Startnotitie H2M2M

De toekomst van gegevensuitwisseling in de sector Onderwijs voor PO, VO en MBO

*Streefbeeld*

|  |  |
| --- | --- |
| **Expertisegroep** H2M2M, bestaande uit:  Brian Dommisse Kennisnet  Erwin Reinhoud Kennisnet  Arjan van Krimpen Kennisnet  Ernst -Jan Heuseveldt VDOD  Joost van Dijk VDOD  Edmar Kok DUO  Gerald Groot Roessink DUO  Meint de Vries DUO  Frank Colstee DUO | [http://plzcdn.com/resize/500-500/upload/117cdc17fa822afc77008dd9ba74b6afZG9lbCAzLmpwZw==.jpg](https://www.google.nl/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwj-h4bgtrPLAhXGHpoKHch6BDkQjRwIBw&url=https://tallsay.com/page/4294970514/slim-focussen-om-je-doel-te-halen&bvm=bv.116274245,d.bGs&psig=AFQjCNEo1jInHsih_sAPXfhxWiGtX7N6lg&ust=1457606417856568) |

Geadopteerd door **Strategiegroep** H2M2M op 17 maart 2016

Strategiegroep bestaande uit:

Anna Serraris, VO-Raad

Maurits Huigsloot PO Raad

Theo Joosten VDOD

Martin de Goffau VDOD

Ben Koers Iddink/Schoolmaster

Paul Kuijt OCW

Kor Brandts DUO

Harry Blankena DUO

Inhoud

[Inleiding 3](#_Toc445284566)

[Achtergrond 5](#_Toc445284567)

[Inleiding 5](#_Toc445284568)

[M2M 5](#_Toc445284569)

[Vraagkant 6](#_Toc445284570)

[Aanbodkant 7](#_Toc445284571)

[H2M 8](#_Toc445284572)

[Vraagkant 8](#_Toc445284573)

[Aanbodkant 8](#_Toc445284574)

[Streefbeeld 9](#_Toc445284575)

[Elementen 9](#_Toc445284576)

[Architectuuruitgangspunten 11](#_Toc445284577)

[Conclusie 11](#_Toc445284578)

[Bijlage: Architectuurvisie H2M2M 13](#_Toc445284579)

[Wat willen we en waarom? 13](#_Toc445284580)

[1. Gebruik Edukoppeling voor vertrouwelijke uitwisseling (m2m) 14](#_Toc445284581)

[2. Service-informatie wordt samenhangend openbaar gemaakt. 14](#_Toc445284582)

[3. Gemeenschappelijk IAA kent gemeenschappelijke governance 15](#_Toc445284583)

# Inleiding

Leerlinggegevens worden binnen en buiten het onderwijs gebruikt in een groot aantal toepassingen van verschillende publieke en private partijen: softwareleveranciers van leerling administratiesystemen (LAS), DUO, Inspectie, Kennisnet, Samenwerkingsverbanden Passend Onderwijs, FACET, educatieve uitgeverijen, toets leveranciers, Gemeente, Jeugdzorg, GGZ. Veel van die gegevens zijn te raadplegen, te uploaden of te downloaden via zogeheten digitale loketten of portals. Voor al deze loketten moet de school zich 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.

Bij het inloggen op een portal of loket is er gezien de privacy-gevoeligheid van de gegevens vaak extra zekerheid vereist bijvoorbeeld door het gebruik van bijvoorbeeld token. Om te voorkomen dat scholen zich voor ieder loket apart en op verschillende manieren (verschillende tokens) moeten aanmelden is een onderwijssector brede aanpak voor H2M gewenst.

Een groot deel van de verwerking vindt plaats door de leverancier van het LAS. Hiervoor heeft de school en bewerkersovereenkomst gesloten met de softwareleverancier.

Vanuit het LAS van een school worden gegevens vaak ook rechtstreeks (dus zonder tussenkomst van een loket) uitgewisseld met BRON, Verzuimregister en met andere scholen in het kader van OSO. En in de toekomst ook met Facet en toetsleveranciers.

Dit gebeurt (ieder op zijn eigen manier) beveiligd via een **M2M** (Machine-to-Machine) koppeling.



Het bevoegd gezag van 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 een werkgroep ingesteld met vertegenwoordigers van die partijen. Eerste stap is 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 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[[1]](#footnote-1), hoewel de hier genoemde principes ook daar grotendeels van toepassing zijn.

