Startnotitie H2M2M

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

*Implementatie aanpak*

|  |  |
| --- | --- |
| 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://www.stichtinggetontrack.nl/images/doel1.jpg](http://www.google.nl/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwi7wZiktrPLAhUBLZoKHTTXD2gQjRwIBw&url=http://www.stichtinggetontrack.nl/doel.html&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](#_Toc445285103)

[Ontwikkelingen 4](#_Toc445285104)

[1. OSO via SaaS-model 4](#_Toc445285105)

[Uitgangssituatie 4](#_Toc445285106)

[Voorgestelde oplossing korte termijn 4](#_Toc445285107)

[Voorgestelde stappen vervolgtermijn 4](#_Toc445285108)

[Voorgestelde stappen langere termijn 4](#_Toc445285109)

[2. DUO/PO aansluiten via Edukoppeling en SaaS-model 5](#_Toc445285110)

[Uitgangssituatie 5](#_Toc445285111)

[Voorgestelde oplossing korte termijn 5](#_Toc445285112)

[Voorgestelde stappen vervolgtermijn 5](#_Toc445285113)

[Voorgestelde stappen langere termijn 5](#_Toc445285114)

[3. VO aansluiten via Edukoppeling en SaaS-model 6](#_Toc445285115)

[Uitgangssituatie 6](#_Toc445285116)

[Voorgestelde oplossing korte termijn 6](#_Toc445285117)

[Voorgestelde stappen langere termijn 6](#_Toc445285118)

[4. MBO aansluiten via Edukoppeling en SaaS-model 7](#_Toc445285119)

[Uitgangssituatie 7](#_Toc445285120)

[Voorgestelde oplossing korte termijn 7](#_Toc445285121)

[Voorgestelde stappen langere termijn 7](#_Toc445285122)

[5. Identificatie- en authenticatie voor LASsen 8](#_Toc445285123)

[Huidige situatie 8](#_Toc445285124)

[Voorgestelde stappen vervolgtermijn 8](#_Toc445285125)

[6. Integratie afzonderlijke service registers 8](#_Toc445285126)

[Situatie vooraf 8](#_Toc445285127)

[Voorgestelde stappen langere termijn 8](#_Toc445285128)

[7. Integratie Identificatie- en authenticatievoorziening 8](#_Toc445285129)

[Situatie vooraf 8](#_Toc445285130)

[Voorgestelde stappen langere termijn 8](#_Toc445285131)

[Roadmap 9](#_Toc445285132)

# Inleiding

Het Streefbeeld vormt het samenhangende doel waarnaar op termijn toegewerkt wordt. Het streefbeeld is niet in één keer te realiseren en vergt een doorlooptijd van waarschijnlijk enkele jaren.

Op korte termijn zijn er voor afzonderlijke sectoren en domeinen *praktische**ontwikkelingsstappen*nodig. Denk hierbij o.a. aan het vervallen van OSO-certificaten en DUO certificaten voor PO en aan de uitrol van M2M voor verzuim in VO en MBO.

Deze ontwikkelingsstappen moeten qua ontwerp passen in het streefbeeld en een bijdrage leveren aan de realisatie van het streefbeeld.

Deze praktische ontwikkelingsstappen zijn in deze **implementatie aanpak** globaal in de tijd uitgezet.

De focus ligt hieronder op alle door DUO geleverde diensten waarbij gegevensuitwisseling in het geding is (BRON-koppelingen, Verzuimregistratie en –terugkoppeling etc.) en OSO, maar uiteindelijk geldt de implementatie van het streefbeeld voor elke uitwisseling van gevoelige (persoons)gegevens. In nog nieuw te realiseren koppelingen zoals die in de BPV-keten (MBO), Nummervoorziening (PO, VO, MBO) etc. wordt hier reeds rekening mee gehouden, in bestaande koppelingen met ook andere ketenpartners (Uitgevers, toetsleveranciers) zullen er ook migraties plaats moeten gaan vinden.

Voor de afzonderlijke ontwikkelingsstappen moet getoetst worden of, en zo ja welke aanvullende *integratiestappen*noodzakelijk zijn, waarmee het *sectorbrede* karakter van het streefbeeld wordt bereikt.

