|  |
| --- |
| Programma van Eisen Onderwijs service register |
|  |

**Inhoud**

[**1 Document geschiedenis**](#_huqf4uu9kivv) **3**

[1.1 Revisies](#_94kl908h4w9g) 3

[1.2 Goedkeuring](#_c89azpnmncbb) 3

[**2 Inleiding**](#_i7m6gpe7nev1) **4**

[2.1 Achtergrond](#_u51051p3lv3i) 4

[2.2 Doel van dit document](#_b62veupfhvw1) 4

[2.3 Lijst van begrippen](#_grc351xgowi) 4

[**3 Globale beschrijving**](#_q5zoka47t6om) **6**

[3.1 Fasering en scope](#_b0c3sghj661t) 6

[3.1.1 Fase 1: Minimum viable product](#_wlsu3m2v8kuo) 6

[3.1.2 Fase 2: Dienstaanbieders](#_6wfx7m1k9mw1) 7

[3.1.3 Fase 3: Veilige communicatie](#_69rb4awc3m6w) 7

[3.1.4 Fase 4: Organisaties](#_8v33lfgpgquw) 7

[3.1.5 Uitbreiding: internationaal](#_bz7ga2qa5kq8) 7

[3.2 Verdere uitbreidingen: toegang en autorisatie](#_x5zt7lse3z1m) 7

[**4 Taken en verantwoordelijkheden OSR**](#_ctpxosfw76zf) **8**

[4.1 Belanghebbenden en belangen](#_q4txfbks7f6b) 8

[**5 Functionele wensen**](#_83ogr7xzju2a) **10**

[5.1 Bevragingen van het serviceregister](#_4yeidbletois) 10

[5.2 Onderhoud van de informatie in het register](#_p5qiktak9jhk) 11

[5.3 Beheer van het onderwijs service register](#_9fl3g5c8t6s) 11

[**6 Principes en maatregelen**](#_8i3x9fi9pkl5) **13**

[6.1 Inrichtingsprincipes voor het serviceregister](#_k5qzjt6qwlq6) 13

[**7 Kwalitatieve eisen aan het OSR**](#_by6ohil8b594) **16**

[7.1 Complexiteit van adressering](#_j9bt40o147tw) 16

[7.2 Autorisatie (muteren en raadplegen)](#_h359nkeb8uo7) 16

[7.3 Integriteit van organisatie- en service kenmerken](#_h359nkeb8uo7) 16

[7.4 Verwachte omvang en verwacht gebruik](#_o6j0fkkkjbi9) 16

[**8 Concept realisatie**](#_60n1s3dvvzn9) **17**

[**9 Concept architectuur**](#_c8eg8bmqmp2r) **18**

[**10 Bijlage: Huidige servicelandschap in het onderwijsveld**](#_bmzkokfbdd9q) **19**

# 

# 

# 1 Document geschiedenis

## 1.1 Revisies

Onderstaande tabel beschrijft de geschiedenis van dit document

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Versie informatie** |
| 0.1 | 13-12-2017 | Marc Fleischeuers | Eerste revisie |
| 0.2 | 22-12-2017 | Marc Fleischeuers | Commentaar en aanvullingen van Erwin Reinhoud, Gerald Groot Roessink |
| 0.3 | 10-1-2018 | Marc Fleischeuers | Review begeleidingsgroep: stories OSO, BRON VO, positie autorisatie, toegang |
|  |  |  |  |
|  |  |  |  |

## 1.2 Goedkeuring

Dit document is goedgekeurd door de onderstaande personen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 

# 2 Inleiding

In het project ‘Voorziening vroegtijdig aanmelden MBO’ is de noodzaak gebleken van een serviceregister. Dit register dient om een onderwijsinstelling de eigen adres- en routeringsinformatie over diensten voor vroegtijdig aanmelden te laten aanbieden en beheren, zodat andere instellingen aanmeldberichten naar het juiste adres kunnen sturen.

Tegelijkertijd blijkt dat in andere ketenprocessen en/of -diensten zoals Doorontwikkelen BRON VO, OSO en Vensters een dergelijk register ook noodzakelijk en/of wenselijk is. De toepassingen van deze diensten verschillen licht van elkaar, maar ze hebben vrijwel dezelfde informatie nodig.

Bovengenoemde projecten hebben allereerst behoefte aan een standaard oplossing voor routering- en autorisatievraagstukken, waarbij die autorisatie de autorisatie van het bevragende systeem betreft. Een serviceregister zou ook een rol kunnen spelen bij het bepalen van autorisatie en toegang op het niveau van organisaties of organisatieonderdelen of personen, zie verderop (XXX) voor een korte discussie hierover.

## 2.1 Achtergrond

Een serviceregister is geen nieuw concept. Sinds enige tijd is duidelijk dat er voor betrouwbare berichtuitwisseling een noodzaak is voor betrouwbare en up-to-date informatie van organisaties, diensten, serviceproviders en afleveradressen. In het streefbeeld H2M2M[[1]](#footnote-0) is het serviceregister nader gedefinieerd:

*[Het serviceregister is] 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.*

In het streefbeeld wordt ook opgemerkt dat het serviceregister onder meerdere namen bekend staat en mogelijk meerdere concepten dekt. In dit document wordt de scope van het register recies beschreven, in combinatie met een specifiek gebruiksdoel (hier: het project vroegtijdig aanmelden). Belangrijk daarbij is dat het ontwerp zo gemaakt wordt dat uitbreidingen naar andere gebruiksdoelen mogelijk is. De verwachting hierbij is dat het serviceregister zich zal ontwikkelen binnen de contouren van berichtuitwisseling die geschetst wordt in het streefbeeld.

## 2.2 Doel van dit document

Dit document bevat het programma van eisen dat wordt gesteld aan het onderwijs service register voor de voorzieningen voor Vroegtijdig aanmelden MBO, de OVerstapservice Onderwijs (OSO) en voor BRON VO. Waar uitbreidingen worden voorzien voor andere projecten, wordt dit in de tekst opgemerkt maar niet nader uitgewerkt.

Met dit programma van eisen wordt beschreven welke diensten dit onderwijs service register levert, en waar deze diensten aan voldoen. Tegelijkertijd kunnen belanghebbenden nagaan wat het serviceregister voor hen kan betekenen.