Meer specifieke uitgangspunten met betrekking tot de informatiebeveiliging door ketenpartijen zijn de volgende[[2]](#footnote-2):

* Ketenbrede waarborging van vertrouwelijkheid en integriteit
* Ketenbrede waarborging van controleerbaarheid

De specifieke eisen die hierbij horen zijn de volgende:

* Gegevens worden in opdracht van het bevoegd gezag van de scholen veilig tussen de systemen van de SaaS leveranciers uitgewisseld
* voor het uitwisselen van gegevens met andere partijen
* Scholen weten welke personen de uitwisseling hebben geactiveerd van de systemen met andere partijen

# 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 verantwoordelijkheid van de ketenpartijen (Kennisnet, DUO, softwareleveranciers)[[3]](#footnote-3). Het bevoegd gezag van de school is primair verantwoordelijk voor een veilige human-to-machine interface **(H2M)** met de systemen waar zij mee werken.

In de onderstaande uitwerking ligt de focus op de door DUO en OSO geleverde diensten ten opzichte van scholen en softwareleveranciers. Deze uitwerking is niet limitatief. Andere ontwikkelingen en partijen in het onderwijsveld (zoals mogelijk UWLR, nummervoorziening, koppelingen met uitgevers) passen eveneens in het geschetste perspectief.

## 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 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[[4]](#footnote-4)). 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 over het algemeen uitdrukkelijke toestemming van de leerling c.q. zijn/haar ouders (of anders de wettelijke vertegenwoordiger) nodig.

Voor de verwerking in het LAS heeft de school een bewerkersovereenkomst afgesloten met de softwareleverancier. In 2015 zijn bovendien in het kader van het Doorbraakproject convenanten opgesteld voor zowel gegevensverwerking door educatieve uitgevers als door leerling administratiesystemen (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)*.

### Vraagkant

Vanuit DUO en Kennisnet zijn er momenteel 5 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 (oud) (school)certificaat per aanleverpunt | Geen M2M. Batchgewijs via ZP. | Nog geen M2M; Batchgewijs via ZP. |
| **Verzuim** | nog geen | - M2M overheidscertificaat per school  - via loket | - met eigen overheids- certificaat per school  - via loket |
| **Examens Facet** | nog geen | M2M via Edukoppeling | M2M via Edukoppeling |
| **OSO** | M2M met OSO certificaat per aanleverpunt/school | M2M met OSO certificaat per aanleverpunt/school | geen |
| **DAMBO** | Nvt | Nvt | Edukoppeling (oude versie) met certificaat per SaaS |

Voor elk van deze onderdelen zijn er knelpunten die dringend om een oplossing vragen.

* Voor de **sector PO** geldt dat de certificaten in de bestaande M2M koppeling verouderd zijn en dringend vervangen moeten. Vanuit de PO-sector is 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.
* 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.
* **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** wordt in het kader van Doorontwikkelen BRON gewerkt aan een M2M oplossing, allereerst voor het proces ‘Inwinnen’
* Digitaal Aanmelden MBO **(DAMBO**) heeft een voor-versie van Edukoppeling geïmplementeerd, die vervangen moet worden door de nieuwe versie.

De certificaten voor de uitwisseling tussen scholen onderling in het kader van **OSO** zijn verouderd. Een vervanging van de huidige certificaten begin 2017 is noodzakelijk. OSO werkt niet met schoolcertificaten maar met aanleverpunt certificaten. Voor iedere unieke combinatie van schoolsysteem wordt een pki-certificaat gebruikt (er zijn dus scholen met meerdere certificaten).

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

### Aanbodkant

Vanuit de sector zijn voor M2M gemeenschappelijke en geïntegreerde oplossingen uitgewerkt.

Twee oplossingen springen er uit:

* de uitgifte door DUO van onderwijscertificaat (onderwijssector breed) die aan de nieuwste beveiligingseisen (conform PKI-Overheid) voldoen;
* de ontwikkeling van de Edukoppeling Transactiestandaard door de desbetreffende Edustandaard-werkgroep Edukoppeling[[5]](#footnote-5).

Er zijn in principe twee mogelijke oplossingen beschikbaar die voldoen 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[[6]](#footnote-6) een beveiligde verbinding opzet met de externe partij waarmee namens de onderwijsinstelling gegevens uitgewisseld worden. .
* Het ***traditionele model***, waarbij per school één certificaat moet worden geïnstalleerd voor de gegevensuitwisseling met DUO[[7]](#footnote-7).

