS-model kan een SaaS-leverancier ervoor kiezen een ODOC of een PKI-Overheidscertificaat

---

[6] Uiteraard als de school geen SaaS-leverancier gebruikt maar zijn eigen infra beheert, dan moet de school zelf een PKIoverheid-certificaat hiervoor gebruiken. Dit geldt overigens voor alle sectoren.

[7] Per juli 2015 vastgesteld door alle betrokken private en publieke partijen binnen Edustandaard als de standaard van gegevensuitwisseling in de sector Onderwijs. Zie: https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/1.2/

[8] Het is overigens niet per definitie zo dat het SaaS-model slechts één certificaat tussen SaaS en DUO benodigd. Er zijn SaaS-leveranciers die iedere aangesloten school via een apart kanaal richting DUO koppelen. Afhankelijk van de domeinconfiguratie en de manier waarop het SSL-certificaat is uitgegeven kan het zijn dat er meerdere certificaten gebruikt moeten worden.

[9] Dit model is van vóór de Cloud. In huidige situatie blijft de SaaS-leverancier onzichtbaar. Aanvullingen als certificering en service-register zijn daarom nodig.

te gebruiken. Voor beide geldt dat als identificerend gegeven het OIN in het certificaat is opgenomen.

Met deze oplossingen wordt gezorgd voor een veilige uitwisseling tussen twee "endpoints", bijv. tussen SaaS-leverancier en een andere SaaS-leverancier, tussen DUO en een SaaS-leverancier, etc. Eén van deze oplossingen moest in 2016-17 uitgerold gaan worden.

Het SaaS-model had vanuit overwegingen van eenvoud, beheerbaarheid, kosten en administratieve lasten de voorkeur. Dat is ook het streefbeeld dat in de Edukoppeling architectuur is vastgesteld. Naast de bewerkersovereenkomsten en de invoering van het certificeringsschema moet in dit model ook de mandateringsrelatie tussen de school en SaaS-leverancier geregeld worden. Meer hierover in het streefbeeld.

De impact van de implementatie van het SaaS-model is afhankelijk van de inrichting van de systemen bij de SaaS-leverancier en van aantal en omvang van SaaS-softwareleveranciers in de verschillende sectoren. Niet altijd zal implementatie van het SaaS-model op korte termijn volledig mogelijk zijn. Dat is in de loop van 2016 ook gebleken en is voorlopig voor de komende 3 jaar in het PO vastgehouden aan het traditionele model als het gaat om de uitwisseling met BRON en in het verlengde daarvan met Verzuim.

Hoewel het in het PO nauwelijks voorkomt, kan een school ook zelf zijn infrastructuur voor gegevensuitwisseling beheren ipv dat via een SaaS-leverancier te regelen. In dat geval moet de school zelf een PKI-certificaat hebben.
De bovenstaande situatie speelt niet of veel minder in de overige sectoren. Zoals gezegd was er in het VO nauwelijks sprake van M2M verkeer en wordt dit nu zowel bij OSO als bij Doorontwikkelen BRON volgens het SaaS-model icm Edukoppeling (al of niet in een aantal stappen) gerealiseerd. Idem dito voor de MBO-sector.

Er is momenteel ook een discussie gaande over het apart uitgeven van een eigen PKI-certificaat door DUO (PKI-ODOC). Hoewel technisch en functioneel volledig gelijkwaardig aan PKIoverheid-certificaten ziet DUO dit niet meer als haar core business. De ontwikkelingen in het kader van GDI Overheid spelen hierbij ook een rol. Dit is een extra drijfveer om het streefbeeld snel te gaan realiseren voor alle onderwijssectoren incl. het PO.

Het SaaS-model mag niet betekenen dat de school (als de eindverantwoordelijke) niet door ketenpartners wordt geauthentiseerd met fysieke middelen (een harde identiteitsvalidatie). Dit gebeurt in dit model in een aantal stappen:

1. De identiteit (OIN) van de SAAS-leverancier wordt met PKI-Overheid certificaat vastgesteld.
2. In de Edukoppeling-header staat de identiteit (OIN) van de school.
3. In het serviceregister staat de combinatie vermeld als geldig mandaat.

H2M

Vraagkant

Op het gebied van de H2M-interface, de koppeling tussen gebruiker en systeem, zijn er behoeften aan betere, meer generieke voorzieningen. Vanwege de SaaS-oplossingen (maar dit is niet tot beperkt tot SaaS-oplossingen alleen) is authenticatie en identificatie op basis van gebruikersnaam/wachtwoord vaak niet voldoende meer, zeker bij gegevensoverdracht waar een hoge mate van betrouwbaarheid vereist is. Voor het verwerken van privacygevoelige gegevens is over het algemeen *een hogere betrouwbaarheid van de identiteit* vereist. In het eID-stelsel dat via de Wet GDI ook voor dit type gegevensoverdracht verplicht wordt gesteld praat men over een Betrouwbaarheidsniveau Substantieel. Veel handelingen met het Zakelijk Portaal van DUO zouden daar in principe onder vallen en ook de centrale aanmeldvoorzieningen (Studielink in het HO) waar een BSN wordt verwerkt vereisen een dergelijk niveau.
In de nieuwe Europese richtlijn op het gebied van Privacy zijn er per 1 januari 2016 op dit gebied aanvullende eisen gesteld. Primair gaat het hierbij om een verantwoordelijkheid van de scholen. De Europese richtlijn gaat echter uit van het principe van ketenaansprakelijkheid, zodat ook de andere partijen (DUO, softwareleveranciers) in de keten die een gedeelde verantwoordelijkheid dragen.
De nieuwe regelgeving bevat ook de mogelijkheid voor het opleggen van boetes aan partijen die niet voldoen aan de regels. In de nieuwe Europese richtlijn wordt een sterke relatie gelegd tussen de privacygevoeligheid van de te verwerken data en het niveau van benodigde identificatie- en authenticatievoorziening. Vanwege de privacygevoeligheid van de informatie waarmee gewerkt