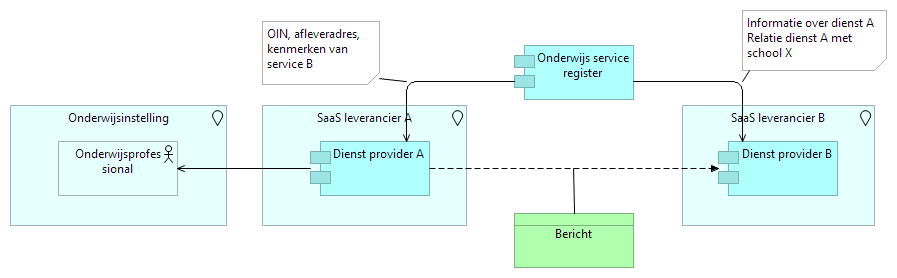
## 2.3 Lijst van begrippen

|  |  |
| --- | --- |
| **Begrip** | **Definitie** |
| Aanleverpunt van een dienst | Keuze van een onderwijsinstelling voor een dienstaanbieder om een dienst te leveren. Een onderwijsinstelling kan meerdere aanleverpunten voor een dienst hebben. De onderwijsinstelling voorziet het aanleverpunt van een uniek (per dienst) kenmerk. |
| Afleveradres van een aanleverpunt | Een url waarop de digitale dienst bereikbaar is. Een aanleverpunt kan over meerdere afleveradressen beschikken. Elk afleveradres is voorzien van een uniek (per aanleverpunt) kenmerk. |
| Autorisatie | Toestemming om bepaalde functionaliteit te mogen gebruiken. De toestemming wordt verleend door een autoriteit bijvoorbeeld de eigenaar van de functionaliteit. |
| Dienst | Verzameling samenhangende (digitale) activiteiten die een dienstaanbieder verricht voor een opdrachtgever. Digitale SOAP diensten worden geïdentificeerd door de namespace van de WSDL waarin ze gedefinieerd zijn. |
| Dienstaanbieder | Partij die (digittale) diensten levert. |
| Edukoppeling | Standaard voor veilige en betrouwbare berichtuitwisseling voor het onderwijs, gebaseerd op Digikoppeling |
| Mandatering | Relatie tussen dienst en dienstaanbieder, gelegd door de opdrachtgever, opdat de dienstaanbieder voor deze dienst namens de opdrachtgever kan optreden. |

# 

# 3 Globale beschrijving

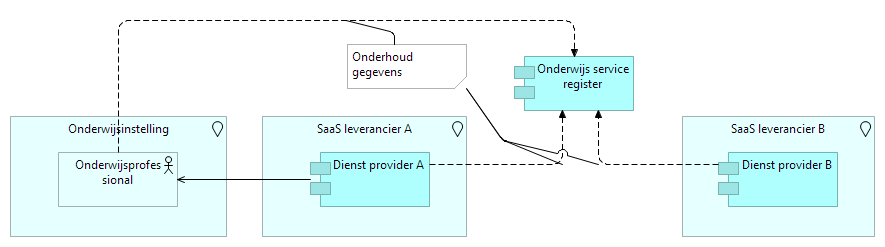
Het serviceregister zal een telefoonboek-functie voor de onderwijsketen leveren. Een gebruiker zoals een onderwijsinstelling of leverancier van diensten voor een onderwijsinstelling kan het register bevragen voor kenmerken en technische details van diensten.

Figuur 1: Abstracte weergave van de keten waarin het OSR functioneert

Bij wijze van voorbeeld, dienstleverancier A wil een bericht sturen naar dienstleverancier B, namens onderwijsinstelling X. Leverancier A vraagt het OSR wat het afleveradres (url) van de dienst is van dienstleverancier B. Hierbij gaan we er van uit dat een onderwijsprofessional bij een onderwijsinstelling heeft bepaald wie zijn dienstverleners zijn. Het serviceregister kan vervolgens de actuele afleveradressen van deze leveranciers door de hele keten beschikbaar stellen.

Dienstleverancier B kan op zijn beurt gegevens over A opvragen en nagaan of school X inderdaad wel een relatie heeft met leverancier A.

Om ervoor te kunnen zorgen dat dit werkt, is het noodzakelijk dat het onderhoud van de gegevens geborgd is. Hiervoor is het in de eerste plaats noodzakelijk dat de onderwijsprofessional aangeeft welke partijen diensten verrichten. Vervolgens zullen deze partijen zelf de afleverinformatie over hun services in het register kunnen onderhouden, zoals weergegeven op onderstaande figuur.



Figuur 2: Abstracte weergave van het gegevensonderhoud in het service register.

## 3.1 Fasering en scope

In de realisatie van het serviceregister worden verschillende fasen voorzien. In elke fase wordt de scope en functionaliteit van het register uitgebreid.

### 3.1.1 Fase 1: Minimum viable product

De eerste versie van het service register zal gebruikt worden door drie diensten: Vroegtijdig aanmelden, OSO Traffic center en BRON VO. Deze diensten hebben behoefte aan 1. identificerende - en adresseringsgegevens van services die onderwijsinstellingen aanbieden voor gebruik door de drie launching customers, plus informatie over de relatie tussen onderwijsinstelling en SaaS leverancier (mandateringsrelaite, tbv autorisatie van requests). Zie [5 Functionele wensen](#_83ogr7xzju2a) voor de functionaliteit die deze versie van het register zal ondersteunen.

Dit betekent dat er in deze versie van het register geen informatie over andere dienstaanbieders (bijvoorbeeld uitgevers, DUO) in het service register wordt opgenomen.

### 3.1.2 Fase 2: Dienstaanbieders

De tweede iteratie van het service register breidt de beschikbare gegevensset uit naar gegevens van services van dienstaanbieders. Ook wordt het aantal bevragende partijen uitgebreid naar alle belanghebbende partijen (informatie in het service register is alleen beschikbaar voor geautoriseerde partijen). Voor deze iteratie wordt geen uitbreiding in de functionaliteit voorzien; bevragende partijen kunnen dezelfde vragen stellen en ontvangen dezelfde soorten informatie.

### 3.1.3 Fase 3: Veilige communicatie

Belangrijke uitbreiding in deze iteratie is dat de publieke sleutels van alle SaaS leveranciers en dienstaanbieders in het register worden opgenomen. Hiermee zal het service register geencrypt berichtverkeer tussen partijen in het onderwijs bereikbaar gaan maken. Bevragingen aan het register worden uitgebreid met bevragingen naar de publieke sleutel, en resultaatgegevens zijn uitgebreid met een veld voor de publieke sleutel.