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 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 moet de komende periode uitgerold gaan worden.

Het SaaS-model heeft 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.

Naast het SaaS-model dient daarom ook altijd het traditionele model beschikbaar te blijven voor school en/of softwareleverancier (voor lokale installaties - on premise)[[8]](#footnote-8).

## H2M

### Vraagkant

Op het gebied van de H2M-interface, de koppeling tussen gebruiker en systeem, zijn er behoeften aan betere 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 de nieuwe Europese richtlijn op het gebied van Privacy worden er per 1 januari 2016 op dit gebied bovendien 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 privacy gevoeligheid van de te verwerken data en het niveau van benodigde identificatie- en authenticatievoorziening. Vanwege de privacy gevoeligheid 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[[9]](#footnote-9). De uiteindelijke beoordeling hieromtrent is een verantwoordelijkheid van het bevoegd gezag van de scholen, met daarbij een sturende en ondersteuning rol van de Raden.

### 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 (geen ‘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 (bijv. token)[[10]](#footnote-10) kan ingelogd worden op de omgevingen van de verschillende betrokken partijen, zoals de zakelijke site van DUO, de toets leverancier, Kennisnet/OSO, de leverancier van het helpdeskpakket, Facet etc.[[11]](#footnote-11).

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[[12]](#footnote-12). Voor het hoger onderwijs heeft Surfconext op dit moment een centrale oplossing werkend[[13]](#footnote-13).

# 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. 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 de mandateringsrelatie tussen de school en de SaaS-leverancier, dit zowel voor 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 waarmee 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 heeft de SaaS-leverancier die gegevens namens de school verstrekt hier ook zekerheid over (er kan aangetoond worden dat een medewerker van de betreffende onderwijsinstelling gehandeld heeft).

Voor de partij die de gegevens ontvangt kan aan de inzet van een serviceregister gedacht worden. De ontvangende partij kan de mandateringsrelatie verifiëren bij het serviceregister die een medewerker van de onderwijsinstelling daar geregistreerd heeft.

Als alternatief voor een service register kan er ook gekozen worden om de identiteitsverklaring van de medewerker en de machtigingsverklaring om namens de school te handelen in het M2M verkeer door te geven aan de ontvangende partij. Hiermee heeft deze 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. Voor de school heeft deze vorm de voorkeur: veilig en eenvoudig en bovendien een profiel van een nationale standaard, waardoor uitwisselingen met partijen buiten het onderwijs tot minder discussie en afstemming zullen leiden.

M2M oplossing

Van de twee 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 serviceregister welke run-time kan worden bevraagd en uiteindelijk ook een certificeringsschema en daarbij horende audit trails.

De opname in het serviceregister moet gedaan worden door de beheerders van de scholen en betrouwbaarheid hiervan moet via een betrouwbaar identificatieproces en een sterke authenticatie geregeld zijn.

Serviceregister

Streefbeeld is dat op termijn alle services in het onderwijs in hetzelfde serviceregister worden opgenomen en de informatie erover wordt ontsloten.

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, bijvoorbeeld:
  + afzonderlijk voor OSO, DUO
  + eventueel afzonderlijk per sector of per service.
* Een ***centrale opzet*** met als oplossing een onderwijssector breed serviceregister.

