Programma van Eisen Onderwijs serviceregister

Kennisnet

Inhoud

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
0.4	19-1-2018	Marc Fleischeuers	Aanvullingen user stories input begeleidingegroep
0.5	31-1-2018	Marc Fleischeuers	WG Edukoppeling, Architectuurscan, BIV
0.6	23-2-2018	Marc Fleischeuers	Commentaar begeleidingsgroep

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 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] 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 precies beschreven, in combinatie met specifieke gebruiksdoelen (hier: functionele beheoften van project vroegtijdig aanmelden, OSO en BRON VO). 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 serviceregister 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 serviceregister levert, en waar deze diensten aan voldoen. Tegelijkertijd kunnen belanghebbenden nagaan wat het serviceregister voor hen kan betekenen.

[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

2.3 Lijst van begrippen

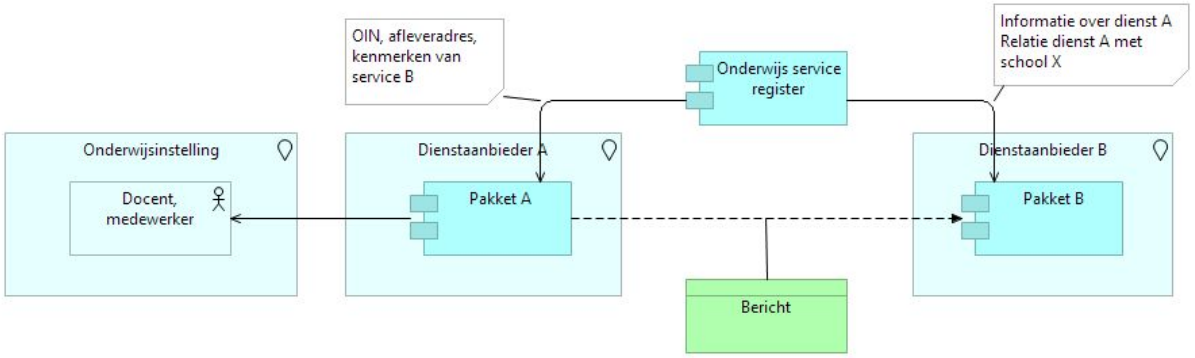
Onderstaande lijst beschrijft de specifieke betekenis van enkele termen in dit document. De definities zijn ontleend aan de Begrippenlijst van Edukoppeling[2] en waar nodig iets generieker gedefinieerd.

Begrip	Definitie
Aanleverpunt van een dienst	Virtuele locatie van een dienstaanbieder die een onderwijsinstelling heeft gekozen voor de levering van een of meer diensten. Een onderwijsinstelling kan meerdere dienstleveranciers voor een dienst, en daarmee ook meerdere aanleverpunten hebben. De onderwijsinstelling voorziet het aanleverpunt van een uniek kenmerk.
Afleveradres van een aanleverpunt	Een digitaal adres (url) waarop de dienst bereikbaar is. Een aanleverpunt kan over meerdere afleveradressen beschikken. Elk afleveradres is voorzien van een (per aanleverpunt) uniek kenmerk.
Autorisatie	Toestemming om bepaalde functionaliteit te mogen gebruiken. De toestemming wordt verleend door een autoriteit bijvoorbeeld de eigenaar van de functionaliteit.
Betrouwbaarheid	Mate van zekerheid waarmee een dienst wordt uitgevoerd. Wordt uitgedrukt in termen van beschikbaarheid, integriteit en vertrouwelijkheid.
Dienst	Verzameling samenhangende (digitale) activiteiten die een dienstaanbieder beschikbaar stelt aan een opdrachtgever. Zie ook service.
Dienstaanbieder	Partij die (digitale) diensten levert. In de context van het onderwijs kan dit een externe, private of publieke partij zijn, maar het kan ook een onderwijsinstelling zijn.
Edukoppeling	Standaard voor betrouwbare berichtuitwisseling voor het onderwijs, gebaseerd op Digikoppeling. Bestaat uit koppelvlakspecificatie en architectuur.
Mandatering	Relatie tussen dienst en dienstaanbieder, gelegd door de opdrachtgever, opdat de dienstaanbieder voor deze dienst namens de opdrachtgever kan optreden.
Onderwijsinstelling	Organisatie die onderwijsdiensten levert en daarvoor diensten van dienstaanbieders afneemt.
Pakket	Softwaresysteem dat een dienst levert
Partij	(Publieke) organisatie aangesloten op het onderwijs serviceregister die diensten aanbiedt aan andere organisaties of afneemt van andere organisaties.
Service	Uitwisseling van berichten in het kader van een dienst.
Serviceaanbieder	Partij die een servide aanbiedt
Serviceafnemer	Partij die een service afneemt

[2] *Edukoppeling - Begrippen v1.0*, werkgroep Edukoppeling, https://www.edustandaard.nl/app/uploads/2017/07/2017-07-05-Edukoppeling-Begrippen-versie-1.0.pdf

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.



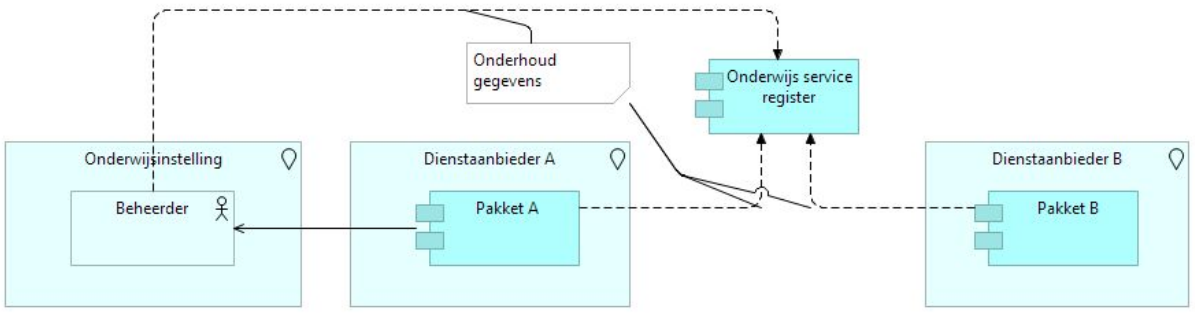
Figuur 1: Illustreert het serviceregister in gebruik.

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

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

Een variant van deze situatie waarbij de onderwijsinstelling ‘on premise’ systemen gebruikt werkt analoog hieraan. In deze situatie is de onderwijsinstelling zijn eigen dienstaanbieder.

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 een beheerder aangeeft welke dienstaanbieders door de onderwijsinstelling gekozen zijn om hun diensten aan te bieden. Vervolgens zullen deze aanbieders 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 serviceregister.

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 serviceregister zal gebruikt worden door drie diensten: Vroegtijdig aanmelden, OSO Traffic center en BRON VO. Deze diensten hebben behoefte aan
    - Identificerende gegevens (BRIN, OIN), en naam van onderwijsinstellingen.
    - Kenmerken en adresgegevens van diensten in het kader van Vroegtijdig aanmelden, OSO en BRON VO die dienstaanbieders (LAS- en SIS leveranciers) namens de onderwijsinstellingen aanbieden.
    - Informatie over de relatie tussen onderwijsinstelling en dienstaanbieder (mandateringsrelatie).

  Identificerende gegevens van onderwijsinstellingen zullen worden ontleend aan RIO, het OIN register van Logius en andere authentieke bronnen. Het OSR is zelf niet de bron van deze gegevens. Partijen gebruiken de gegevens ten behoeve van het adresseren en routeren van berichtverkeer en voor autorisatie van binnenkomende berichten. Zie 5 Functionele wensen 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 serviceregister wordt opgenomen.

- **Fase 2: Uitbreiding naar 'alle' diensten en dienstaanbieders.** Bij de tweede iteratie van het serviceregister wordt het register opengesteld voor andere diensten en dienstaanbieders. Waar organisatiegegevens en -kenmerken voor onderwijsinstellingen afkomstig zijn uit RIO, zullen de organisatiegegevens en -kenmerken (o.a. het OIN) voor dienstverleners ofwel worden betrokken uit het OIN register (indien beschikbaar) of door de dienstverlener zelf ingevoerd. Voor deze iteratie wordt geen uitbreiding in de functionaliteit voorzien; het register legt hetzelfde type gegevens vast en ondersteunt dezelfde typen berichten en bevragingen als in fase 1.