### 3.1.4 Fase 4: Organisaties

In deze iteratie zal de organisatie-informatie (afkomstig uit RIO) worden uitgebreid met de publieke sleutels van de certificaten van onderwijsnstellingen. Op deze manier kan end-to-end geencrypte communicatie tussen onderwijsinstellingen en hun dienstverleners worden ondersteund.

### 3.1.5 Uitbreiding: internationaal

Enigszins onafhankelijk van bovenstaande fasering is de uitbreiding van het service register naar internationale aanbieders van onderwijs en onderwijsdiensten. DUO participeert in pilot projecten op dit gebied. Functionele wens hiervoor is voornamelijk dat DUO inschrijf- en vooropleidinggegevens bij buitenlandse instellingen wil opvragen en dat bevragingen naar inschrijf- en vooropleidinggegevens aan Nederlandse onderwijsinstellingen vanuit buitenlandse toezichthuiders zou moeten worden ondersteund.

## 3.2 Verdere uitbreidingen: toegang en autorisatie

De hier beschreven functionaliteit van het service register is beperkt tot de routering- en autorisatie vragen bij interacties tussen *systemen*. Systemen opereren echter namens gebruikers en gebruikersorganisaties. De vraagstukken achter de identificatie en autorisatie (machtiging, mandaat) van gebruikers en gebruikersorganisaties zijn van belang om uiteindelijk te komen tot veilige en werkbare end-to-end communicatie in het onderwijs.

Om te komen tot een veilige en werkbare end-to-end communicatie moeten we in staat zijn om de partijen (medewerker onderwijsinstelling, onderwijsinstelling, dienstaanbieder) te identificeren en hun relaties (medewerker - instelling, instelling - dienstaanbieder) vast te stellen. Het is duidelijk dat er niet één oplossing is die dit allemaal kan gaan doen, bovendien zijn een aantal van deze vraagstukken groter dan het onderwijs alleen (sterke identificatie van personen speelt overheidsbreed en internationaal, net als identificatie van organisaties). De uiteindelijke oplossing zal een stelsel zijn, waarbij het OSR en RIO een deel kunnen invullen. Van belang is daarmee wel dat er bij dit ontwerp rekening gehouden wordt met de gedachte dat het zal moeten functioneren in een dergelijk stelsel.

# 

# 

# 4 Taken en verantwoordelijkheden OSR

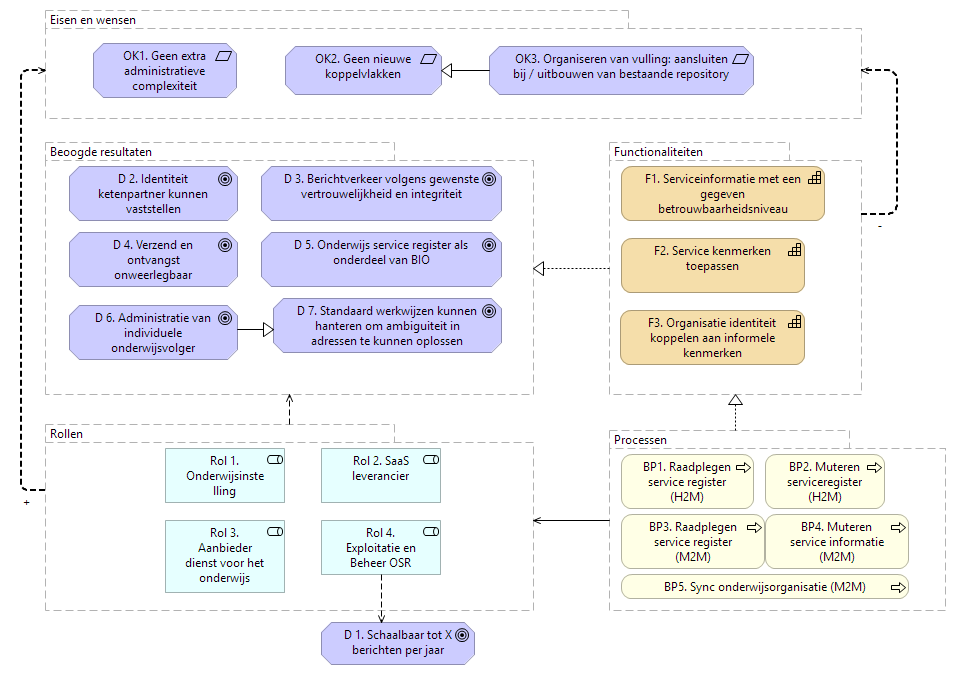
## 4.1 Belanghebbenden en belangen

In onderstaande tabel is nader beschreven welke rol (partij) welke doelstellingen nastreeft.

Tabel 3: Belanghebbenden (bovenste rij) en belangen (1e kolom), met op de kruispunten de achtergrond van het belang.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Rol 1. Onderwijs instellingen** | **Rol2. SaaS leveranciers** | **Rol 3. Dienstaanbieders** | **Rol 4. Beheerder** |
| D1. schaalbaar tot X berichten per jaar |  |  |  | Doel van M2M bericht uitwisselingen volgens streefbeeld |
| D2. Identiteit van ketenpartner kunnen vaststellen | Noodzakelijk voor communicatie | Noodzakelijke voorwaarde voor bepaalde uitwisselingen | Noodzakelijke voorwaarde voor bepaalde uitwisselingen |  |
| D3. Berichtverkeer volgens de gewenste vertrouwelijkheid | Noodzakelijk voor communicatie | Noodzakelijke voorwaarde voor bepaalde uitwisselingen | Noodzakelijke voorwaarde voor bepaalde uitwisselingen |  |
| D4. Verzend en ontvangst van berichten onweerlegbaar | Noorzakelijk voor communicatie | Noodzakelijke voorwaarde voor bepaalde uitwisselingen | Noodzakelijke voorwaarde voor bepaalde uitwisselingen |  |
| D5. Serviceregister is onderdeel van de basisinfrastructuur van het onderwijs |  |  |  | bouwsteen voor hoogwaardige dienstverlening voor het onderwijs |
| D6. De administratie van individuele onderwijsvolger kunnen adresseren |  |  | Noodzakelijke voorwaarde voor bepaalde uitwisselingen |  |
| D7. Standaard werkwijzen kunnen hanteren om ambiguiteit in adressen te kunnen oplossen |  | Niet elke keer wiel hoeven uitvinden | Niet elke keer wiel hoeven uitvinden |  |
| OK1. Geen extra admininstratieve complexiteit | administratie van services is geen kerntaak | administratie van services is geen kerntaak | administratie van services is geen kerntaak | administratie van services is geen kerntaak |
| OK2. Geen nieuwe koppelvlakken |  | elk koppelvlak is een onderhoudsrisico | elk koppelvlak is een onderhoudsrisico |  |
| OK3. Voor vulling aansluiten bij bestaande repositories | vloeit voort uit OK1 | vloeit voort uit OK1 en OK2. | vloeit voort uit OK1 en OK2. |  |

Zie [6.1 Inrichtingsprincipes voor het serviceregister](#_k5qzjt6qwlq6) voor de omschrijving van de doelen en ontwerpkaders.