H2M oplossing

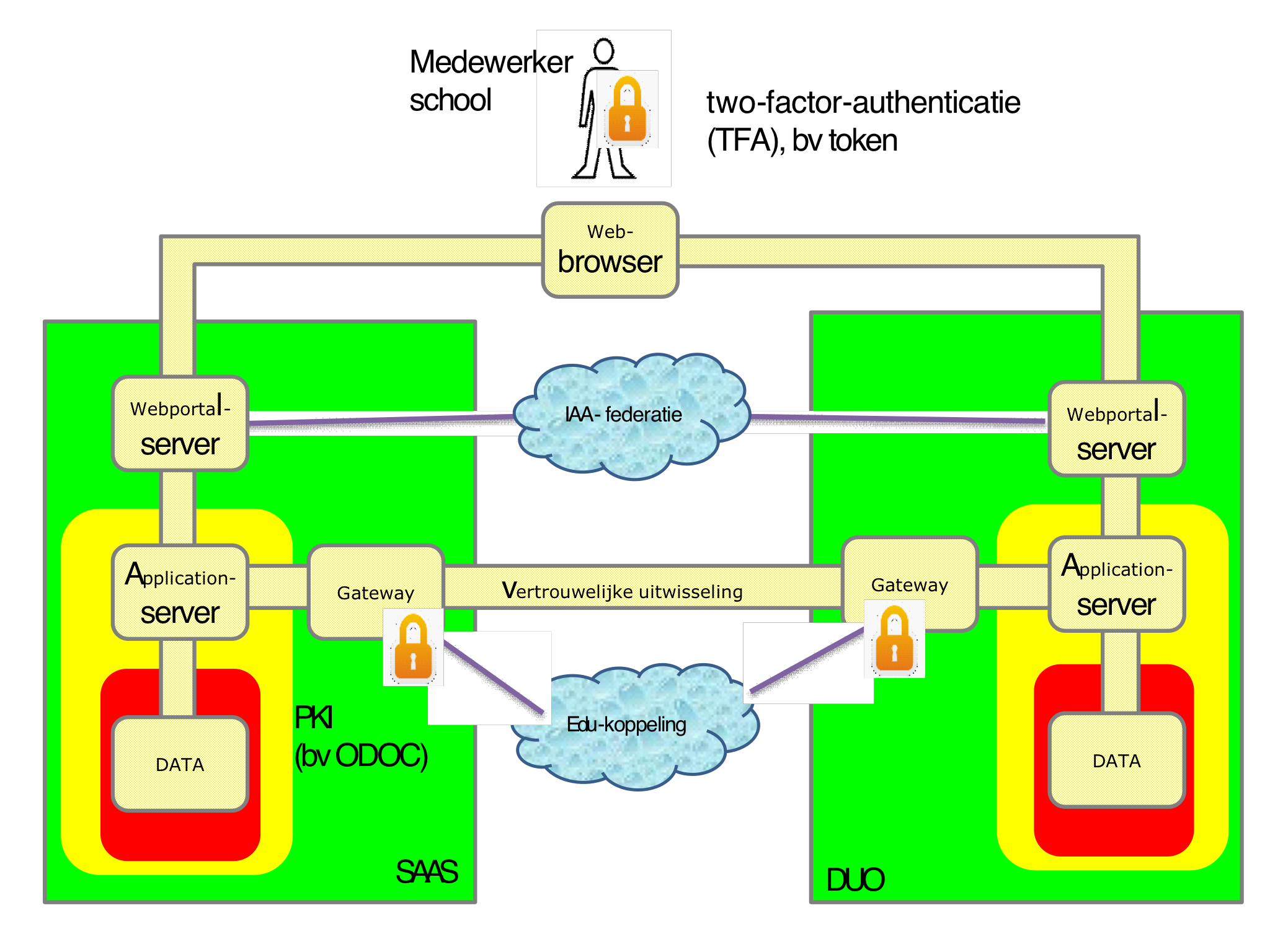
Bij de H2M-interface niet alleen gericht op de beheerders, maar ook op ander onderwijspersoneel die belast zijn met processen waarin gevoelige gegevens worden uitgewisseld is de komende periode een uitbreiding van voorzieningen met een sterkere identificatie/authenticatie noodzakelijk.

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.

# 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 |
| Scholen weten welke personen de uitwisseling hebben geactiveerd van de systemen met andere partijen | Two Factor Authentication van de gebruiker | -Username password en Token voor de gebruiker  -Register van gebruikers |



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 de IAA federatie.*

## 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 toegang van medewerkers tot de keten die samen de drie onderkende lagen van vertrouwensrelaties afdekken.

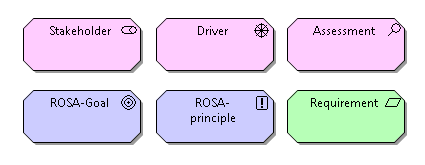
# Bijlage: Architectuurvisie H2M2M

## 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.

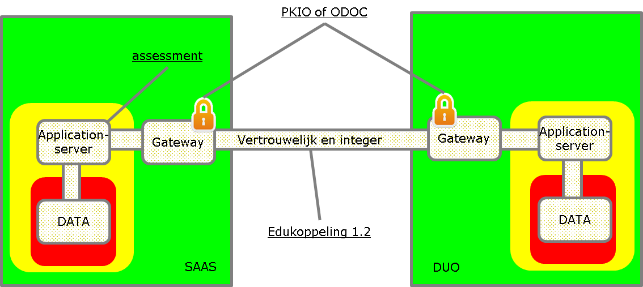


Binnen de veranderde wettelijke, financiële, technische randvoorwaarden voor administratieve en educatieve processen heeft cloudcomputing, in het bijzonder Software-as-a-service (SaaS), de afgelopen jaren in het onderwijs een grote vlucht genomen. SaaS-leveranciers spelen anno 2016 een belangrijke rol 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[[14]](#footnote-14) principes/ontwerpkaders**.