- **Fase 3: Betrouwbare berichtuitwisseling van dienstverleners.** Belangrijke uitbreiding in deze iteratie is dat de publieke sleutels van alle dienstaanbieders in het register worden opgenomen. Hiermee zal het serviceregister geencrypt berichtverkeer van dienstverleners naar onderwijsinstellingen ondersteunen. Bevragingen aan het register worden uitgebreid met bevragingen naar de publieke sleutel, en resultaatgegevens zijn uitgebreid met een veld voor de publieke sleutel.

  NB de manier waarop publieke sleutels in het gegevensmodel worden toegevoegd is nog niet bekend, onderdeel van deze fase is een analyse van het beoogd gebruik. Er zijn al enkele user stories over deze fase opgenomen, ter illustratie van de functionele wensen.

- **Fase 4: Betrouwbare berichtuitwisseling van onderwijsinstellingen.** 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 alle partijen in het onderwijs worden ondersteund.

  Het zal nog nader worden onderzocht of het mogelijk is om het publieke certificaat van de onderwijsinstelling onderdeel kan worden van de gegevensset van RIO, of dat deze gegevens in het serviceregister worden ondergebracht.

- **Uitbreiding: internationaal.** Enigszins onafhankelijk van bovenstaande fasering is de uitbreiding van het serviceregister 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: end to end toegang en autorisatie

De hier beschreven functionaliteit van het serviceregister 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 Gegevens en zeggenschappen

Het serviceregister zal vier centrale gegevenselementen bevatten:

- **Organisatie** inclusief kenmerken (o.a. OIN).
    - Voor onderwijsinstellingen is dit informatie over het bestuur en over de instellingen die onder dit bestuur vallen, inclusief de formele en informele kenmerken van bestuur en instelling zoals BRIN en OIN[3]. Voor onderwijsinstellingen wordt deze informatie betrokken van RIO indien beschikbaar, en anders van de bestuur- en instellingsgegevens die DUO publiceert.
    - Voor andere partijen (privaat en publiek) die vanaf Fase 2 worden opgenomen in het register zijn dit gegevens overgenomen uit het HRN, het OIN register inclusief het OIN van de partij. Als een dergelijk register niet beschikbaar is, kan de partij in het uiterste geval de gegevens zelf ingeven.
- **Diensten en dienstaanbieders**. Betreft de lijst van diensten en dienstaanbieders waarvoor het register de registratie kan verwerken. Digitale diensten worden geïdentificeerd aan de hand van een uniek kenmerk (bijv een namespace) uit de technische beschrijving van de dienst.
- **Aanleverpunt**. Toegangspunt dat ontstaat in de combinatie van een dienst en een dienstaanbieder, die een onderwijsinstelling heeft gekozen het leveren van de dienst. Onderwijsinstellingen kunnen meerdere dienstaanbieders gebruiken voor dezelfde dienst. Elk aanleverpunt heeft een uniek kenmerk, dat geregistreerd wordt in het serviceregister.
- **Afleveradres**. Technisch adres waarop de specifieke dienst van de dienstaanbieder beschikbaar is. Een dienstaanbieder kan de dienst koppelen aan meerdere afleveradressen. Elk afleveradres heeft een uniek kenmerk, dat geregistreerd wordt in het serviceregister.

Daarnaast zijn er vier soorten gebruikers die het OSR zullen gebruiken:

- **Onderwijsinstelling**. Beheert zijn aanleverpunten in het OSR zodat de berichtuitwisseling met externe partijen betrouwbaar is.
- **Dienstaanbieder**. Beheert de afleveradressen van de diensten die hij levert aan onderwijsinstellingen, zodat partijen de diensten kunnen vinden.
- **Partij**. Wil berichten uitwisselen met onderwijsinstelling, heeft informatie nodig over afleveradres, aanleverpunt, dienstaanbieder om dit betrouwbaar te kunnen doen.
- **Beheerder OSR**. Verantwoordelijk voor een betrouwbare serviceregister en betrouwbare informatie in het register.

De zeggenschappen over deze gegevenstypen voor elk van de gebruikers zijn weergegeven in onderstaande tabel.

Tabel 1: Gegevenstypen en zeggenschappen

	Gegeven			
	Diensten en dienstaanbieders	**Aanleverpunt + kenmerk(en)**	**Afleveradres + kenmerk(en)**	**Organisatie + OIN**
Registreren	Beheerder OSR	Onderwijsinstelling	Dienstaanbieder	RIO (onderwijsinst), dienstaanbieder
Vernietigen	Beheerder OSR	Onderwijsinstelling	Dienstaanbieder	RIO (onderwijsinst), dienstaanbieder

[3] DUO is sectoraal beheerder van OIN's voor onderwijsinstellingen. Voor zover bekend worden de OIN's van onderwijsinstellingen echter nog niet gepubliceerd.

Beschikbaar stellen	Beheerder OSR	Beheerder OSR	Beheerder OSR	Beheerder OSR
Accorderen uitwisseling	nvt	nvt	nvt	nvt
Inzien	Partij	Partij	Partij	Partij
Inwinnen	nvt	Partij	Partij	Partij
Corrigeren	Beheerder OSR	Onderwijsinstelling	Dienstaanbieder	RIO (onderwijsinst), dienstaanbieder

5 Functionele wensen

5.1 Bevragingen van het serviceregister

FR.1	**Opvragen OIN van een onderwijs instelling**
Als …	partij die een bericht naar een dienst 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

Toelichting

- Het OIN van een onderwijsinstelling is een parameter die noodzakelijk is in berichtverkeer op basis van Edukoppeling. Een onderwijsorganisatie is in diverse registers geregistreerd, en kan mogelijk over meerdere OINs beschikken (bijvoorbeeld gebaseerd op BRIN en op HRN nummer).
- De OIN van een organisatie is een stabiel gegeven. De verwachting is dat dit zelden wijzigt, en afnemers moeten er van uit kunnen gaan dat de gevraagde gegevens langere tijd geldig zijn. Voorstel is om het serviceregister deze resultaten voorziet van een verwachte levensduur (TTL, time to live) van een week. Op basis hiervan zou de afnemer deze gegevens gedurende minstens een week in een eigen cache bewaren.

Specifieke variant
Als koppelpunt voor het VO wil ik het BRIN afkomstig uit aanmeldberichten van MBO instellingen vertalen naar het OIN dat gevoerd wordt door de geadresseerde VO instelling, zodat ik dit bericht volgens Edukoppeling kan adresseren aan de VO instelling.

FR.2	**Routering naar dienst van een onderwijsinstelling**
Als …	partij die een bericht naar een dienst 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

Toelichting

- Deze user story beschrijft zowel de situatie waarin de partij die het adres opzoekt informatie wil leveren aan de onderwijsinstelling, als de situatie dat deze partij een verzoek stuurt om informatie van de instelling wil ontvangen. De activiteit om een afleveradres op te zoeken is in beide situaties gelijk.
- Afleveradressen zijn redelijk stabiel gedurende een schooljaar, maar te laat bijgewerkte afleveradressen leiden onvermijdelijk tot haperend berichtverkeer. Voorstel is om deze gegevens aan een verwachte levensduur (TTL) te koppelen. Hiermee kan een afnemer deze gegevens gedurende minstens deze periode in de eigen cache bewaren.

Specifieke variant

1. Als ‘thuis’ instelling van studenten die aan meerdere onderwijsinstellingen vakken volgen, wil ik in het onderwijs serviceregister de adressen opzoeken van de gastinstellingen, waar ik een

verzoek voor het ophalen van (vastgestelde) resultaten voor mijn studenten kan afleveren (MBO, HO).
2. Als samenwerkingsverband wil ik de lijst met adressen en url's van mijn PO scholen actueel kunnen houden, zodat ik mijn berichten altijd goed kan adresseren.