Figuur 3: Analyse van belanghebbenden en belangen

Om de gewenste resultaten allemaal te kunnen ondersteunen, moet het serviceregister gaan beschikken over twee functionaliteiten die nu niet beschikbaar zijn in bestaande registers:

1. Functionaliteit 1: **Service informatie wordt met een specifiek betrouwbaarheidsniveau vastgelegd**. Deze functionaliteit bepaalt in hoeverre de veiligheid betreffende resultaten Res1, Res2, Res3 opgaan. Echter, een specifiek betrouwbaarheidsniveau wordt nu nergens vastgelegd en er zijn ook geen bestaande koppelvlakken voor. Dat betekent dat deze functionaliteit waarschijnlijk zowel nieuwe (gewijzigde) koppelvlakken als extra administratieve last mee zal brengen.
2. Functionaliteit 2: **Service kenmerken toepassen**. Dit is een van de standaard werkwijzen om ambiguiteit in adressen te kunnen oplossen (zie [2.3](#_equ5riis74bh)), en de gewenste oplossing voor BRON VO om de administraties van individuele onderwijsvolgers te kunnen adresseren. Ook deze functionaliteit echter wordt niet ondersteund in de bestaande registers en koppelvlakken, en zal waarschijnlijk extra administratieve lasten met zich meebrengen.

De derde functionaliteit, organisatiekenmerken koppelen aan informele kenmerken, wordt wel in bestaande registers ondersteund en confliceert niet met de ontwerpkaders.

De voor de hand liggende conclusie hieruit is dat het niet mogelijk gaat zijn om een functioneel compleet service register te realiseren waarbij aan alle gestelde kaders van de belanghebbenden wordt voldaan. Zie [Concept realisatie](#_60n1s3dvvzn9) voor de beoogde werkwijze voor de realisatie, waarbij zoveel mogelijk aan alle belangen recht wordt gedaan.

# 

# 

# 5 Functionele wensen

## 5.1 Bevragingen van het serviceregister

|  |  |
| --- | --- |
| *F.1* | Opvragen OIN van een onderwijs instelling |
| *Als …* | systeem dat een bericht naar een (systeem van een) onderwijsinstelling wil versturen |
| *Wil ik …* | een BRIN of onderwijsaanbieder-id dat ik ken kunnen koppelen aan het actuele formele OIN dat de onderwijsinstelling hanteert |
| *Zodat …* | ik mijn berichten op correcte wijze kan adresseren |

|  |  |
| --- | --- |
| *F.2* | Routering naar onderwijsinstelling |
| *Als …* | systeem dat een bericht naar een (systeem van een) onderwijsinstelling wil versturen |
| *Wil ik …* | een OIN van een onderwijsaanstelling dat ik ken kunnen koppelen aan het actuele afleveradres (of de actuele afleveradressen) van een dienst van de onderwijsinstelling waar ik mijn bericht aan wil leveren |
| *Zodat …* | ik mijn berichten kan routeren naar het (de) juiste afleveradres of -adressen |

|  |  |
| --- | --- |
| *F.3* | Unieke routering naar onderwijsinstelling |
| *Als …* | systeem dat een bericht naar een uniek geidentificeerd adres van een systeem van een onderwijsinstelling wil versturen |
| *Wil ik …* | een OIN van een onderwijsaanstelling dat ik ken kunnen koppelen aan het actuele en afleveradres van een dienst van de onderwijsinstelling waar ik mijn bericht aan wil leveren, waarbij ik een kenmerk opgeef dat de leverancier van de dienst (d.i. het aanleverpunt) voor de onderwijsinstelling uniek identificeert en / of een kenmerk opgeef dat het afleveradres van de dienst van de onderwijsinstelling uniek identificeert |
| *Zodat …* | ik mijn berichten kan routeren naar het juiste afleveradres |

### 

**Toelichting**

Deze user story is gemotiveerd door de huidige praktijk dat onderwijsinstellingen meerdere deeladministraties kunnen voeren, die elk een deel van hun leerlingbestand bevatten. Elk administratiesysteem kan daarnaast meerdere afleveradressen voeren. De user story beschrijft de gewenste functionaliteit dat een aanroepende partij op basis van additionele kenmerken een afleveradres van een dienst van een onderwijsinstelling uniek kan identificeren, ongeacht de wijze waarop de onderwijsinstelling zijn administratie inricht en bestand tegen wijzigingen in afleveradressen van de administratiesystemen.

De beoogde werkwijze is als volgt. De onderwijsinstellig voorziet zijn aanleverpunten en diens adressen van unieke kenmerken. Deze kenmerken zijn ook beschikbaar in het onderwijs service register. Het aanroepende systeem kent (bijvoorbeeld uit eerdere communicatie) de kenmerken van de aanleverpunten en / of afleveradressen, en gebruikt deze kenmerken om het actuele afleveradres op te vragen.

|  |  |
| --- | --- |
| *F.4* | Mandatering van het bevragende systeem |
| *Als …* | systeem van een dat een bericht ontvangt van een systeem namens een onderwijsinstelling |
| *Wil ik …* | nagaan dat de afzender van het bericht inderdaad door de onderwijsinstelling gemandateerd is om deze dienst te gebruiken |
| *Zodat …* | ik de autorisatie van mijn dienst op de juiste manier kan uitvoeren |

### 

**Toelichting**

Onderdeel van de autorisatie van systemen die gevoelige gegevens verwerken kan zijn dat er een controle plaatsvindt of de onderwijsinstelling daadwerkelijk een relatie heeft met het bevragende systeem voor de betreffende dienst.