wordt, is het huidige niveau van identificatie/authenticatie van de administratieve krachten van scholen die werken met de leerlinggegevens in het LAS over het algemeen onvoldoende. Het huidige niveau is veelal gebaseerd op username/wachtwoord en is op basis van bestaande richtlijnen en best practices niet voldoende betrouwbaar[10]. De uiteindelijke beoordeling hieromtrent is een verantwoordelijkheid van de scholen, met daarbij een sturende en ondersteunende rol van de Raden.

Met name de VDOD heeft de nadrukkelijke wens geuit dat een medewerker/professional van de school sterker is te relateren aan de organisaties waarvoor hij/zij werkt. Een oplossing kan zijn dat deze delegatie- of machtigingsrelatie wordt beheerd door de federatie die inlogprocedure faciliteert en dat in het zogenaamde SAML-token wordt meegegeven.

Aanbodkant

Bij verschillende partijen zijn er ***decentraal*** oplossingen beschikbaar voor identificatie/authenticatie van personen en worden er nieuwe decentrale oplossingen uitgewerkt. Een alternatief is dat er een ***centrale*** voorziening voor identificatie/authenticatie van personen voor de onderwijssector wordt ontwikkeld en beschikbaar gesteld aan de verschillende participanten.
Omdat eindgebruikers betrokken zijn bij meerdere ketens in het onderwijs is het wenselijk om voor de sector Onderwijs als geheel een centrale voorziening in te richten. Dit levert aanzienlijk efficiencywinst op bij beheer en gebruik (inperken 'sleutelbos').
Waar mogelijk zouden ook andere maatschappelijke instellingen, waar de school gegevens mee uitwisselt (jeugdzorg, GGZ etc.), toegang tot deze sectorvoorziening moeten krijgen.
Bij een centrale voorziening wordt voor verschillende soorten gebruikers de administratie gevoerd van identiteit en functie van de medewerker die het betreft. Met één authenticatiemiddel[11] kan ingelogd worden op de omgevingen van de verschillende betrokken partijen, zoals de zakelijke site van DUO, de toetsleverancier, Kennisnet/OSO, de leverancier van het helpdeskpakket, Facet etc.[12].
Belangrijk voordeel van een centrale voorziening is dat scholen daarmee voor een belangrijk deel ontlast worden van vraagstukken rond privacy en beveiliging. Overigens is dit niet alleen een hulpmiddel voor scholen zelf om beveiliging en privacy beter en makkelijker te kunnen regelen, maar ook voor de eerder genoemde publieke en private partijen. Die hoeven niet ieder voor zich eigen authenticatie-oplossingen te ontwikkelen en te onderhouden (al of niet inclusief tokens) maar kunnen gebruikmaken van die sectorbrede oplossing.
Een vergelijkbare voorziening is voor de zorgsector ingericht, door middel van het UZI-Register[13].
Voor het hoger onderwijs heeft Surfconext op dit moment een centrale oplossing werkend[14].

In dit kader is het belangrijk te kijken naar de laatste ontwikkelingen van het eID-stelsel en datgene wat daarover in de Generieke Digitale Infrastructuur (GDI) van de overheid is opgenomen en ook wettelijk verplicht wordt gesteld (middels de wet GDI). In principe gaat het eID-stelsel voorzieningen bieden die hierboven beschreven worden. Het is derhalve zaak om bij de realisatie van het streefbeeld na te gaan welke voorzieningen ook voor het onderwijs bruikbaar en toepasbaar zijn en dit afwegen tegen het zelf realiseren en aanbieden van dergelijke voorzieningen. Zowel vanuit OCW en als de sectorraden wordt dit onderkend.

DUO heeft bijvoorbeeld vele duizenden 'hardwaretokens' gedistribueerd aan medewerkers en professionals in alle sectoren om de uitvoeringsprocessen te faciliteren, maar heeft als architectuurprincipe dat uitgifte van veilige inlogmiddelen geen kerntaak is. DUO wil graag gebruik maken van een collectieve voorziening.

---

[10] Het goed kunnen identificeren/authentiseren van een gebruiker door een systeem is noodzakelijk voor het borgen van de privacy en is een combinatie van meerdere maatregelen. Ten eerste moet bij het aanmaken de identiteit van de persoon geverifieerd worden bij het aanmaken van een account. Ten tweede moeten er maatregelen getroffen worden om de gebruiker goed te authentiseren in het systeem bij het inloggen. Tot slot moet het intrekken van toegang ook goed geregeld zijn, immers een persoon houdt niet voor eeuwig toegang. In beginsel is dat nog niet genoeg voor de ISO270001/2: ook zullen maatregelen nodig zijn voor bijvoorbeeld personeels- of huisvestigingsafspraken binnen een school. Daarover gaat deze notitie echter niet.
[11] Overigens kan hierbij worden uitgegaan van een federatief model, waarbij er een keuze is in beschikbare authenticatiemiddelen.
[12] Uiteraard afhankelijk van autorisatieniveau.
[13] https://www.uziregister.nl/
[14] https://www.surf.nl/diensten-en-producten/surfconext/index.html

3. Streefbeeld

Voorop staat het belang van de school, die door een oplossing gefaciliteerd wordt om aan de eisen van privacy en informatiebeveiliging te kunnen voldoen en zo de privacy van haar leerlingen cq studenten te borgen. Het gaat dan om een oplossing die eenvoudig en generiek is en bijdraagt aan een beperking van administratieve lasten en integrale kosten.