FR.3	**Routering naar dienst binnen onderwijsinstelling op basis van kenmerk**
Als …	partij die een bericht naar een uniek geidentificeerd adres van een dienst 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, al dan niet geleverd in de vorm van een SaaS dienst, die elk een deel van hun leerlingbestand bevatten. Elke deeladministratie kan meerdere afleveradressen voeren (zie 10.1 Complexiteit van adressering voor een uitgebreidere toelichting).

  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. Door gebruik te maken van een extern register met aanleverpunten en adressen is de koppeling tussen systemen bestand tegen wijzigingen in afleveradressen van die systemen. De veronderstelling hierbij is dat de unieke kenmerken van de aanleverpunten persistent blijven ook als de onderliggende dienstaanbieder wijzigt.

  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 serviceregister. 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.

Specifieke variant

Als BRON wil ik het internetadres weten van een leerlingadministratie ingericht door een onderwijsinstelling of diens SAAS-leverancier, omdat ik een elektronisch bericht met gevoelige gegevens over een leerling wil versturen aan de specifieke administratie die deze leerling beheert ter verwerking door de onderwijsinstellling.

FR.4	**Mandatering van het bevragende systeem**
Als …	systeem 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. Dit is (deel van) het autorisatievraagstuk van een dienstverlener; het is aan de dienstverlener zelf om te bepalen hoe de afhandeling plaatsvindt van een binnenkomend bericht waar geen mandateringsrelatie voor is.

Specifieke variant

1. Als BRON wil ik de identiteit van de onderwijsinstelling die een service aanvraagt met zekerheid vaststellen, omdat die, bijvoorbeeld uit privacy-optiek, alleen toegankelijk is voor gekende onderwijsinstellingen of hun SAAS-leverancier. (alle sectoren)
2. Als (VO, PO) school wil ik nagaan of een verzoek voor een overstapdossier van een van mijn leerlingen verstuurd is door een dienstleverancier die door de ontvangende school hiervoor gemandateerd is.
3. Als partij die diensten voor buitenschoolse activiteiten voor PO scholen levert, wil ik na kunnen gaan of een binnenkomend verzoek verzonden is door een dienstleverancier die gemandateerd is door een PO school waar ik een overeenkomst mee heb

5.1.1 Uitbreiding fase 3 (Veilige communicatie)

FR.30a	**Opvragen van publieke certificaat van ketenpartner**
Als …	systeem dat een bericht met gevoelige inhoud wil sturen naar een ketenpartij
Wil ik …	de publieke sleutel van de ketenpartij in het serviceregister kunnen raadplegen
Zodat …	ik dit bericht kan versleutelen met mijn eigen private sleutel en de publieke sleutel van de ketenpartij en onze communicatie met het gewenste niveau van vertrouwelijkheid kan plaatsvinden

FR.30b	**Opvragen van publieke certificaat van ketenpartner**
Als …	systeem dat een versleuteld bericht ontvangt van een ketenpartij
Wil ik …	de publieke sleutel van de ketenpartij in het serviceregister kunnen raadplegen
Zodat …	ik het versleutelde bericht kan ontsleutelen met mijn eigen private sleutel en de publieke sleutel van mijn ketenpartij en wij op deze manier met het gewenste niveau van vertrouwelijkheid berichten kunnen uitwisselen

Toelichting
Deze fase in de roadmap ondersteunt de infrastructuur om end-to-end versleuteling tussen ketenpartijen (onderwijsinstellingen en leveranciers) te realiseren. De user stories beschrijven de functionaliteit die hiermee gerealiseerd wordt.

Specifieke variant
Als BRON wil ik de publieke sleutel van mijn ketenpartners kunnen raadplegen, omdat ik uitgaand verkeer wil versleutelen en van inkomend verkeer de handtekening wil controleren

5.2 Onderhoud van de informatie in het register

OR.1	**Opgeven van aanleverpunten van diensten**
Als …	bevoegde medewerker van een onderwijsinstelling
Wil ik …	aangeven welke dienstleverancier(s) ik heb gekozen voor het leveren van diensten, en het kenmerk dat ik aan deze keuze wil koppelen
Zodat …	deze leverancier berichten namens mij kan versturen en ontvangen

OR.2	**Wijzigen en verwijderen van aanleverpunten van diensten**
Als …	bevoegde medewerker van een onderwijsinstelling
Wil ik …	de door mij gekozen dienstleverancier en mijn kenmerk wijzigen of verwijderen in het serviceregister, zonder dat ik hierbij de leverancier of zijn programmatuur nodig heb
Zodat …	ik berichtverkeer door de door mij gekozen dienstleverancier kan versturen en ontvangen

Toelichting

- Deze story's beschrijven het onderhoud aan aanleverpunten. De onderwijsinstelling wijzigt of verwijdert aanleverpunten en moet dit kunnen doen zonder hierbij afhankelijk te zijn van de medewerking van de dienstleverancier en diens programmatuur. Dit betekent dat het register zijn eigen toegangsportaal (website) hiervoor moet inrichten, en identificatie en autorisaties van de medewerkers van onderwijsinstellingen zal onderhouden.
- Een onderwijsinstelling kan meerdere aanleverpunten voor een dienst opgeven, en hiervoor dezelfde dienstleverancier of verschillende dienstleveranciers kiezen.
- Als de bevoegde medewerker een aanleverpunt verwijdert, worden alle afleveradressen gekoppeld aan dat aanleverpunt mee verwijderd.

OR.3	**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

Toelichting

- Deze story beschrijft het onderhoud aan toegangsadressen (URL's) van digitale diensten die gekoppeld zijn aan de aanleverpunten. Dit onderhoudt vindt plaats vanuit de programmatuur van de gekozen dienstverlener (zie OR.1, OR.2). Het OSR autoriseert de dienstverlener aan de hand van het aanleverpunt: alleen de door de onderwijsinstelling gekozen dienstverlener kan de adressen wijzigen. Dienstverleners worden geïdentificeerd aan de hand van het OIN in het PKIo-certificaat.

OR.4	**Onderhoud van gegevens afkomstig van externe partijen**

Als …	Beheerder van het onderwijs serviceregister
Wil ik …	gegevens betrokken van externe partijen (DUO, Handelsregister) kunnen bijwerken en de integriteit van de gegevens in het serviceregister hierbij in stand houden
Zodat …	alle adressen altijd bij een in het register bestaand aanleverpunt horen en alle aanleverpunten gekoppeld zijn aan on het register bestaande dienstleveranciers, diensten en onderwijsorganisaties

Toelichting

- Deze story ziet er op toe dat de gegevensintegriteit in het register in stand blijft. De organisatie van onderwijsinstellingen en dienstverleners is voortdurend aan veranderingen onderhevig. Het kan bijvoorbeeld voorkomen dat onderwijsinstellingen verdwijnen; bijbehorende aanleverpunten en adressen kunnen dan niet meer gebruikt worden.

OR.5	**Rapportage over de integriteit van het register**
Als …	Beheerder van het onderwijs serviceregister
Wil ik …	een overzicht over de integriteit van de relaties in het register
Zodat …	ik actie kan ondernemen op verweesde aanleverpunten, adressen en gebruikers

Toelichting

- Het zal voorkomen dat een onderwijsinstelling of een bestuur verdwijnt bij een synchronisatie terwijl er nog aanleverpunten en bijbehorende adressen aan zijn gekoppeld. In de praktijk zal het er vaak op neerkomen dat de diensten en verplichtingen van een organisatie worden overgedragen aan een andere organisatie, en dat zal ook voor de digitale dienstverlening gelden. In deze situaties is het van belang om de administratieve werkelijkheid weer in lijn te brengen met de echte werkelijkheid, door de geregistreerde aanleverpunten te integreren bij de organisatie die de dienstverlening overneemt. Dit is naar verwachting een handmatige actie. Deze user story is bedoeld om inzichtelijk te maken op welke aanleverpunten en adressen er actie moet worden ondernomen.
- Accounts van gebruikers die gegevens van hun instelling kunnen inzien en muteren, worden inactief gemaakt als de instelling of het bestuur waar ze aan gekoppeld zijn verdwijnen. De medewerkers van de onderwijsinstelling kunnen eventueel een nieuw account laten aanmaken als ze aan een nieuwe instelling zijn gekoppeld.

