Edukoppeling

***MDX OSR protocol***

Mandated Data eXchange (MDX) protocol voor mandatering en endpoint registratie met een Onderwijs Service Register

Edustandaard

Datum: mei 2023

Versie: 0.8

Status: concept

**Inhoudsopgave**

[1. Documenthistorie 3](#_Toc135825165)

[2. Inleiding 4](#_Toc135825166)

[2.1. Aanleiding voor het ontwikkelen van de Edukoppeling standaard 4](#_Toc135825167)

[2.1. Doel en doelgroep 4](#_Toc135825168)

[2.1. Positionering binnen Edukoppeling Architectuur 4](#_Toc135825169)

[2.2. MDX OSR protocol, functioneel toepassingsgebied 5](#_Toc135825170)

[2.2.1. Mandatering 5](#_Toc135825171)

[2.2.1. Authentieke bron van OIN’s en HRN’s 7](#_Toc135825172)

[2.2.1. Authentieke bron van Systeem UUIDs 7](#_Toc135825173)

[2.2.1. Beheer webservice-informatie inclusief endpoints 7](#_Toc135825174)

[2.2.1. Beheer publieke certificaten t.b.v. versleutelen berichten 7](#_Toc135825175)

[2.3. Notatiewijze voorschriften 8](#_Toc135825176)

[2.4. Leeswijzer 8](#_Toc135825177)

[3. Use cases MDX OSR protocol 9](#_Toc135825178)

[3.1. Uitwisseling tussen gemandateerde verwerkers 9](#_Toc135825179)

[3.2. Uitwisseling met niet-mandaatplichtige verwerker 10](#_Toc135825180)

[3.3. Uitwisseling met gebruik van endpoints 11](#_Toc135825181)

[4. Normatieve voorschriften 11](#_Toc135825182)

[4.1. Algemeen 11](#_Toc135825183)

[4.2. Mandateringsregister functie 12](#_Toc135825184)

[4.3. Endpoint register functie 13](#_Toc135825185)

[4.4. Inrichten van het register 15](#_Toc135825186)

[5. Bijlage: Rollen 17](#_Toc135825187)

[5.1. Mogelijke eindorganisaties in het onderwijs 17](#_Toc135825188)

[5.2. Mogelijke routeringskenmerken in het onderwijs 17](#_Toc135825189)

[5.3. Mogelijke verwerkers 18](#_Toc135825190)

[5.4. Beheerorganisatie van het register 18](#_Toc135825191)

# Documenthistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Auteur | Datum | Opmerking |
| 0.1 | E. Reinhoud | November 2022 | Outlines |
| 0.2, 0.3 | E. Borgers | November 2022 | Verdere invulling |
| 0.4 | E. Borgers | November 2022 | Verspreid ter review aan de Edukoppeling werkgroep |
| 0.5 | E. Borgers | Januari 2023 | Commentaar Don de Lange (Technisch Specialist OSR) en Werkgroep Edukoppeling review verwerkt |
| 0.6 | E. Borgers | Maart 2023 | Commentaar review werkgroep verwerkt, verspreid voor Edukoppeling werkgroep Maart 2023. Niet besproken |
| 0.7 | E. Borgers | April 2023 | Aangescherpt wanneer een mandaat verplicht is. Toevoeging routeringskenmerken. Verwijderen concept administratie. |
| 0.8 | E. Borgers | Mei 2023 | Mandaat verplicht gekoppeld aan systeem. Inleiding toegevoegd. |

# Inleiding

## Aanleiding voor het ontwikkelen van de Edukoppeling standaard

<overnemen uit overige documenten>

## Doel en doelgroep

<overnemen uit algemeen>

## Positionering binnen Edukoppeling Architectuur

Dit Architectuurdocument is één van de normatieve documenten binnen de Edukoppeling-afspraak. Edukoppeling is een afgeleide van Digikoppeling[[1]](#footnote-3) en een aantal documenten binnen deze afspraak zijn dus ook relevant voor Edukoppeling. Een overzicht hiervan wordt gegeven in het Edukoppeling ‘Overzicht actuele documentatie en compliance’ document en Figuur 1.