De volgende beoordelingscriteria liggen onder het streefbeeld:
- Integrale beveiligingsoplossing voor de hele keten van handelingen.
- Toekomstvast, d.w.z. de oplossing moet de komende jaren mee kunnen.
- Relatief lage kosten en administratieve lasten.

Het SaaS-model heeft de voorkeur als streefbeeld. In dit model ontbreekt nog wel een mogelijkheid om de mandateringsrelatie (ook wel bewerkersrelatie genoemd) tussen de school en de SaaS-leverancier te verifiëren, dit zowel door de SaaS-leverancier die de gegevens verstuurt, als de partij die de gegevens ontvangt en wil verifiëren of de SaaS namens de school deze gegevens mag aanleveren.
Dit kan opgelost worden door net als in het traditioneel model nog steeds een certificaat per school uit te geven, maar dat is niet voldoende afdekkend. Een betere optie is het realiseren van een veilige H2M voorziening voor de gehele keten, een mandateringsregister, waarmee bovenstaande eisen ingevuld kunnen worden. In feite is zo'n register de digitale weerslag van wat er hierover ook in een bewerkersovereenkomst moet worden opgenomen. De ontvangende partij kan de mandateringsrelatie verifiëren bij het mandateringsregister die een daartoe bevoegde medewerker van de onderwijsinstelling daar geregistreerd heeft. Lokale oplossingen zoals het RAV van DUO vullen maar voor een beperkt deel deze functie in nl. alleen voor DUO-diensten intern raadpleegbaar en niet rechtstreeks door bevoegde medewerkers van een school in te stellen.

Verder is het gewenst om door een vertrouwde derde partij een betrouwbare identificatie/authenticatie van de onderwijsinstelling medewerker en zijn of haar machtiging om namens de onderwijsinstelling te handelen geleverd kan worden. Hiermee kan de SaaS-leverancier het autorisatieniveau instellen voor de gebruiker en heeft de SaaS-leverancier die gegevens namens de school verstrekt hier ook meer zekerheid over. Veelal wordt het machtigingen van gebruikers via autorisatiematrices ingevuld.
In een andere context, nl. voor diensten die via portalen rechtstreeks worden geleverd, zijn het inzicht geven in machtigingen ook een mogelijke oplossing. Het portaal moet de gebruiker kunnen autoriseren op basis van bijv., de machtiging die deze gebruiker heeft namens zijn organisatie. Inzicht in machtigingen zou via een machtigingsregister geboden kunnen worden.

Als alternatief voor een mandateringsregister kan er ook gekozen worden om de identiteitsverklaring van de ingelogde medewerker en de machtigingsverklaring om namens de school te handelen in het M2M-verkeer door te geven aan de ontvangende partij. Het token dat de technische vertaling is van de verklaringen is in dit geval afkomstig uit het "H2M-domein". Dit alternatief vergt dus eerst een goed werkende authenticatiefederatie. Als de SaaS in M2M-communicatie de authenticatie/machtigingsverklaring opneemt van de gebruiker, kan de ontvangende partij bepalen of een geautoriseerde gebruiker heeft gehandeld binnen een ingelogde sessie. Dit is in principe dus een alternatief voor een mandateringsregister (als je de machtiging vertrouwt die de school/federatie beheert, kun je ook aannemen dat deze school de betreffende SaaS-leverancier gemandateerd heeft). Hiermee heeft de ontvangende partij ook zekerheid dat de SaaS-leverancier namens de school gegevens mag uitwisselen (ook hierbij is vertrouwen van belang, maar dit geldt ook bij de andere scenario's).

Elementen

Het streefbeeld bestaat uit de volgende elementen.

Edukoppeling
De standaard voor gegevensuitwisseling vanuit het LAS naar de verschillende partijen in de keten in het Onderwijsveld is M2M via Edukoppeling 1.2[15]. Voor de school heeft deze vorm de voorkeur: gevalideerd veilig en eenvoudig en bovendien een profiel van een nationale standaard, waardoor uitwisselingen met partijen binnen maar ook buiten het onderwijs tot minder discussie en afstemming zullen leiden.

M2M oplossing
Van de twee beschreven varianten heeft het SaaS-model de voorkeur, zowel op basis van gebruikersgemak voor de school, als van integrale kosten voor de sector. Dit is ook in Edukoppeling architectuur als doelsituatie beschreven.

Mandatering
De mandateringsrelatie tussen school en SaaS-leverancier kan met een aantal instrumenten worden vastgelegd en geverifieerd nl. een bewerkersovereenkomst, opname van die relatie in een mandateringsregister (bewerkersregister) welke run-time kan worden bevraagd en uiteindelijk ook een certificeringsschema en daarbij horende audit trails.
De opname in het mandateringsregister moet gedaan worden door de beheerders van de scholen en betrouwbaarheid hiervan moet via een betrouwbaar identificatieproces en een sterke authenticatie geregeld zijn.
Alternatief is dus het doorgeven in de keten van een authenticatie- en machtigingsverklaring van de gebruiker. Dit is echter nu niet heel gebruikelijk in bestaande lokale oplossingen[16]. Bovendien vergt dit eerst een goed werkende authenticatiefederaties. Welke impact dit heeft in de keten en wanneer dat haalbaar is moet derhalve nader onderzocht worden.