### 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)

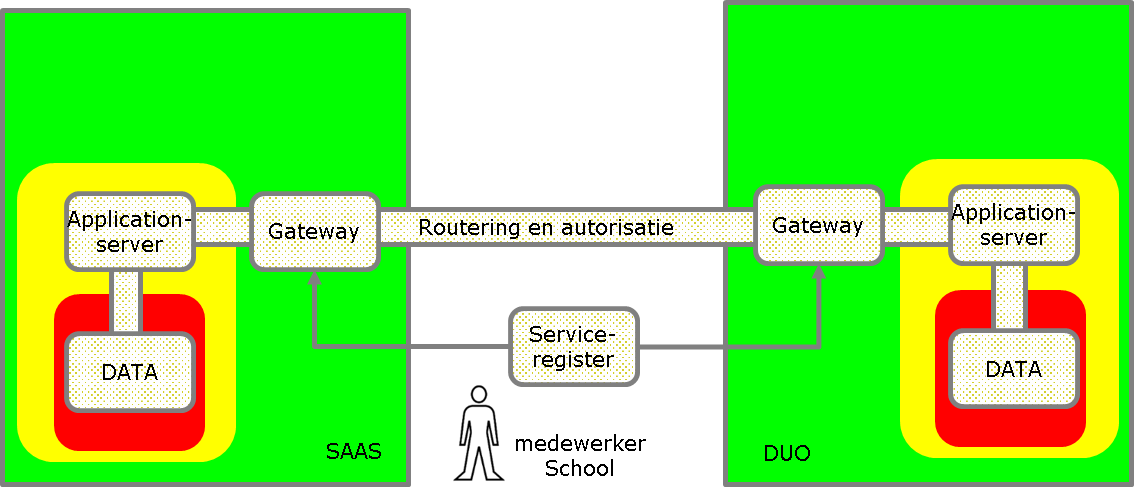


De gegevens worden technisch door de SaaS-leverancier verwerkt (bijv. opgestuurd, ontvangen, opgeslagen, berekend). Edukoppeling, PKI[[15]](#footnote-15) en Assessment voldoen aan de requirement dat de identiteit van de bewerker bekend is, dat het gegevens verkeer niet door derden kunnen worden ingezien (vertrouwelijke, integer) en dat de oplossing zonder aanpassing voor andere toepassingen kan worden gebruikt (schaalbaar).

### Service-informatie wordt samenhangend openbaar gemaakt.

De omschrijving van dit ROSA-ontwerpkader is misschien niet meer helemaal actueel, maar het onderwerp, een serviceregister, is dat wel. De service-informatie heeft betrekking op “wie stelt welke service namens wie beschikbaar en wie mogen daarvan gebruik maken”. 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 serviceinformatie 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 servicecalls routeren (naar een URL) en inkomende servicecalls autoriseren (als de SaaS voor de betreffende school werkt).