De volgende praktische ontwikkelingsstappen en integratiestappen worden hier onderkend:

1. OSO
   1. via SaaS-model (korte termijn)
   2. via Edukoppeling (vervolgtermijn)
2. DUO/PO aansluiten via Edukoppeling en SaaS-model
3. DUO/VO aansluiten via Edukoppeling en SaaS-model
4. DUO/MBO aansluiten via Edukoppeling en SaaS-model
5. Identificatie en authenticatie voor LASsen
6. Onderwijssector breed service register
7. Onderwijssector brede H2M voorziening

Er worden drie termijn voor de realisatie onderscheiden, met daarbij een globale indicatie van de verwachte tijdsperiode:

* Korte termijn (2016 en 1e helft 2017)
* Vervolgtermijn (2017 en 1e helft 2018)
* Lange termijn (2018)

Voor elk van de onderdelen geldt dat het een gaat om een indicatie, een globale inschatting van de onderdelen vanuit het streefbeeld en de huidige inschatting van wat realistisch is. Een definitieve planning en uitwerking kan uiteraard pas gegeven worden na uitwerking en in overleg tussen de partijen in de sector.

# Ontwikkelingen

## OSO via SaaS-model

### Uitgangssituatie

De bestaande OSO certificaten zijn verouderd, waarvoor een oplossing gevonden moet worden. Bovendien bestaat het doel om de OSO dienstverlening uit te breiden naar meer scholen. Hiertoe is het gewenst om een generieke oplossing (zonder aparte certificaten) beschikbaar te stellen.

### Voorgestelde oplossing korte termijn

De voorgestelde oplossing bestaat uit toepassing van het SaaS-model uit de Edukoppeling architectuur. Dit betekent:

1. Een certificaat per gegevensverwerkende instantie (‘in de cloud’ bij SaaS-leverancier of ‘on premise’ bij een instelling). Er wordt echter geen gebruik gemaakt van Edukoppeling voor routering (geen WS-Addressing). Dit is niet in de korte termijn oplossing meegenomen, omdat adressering oplosbaar is binnen de reeds bestaande en werkende infrastructuur.
2. De SaaS-leverancier (LAS) gebruikt een PKI-overheidscertificaat (geen PKI-ODOC)
3. Er ligt een expliciete verklaring (mandatering) van de school dat de SaaS-leverancier deze dienst mag afhandelen. Dit is vastgelegd in de service-registratie (OSO TC) en daarnaast in een toevoeging op de bewerkersovereenkomst.
4. Er wordt gebruik gemaakt van een eigen oplossing voor de registratie van mandaat van de school en de services (afzonderlijke serviceregistratie).
5. Voor identificatie/authenticatie van de medewerker van de school die via MijnOSO de mandatering registreert wordt de huidige werkwijze en mate van betrouwbaarheid gehandhaafd.
6. Binnen OSO worden nu aansluitovereenkomsten (ipv bewerkingsovereenkomst) gesloten met de aangesloten SWL’s. De SaaS zou ook ‘geassessed’ kunnen worden aan de hand van het certificeringsschema[[1]](#footnote-1).
7. Het OSO TC controleert tijdens het transport deze relatie (ook die van de ontvanger). Gegevens zouden daardoor nooit van/naar partij kunnen gaan/komen die niet namens school gemandateerd is Partijen die namens een school van een SaaS-leveranciers gegevens aangeleverd krijgen kunnen hierop vertrouwen.

### Voorgestelde stappen vervolgtermijn

Voor aansluiting op het streefbeeld en andere aanvullende eisen worden de volgende stappen onderkend[[2]](#footnote-2):

* M2M koppeling volgens Edukoppeling (onder meer ondersteunen WS-Addressing).
* Hogere betrouwbaarheid realiseren rond identiteit medewerker van onderwijsinstelling (identificatie/authenticatie). Dit is een meer algemene eis die ketenbreed speelt. OSO wil hiervoor aansluiten op landelijke of sectorale voorzieningen en afspraken.
* Hogere betrouwbaarheid realiseren rond identiteit medewerker en namens welke instelling deze een bepaalde handeling bij een SaaS-dienst mag uitvoeren (machtiging). Dit moet de betrouwbaarheid van het ‘mijnOSO’ account (backoffice TC) verhogen. Op zal aangesloten worden op landelijke of sectorale voorzieningen en afspraken.

### Voorgestelde stappen langere termijn

Op langere termijn wordt voorzien in het aansluiten op een onderwijssector brede oplossing voor service register en van identificatie en authenticatievoorziening. Zie hiervoor onderdeel 6 en 7.

## DUO/PO aansluiten via Edukoppeling en SaaS-model

### Uitgangssituatie

De bestaande DUO certificaten in het PO zijn verouderd. Er zijn weliswaar nieuwe certificaten beschikbaar, maar één op één uitrol van deze nieuwe certificaten voor 9000 scholen is kostbaar en arbeidsintensief voor DUO, school en softwareleverancier. Om nieuwe certificaten te installeren moeten scholen eerst toegang krijgen tot het Zakelijk Portaal.