Machtiging(sregister)
Om de medewerker te kunnen autoriseren (H2M) voor het afnemen van een bepaalde dienst namens zijn organisatie kunnen er machtigingen overlegd worden. Die kunnen voor de ketenpartijen die daar recht toe hebben geraadpleegd worden via een machtigingsregister of worden in de keten doorgegeven. Het doorgeven van de authenticatie- en machtigingsverklaring (via SAML) wordt dan een standaard onderdeel van de inlogprocedure.

Serviceregister
Bedoeld als een soort van "gouden gids" waarin partijen digitale services in het onderwijs kunnen opzoeken incl. informatie over afleverpunten ("digitale adressen"), condities etc. Streefbeeld is dat op termijn alle services in het onderwijs in hetzelfde serviceregister worden opgenomen en de informatie erover wordt ontsloten of dat dit decentraal gebeurt maar wel op basis van dezelfde specificaties, koppelvlakken etc.
Bij de uitwerking van een serviceregister bestaan er op hoofdlijnen twee varianten:

- een ***decentrale opzet***, waarbij per afzonderlijk gebied een oplossing geboden wordt, door middel van een aantal decentrale serviceregisters, die wel alle conform dezelfde standaarden e.d zijn ingericht, bijvoorbeeld:
  - afzonderlijk voor OSO, DUO.
  - eventueel afzonderlijk per sector of per service.
- Een ***centrale opzet*** met als oplossing een onderwijssector breed serviceregister.

Nota bene: voorlopige aanname is dat de inhoud van het serviceregister niet openbaar mag zijn omdat hiermee teveel informatie wordt weggegeven aan hackers. De data in een centraal register mag daarom alleen toegankelijk zijn voor vertrouwde ketenpartners (d.w.z. met een goed PKI-certificaat geïdentificeerd).

NB de termen serviceregister, mandateringsregister en machtigingsregister lopen soms door elkaar. We hebben in dit document ze afzonderlijk beschreven gegeven ook hun verschillende

[15] Deze versie is sinds 2015 de vigerende versie, vastgesteld door alle ketenpartijen in het onderwijs via Edustandaard.
[16] Dit is bijvoorbeeld iets wat ook wordt toegepast voor MijnOverheid.nl en DigiD. DUO gaat dit toepassen voor Diplomaregister.

doelen en functies. Niettemin kunnen deze functies best in een overkoepelende dienst worden ondergebracht en ontsloten.

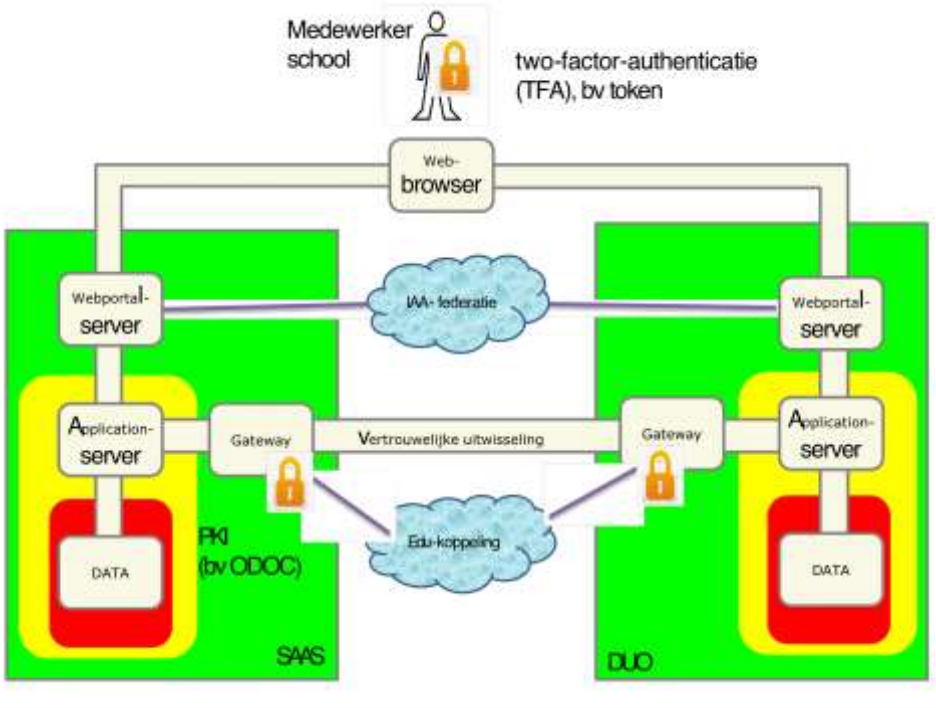
H2M oplossing

Bij de H2M-interface niet alleen gericht op de beheerders, maar ook op ander onderwijspersoneel die belast zijn met processen waarin gevoelige gegevens worden uitgewisseld is de komende periode een uitbreiding van voorzieningen met een sterkere identificatie/authenticatie noodzakelijk. Een centrale oplossing heeft de voorkeur vanuit het oogpunt van beveiliging, beheerbaarheid, gebruikersgemak en integrale kosten. Hiermee wordt een belangrijk deel van het in de dagelijkse praktijk optredende beveiligingsvraagstuk voor de scholen opgelost. Met centraal bedoelen we dus niet per se een centrale oplossing voor het onderwijs alleen, maar kijken we ook naar de generieke mogelijkheden die het eID-stelsel en het GDI te bieden hebben waarop het onderwijs (deels) kan aansluiten.