OR.6	**Hanteren van 4-ogen principe voor mutaties aanleverpunten configureren**
Als …	dienstaanbieder van diensten in het serviceregister
Wil ik …	kunnen aangeven dat mutaties in aanleverpunten en afleveradressen die zijn aangebracht moeten worden goedgekeurd door mijn medewerkers voordat ze worden gepubliceerd
Zodat …	ik een kans heb om eventuele fouten en verkeerde instellingen te verwerpen voordat ze worden gepubliceerd

OR.7	**Mutaties aanleverpunten goed- of afkeuren**
Als …	dienstaanbieder van diensten in het serviceregister

Wil ik …	mutaties in aanleverpunten en afleveradressen die onderwijsinstellingen hebben opgegeven, publiceren of afwijzen
Zodat …	ik zeker weet dat ik de geregistreerde informatie over mijn diensten overeenkomstig de werkelijkheid is

Toelichting

- Deze user story geeft aan dat het mogelijk is om een vier-ogen principe te hanteren bij het beschikbaar maken van gegevens. Dit is een maatregel die beoogt de kwaliteit van de geregistreerde gegevens te verhogen, en is van toepassing op diensten waarbij gevoelige gegevens worden uitgewisseld. De dienstaanbieder (bijv OSO, BRON) geeft aan dat dit van toepassing is. Medewerkers van de dienstaanbieder hebben toegang tot het reigster, zien welke wijzigingen er door de onderwijsinstelling zijn aangepast voor hun dienst en kunnen deze wijzigingen goedkeuren of verwerpen. Bij goedkeuring wordt een wijziging gepubliceerd en is beschikbaar voor alle partijen. Bij verwerping wordt de wijziging niet doorgevoerd (nice to have: opgave redenen, bericht terug naar onderwijsinstelling).

OR.8	**Beheer van diensten**
Als …	beheerder van het onderwijs serviceregister
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

OR.9	**Beheer van autorisaties**
Als …	beheerder van het onderwijs serviceregister
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

5.2.1 Uitbreiding fase 2 (Dienstaanbieders)

OR.20	**Onderhoud van organisatie-informatie van dienstverleners**
Als …	leverancier van diensten aan onderwijsinstellingen
Wil ik …	mijn organisatie-informatie en formele kenmerken zoals OIN kunnen beheren
Zodat …	de informatie van mijn organisatie beschikbaar is voor andere partijen in de onderwijsketen

Toelichting

De organisatie-informatie van onderwijsinstellingen is afkomstig uit RIO en wordt niet door instellingen beheerd in het onderwijs serviceregister. Voor dienstverleners ligt dat anders. Informatie over de organisatie van dienstverleners kan (deels) afkomstig zijn uit een externe bron eventueel in combinatie met beheer in het serviceregister. Dit betekent dat het register zijn eigen toegangsportaal (website)

hiervoor moet inrichten, en identificatie en autorisaties van de medewerkers van dienstverleners zal onderhouden.

5.2.2 Uitbreiding fase 3 (Veilige communicatie)

OR.30	**Publiceren van publieke sleutels**
Als …	partij die informatie in het register beschikbaar stelt
Wil ik …	mijn publieke sleutel kunnen publiceren
Zodat …	ik mijn berichtverkeer met andere partijen met de gewenste mate van vertrouwelijkheid en integriteit kan uitvoeren

Toelichting
Deze user story beschijft dat een organisatie zijn publieke sleutel beschikbaar maakt. Deze story kan voor elk type organisatie gelden, zowel voor onderwijsinstellingen als voor dienstaanbieders.

6 Principes en maatregelen

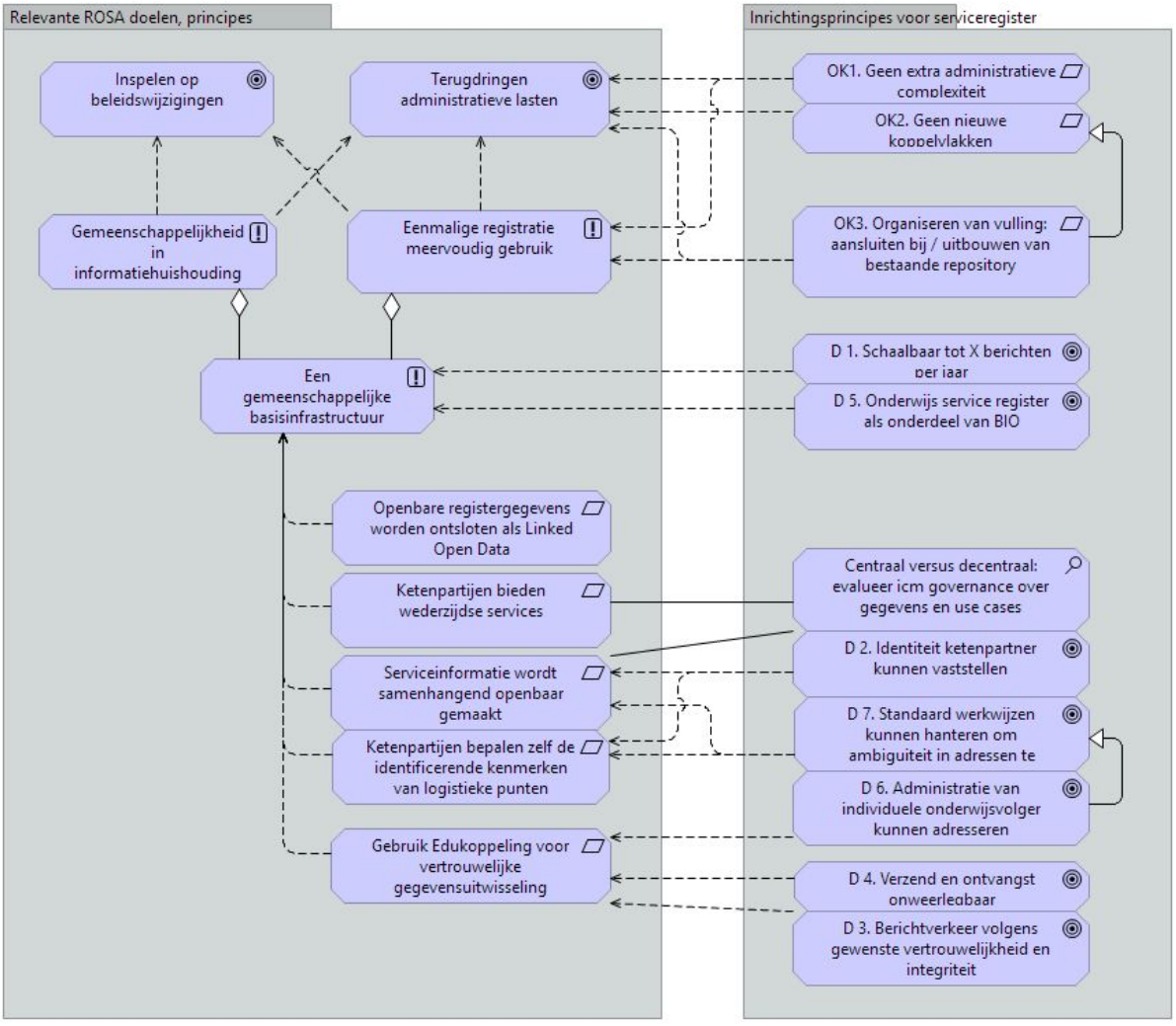
Het serviceregister heeft een ondersteunende rol bij het uitvoeren van interoperabiliteitsdiensten met als kern het inwinnen, beheren en ter beschikking stellen van informatie over diensten, webservices en organisatie-kenmerken van aanbieders en afnemers van deze diensten. Het serviceregister heeft geen 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 3.