### Voorgestelde oplossing korte termijn

Het voorgestelde alternatief is de overgang naar het SaaS-model met Edukoppeling.

Hierbij gelden grotendeels dezelfde uitgangspunten als bij de OSO oplossing via het SaaS-model. De verschillen zijn:

* Er wordt gebruik gemaakt van het Edukoppeling versie 1.2 protocol. Routering met WS-addressing is hierin opgenomen.
* Er ligt een expliciete verklaring van de school dat SaaS-leverancier deze dienst mag afhandelen. Dit is vastgelegd in het eigen service-register van DUO en daarnaast in een toevoeging op de bewerkersovereenkomst.
* Er wordt gebruik gemaakt van een afzonderlijke oplossing voor de registratie van mandaat van de school en de controle op de services, via een service-register[[3]](#footnote-3).
* Runtime wordt gecontroleerd of de certificaathouder is gemandateerd door de school, vermeld in de soap-header van Edukoppeling, om een PO-service aan te roepen.
* Voor mandatering van de school en voor identificatie/authenticatie van de school bij het service-register wordt gebruik gemaakt van een procedure waarbij de SaaS-leveranciers de identiteit van een beheerder van een school kunnen verifiëren. Deze gegevens zijn geregistreerd in DUO/MijnBron (dit is geen 2FA oplossing)[[4]](#footnote-4).

### Voorgestelde stappen vervolgtermijn

Voor een acceptabele definitieve oplossing voor mandatering en identificatie/authenticatie bij het service register is een 2FA oplossing noodzakelijk. De gebruikelijke oplossing binnen DUO hiervoor is door middel van tokens via het Zakelijk Portaal, maar ook andere 2FA middelen zijn denkbaar. In principe wil DUO hiervoor aansluiten op landelijke of sectorale voorzieningen (uitspraak VDO).

### Voorgestelde stappen langere termijn

Op langere termijn wordt voorzien in een onderwijssector brede oplossing voor service register en van identificatie en authenticatievoorziening. Zie hiervoor onderdeel 6 en 7.

## VO aansluiten via Edukoppeling en SaaS-model

### Uitgangssituatie

**Facet**

Voor Facet zijn de onderdelen uit het model gerealiseerd:

* voor de M2M tussen Facet en LASsen wordt gebruik gemaakt van Edukoppeling en het SaaS-model[[5]](#footnote-5),
* hierbij wordt een (afzonderlijk) service register bijgehouden bij een derde partij (Yenlo).
* Voor identificatie/authenticatie van scholen bij het service-register wordt gebruik gemaakt van een eigen oplossing.
* voor de toegang tot de applicatie Facet (gebruik) wordt gebruik gemaakt van een IAA voorziening gebaseerd op OpenAM (rollen en autorisaties) met (beperkte) 2FA op basis van e-mail bevestiging (eenmalig password).

**Verzuim**

De meldingen relatief verzuim VO lopen nu nog grotendeels via het Verzuimloket via het Zakelijk Portaal; daarnaast is een aantal scholen aangesloten op de M2M variant via een (zelf aangeschaft) PKI-overheidscertificaat.

**BRON**

BRON VO werkt nu nog op basis van batchgewijze uitwisseling via het Zakelijk Portaal (H2M). Dat zal nog enige tijd zo blijven

### Voorgestelde oplossing korte termijn

**Facet** blijft op korte termijn uitgaan van de huidige oplossing.

**BRON VO** blijft voorlopig nog op basis van batchgewijze verwerking. BRON VO werkt nu nog op basis van batchgewijze uitwisseling via het Zakelijk Portaal (H2M). Modernisering van deze uitwisseling valt onder regime van Doorontwikkelen BRON (2016-2018).

VO gaat voor **Verzuim** aan de scholen kant over naar M2M op basis van het SaaS-model met Edukoppeling. Aanvullende kenmerken hierbij zijn:

* Het gebruik van het PKI-ODOC of PKIO certificaat per SaaS-leverancier.
* Gebruik van een serviceregister met mandateringsrelatie en servicerelaties.
* Voor mandatering en identificatie/authenticatie kan gebruik gemaakt worden van het Zakelijk Portaal en de bijbehorende tokens (2FA).

### Voorgestelde stappen langere termijn

Op langere termijn wordt voorzien in een onderwijssector brede oplossing voor service register en van identificatie en authenticatievoorziening. Zie hiervoor onderdeel 6 en 7.