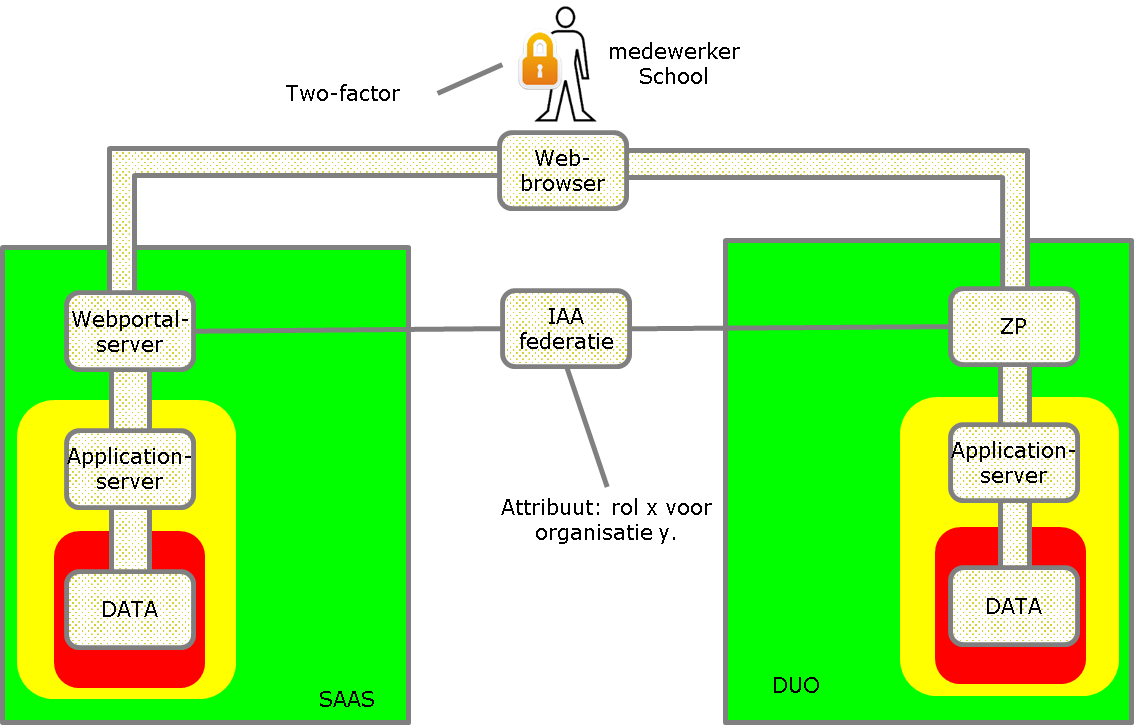


Door het serviceregister wordt de link gelegd tussen de identiteit van de functioneel verantwoordelijke (de school) en de bewerker (de SaaS-leverancier). Het serviceregister houdt verband met de zogenaamde ketenaansprakelijkheid van de Europese Privacy Verordening. Een organisatie (zoals DUO) dient zich in dit kader er van te vergewissen dat de levering van privacygevoelige gegevens een contractuele basis heeft. De inhoud moet authentiek en onweerlegbaar zijn en is tot op zekere hoogte openbaar.

### 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. 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 de federatie (om precies te zijn de attributendienst) aan de serviceproviders kan melden namens wie de persoon inlogt. 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)”.

1. Met name de positie van Studielink in de gegevensuitwisseling [↑](#footnote-ref-1)
2. Zie <https://www.edustandaard.nl/fileadmin/edustandaard/Bestanden/Bijeenkomsten/Standaardisatieraad/02-07-2015_Bijlage_VI_-_ROSA_Katern_Privacy_en_informatiebeveiliging_v1.0.pdf> [↑](#footnote-ref-2)
3. het komt ook nog voor dat scholen een eigen ICT-infrastructuur hebben met een eigen “endpoint” waarmee de M2M wordt geregeld [↑](#footnote-ref-3)
4. Edukoppeling:<https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/1.2/> [↑](#footnote-ref-4)
5. 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/> [↑](#footnote-ref-5)
6. 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. [↑](#footnote-ref-6)
7. Dit model is van vóór de Cloud. In huidige situatie blijft de SaaS-leverancier onzichtbaar. Aanvullingen als certificering en service-register zijn daarom nodig. [↑](#footnote-ref-7)
8. Bij de toepassing van de SaaS-model in het PO is er een verzwakking in de relatie tussen school en softwareleverancier, doordat de eenmalige upload van het certificaat door de school vervalt.

   De hier boven genoemde extra kwetsbaarheid vanwege het ontbreken van de upload van het certificaat vervalt bij toepassing van 2FA identificatie/authenticatie en verstrekking van het attribuut: deze persoon heeft rolx voor school y. [↑](#footnote-ref-8)
9. 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 authenticeren 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 huisvestingingsafspraken binnen een school. Daarover gaat deze notitie echter niet. [↑](#footnote-ref-9)
10. Overigens kan hierbij worden uitgegaan van een federatief model, waarbij er een keuze is in beschikbare authentiecatiemiddelen. [↑](#footnote-ref-10)
11. Uiteraard afhankelijk van autorisatieniveau. [↑](#footnote-ref-11)
12. https://www.uziregister.nl/ [↑](#footnote-ref-12)
13. https://www.surf.nl/diensten-en-producten/surfconext/index.html [↑](#footnote-ref-13)
14. 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> [↑](#footnote-ref-14)
15. 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. [↑](#footnote-ref-15)