4. Architectuuruitgangspunten

De architectuureisen uit de inleiding zijn in de tabel uitgewerkt in criteria en bijbehorende in te zetten middelen volgens het streefbeeld.

Wat	Hoe	Middel
Gegevens worden in opdracht van de scholen veilig tussen de systemen van de SaaS leveranciers uitgewisseld	Beveiligde verbinding tussen de systemen en de leverancier is identificeerbaar.	-TLS1.2 voor beveiligde verbinding -PKI certificaat van de SaaS leverancier voor identificatie.
Er is zekerheid over de juistheid van de school en over het mandaat dat is verstrekt aan de SaaS leverancier voor het uitwisselen van gegevens met andere partijen	Controle of SaaS leverancier voor onderwijsinstelling een dienst mag uitvoeren	-Register van onderwijsinstellingen -Vastlegging welke dienst door een leverancier mag worden uitgevoerd (tezamen Mandateringsregister)
Scholen weten welke personen de uitwisseling hebben geactiveerd van de systemen met andere partijen	Sterk identificatieproces Two Factor Authentication van de gebruiker	-Username password en Token voor de gebruiker -Register van gebruikers (machtigingsregister)



Toelichting (*bron: werkgroep Edukoppeling*)
In het plaatje vindt de M2M-uitwisseling plaats op basis van de Edukoppeling-werkwijze die in Edustandaard is afgesproken (blauwe wolk). Voor de H2M-uitwisseling wordt een set afspraken ontwikkeld in het IAA stelsel Onderwijs (aansluitend op het eID stelsel en wet GDI).

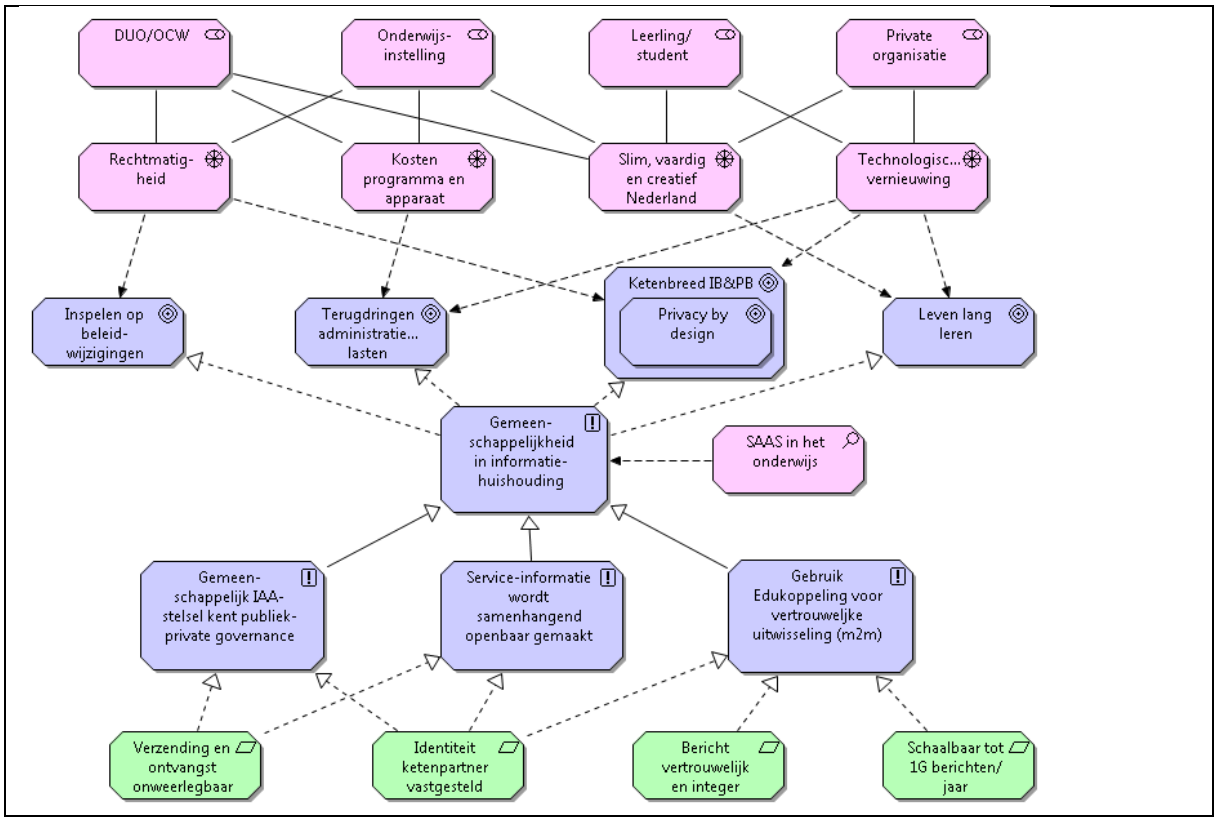
Conclusie

Het streefbeeld voor de lange termijn voor de keten bestaat uit een geïntegreerde oplossing (M2M) voor de gegevensuitwisseling tussen de partijen, gebaseerd op Edukoppeling 1.2 en het in de Edukoppeling-architectuur beschreven SaaS-model, én een geïntegreerde oplossing (H2M) voor zowel het kunnen aangeven van de mandateringsrelatie tussen school en leverancier alsmede de machtiging voor toegang van medewerkers tot de keten die samen de drie onderkende lagen van vertrouwensrelaties afdekken.