## MBO aansluiten via Edukoppeling en SaaS-model

### Uitgangssituatie

**DAMBO**

MBO is op dit moment deels verbonden via de Edukoppeling voor Digitaal Aanmelden MBO (DAMBO). Het betreft hier versie 0.93 van Edukoppeling, met daarbij nog wat specifieke aanpassingen. Bijzonder vanuit DUO-perspectief is dat DUO hier een service van de school aanroept met als doel om persoonsgegevens te leveren. Hierbij is het SaaS-model van toepassing, met een service-register gebaseerd op de RAV. Het serviceregister is via formulieren via DUO toegankelijk voor de school.

**Facet**

Voor Facet geldt voor MBO dezelfde uitgangssituatie als voor VO

**Verzuim**

Voor verzuim wordt er in de huidige situatie nog gebruik gemaakt van de loket variant, of van de M2M oplossing via een afzonderlijk PKI-overheidscertificaat.

Het is in het belang van de instellingen om over te gaan op de M2M variant via het SaaS-model.

**BRON**

BRON MBO werkt nu nog op basis van batchgewijze uitwisseling via het Zakelijk Portaal (H2M). Modernisering van deze uitwisseling valt onder regime van Doorontwikkelen BRON (2016-2018).

### Voorgestelde oplossing korte termijn

Omdat bij **DAMBO** de huidige versie van Edukoppeling enigszins afwijkt van de actuele 1.2 versie moet hier een aanpassing plaats vinden. Verder op korte termijn geen aanpassingen[[6]](#footnote-6).

**Facet** blijft op korte termijn uitgaan van de huidige oplossing.

**BRON MBO** gaat over op een berichtsgewijze uitwisseling op basis van M2M.

Doel hierbij is het toepassing van het SaaS-model met Edukoppeling 1.2, met een service-register (gebaseerd op RAV of Yenlo). Voor identificatie/authenticatie kan gebruik gemaakt worden tokens en Zakelijk Portaal.

MBO gaat voor **Verzuim** aan de scholen kant over naar M2M op basis van het SaaS-model met Edukoppeling. Aanvullende kenmerken hierbij zijn:

* het gebruik van het PKI-ODOC certificaat per SaaS-leverancier
* gebruik van een serviceregister met mandateringsrelatie en servicerelaties (toegankelijk gemaakt voor betrokken partijen).
* voor identificatie/authenticatie kan eventueel (met name voor de beheerders) gebruik gemaakt worden van het Zakelijk Portaal en de bijbehorende tokens (2FA).

### Voorgestelde stappen langere termijn

Op langere termijn wordt voorzien in een onderwijssector brede oplossing voor service register en van identificatie en authenticatievoorziening. Zie hiervoor onderdeel 6 en 7.

## Identificatie- en authenticatie voor LASsen

### Huidige situatie

Op dit moment is er nog geen duidelijk voorgeschreven inrichting van identificatie en authenticatie voor gebruikers van de LASsen. Op korte termijn is dit ook niet realiseerbaar.

### Voorgestelde stappen vervolgtermijn

Voorafgaand aan en I&A voorziening moet er duidelijkheid bestaan over het gewenste minimale beveiligingsniveau van een I&A voorziening en de rollen waarvoor dit beveiligingsniveau van toepassing is.

Op basis van dit uitgangspunt wordt er gekozen voor een oplossing voor iedere softwareleverancier.

Uitgangspunt is dat er een centraal platform komt die verschillende authenticatiemiddelen kan ondersteunen. Hierop kunnen de softwareleveranciers aansluiten. Ook andere aan het onderwijs gerelateerde organisaties hierop aansluiten.

Uitgangspunt hierbij is een scheiding tussen serviceproviders (alle dienstverleners) en identityproviders. Door service providers en identity providers van aelkaar los te koppelen wordt het mogelijk om onderwijssector breed zaken mogelijk te maken als single-signon, samenstelling van diensten e.d.[[7]](#footnote-7).

Voorgestelde stappen langere termijn

Op langere termijn wordt voorzien in een onderwijssector brede oplossing voor service register en van identificatie en authenticatievoorziening. Zie hiervoor onderdeel 6 en 7.

## Integratie afzonderlijke service registers

### Situatie vooraf

Voor Edukoppeling wordt gebruik gemaakt van een aantal verschillende service registers.

Online toegang op basis van afdoende 2FA authenticatie voor alle betrokken partijen is daarbij niet altijd gerealiseerd.