## 5.2 Onderhoud van de informatie in het register

|  |  |
| --- | --- |
| *O.1* | Onderhoud van aanleverpunten van diensten |
| *Als …* | bevoegde medewerker van een onderwijsinstelling |
| *Wil ik …* | de door mij gekozen dienstleverancier en mijn kenmerk opgeven, wijzigen of verwijderen in het service register, voor de diensten die ze namens mij leveren |
| *Zodat …* | deze leverancier berichten namens mij kan versturen en ontvangen |

|  |  |
| --- | --- |
| *O.2* | Onderhoud van afleveradressen van aanleverpunten |
| *Als …* | leverancier van diensten aan onderwijsinstellingen |
| *Wil ik …* | het afleveradres of de afleveradressen van diensten die ik voor een onderwijsinstelling verricht, en de kenmerken die de beheerder van de dienst bij de onderwijsinstelling hierin heeft aangegeven, kunnen invoeren, actualiseren of verwijderen |
| *Zodat …* | de bereikbaarheidsinformatie voor de diensten die ik lever beschikbaar is voor andere partijen in de onderwijsketen |

## 5.3 Beheer van het onderwijs service register

|  |  |
| --- | --- |
| *B.1* | Beheer van diensten |
| *Als …* | beheerder van het onderwijs service register |
| *Wil ik …* | definities van door het systeem ondersteunde diensten kunnen invoeren, bijwerken en verwijderen |
| *Zodat …* | gebruikers van het reigster altijd een complete en acutele lijst met diensten zien |

|  |  |
| --- | --- |
| *B.2* | Beheer van autorisaties |
| *Als …* | beheerder van het onderwijs service register |
| *Wil ik …* | bevoegde medewerkers van onderwijsinstellingen en leveranciers van diensten aan onderwijsinstellingen kunnen identificeren |
| *Zodat …* | ik de de medewerkers en leveranciers kan autoriseren voor de onderhoudsfuncties |

# 

# 

# 6 Principes en maatregelen

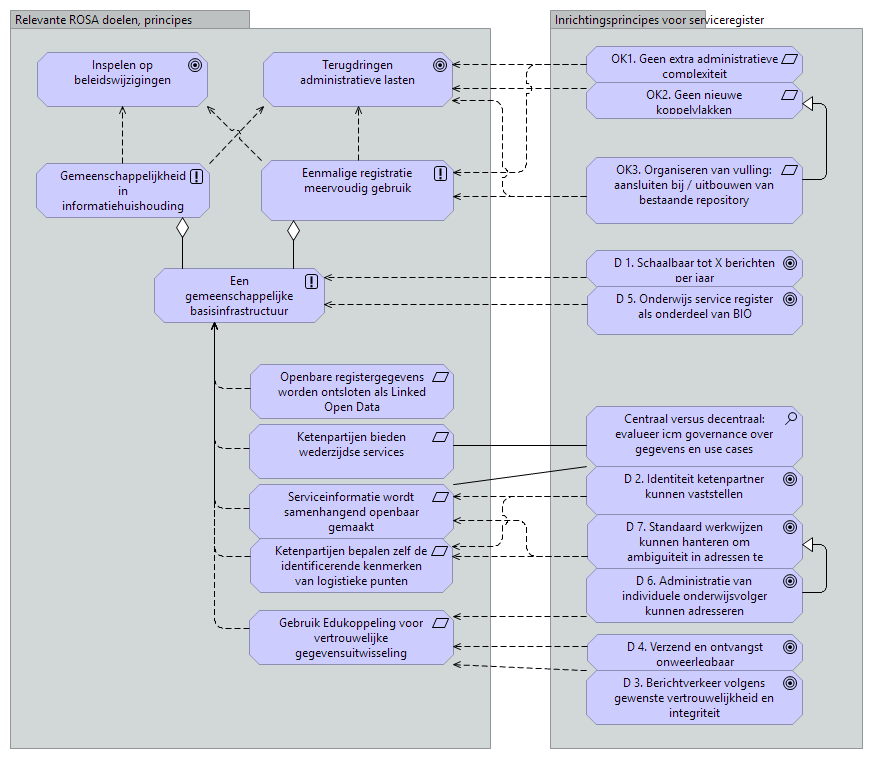
Het serviceregister heeft een ondersteunende rol bij het uitvoeren van interoperabiliteitsdiensten met als kern het inwinnen, beheren en ter beschikking stellen van informatie over diensten, webservices en organisatie-kenmerken van aanbieders en afnemers van deze diensten. Het serviceregister heeft geen taak in de uiteindelijke berichtenstroom tussen aanbieder en afnemer.

Het serviceregister zal informatie over de organisatie, de diensten en de technische eigenschappen van de diensten (met name "het technische afleveradres") bevatten. Voor informatie over de organisatie (en -structuur) zal het serviceregister koppelen met RIO, zodra deze beschikbaar is. Tot die tijd is de registratie in BRIN hierin leidend. Het register gaat voor de indeling van organisatie-informatie uit van de structuur die RIO hanteert.

Het serviceregister zal ook informatie bevatten over services die gevoelige gegevens verwerken. De organisatorische en technische maatregelen die het register neemt om de betrouwbaarheid van de adresinformatie over deze services te kunnen waarborgen, moeten expliciet gemaakt worden in het ontwerp en in overeenstemming zijn met de beveiligingsbehoeften van aansluitende projecten.

## 6.1 Inrichtingsprincipes voor het serviceregister

Het serviceregister zal onderdeel gaan worden van de Basis infrastructuur van het onderwijs, en zal daarmee gaan passen in de doelen, principes en afspraken van ROSA. Op basis van deze randvoorwaarden kunnen we een aantal specifieke inrichtingseisen voor het serviceregister formuleren, zoals weergegeven in figuur 1.