Figuur 3: Overzicht van relevante doelen, principes en afspraken uit ROSA, en daaruit afgeleide afspraken en beoogde resultaten voor het onderwijs serviceregister

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:

3. Principe: gemeenschappelijkheid in informatiehuishouding
4. Principe: eenmalige registratie, meervoudig gebruik
5. Principe: een gemeenschappelijke basisinfrastructuur

De daaruit afgeleide ontwerpkaders zijn

6. Ontwerpkader: openbare registergegevens worden ontsloten als linked open data
7. Ontwepkader: ketenpartijen bieden wederzijdse services
8. Ontwerpkader: serviceinformatie wordt samenhangend openbaar gemaakt
9. Ontwerpkader: ketenpartijen bepalen zelf de identificerende kenmerken van logistieke punten
10. Ontwerpkader: gebruik Edukoppeling voor vertrouwelijke gegevensuitwisseling

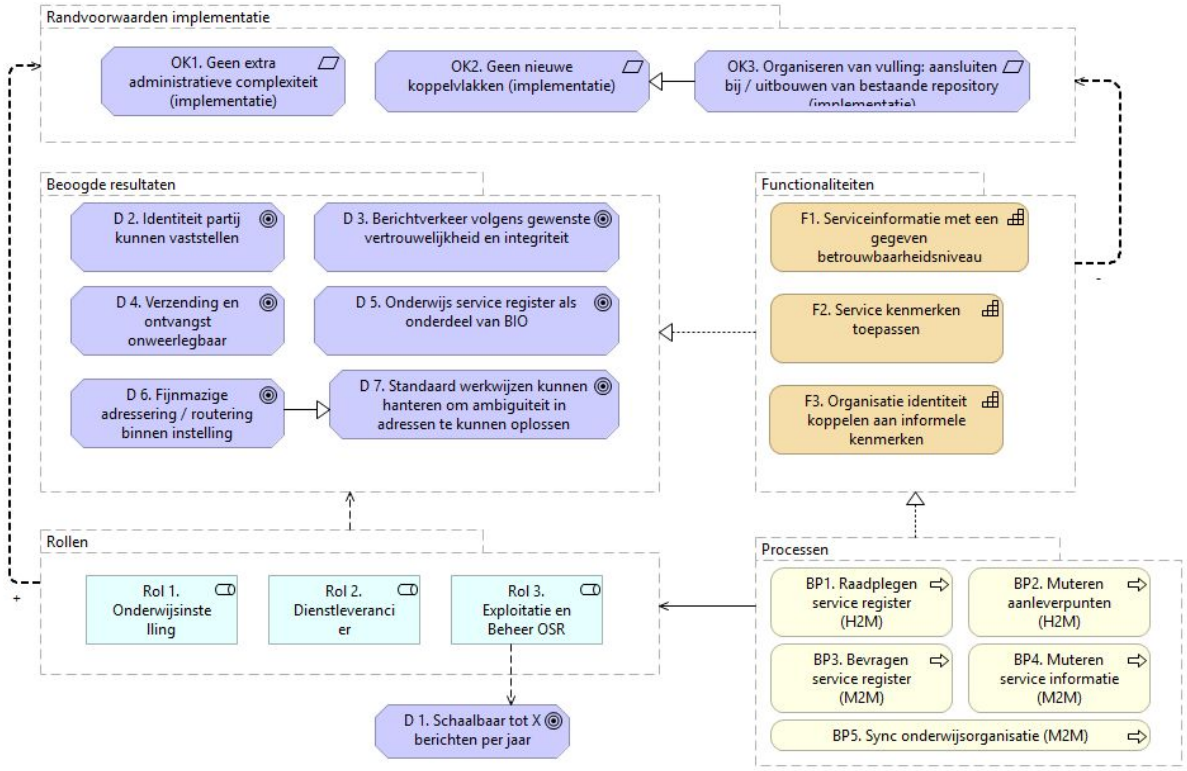
De beoogde resultaten van het register:

1. Doel 1: **Schaalbaar tot meer dan 500k bevragingen per dag.** 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, zie 7.4 Verwachte omvang en verwacht gebruik voor inschattingen voor de gewenste schaalbaarheid.
2. Doel 2: **De identiteit van ketenpartner kunnen vaststellen.** Dit is het belangrijkste doel van het serviceregister 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. Zie 7.5 BIV Classificatie en maatregelen voor inschattingen van de gewenste mate van vertrouwelijkheid en integriteit.
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 serviceregister 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.

Randvoorwaarden voor de implementatie van het serviceregister zijn gesteld door onderwijsorganisaties en dienstaanbieders. Deze partijen dringen aan op verlaging van de operationele lasten en op vermindering van de ondehoudslasten van systemen.

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.



Figuur 4: Analyse van belanghebbenden en belangen

Om de gewenste resultaten allemaal te kunnen ondersteunen, moet het serviceregister gaan beschikken over drie functionaliteiten die nu niet beschikbaar zijn in bestaande registers. Dit zal er bij de implementatie toe leiden dat niet overal aan de gestelde randvoorwaarden kan worden voldaan.

1. Functionaliteit 1: **Service informatie wordt met een specifiek betrouwbaarheidsniveau vastgelegd**. Deze functionaliteit bepaalt in hoeverre de veiligheid betreffende resultaten Res1, Res2, Res3 opgaan. In de praktijk is het vastleggen van de service informatie nu per dienst ingericht, en elke dienst hanteert zijn eigen normen voor de kwaliteit van de vastgelegde gegevens.

   Bij de implementatie van het register verwachten we dat er een verschuiving optreedt, van een registratie per dienst naar eenmalige registratie en meervoudig gebruik in het serviceregister. Echter, gezien het grotere belang dat meervoudig gebruik kan vragen, kan het zijn dat deze centrale administratie complexer wordt.

2. Functionaliteit 2: **Service kenmerken toepassen**. Dit is een van de standaard werkwijzen om ambiguiteit in adressen te kunnen oplossen (zie 5.1 Bevragingen van het serviceregister), en de gewenste oplossing voor BRON VO om de administraties van individuele onderwijsvolgers te kunnen adresseren.

   Op dit moment zijn de diensten waarbij deze functionaliteit noodzakelijk is nog beperkt: OSO heeft een eigen variant gemaakt, en de nieuwe diensten BRON VO en Vroegtijdig aanmelden hebben een serviceregister hiervoor nodig. Als deze manier van routeren en adresseren een reguliere werkwijze wordt, zal elke dienstaanbieder zijn diensten hierop moeten aanpassen.

3. Functionaliteit 3: **Organisatiekenmerken koppelen aan informele kenmerken**. Op basis van deze functionaliteit is het bijvoorbeeld mogelijk om een OIN te vinden op basis van een BRIN. Verwachte gebruiksscenario's zijn analoog aan functionaliteit 2, en treden op bij uitwisselingen van onderwijsinstelling naar onderwijsinstelling.

7 Kwalitatieve eisen aan het OSR

7.1 Autorisatie (muteren en raadplegen)

Het serviceregister zal geen persoonsgegevens bevatten, alleen informatie over diensten, hun kenmerken en toegangsadressen. Toch kan dit ook informatie met een zekere gevoeligheid zijn. Er worden twee maatregelen genomen om de toegang tot de gegevens te beperken:

- Het serviceregister zal toegang *beperken tot geautoriseerde organisaties*. De drempel voor autorisatie wordt laag, het register heeft immers tot doel om de gegevensuitwisseling te bevorderen.
- Mogelijke bevragingen zijn *doelgericht*. Services worden zodanig ingericht dat het makkelijk is om vragen naar routering en mandatering te stellen, en dat het niet makkelijk is om alle informatie uit het register systematisch te kopieren.

De dienst wordt zowel voor bevragingen als voor mutaties op basis van berichtverkeer (dwz de API) ontsloten via Edukoppeling. Voor identificatie van de aansluitende partij wordt gebruik gemaakt van het OIN dat onderdeel is van het certificaat.

Voor mutaties zal het register ook een eigen user interface in de vorm van een website hebben, hiervoor is Edukoppeling niet van toepassing. Voor de beveiliging van het transport wordt een met Edukoppeling equivalent beveiligingsniveau geconfigureerd. Voor identificatie van de gebruiker moet een identificatiemiddel worden gekozen. De verwachting is dat dezelfde medewerkers van onderwijsinstellingen zowel de mutaties in RIO als in het serviceregister uitvoeren. Handmatige mutaties in RIO worden doorgevoerd vanuit het zakelijk portaal van DUO. Medewerkers van onderwijsinstellingen loggen hier in met behulp van een door DUO uitgegeven token als tweede factor. Het is aan te bevelen dat het serviceregister hierbij aansluit indien mogelijk. Vanuit de eisen voor vertrouwelijkheid (zie 7.6 BIV Classificatie en maatregelen) wordt in elk geval een authenticatie met een tweede factor vereist.