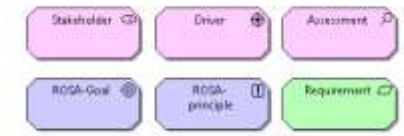
Bijlage: Architectuurvisie H2M2M

Wat willen we en waarom?

Redenerend vanuit de stakeholders en de factoren die voor hen veranderingen in gang zetten zijn de 4 - 5 gemeenschappelijke doelen in de ROSA geformuleerd. Deze doelen zijn publiek-privaat-, sector- en organisatieoverstijgend en worden, net als de Gemeenschappelijke Digitale Infrastructuur (GDI) van de landelijke overheid, gerealiseerd door betere afstemming en meer gemeenschappelijkheid in de informatiehuishouding.



Legenda bij de figuur.



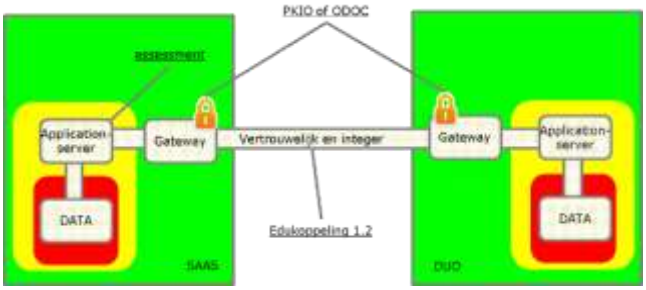
Binnen de veranderde wettelijke, financiële, technische randvoorwaarden voor administratieve en educatieve processen heeft cloudcomputing, in het bijzonder Software-as-a-service (SaaS), de afgelopen jaren in het onderwijs een grote vlucht genomen. SaaS-leveranciers spelen anno 2016 een belangrijke rol bij wat in de gemeenschappelijke digitale infrastructuur mogelijk en wenselijk is. De uitwisselingsovereenkomsten of programma's van eisen van de overheid zijn vaak nog gebaseerd op het idee dat een school zelf een lokaal pakket heeft draaien en dat de SaaS-leveranciers onzichtbaar blijven.In dit streefbeeld wordt dit niet alleen bijgesteld, maar ook nuttig aangewend. Dit wordt hieronder uitgewerkt aan de hand van **drie ROSA[17] principes/ontwerpkaders**.

[17] Dit zijn niet alle ontwerpkaders. Ze zijn er ook met betrekking tot onderwerpen als semantiek, hergebruik van gegevens e.d. De aanname is dat deze voor dit onderwerp niet relevant zijn. De ROSA kent verder tussen doel en ontwerpkader een netwerk van basis en afgeleide principes, vaak met link naar de NORA. Dat netwerk wordt hier niet herhaald. Het kan worden geraadpleegd op: http://www.wikixl.nl/wiki/rosa/index.php/Doelen_en_principes#Visie_en_doelen

1. Gebruik Edukoppeling voor vertrouwelijke uitwisseling (M2M)

Edukoppeling is het door Edustandaard beheerde en op Digikoppeling gebaseerde M2M-koppelvlak voor uitwisseling door scholen. Uitgangspunt is dat uitwisselingen met de overheid, tussen scholen onderling en tussen scholen en private partijen met hetzelfde logistieke protocol ingericht kunnen worden. In veel gevallen is het niet de school die dit koppelvlak inricht, maar de SaaS-leverancier:

- Het M2M verkeer wordt beveiligd in een tweezijdige TLS-verbinding. Het PKI-certificaat (PKIO of ODOC) dat daarvoor wordt gebruikt staat op naam van de SaaS-leverancier.
- Middels de SOAP-envelop van Edukoppeling wordt doorgegeven voor welke school een bericht bestemd is dan wel van welke school een bericht afkomstig is.
- Er is een assessment uitgevoerd over de interne werking van het SaaS-pakket (van de poort tot en met de data in de virtuele schoolomgeving)

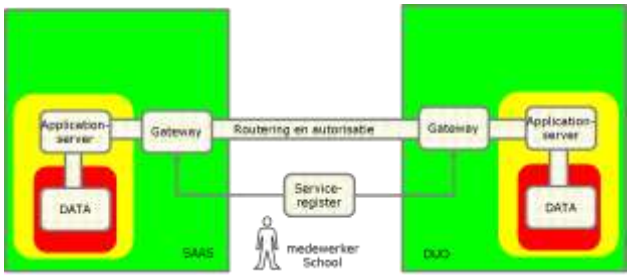


De gegevens worden technisch door de SaaS-leverancier verwerkt (bijv. opgestuurd, ontvangen, opgeslagen, berekend). Edukoppeling, PKI[18] en Assessment voldoen aan de requirement dat de identiteit van de bewerker bekend is, dat het gegevens verkeer niet door derden kunnen worden ingezien (vertrouwelijke, integer) en dat de oplossing zonder aanpassing voor andere toepassingen kan worden gebruikt (schaalbaar).

2. Service-informatie wordt samenhangend openbaar gemaakt.

De omschrijving van dit ROSA-ontwerpkader is misschien niet meer helemaal actueel, maar het onderwerp, een service- of mandateringsregister, is dat wel. De service-informatie heeft betrekking op "wie stelt welke service namens wie beschikbaar en wie mogen daarvan gebruik maken" (mandateringsrelatie). Hier komt de SaaS-leverancier expliciet naar voren als de partij die namens een school een bewerking (bijvoorbeeld: gegevens verzenden of ontvangen) uitvoert.