Figuur 4: Overzicht van relevante doelen, principes en afspraken uit ROSA, en daaruit afgeleide afspraken en beoogde resultaten voor het onderwijs service register

De eisen en wensen die de verschillende belanghebbenden stellen aan het serviceregister vloeien voort uit deze ROSA doelstellingen:

1. Doel: Terugdringen van administratieve lasten
2. Doel: Inspelen op beleidswijzigingen

De principes die deze doelen realiseren:

1. Principe: gemeenschappelijkheid in informatiehuishouding
2. Principe: eenmalige registratie, meervoudig gebruik
3. Principe: een gemeenschappelijke basisinfrastructuur

De daaruit afgeleide ontwerpkaders zijn

1. Ontwerpkader: openbare registergegevens worden ontsloten als linked open data
2. Ontwepkader: ketenpartijen bieden wederzijdse services
3. Ontwerpkader: serviceinformatie wordt samenhangend openbaar gemaakt
4. Ontwerpkader: ketenpartijen bepalen zelf de identificerende kenmerken van logistieke punten
5. Ontwerpkader: gebruik Edukoppeling voor vertrouwelijke gegevensuitwisseling

Voor het serviceregister kunnen we hier de volgende afspraken en beoogde resultaten uit afleiden::

1. Ontwerpkader 1: **Geen extra admininstratieve complexiteit.** Het serviceregister zal diensten leveren aan onderwijsinstellingen en dienstleveranciers voor het onderwijs, en deze partijen zitten niet te wachten op extra handelingen.
2. Ontwerpkader 2: **Geen nieuwe koppelvlakken.** In het verlengde van OK1, specifiek geredeneerd vanuit dienstleveranciers, is de wens om geen nieuwe koppelvlakken te introduceren. Elk nieuw koppelvlak heeft onderhoud, testen nodig en introduceert een afhakelijkheid in de keten.
3. Ontwerpkader 3: **Organiseren van vulling van het register: aansluiten bij / uitbouwen van bestaande repository.** Eveneens in het verlengde van OK1, en dan geredeneerd vanuit onderwijsinstellingen: sluit voor de vulling van het register aan bij de vulling van al bestaande registers.

De beoogde resultaten van het register:

1. Doel 1: **Schaalbaar tot X berichten per jaar.** Onderdeel van de eisen aan de basisinfrastructuur voor het onderwijs is dat de componenten schaalbaar zijn. Voor de berichtuitwisseling in het primaire proces is hiervoor een norm afgesproken. Voor deze toepassing (secundair proces, bovendien bij clients goed cachebaar) geldt een lagere norm.
2. Doel 2: **De identiteit van ketenpartner kunnen vaststellen.** Dit is het belangrijkste doel van het service register voor het onderwijs.
3. Doel 3: **Het berichtverkeer verloopt met de gewenste vertrouwelijkheid en integriteit.** De mate van vertrouwelijkheid en integriteit van berichtuitwisseling is afhankelijk van de aard van die uitwisseling; het serviceregister zal de gewenste mate van vertrouwelijkheid en integriteit inventariseren en zijn processen en werkwijze hierop aanpassen.
4. Doel 4: **Het verzenden en de ontvangst van berichten is onweerlegbaar.** Onderdeel van de mate van integriteit en vertrouwelijkheid, kan onweerlegbaarheid voor bepaalde vormen van uitwisseling noodzakelijk zijn.
5. Doel 5: **Het serviceregister is onderdeel van de basisinfrastructuur van het onderwijs.** Daarmee past het streven naar een infrastructuur die hergebruik, beveiliging, interoperabiliteit mogelijk maakt.
6. Doel 6: **Het is mogelijk om de administratie van individuele onderwijsvolger te adresseren.** Er zijn instellingen met meerdere leerlingadministraties. Op basis van extra kenmerken zal het mogelijk zijn om te onderscheiden welke administratie een leerling bevat; op basis van deze informatie is het mogelijk om vertrouwelijke berichten op het juiste adres te bezorgen.
7. Doel 7: **Standaard werkwijzen kunnen hanteren om ambiguiteit in adressen te kunnen oplossen.** Het landschap van informatiesystemen in het onderwijs is divers en redelijk complex. Op basis van de informatie in het service register moet het mogelijk zijn om op basis van standaard werkwijzen altijd de juiste adressering te kunnen achterhalen.

De vraag of een dergelijk register centraal (landelijk, voor het hele onderwijs) of decentraal (opgedeeld naar bijvoorbeeld sector) moet worden onderverdeeld is afhankelijk van vragen zoals governance over de gegevens en op welke wijze de gewenste functionaliteit het best wordt ondersteund. Duidelijk is dat inrichting moet voldoen aan de ROSA principes over het wederzijds bieden van diensten, en het in samenhang beschikbaar maken van (informatie over) diensten.

# 

# 

# 7 Kwalitatieve eisen aan het OSR

Beveiligingseisen - opnemen van DUO servicegegevens (fase 2 in [Fasering en scope](#_b0c3sghj661t)) stelt randvoorwaarde BIR Rijk niveau Substantieel. Maatregelen hierin (<https://www.earonline.nl/images/earpub/5/5c/BIR_Operationele_Handreiking_v1_0.pdf> hoofdstuk 2.9) lijken niet buitensporig, komen behoorlijk overeen met normale beveiligde webapplicatie.

## 7.1 Complexiteit van adressering

In het streefbeeld is een uitvoerig overzicht gegeven over de aard van de communicatie- en berichtenstromen in het onderwijsveld, in combinatie met de huidige ontwikkelingen. De belangrijkste uitkomsten uit het streefbeeld zijn:

* Voor het onderwijs wordt gebruik gemaakt van het SaaS model (waarbij de onderwijsinstelling een service leverancier inschakelt om diensten te leveren en af te nemen namens de school, waarbij gebruik gemaakt wordt van het certificaat van de service leverancier).
* Voor de uitwisseling van M2M berichten wordt gebruik gemaakt van Edukoppeling, waarin eisen opgenomen zijn over unieke kenmerken (OINs) van de organisaties die deelnemen in de conversatie
* Er is een mandateringsrelatie tussen onderwijsinstelling en dienstleverancier, en deze relatie kan worden vastgelegd en inzichtelijk gemaakt.

Het streefbeeld zet hiermee een stap in de richting van eenduidige, veilige berichtuitwisseling in de onderwijsketen, maar hiermee zijn we er nog niet.

* Onderwijsinstellingen zijn organisaties met complexe interne inrichting. Instellingen zijn georganiseerd over meerdere lagen (normaal wordt onderscheid gemaakt in bestuur - instelling - vestiging), waarbij de wijze waarop de leerlingadministraties zijn verdeeld over de organisatie verschillende modellen kent.
* Serviceleveranciers exploiteren voorzieningen van diverse inrichting. Er zijn inrichtingen waarbij elke *tenant* zijn eigen (virtuele) omgeving heeft, en er zijn inrichtingen waarbij meerdere tenants in een omgeving zijn ondergebracht met logische scheidingen tussen de omgevingen.
* Unieke kenmerken van (onderwijs) organisaties, diensten en administraties zijn niet algemeen in gebruik.