7.2 Integriteit van organisatie- en service kenmerken

De maatregelen van onderdeel ‘Integriteit’ (7.5 BIV Classificatie en maatregelen) worden doorgevoerd.

7.3 Toegang en beveiliging

Het serviceregister heeft een website waar medewerkers van onderwijsinstellingen wijzigingen kunnen doorvoeren, en een service-interface (API) waar informatie kan worden opgevraagd en mutaties kunnen worden doorgegeven. Voor beide kanalen wordt een toegangsbeveiliging ingericht die proportioneel is voor het beoogde gebruik. Het normenkader van het Certificeringsschema is van toepassing (zie 7.6 BIV Classificatie en maatregelen) en waar toepasselijk worden de maatregelen geformuleerd uit de Basline informatiebeveiliging Rijk (https://www.earonline.nl/images/earpub/5/5c/BIR_Operationele_Handreiking_v1_0.pdf) gevolgd. Specifiek geldt:

- Toegang tot de service-interface (koppelvlak) is beveiligd met Edukoppeling (de laatste versie die door de standaardisatieraad is goedgekeurd).
    - De informatie in het serviceregister zal cruciaal zijn voor alle partijen in de educatieve keten. Partijen moeten beschikken over een aansluiting op Edukoppeling, maar verder zullen er geen drempels worden opgeworpen voor partijen die willen aansluiten.
- De website is voorzien van aan Edukoppeling equivalente transportbeveiliging (https)

7.4 Verwachte omvang en verwacht gebruik

De verwachte omvang van het serviceregister, dat wil zeggen het aantal koppelpunten en adressen dat er is geregistreerd, kan op basis van een aantal aannames worden ingeschat. De inschattingen

hierbij gaat over 1. de initiële vulling en gebruik van het register, 2 een minimale variant die vanaf fase 2 in productie draait, en 3. een variant waarbij alle instellingen en diensten maximaal gebruik maken van het systeem.

- Aantal ondersteunde diensten: initieel 3, minimaal 10, maximaal 100 (eigen inschatting)
- Aantal onderwijsinstellingen: op dit moment zijn ongeveer 7500 instellingen aangesloten op OSO en actief, de verwachting is dat deze groep grotendeels overlapt met de doelgroepen van Vroegtijdig aanmelden en BRON VO. Het aantal instellingen loopt op tot maximaal 9000.
- Aantal administraties per instelling: op basis van de cijfers in de OSO database zien we 1,75 administratie per instelling.
- Aantal aanleverpunten met meer dan 1 adres: maximaal 1% (ervaringscijfers OSO)

Op basis hiervan schatten we de omvang van het aantal aanleverpunten en adressen dat in het serviceregister zal worden geregistreerd.

Tabel 2: Geschatte omvang van het serviceregister

	Label	**Initieel**	**Minimum**	**Maximum**
Diensten	A	3	10	100
Onderwijsinstellingen	B	7.500	5.000	9.000
Aantal administraties per instelling	C	1,75	1,00	2,00
Aantal aanleverpunten	**D = A x B x C**	**39.375**	**50.000**	**1.800.000**
Aantal adressen per aanleverpunt	E	1,00	1,00	1,01
Aantal adressen	**F = D x E**	**39.375**	**50.050**	**1.818.000**

De grootste impact op de variatie is het aantal diensten dat het register ondersteunt. Het is mogelijk om dit redelijk geleidelijk uit te breiden (zie ook 3.1 Fasering en scope), zodat het mogelijk is om het systeem geleidelijk op te schalen.

De verwachte omvang van het gebruik is lastiger in te schatten. Er zullen tussen 5 en plm 50 dienstleveranciers aansluiten aan het serviceregister (eigen inschatting), en er zijn dienstverleners die met alle onderwijsinstellingen communiceren (bijv BRON), en er zijn dienstverleners die met een subset van de instellingen communiceren. De verwachting is dat dienstverleners in het kader van een specifieke dienst communiceren met een onderwijsinstelling (bijvoorbeeld terugkoppeling bekostiging, uitwisseling overstapdossier enzovoort). Hiermee schatten we dat dienstverleners behoefte hebben aan de adressen van een aansluitpunt van een proportie (tussen 10% en 100%) van de onderwijsinstellingen.

Het is nog lastiger in te schatten hoe vaak dienstleveranciers met een school communiceren. Er zijn diensten waarvoor meerdere berichten per dag worden uitgewisseld, en er zijn diensten waarvoor een bericht per jaar wordt uitgewisseld. Analyse van berichtuitwisseling van BRON VO wijst op 10 tot 20 berichten per leerling per jaar, voor Vroegtijdig aanmelden wordt 3 berichten per aanmelding geschat, waarbij een leerling naar schatting 3 aanmeldingen heeft, en bij OSO is er een bericht per leerling per jaar. De gegevens van de diensten kunnen natuurlijk worden hergebruikt voor meerdere leerlingen, zodat het aantal leerlingen ‘wegvalt’ uit de schattingen. Voor de eerste fase verwachten we hiermee enkele tientallen bevragingen per jaar, of ongeveer 0,13 per dag.

Onderwijsinstellingen communiceren ook met andere onderwijsinstellingen, zij het doorgaans veel minder frequent. De verwachting is dat dit vooral over regionale uitwisseling gaat (OSO en Vroegtijdig aanmelden). Het is denkbaar dat instellingen voor meerdere diensten met andere instellingen communiceren. Gezien de situatie dat er nu weinig structureel berichtverkeer tussen instellingen onderling plaatsvindt, schatten we de te verwachten hoeveelheid berichtverkeer laag in.

Tabel 3: Geschatte aantal bevragingen per dag naar het serviceregister

	Label	Initieel	Minimum	Maximum
Dienstleveranciers	G	3	5	50
Proportie instellingen	H	50%	10%	100%
Berichten per dag	I	0,13	0,10	1,00
Dienstleveranciers: berichten per dag	J = G x (H x B) x I	1.463	250	450.000
Onderwijsinstellingen	B	1.500	5.000	9.000
Aantal instellingen	K	5	5	20
Berichten per dag	L	0,05	0,01	0,10
Instellingen: berichten per dag	M = B x K x L	375	125	18.000
Totaal: berichten per dag	N = J + M	1.838	375	468.000

De verwachte omvang van het gebruik zal variëren tussen enkele duizenden en enkele honderdduizenden berichten per dag naar het serviceregister. De grootste bron van onzekerheid zit in het aantal dienstleveranciers en de intensiteit waarmee zij het register zullen gebruiken. De inschatting is dat 50 leveranciers, die elk een bericht per dag naar alle onderwijsinstellingen sturen een onrealistisch hoge inschatting is. Voor een modern systeem is dit aantal bevragingen echter niet een heel grote uitdaging. Tegelijkertijd is het ook duidelijk dat het aantal bevragingen op het serviceregister niet veel hoger zal worden: het aantal onderwijsinstellingen wordt niet groter, het aantal leveranciers hoogstens een klein beetje, en de informatie uit het serviceregister is tenminste een werkdag houdbaar (zie 5.1 Bevragingen van het serviceregister) dus zal het aantal bevragingen per berichtuitwisseling van de serviceleverancier ook niet veel hoger worden dan 1 per dienst per instelling per dag.

7.5 BIV Classificatie en maatregelen

De tabel met de samenvattende uitkomst is hieronder weergegeven. De complete sheet met classificatie en toelichting is toegevoegd als bijlage bij dit document.

Tabel 3: Samenvatting van de BIV classificatie van het Onderwijs serviceregister

Naam project/dienst/document:	Onderwijs serviceregister			
Naam Data Classificeerder:	Marc Fleischeuers			
Functie:	ICT Architect Kennisnet			
Datum ingevuld:	7-feb.-17			
Aantal gebruikers van de dienst/afdeling:	Alle onderwijsinstellingen + dienstleveranciers			
Beschikbaarheid	**B =**	**2**		
Integriteit	**I =**	**2**		
Vertrouwelijkheid	**V =**	**2**		
Toelichting uitkomst				
1 = Laag	Het aspect is niet belangrijk. De potentiële schade is beperkt tot geen.			