De kern van de Edukoppeling MDX profielen wordt gevormd door de mandatering waarmee een eindorganisatie (vaak een onderwijsorganisatie) een verwerker (vaak een SaaS-leverancier) toestemming geeft om binnen een bepaalde ketensamenwerking vertrouwelijke gegevens uit te wisselen met een derde partij (verwerker). Deze mandaten zijn vastgelegd in een centraal register dat voldoet aan het MDX OSR protocol. Dit document beschrijft dit protocol.

Afbeelding met diagram

Automatisch gegenereerde beschrijving

Figuur 1 - Positionering van MDX-OSR protocol binnen de Edukoppeling Architectuur

## MDX OSR protocol, functioneel toepassingsgebied

### Mandatering

De MDX-profielen kunnen worden toegepast bij verschillende transactiepatronen waarbij het register een rol heeft, dit zijn:

* een bevraging (pull);
* een melding (push).

In beide gevallen moet het mogelijk zijn om bij de gegevensuitwisseling de mandatering tussen eindorganisatie en gegevensverwerker te kunnen verifiëren via de gegevens in het register.

**Verwerker mandatering bij bevragingen (request-response bedrijfstransactiepatroon)**

Dit begint met het mandateren van de verwerkers door een medewerker van de onderwijsorganisatie. Dit wordt expliciet gemaakt door een registratie hiervan in het register.

Indien een verwerker (vrager) een andere verwerker (aanbieder) bevraagt (M2M) en er is sprake van vertrouwelijke gegevens die uitgewisseld gaan worden dan

* wil de vrager vaststellen of de aanbieder gemandateerd is om namens de eindorganisatie van de aanbieder in deze ketensamenwerking de vraag te beantwoorden
* wil de aanbieder vaststellen of de vrager gemandateerd is om namens de eindorganisatie van de vrager in deze ketensamenwerking de vraag te stellen

(zie Figuur 4).

Wanneer de bevragende verwerker de gegevens bij de aanbieder opvraagt, doet hij dit met zijn eigen PKI-certificaat (TLS en mogelijk ondertekening en versleuteling van het bericht) en geeft daarbij aan (middels de zogenaamde ‘FROM’-parameter) namens welke onderwijsorganisatie het vraagbericht opgesteld is. Voor identificatie van de onderwijsorganisatie wordt een Organisatie Identificerend Nummer (OIN) gebruikt (zie voor details het *Identificatie en Authenticatie document*). De aanbieder verifieert vervolgens of de verwerker namens de eindorganisatie mag aanleveren aan de hand van de vastgelegde mandateringsrelatie in het register.

Afbeelding met diagram

Automatisch gegenereerde beschrijving

*Figuur 4 – SaaS leverancier mandatering bij bevragingen*

**SaaS-leverancier mandatering bij melding (melding-bevestiging bedrijfstransactiepatroon)**

Het patroon melding-bevestiging wordt gebruikt om vertrouwelijke gegevens te versturen. Als de ontvanger een onderwijsorganisatie is die gebruik maakt van SaaS, dan moeten de gegevens ‘in het goede bakje’ terecht komen (zie Figuur 5). Mogelijk was ook de verzender een SaaS-leverancier en heeft de ontvanger ook nu de mogelijkheid om te valideren of de SaaS-leverancier voor deze uitwisseling gemandateerd is.

De onderwijsorganisatie heeft de SaaS-leverancier gemandateerd. Wat er aan toe moet worden gevoegd is op welk internetadres of URL de gegevens afgeleverd moeten worden. Dit wordt gebruikt om de gegevens te versturen. Tevens wordt de geadresseerde onderwijsorganisatie meegegeven (in de zogenaamde ‘TO’ -parameter). Hiermee kan de SaaS-leverancier ‘routeren achter de voordeur’. Het certificeringsschema[[2]](#footnote-5) geeft de verzender zekerheid dat de dienstverlener geregeld heeft dat de gegevens bij de goede onderwijsorganisatie terechtkomen.