Een serviceregister zal deze wereld op eenduidige manier in kaart brengen, waarbij ambiguiteiten (onderwijsinstelling kent meerdere leveranciers voor een dienst; leveranciers kunnen meerdere aanleverpunten voor services aanbieden) helder worden gemaakt en waarbij de invoering van extra kenmerken voor het uniek kunnen identificeren van diensten wordt ondersteund.

## 7.2 Autorisatie (muteren en raadplegen)

## 7.3 Integriteit van organisatie- en service kenmerken

## 7.4 Verwachte omvang en verwacht gebruik

# 

# 

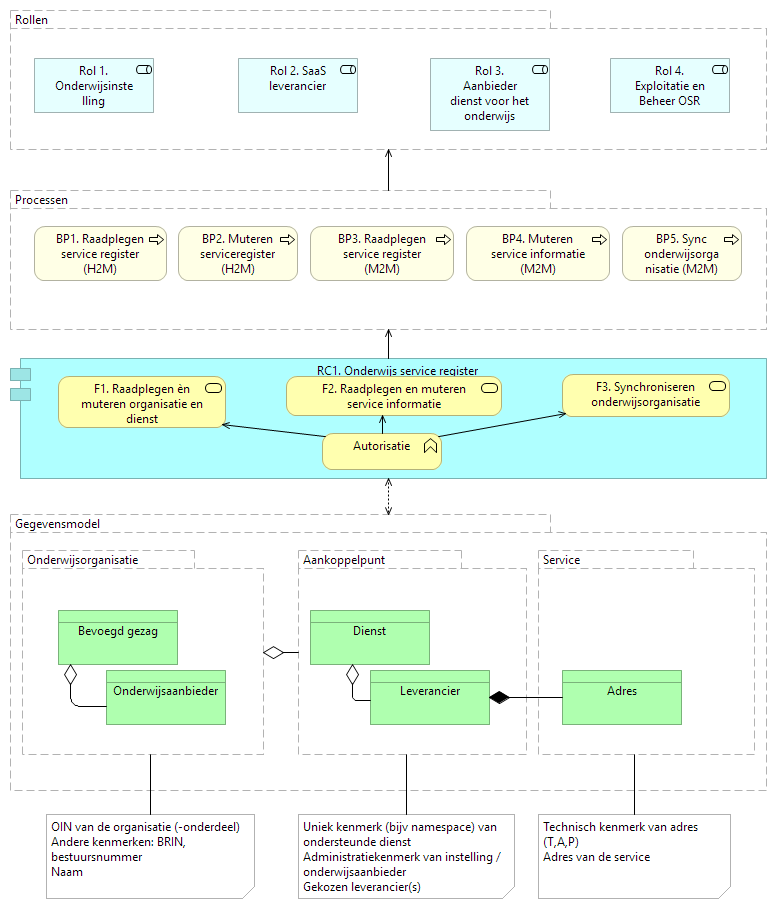
# 8 Concept realisatie

Het voorstel is om het service register voor het onderwijs te baseren op de huidige service register functionaliteit in OSO. In dit service register onderhouden al vrijwel alle VO scholen en een grote meerderheid van de PO scholen de serviceinformatie die nodig is voor het overstapdossier. Alle LAS leveranciers die actief zijn voor de PO- en VO-markt zijn aangesloten op het register van OSO.

Het nieuwe onderwijs service register wordt helemaal onafhankelijk van OSO en zal alle servicegegevens van OSO bevatten. Instellingen blijven hun gegevens onderhouden in MijnOSO, deze stuurt de relevante servicegegevens door naar het onderwijs serice register. OSO zelf wordt een afnemer van het register. Het onderwijs service register heeft nieuwe services en een nieuw koppelvlak waarmee de additionele functionaliteit kan worden gebruikt, maar heeft ook een adapter waar bestaande koppelingen op kunnen worden aangesloten en waarmee de OSO berichten kunnen worden afgehandeld.

De stappen die deze realisatie gaat volgen worden nu in concept uitgetekend. De gedachte is dat we hiermee in staat zijn om zowel de nieuwe gewenste functionaliteit te realiseren als, door aan te sluiten op een bekend en beschikbaar systeem, de administratieve overlast zoveel mogelijk te beperken.

# 9 Concept architectuur



Figuur 5: Concept architectuur van het onderwijs service register.

# 10 Bijlage: Huidige servicelandschap in het onderwijsveld

De gewenste ondersteuning van het serviceregister is afhankelijk van de wijze waarop diensten met hun afnemers communiceren. Afhankelijk van de aard van de dienst en de beschikbare mogelijkheden tijdens de realisatie zijn hier verschillende oplossingen gekozen. Als het servieregister een breed toepasbare (en toegepaste) dienst wil worden, is het daarmee relevant om zicht te krijgen op de wijze waarop diensten met hun afnemers communiceren.

In een korte analyse is van een representatief aantal services beschreven hoe ze communiceren. Hiervoor is gebruik gemaakt van een beschrijvingsmodel van G. Hohpe, “Conversation patterns”[[2]](#footnote-1) Een uitwisseling wordt beschreven aan de hand van de partijen en hun rollen, de soorten van berichten die worden uitgewisseld en de gebruikte protocollen. Daarnaast worden er een aantal focusgebieden (*focus areas*) beschreven waarmee de aard van een uitwisseling tussen dienst en afnemer kan worden beschreven met behulp van design patterns. De voor deze toepassing interessante focusgebieden zijn

1. **Ontdekken** (*discovery*). Voordat partijen met elkaar communiceren moeten ze elkaar kunnen vinden.
2. **Vaststellen** (*esablishing a conversation*). Als de partijen elkaar hebben geïdentificeerd, zullen de partijen elkaar authenticeren, autoriseren en andere parameters vaststellen voordat de feitelijke uitwisseling start.
3. **Converseren** (*Basic* en *multi-party conversations*). Welke communicatiepatronen worden gebruikt om berichten uit te wisselen, en hoe worden hierbij evt derde partijen ingezet

De resultaten van de analyse zijn samengevat in de volgende twee tabellen.