- Het is de school die deze service-informatie beheert in een serviceregister. In beginsel doen ze dat in een beveiligde webomgeving. Niet meer actuele bewerkersrelaties kan de school verwijderen.
- Elke servicepoort (bijvoorbeeld bij DUO of bij SaaS-leverancier) heeft toegang tot deze informatie en kan op basis hiervan uitgaande service calls routeren (naar een URL) en inkomende service calls autoriseren (als de SaaS voor de betreffende school werkt).



Door het serviceregister wordt de link gelegd tussen de identiteit van de functioneel verantwoordelijke (de school) en de bewerker (de SaaS-leverancier). Het serviceregister houdt verband met de zogenaamde ketenaansprakelijkheid van de Europese Privacy Verordening. Een organisatie (zoals DUO) dient zich in dit kader er van te vergewissen dat de levering van

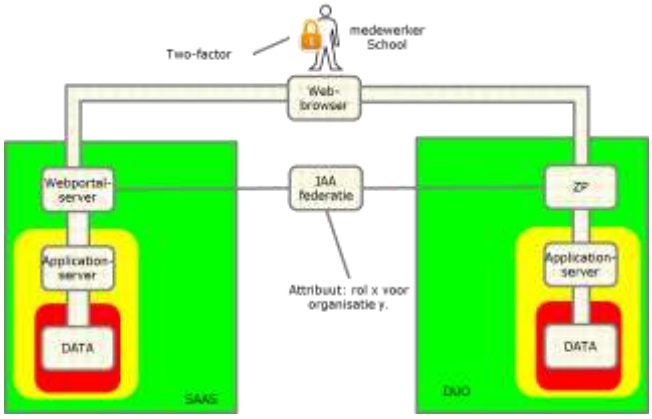
[18] PKI kan meer dan dat. In theorie kan het worden gebruikt om identificerende attributen geëncrypt aan te leveren slaan zodat uitsluitend de beoogde ontvanger het kan ontcijferen. Ook kan naar Europees recht met PKI een geavanceerde of gekwalificeerde digitale handtekening worden gezet. Vooralsnog zijn die functies waarbij certificaten per gedelegeerde medewerker worden ingezet, niet voorzien.

privacygevoelige gegevens een contractuele basis heeft. De inhoud moet authentiek en onweerlegbaar zijn en is tot op zekere hoogte openbaar.

3. Gemeenschappelijk IAA kent gemeenschappelijke governance

De onderwijspopulatie bestaat enerzijds uit leerlingen/studenten en anderzijds uit onderwijspersoneel. Uitgangspunt is dat in elk geval het personeel beveiligde toegang nodig heeft tot meerdere systemen. Het (ROSA) streven is dat de digitale sleutelbos wordt geminimaliseerd en dat daarvoor een sectorale voorziening wordt ingezet:

- Inloggen op Zakelijk Portaal van DUO. Hier kan men bijvoorbeeld de status van een uitwisseling bekijken, PKI-certificaten aanvragen of examens plannen/corrigeren. In VO en BVE is het Zakelijk Portaal ook nog de plek om BRON-bestanden te up- of downloaden.
- Inloggen in het serviceregister (zie punt 2). Hier kan men aangeven wie de bewerker is bij een servicecontract (mandateringen). Dit komt momenteel voor bij DUO én bij OSO, maar nog niet op een beveiligde site.
- Inloggen in het SaaS-systeem. Dit als de medewerker van een school expliciet opdracht moet geven voor een formele handeling als het geven van opdracht om BRON-gegevens naar DUO te sturen.



Essentieel voor het verlenen van (data)toegang is dat een (centrale) dienst in het stelsel (om precies te zijn de attributendienst) aan de serviceproviders kan melden namens wie de persoon inlogt (machtiging). Het inloggen is in dit verband extra bijzonder omdat personeel in bepaalde rollen toegang heeft tot gegevens van grote groepen leerlingen/studenten. Dit betekent in deze rollen een hogere risico-klasse en daarmee de noodzaak om een "substantieel" beveiligingsmiddel te -hanteren. Voor DUO is deze eis momenteel geformuleerd als: "hardwaretoken (two-factor) waarbij de identiteit van de houder is vastgesteld door middel van visuele controle (face2face)". In het kader van de invoering van het eID-stelsel middels de wet GDI is hier een verdere invulling aan gegeven waar partijen in het onderwijs zoals DUO aan moeten gaan voldoen.