	Toch geldt er een basisbeveiliging die elke ict-toepassing op orde zou moeten hebben. Mocht het aspect belangrijker worden, dan kan hierop verder gebouwd worden.
2 = Midden	Het aspect is wel belangrijk. De potentiële schade is substantieel. Dit kan voortvloeien uit eisen vanuit de gebruiker en/of contractuele eisen. Omdat processen niet verstoord mogen worden gelden aanvullende beveiligingsmaatregelen.
3 = Hoog	Het aspect is zeer belangrijk. De potentiële schade is ernstig. Dit vloeit vaak voort uit wettelijke eisen. Omdat het onderwijsproces verstoord wordt of omdat de veiligheid of privacy van personen in gevaar komt, gelden strenge beveiligingseisen.

De belangrijste risico's van deze dienst liggen in eerste instantie op het vlak van reputatie van de dienst. Het serviceregister zal een betrouwbare informatiebron moeten zijn voor alle ketenpartijen, en kan dit realiseren als 1. de dienst beschikbaar is, en 2. de informatie verkregen uit de dienst betrouwbaar is.

De bijbehorende maatregelen voor Beschikbaarheid:

	Beschikbaarheid	**Niveau 2** **Midden**
	Omschrijving	Beschikbaarheid is belangrijk. Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.
	Kenmerken	Beschikbaarheid > 97% RTO= 8-24 uur, afhankelijk van de categorie informatie
Overbelasting		Er is regulering: maatregelen zijn aanwezig om onevenredige belasting per gebruiker te voorkomen of te reguleren middels load balancers of een soortgelijke oplossing. Er zijn maatregelen getroffen om overbelasting van het systeem te voorkomen, middels trafficshapers of soortgelijke oplossing.
Business continuity		Er is een 'Warm Standby' aanwezig: - redundant systeem - specifieke spare (active-passive) - local cluster of geo cluster - replicatie door mirroring
Backup/ restore/ recovery		Backup verplicht, minimaal dagelijks. Recovery test= 2x per jaar. RPO max= 1 dag. RTO max= 24 uur. Automatische online failover bij uitval van 1 node (session lost) Automatisch opnieuw opstarten van systeem (session lost, transaction lost)
Single points of failure		Single point of failures zijn niet toegestaan in ketens.
Software		Patchen en updates van firmware en software zijn ingeregeld en

		worden periodiek uitgevoerd.
Logging / monitoring / testen		Onbeschikbaarheid en afname van performance wordt gemeten en geregistreerd / gelogd.
Actuele dreigingen (DDoS, ransomware)		Je bent in staat om spoedig te detecteren of een risico optreedt door bijvoorbeeld antivirus, anti-malware, intrusion detection

De bijbehorende maatregelen voor Integriteit:

	Integriteit	**Niveau 2** **Midden**
	Omschrijving	Integriteit is beschermd. Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.
	Kenmerken	Een zeer beperkt aantal fouten is toegestaan
Herleidbaarheid		Herleidbaarwie, wanneer, welkegegevens/configuraties gewijzigd heeft. Invoer syntax controle niet noodzakelijk wel wenselijk
Functiescheiding		Functiescheiding noodzakelijk- Goedkeuring door een tweede persoon is noodzakelijk. (Risico: "Beperking tegen het misbruik van tegengestelde belangen door meerdere functies en mogelijkheden voor één persoon").
Application controls		Verschillende groepen van informatie of diensten, gebruikers en informatiesystemen moeten gescheiden worden op het netwerk. Hashing wordt gebruikt ter controle van integriteit gegevens.
Manual controls		Bevestiging/verificatie van de gebruiker (bijvoorbeeld handtekening of actieve handeling) Handmatige controle/verificatie (bijvoorbeeld bij paspoort)
Onweerlegbaarheid		Logging is verplicht. - 90 dagen bewaren - Logging events beveiligd tegen aanpassingen - maandelijks rapportage - Tijd gesynchroniseerd met stratum 4 tijdbron Gelogd wordt: - handelingen van beheerders - beveiligingsovertredingen Een logregel bevat: - Datum en tijdstip, minimaal tot op secondeniveau - Gebruikersnaam/ identificatie - Werkstation/locatie informatie - Activiteit - Het object waarop de activiteit werd uitgevoerd
Actuele dreigingen (DDoS, ransomware)		Bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan 24 uur geleden

De bijbehorende maatregelen voor Vertrouwelijkheid:

	Vertrouwelijkheid	**Niveau 2** **Midden**
	Omschrijving	Informatie is vertrouwelijk. De organisatie, instelling of betrokkene kan substantiële schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag alleen toegankelijk zijn voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Hieronder vallen onder andere persoonsgegevens.
	Kenmerken	Gegevens alleen toegankelijk voor direct betrokkenen binnen de organisatie op basis van functie of rol.
Levenscyclus gegevens		De data moet gewist en overschreven worden (met random data) voordat de apparatuur afgevoerd mag worden.
Fysieke toegang		Fysieke toegangscontrole middels toegangspas met extra privileges. Informatie blijft binnen locaties van de organisatie of technische partners. Informatie is toegankelijk voor een beperkte groep mensen binnen de organisatie. - Alleen intern direct benaderbaar, voor specifiek aangewezen personen. - Toegang vanuit andere zones via Firewall, voor specifiek aangewezen personen. - Geen directe toegang vanuit externe netwerken, altijd via een front-end server of stepping-stone, middels beveiligde verbinding
Logische toegang		Authenticatie/autorisatie afhankelijk van locatie gebruiker: - Binnen eigen locaties: Gebruikersnaam en wachtwoord. - Vanaf buiten eigen locaties: Gebruikersnaam en wachtwoord en eventueel two factor Two factor authenticatie, bijvoorbeeld met mobiele telefoon of hardware tokens. Ter illustratie van need to know: - Er bevinden zich geen daadwerkelijke persoonsgegevens in O, T en (wanneer mogelijk) A omgevingen

Opslag en transport		Altijd encryptie van opslag en transport Naast gebruik maken van de richtlijnen/best practices/standaarden van NCSC, ENISA, NIST of vergelijkbaar: Encryptie welke niet te kraken is binnen de verwachtte levensduur van de versleutelde informatie. - Voor transport: - TLS 1.2 of hoger (vergelijk: de versie die door NCSC als 'goed' wordt beoordeeld) - IPSEC - Voor opslag: - AES (128 bit of hoger) - RSA, ECC, Diffie-Helman
Logging / auditing		Handelingen van beheerders moeten worden gelogd en traceerbaar zijn naar individuele personen
Actuele dreigingen (DDoS, ransomware)		Je bent in staat om spoedig te detecteren of een risico optreedt door bijvoorbeeld antivirus, anti-malware, intrusion detection

8 Concept realisatie

Het voorstel is om het serviceregister voor het onderwijs te baseren op de huidige serviceregister functionaliteit in OSO. In dit serviceregister 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 serviceregister 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 serviceregister 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.