Tabel 1: Analyse van een aantal belangrijke diensten in het onderwijs, deel 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **status** | **partijen** | **berichten** | **protocol** |
| RIO | concept | LAS, ?: client; RIO: service | nnb | nnb |
| BRON VO | ontwerp | LAS: client, BRON: service. | XML berichten over SOAP. Bevatten PGN en andere persoonsgegevens | Request (LAS) - reply (BRON). BRON stuurt ook spontane berichten, n.a.v. eerdere requests LAS |
| Vroegtijdig aanmelden | ontwerp | SIS, LAS: client; Knooppunt: proxy; LAS, gemeente: service | XML berichten over SOAP. Bevatten PGN | spontane berichten, gerouteerd via koppelpunt (proxy). |
| Verzuim | productie | LAS: client, Verzuimloket: service | ? | ? |
| Examens Facet | productie | ? | ? | ? |
| OSO | productie | LAS ontvangende school: client, LAS latende school: service; TC: service | XML berichten over SOAP. Berichten bevatten PGN | Uitwisseling LAS - TC wordt gebruikt om overdracht dossier te kunnen doen |
| BPV | productie | SIS: client, SBB: service. SIS kan abonneren op wijzigingen | XML berichten over SOAP. Berichten bevatten geen persoonsgegevens. | Request (LAS) - reply (SBB). SBB stuurt ook spontane berichten, na abonnement LAS |
| UWLR | productie | EA: client, LAS: service | XML berichten over SOAP. Berichten bevatten pseudoniem en persoonsgegevens. | Uitwisseling leerlinggegevens: request (EA) - reply (LAS). Uitwisseling resultaten: Request (EA) - reply (LAS). |
| D&T services (catalog, contentlist, order, specify, license, activationcode) | productie | div client - service | XML berichten ovr SOAP. Sommige berichten bevatten pseudoniem en persoonsgegevens. | request - reply, diverse uitwisselingen |
| D&T Toegang | productie | leerling in ELO: client, EA: service, Entree fed: service | HTTP request. Bericht bevat pseudoniem. | request (ELO) - reply (EA) |

Tabel 2: Analyse van een aantal belangrijke diensten in het onderwijs, deel 2.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Ontdekken** | **Vaststellen** | **Converseren** |
| RIO | CONFIGURATIE | TOKEN (PKIO) | RR |
| BRON VO | CONFIGURATIE (las - BRON), CONSULTEER DIRECTORY + SERVICE KENMERK (BRON - las) | TOKEN (PKIO) | LRBT(2xRR) |
| Vroegtijdig aanmelden | CONFIGURATIE (client - proxy) en CONSULTEER DIRECTORY (proxy - bestemming) + SCATTER GATHER (bij meerdere aanleverpunten per school) | TOKEN (PKIO) | RR via PROXY |
| Verzuim | CONFIGURATIE | TOKEN (PKIO) | RR |
| Examens Facet | CONFIGURATIE | TOKEN (?) | RR |
| OSO | CONSULTEER DIRECTORY (ontvangende school - traffic center), SCATTER GATHER (bepaal afleverpunt latende school) | TOKEN (PKIO) + MANDATERING | RR |
| BPV | CONFIGURATIE + VERWIJZING (abonnement op wijzigingen) | TOKEN (PKIO) | RR, PUB-SUB (wijzigingen) |
| UWLR | CONFIGURATIE | TOKEN (eigen) | RR (leerlinggegevens), FF (resultaten) |
| D&T services (catalog, contentlist, order, specify, license, activationcode) | CONFIGURATIE | ? | RR |
| D&T Toegang | VERWIJZING (uit D&T Catalogservice) | SAML Authenticatie | RR |

De beschrijving in tabel 2 gebeurt aan de hand van *patterns*.

Ontdekken:

* CONFIGURATIE: De client beschikt over een configuratie met het adres van de service.
* CONSULTEER DIRECTORY: De client beschikt over een kenmerk van de dienst en zoekt aan de hand hiervan het adres van de service op
* SERVICE KENMERK: naast een kenmerk van de dienst beschikt de client over extra informatie (kenmerk) om in het geval van meerdere adressen te kunnen onderscheiden
* SCATTER GATHER: client stuurt verzoek naar meerdere adressen, verzamelt antwoorden
* VERWIJZING: De client beschikt over een verwijzing naar een specifiek adres uit een eerdere uitwisseling

Vaststellen:

* TOKEN: Client en / of service beschikken over eerder ingebrachte unieke kenmerken waarmee de identiteit kan worden vastgesteld
* MANDATERING: De service gaat na of de client door de onderwijsinstelling gemandateerd is om het verzoek te doen
* SAML Authenticatie: Partijen gebruiken SAML om informatie over identiteit van personen uit te wisselen

Converseren:

* RR: request - reply, client doet een verzoek (voor informatie, mutatie) aan server, en server beantwoordt dit verzoek
* FF: Fire and forget. Client stuurt bericht naar server, verwacht geen antwoord of antwoord is niet relevant.
* LRBT:
* PUB - SUB: publish - subscribe. Client abonneert zichzelf, server stuurt berichten volgens specificaties in abonnement (abonnement kan VERWIJZING bevatten waar berichten kunnen worden geadresseerd)

Het serviceregister zal een rol gaan spelen tijdens het ontdekken en vaststellen. Vroegtijdig aanmelden heeft hierbij behoefte aan ondersteuning voor het CONSULTEER DIRECTORY pattern aangevuld met SCATTER GATHER, hiermee is het mogelijk voor het serviceregister om meerdere adressen op te leveren. Er zijn geen speciale wensen voor het vaststellen bekend.

Kijkend naar mogelijke toekomstige uitbreidingen ontstaat het volgende beeld.

* BRON VO heeft behoefte aan een SERVICE KENMERK als onderdeel van de informatie; in de services en het gegevensmodel kan hier rekening mee worden gehouden.
* OSO (en wellicht nog meer diensten) gebruikt nu MANDATERING als onderdeel van het vaststellen van de relatie.
* Voor uitwisselingen waarvoor CONFIGURATIE en VERWIJZING wordt gebruikt, zal in eerste instantie geen service register nodig zijn maar het is niet uitgesloten; het is mogelijk om een kenmerk in de configuratie of verwijzing op te nemen waarmee een (altijd actueel!) adres in het service register kan worden opgezocht.

1. *Streefbeeld Veilige gegevensuitwisseling binnen de onderwijsketen v2017-09-29*. Dit streefbeeld is recent onder aansturing van OCW geactualiseerd en afgestemd met de sectorraden, HO-organisaties en de VDOD [↑](#footnote-ref-0)
2. *Conversation patterns: Interactions between loosely coupled services*. Gregor Hohpe, juni 2008; [www.eaipatterns.com](http://www.eaipatterns.com) [↑](#footnote-ref-1)