Bijlage: Begrippen

Begrip	Omschrijving
Aanleverpunt	Een aanleverpunt is een technische locatie die is gekoppeld aan een formele partij waarmee men via deze locatie mee kan communiceren. In de context van OSO is dit het gegeven waarmee het Traffic Center kan opmaken met welke onderwijsinstelling het communiceert.
Authenticatie (authenticeren)	De controle (het staven) van een geclaimde identiteit van een Gebruiker
Authenticatiedienst (AD)	Een Authenticatiedienst (AD) voert authenticatieprocedures uit waarmee Gebruikers worden geauthentiseerd daarbij gebruikmakend van elektronische Authenticatiemiddelen verstrekt door een Middelenuitgever. De Authenticatiedienst levert op basis van de authenticatieprocedure een Authenticatieverklaring aan de Toegangsdienst.
Authenticatiemiddel	Een middel op grond waarvan authenticatie van een gebruiker kan plaatsvinden. Multi-factor authenticatie houd in dat er voor de authenticatie gebruikt wordt gemaakt van verschillende middelen, een combinatie van iets wat je hebt, kent of bent. In de eIDAS uitvoeringsverordening EU 2015 / 1502 wordt aan Authenticatiemiddelen gerefereerd als "elektronisch identificatiemiddel".
Autorisatie	Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren. Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie.
Batchgewijs	Een hoeveelheid gegevens (batch) wordt in één enkele actie geleverd.
Bewerkersovereenkomst	Indien een verantwoordelijke partij een andere partij (bewerker) inschakelt om hem te helpen met de verwerking van persoonsgegevens, dient de verantwoordelijke een bewerkersovereenkomst met bewerker af te sluiten. Hierin worden onder andere de volgende zaken opgenomen: • het doel van de verwerking door de Bewerker; • de beveiligingsmaatregelen die de Bewerker moet treffen om een passend beveiligingsniveau te garanderen; • de wijze waarop de Bewerker over beveiligingsincidenten/datalekken rapporteert; • de rol van de Bewerker bij eventuele meldingen aan de Autoriteit Persoonsgegevens en de Betrokkenen;
Certificeringsschema	Met het Certificeringsschema kunnen binnen het onderwijsdomein organisaties die ict-diensten leveren worden getoetst op basis van een gezamenlijk opgesteld 'normenkader' dat wordt beheerd binnen Edustandaard. Het (versie 2.0) is gebaseerd op ISO 27001 en ISO 27002 en uitgebreid met beschrijvingen over o.a. het proces en toezicht. (https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema/2.0/)
Delegatie	Van delegatie is sprake als de bevoegdheid om een handeling te verrichten door een partij is overgedragen aan een andere partij. De partij (gedelegeerde) die de handeling verricht op grond van delegatie doet dit op eigen naam en verantwoordelijkheid.
Edukoppeling	Edukoppeling[19] is een gedeelde onderwijsvoorziening voor vertrouwelijk machine-machine uitwisseling in het onderwijs.
Eindorganisatie	De organisatie die in het kader van zijn doelstellingen samenwerkt met een andere organisatie (gegevensbewerker/logistieke dienstverlener).
End-to-end	Van het systeem van de ene eindorganisatie naar het systeem van de andere eindorganisatie

[19] https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard

Begrip	Omschrijving
Gegevensbewerker	De gegevensbewerker is een organisatie die in opdracht van de eindorganisatie gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke.
H2M2M	H2M - Human-to-Machine De interface die een persoon gebruikt bij het raadplegen, uploaden of downloaden van gegevens. Voor toegang tot deze zogeheten digitale loketten of portals moet de gebruiker geauthentiseerd en geautoriseerd worden. M2M - Machine-to-Machine Technische koppeling om gegevens uit te kunnen wisselen. In de context van dit document is dit een gegevensuitwisseling tussen verschillende partijen.
LAS	Een Leerling Administratie Systeem, ook wel SIS (Student Informatie Systeem) is een informatiesysteem dat door scholen en instellingen wordt gebruikt voor het administreren van leerlingen, studieresultaten en andere zaken. Het heeft technische (M2M) koppelingen ingericht om gegevens met systemen van andere partijen uit te kunnen wisselen.
Logistieke dienstverlener	Een organisatie die faciliteert bij de verzending en ontvangst van berichten. Deze stuurt de berichten onverwerkt door naar de Gegevensbewerker en wordt typisch als een transparante intermediair gezien.
Loket	Zie portaal.
Mandaat	De bevoegdheid om in naam van een partij besluiten te nemen. Een door de gemandateerde binnen de grenzen van zijn bevoegdheid genomen besluit geldt als een besluit van de mandaatgever. Kenmerkend voor mandaat is dat de mandaatgever de verantwoordelijkheid en zeggenschap behoudt.
Machtiging	De bevoegdheid aantonen om te kunnen handelen namens iemand die jou gemachtigd heeft (bijvoorbeeld ten bate van rechtspersonen).
OSO	De Overstapservice Onderwijs, hiermee kunnen de meeste (leerling)administratiesystemen in het primair, speciaal onderwijs en voortgezet onderwijs digitaal overstapdossiers uitwisselen.
PKI	Public Key Infrastructure. Is een samenstel van hardware, software, architectuur, organisatie, regels en procedures om digitale certificaten te creëren, distribueren, gebruiken, op te slaan of in te trekken.
PKI certificaat	Een digitaal certificaat dat de betrouwbaarheid van informatie-uitwisseling via websites of M2M koppelingen waarborgt.
Portaal	Digitale dienst die een gebruiker online toegang geeft tot gegevens.
ROSA	De Referentie Onderwijssector Architectuur is de verbijzondering van de NORA voor de sector onderwijs. (http://www.wikixl.nl/wiki/rosa/index.php/Hoofdpagina).
SaaS	Software as a Service (SaaS) is een vorm van Cloud Computing, een patroon voor uitbesteding van IT-diensten (http://www.noraonline.nl/wiki/Patroon_voor_uitbesteding_van_IT-diensten).
SaaS-model	Model voor gegevensuitwisseling conform de Edukoppeling Architectuur.
Zakelijk portaal (ZP)	Een portaal waar een gebruiker (medewerker van onderwijsinstelling) bijvoorbeeld de status van een uitwisseling kan bekijken, PKI-certificaten aanvragen of examens plannen/corrigeren. In VO en BVE is het Zakelijk Portaal ook nog de plek om BRON-bestanden te up- of downloaden.