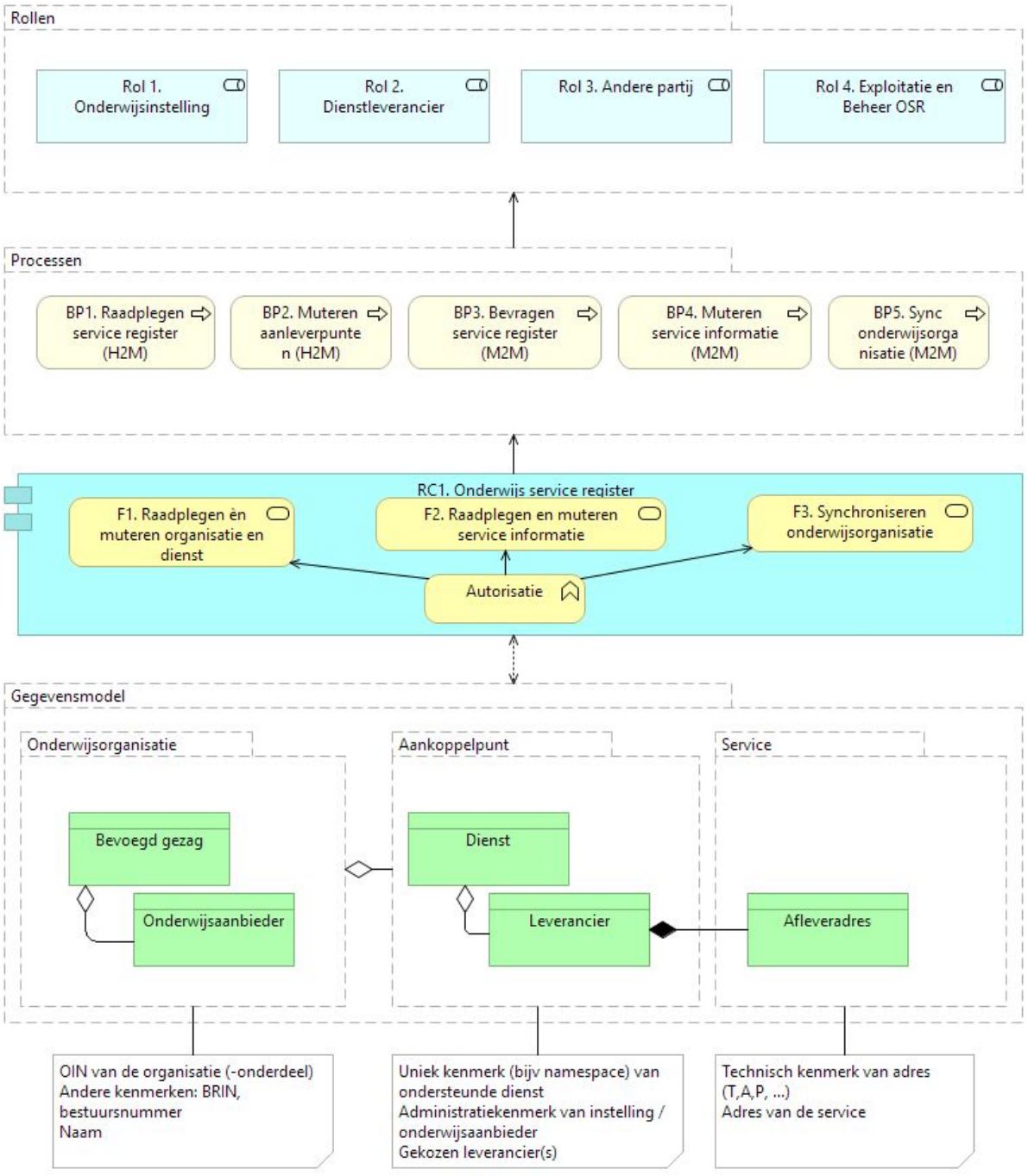
De stappen die deze realisatie gaat volgen worden nu in concept uitgetekend. De gedachte is dat we hiermee in staat zijn om zowel de nieuwe gewenste functionaliteit te realiseren als, door aan te sluiten op een bekend en beschikbaar systeem, de administratieve overlast zoveel mogelijk te beperken.

9 Concept implementatie

Er zijn een aantal zaken waar tijdens de implementatie rekenening mee moet worden gehouden.

- **Afweging verlagen administratieve lasten versus eenmalige registratie, meervoudig gebruik**. Op dit moment is het zo dat veel diensten een eigen 'serviceregister' hebben ingebouwd, waar adressen van aanleverpunten van onderwijsinstellingen in worden geregistreerd. Onderhoud van deze adressen is verdeeld over de onderwijsinstelling zelf, de leverancier van het administratiesysteem van de onderwijsinstelling en de dienstleverancier. Verschillende diensten vragen echter veelal dezelfde gegevens aan soms dezelfde medewerkers van onderwijsinstellingen. Het is de intentie van het serviceregister om deze informatie centraal te bundelen en voor meerdere toepassingen beschikbaar te maken. Tijdens de geleidelijke invoer van het register zal het echter voorkomen dat informatie dubbel wordt ingevoerd, omdat niet alle bestaande registers in een keer overbodig zijn.
- **Afweging geen nieuwe koppelvlakken versus additionele functionaliteit**. De registratie in het serviceregister houdt rekening met meerdere aankoppelpunten voor dezelfde dienst binnen een onderwijsinstelling, die kunnen worden onderscheiden op basis van een kenmerk. Dergelijke functionaliteit is echter in bestaande eigen serviceregisters (zie hierboven) vrijwel nooit aanwezig. Als een dienstafnemer gebruik wil maken van het kenmerk om binnen de onderwijsinstelling te kunnen navigeren, zal de dienstafnemer een nieuw koppelvlak moeten implementeren.
- **Patronen van gebruik.** Er zijn diverse interactiepatronen waarmee de gegevensuitwisseling tussen dienstaanbieders en hun afnemers kan verlopen (zie ook 11 Bijlage: Huidige servicelandschap in het onderwijsveld). Het serviceregister ondersteunt hierin vooral het ontdekken (*discovery*) onderdeel van het interactiepatroon. Per dienst zal worden uitgewerkt wat de best werkende invulling van het onderdeel is. Dit kan tot gevolg hebben dat er wijzigingen door de dienstaanbieder en mogelijk door diens afnemers moeten worden aangebracht, bijvoorbeeld om gebruik te maken van kenmerken bij het opvragen van aanleverpunten.
    - **Online bevragen of eigen lokale cache opbouwen**. Een belangrijk aspect van elk patroon van gebruik is of dienstleveranciers het serviceregister voor elke berichtuitwisseling bevragen (online, realtime) of dat partijen de opgevraagde informatie voor enige tijd kunnen bewaren en hergebruiken. In principe is de onderwijswereld voortdurend in beweging en kan op elk moment een url van een school wijzigen, maar de praktijk wijst uit dat aanleverpunten en afleveradressen redelijk stabiel zijn. Tegelijkertijd ontstaat er een grote afhankelijkheid als dienstverleners voor elk bericht dat ze uitsturen het serviceregister zouden moeten raadplegen. Het voorstel zal daarom zijn dat elk antwoord van het register een uiterste levensduur (time to live, TTL) zal bevatten die aangeeft hoe lang de informatie bruikbaar is. Partijen kunnen deze informatie gebruiken om eigen caches in te richten.
- **Identificatie en authenticatie van medewerkers van instellingen.** Het beheer van aanleverpunten is belegd bij onderwijsinstellingen, dat betekent dat medewerkers van onderwijsinstellingen toegang kunnen krijgen tot het register om gegevens in te zien en te wijzigen. RIO heeft een soortgelijke functionaliteit, medewerkers van onderwijsinstellingen hebben toegang tot het zakelijk portaal van DUO en kunnen daar gegevens inzien en wijzigen. Het heeft de voorkeur dat het serviceregister aansluit bij de identificatie- en autorisatiemethode van RIO, opdat een zo laag mogelijke administratieve last voor onderwijsinstellingen wordt gecreëerd. Onderdeel van het implementatietraject is om na te gaan wat de mogelijkheden zijn hiervoor. Op lange termijn zal voor de identificatie en authenticatie worden gekoppeld aan de standaard IAA middelen die geschikt zijn voor soortgelijke verantwoordelijkheid.
- **Governance**. Als partijen het serviceregister gaan inzetten betekent dat het aangaan van een afhankelijkheid. Dit heeft gevolgen voor het ontwerp en inrichting van het systeem (zie 7.5 BIV Classificatie en maatregelen) maar ook voor beheer en doorontwikkeling van het systeem. Beheer en doorontwikkeling moet zodanig worden ingericht dat aansluitende partijen vertegenwoordigd zijn.

10 Concept architectuur



Figuur 5: Concept architectuur van het onderwijs serviceregister.

10.1 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.

11 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”[4] 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 4: 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

[4] *Conversation patterns: Interactions between loosely coupled services*. Gregor Hohpe, juni 2008; www.eaipatterns.com

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 5: 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 tabellen 4 en 5 is in termen 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 serviceregister 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 serviceregister kan worden opgezocht.