### Voorgestelde stappen langere termijn

Verschillende serviceregisters worden samengevoegd in een generiek serviceregister dat aan alle gestelde eisen voldoet. Het gaat hierbij o.a. om eisen i.v.m. online toegankelijkheid, beveiliging en centraal beheer.

## Integratie Identificatie- en authenticatievoorziening

### Situatie vooraf

I&A-voorziening is deels centraal (zie punt 5), deels afzonderlijk ingericht. Wellicht niet overal op het vastgestelde minimumniveau.

### Voorgestelde stappen langere termijn

Geïntegreerde, federatieve I&A-voorziening, gebaseerd op vastgestelde rollen en minimum beveiligingsniveau van gebruikte middelen. Bestaande I&A-oplossingen worden indien nodig hierop aangepast en aangesloten.

# Roadmap

De volgende aspecten worden onderscheiden als onderdeel van de tussenoplossingen naar het streefbeeld:

* Realisatie van SaaS-model op basis van Edukoppeling 1.2
* Inrichting decentraal serviceregister
* Decentrale 2FA voorziening voor mandatering en toegang tot service-register
* Decentrale 2FA voorziening voor eindgebruikers LASsen en overige voorzieningen
* Centrale inrichting service register
* Centrale inrichting identificatie/authenticatie voorziening

|  |  |  |  |
| --- | --- | --- | --- |
| **Huidige situatie** | **Korte termijn** | **Vervolgtermijn** | **Lange termijn** |
| Realisatie van SaaS-model op basis van Edukoppeling 1.2 | | | |
| Facet  MBO Dambo (0.93) | Facet  OSO[[8]](#footnote-8)  PO (BRON, verzuim)  VO Verzuim  MBO Dambo (1.2)  MBO BRON  MBO Verzuim | Zie korte termijn | Alle M2M diensten in PO, VO en MBO |
| Inrichting decentraal service register | | | |
| Facet (-)  OSO | Facet (-)  OSO  PO (BRON, Verzuim)  VO Verzuim  MBO Dambo  MBO Verzuim  MBO BRON | Zie korte termijn |  |
| Decentrale 2FA voorziening voor mandatering en toegang tot service-register | | | |
| Facet (-) | Facet (-) | Facet (-)  PO (BRON, Verzuim)  VO Verzuim  MBO Dambo,  MBO Verzuim  MBO BRON |  |
| Decentrale 2FA voorziening voor eindgebruikers | | | |
| Facet (-) | Facet (-) | Facet (-)  LASsen  OSO[[9]](#footnote-9)  DUO  Overige |  |
| Inrichting centraal service-register | | | |
|  |  |  | Alle betrokken partijen |
| Inrichting centrale identificatie/authenticatie voorziening (beheerders, eindgebruikers) | | | |
|  |  |  | Alle betrokken partijen |

1. Voorlopig wordt dan hierbij uitgegaan van self-assessment, maar op langere termijn zal aangesloten worden bij de auditingprocessen die hiervoor worden ingericht. Of dit al voor de korte termijn ingevoerd kan worden of dat dit iets is voor het vervolgtermijn hangt dus af van de voortgang van de invoer van het certificeringsschema. [↑](#footnote-ref-1)
2. Het voorbehoud hierbij is dat besluiten over vervolgstappen en planning binnen OSO gezamenlijk met ketenpartners (Regiegroep) worden genomen. [↑](#footnote-ref-2)
3. Hierbij zijn er twee mogelijkheden: ofwel een interne variant (afgeleid van de RAV), of een externe variant (aansluiten bij FACET Yenlo) [↑](#footnote-ref-3)
4. Dit betekent ook dat voorlopig geen sprake is van aansluiting van PO scholen op het Zakelijk Portaal van DUO. [↑](#footnote-ref-4)
5. Voor ‘beheer van afnamegroepen’ en ‘leveren van examenresultaten’ [↑](#footnote-ref-5)
6. Er zijn in de DAMBO oplossing een paar onvolkomenheden: 1) een OIN-workaround en 2) de mandateringsrelatie is alleen indirect zichtbaar. Er loopt een onderhoudstraject om dat op te lossen. [↑](#footnote-ref-6)
7. Bij DUO wordt gestart we met een IDP service, die we op langere termijn overdragen zou kunnen worden aan een sectorale beheerpartij. . [↑](#footnote-ref-7)
8. Alleen ‘SaaS-certificaat’ (geen volledige Edukoppeling), realisatie in 2016; toepassing vanaf augustus 2016 [↑](#footnote-ref-8)
9. Onder voorbehoud van de nog te nemen besluitvorming hierover. [↑](#footnote-ref-9)