Afbeelding met tekst, schermopname, grafische vormgeving, Lettertype

Automatisch gegenereerde beschrijving

*Figuur 5 - SaaS leverancier mandatering bij melding (push)*

### Authentieke bron van OIN’s en HRN’s

Het register is de authentieke bron van OIN’s binnen het onderwijs. De OIN’s worden samengesteld op basis van andere authentieke bronnen zoals BRON (RIO) en Handels Register Nummers (HRN’s) op basis van het Handelsregister. Hoe OIN’s en HRN’s worden samengesteld staat beschreven in het Edukoppeling Identificatie en Authenticatie document.

### Authentieke bron van Systeem UUIDs

Het register is de authentieke bron van UUIDs van systemen binnen het onderwijs. Deze UUIDs zijn verder betekenisloos . De UUIDs kunnen worden gebruikt als meta informatie bij enpoints en mandaten.

### Beheer webservice-informatie inclusief endpoints

Deze functie beschouwen we als een telefoonboek-functie voor M2M webservices binnen de onderwijsketen. Een ketenpartij die binnen een bepaalde ketensamenwerking bepaalde gegevens moet uitwisselen met een ketenpartner kan het register bevragen voor kenmerken en technische details over de te gebruiken webservice(s). De ketenpartner die de webservice gaat aanroepen kan het endpoint en overige specificaties bij het register ophalen. Met de komst van het REST/SaaS-profiel kan een partij kiezen of de gegevens uitgewisseld worden met WUS of REST. ~~Het register bevat een profielaanduiding die aangeeft welke van de twee gebruikt moet worden om met het endpoint van de service te communiceren.~~

### Beheer publieke certificaten t.b.v. versleutelen berichten

Het transport van vertrouwelijke gegevens vraagt om maatregelen om ervoor te zorgen dat deze niet door onbevoegden kunnen worden ingezien. Het REST/SaaS-profiel en WUS/SaaS-profiel schrijven daarom het gebruik van TLS voor. Daarnaast biedt het WUS/SaaS-profiel de mogelijkheid om berichten te versleutelen wat met name toegepast wordt in het scenario waar er sprake is van een transparante intermediair (bijvoorbeeld een logistieke dienstverlener). Hierbij is het noodzakelijk dat de verzender van het bericht over het publieke certificaat beschikt van de ontvanger.

Degene die het bericht encrypt heeft de publieke sleutel nodig van zijn ketenpartner (zie Figuur 6). De ontvanger kan het vervolgens met zijn private sleutel weer decrypten. Iemand anders kan het niet en daarmee is het externe transport vertrouwelijk. Het interne transport binnen een SaaS-leverancier is vertrouwelijk als naar de normen van het certificeringsschema is gekeken en daarop gepaste maatregelen zijn getroffen. De identiteit van een verwerker is opgenomen als OIN/HRN in het PKI-certificaat (PKI-overheid)

Afbeelding met diagram

Automatisch gegenereerde beschrijving

*Figuur 6 – Versleutelde berichten*

## Notatiewijze voorschriften

Voor elk voorschrift wordt aangegeven in welke mate hier invulling aan moet worden gegeven. Hiermee kunnen we duidelijk aangeven wat de grenzen van dit profiel zijn ten opzichte van de mogelijke externe bron(nen) waar het voorschrift eventueel van wordt overgenomen. We gebruiken hiervoor de notatiewijze van RFC2119[[3]](#footnote-6). Deze gebruikt de volgende termen: "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL".

## Leeswijzer

[todo]

Algemeen verhaal

# Use cases MDX OSR protocol

## Uitwisseling tussen gemandateerde verwerkers

Afbeelding met tekst, schermopname, Post-it-briefje, diagram

Automatisch gegenereerde beschrijvingDeze afbeelding toont de uitwisseling tussen twee verwerkers mogelijk verwerkend voor dezelfde eindorganisatie (A=B) of voor verschillende eindorganisaties, die gebruik maken van mandaatchecks

* Een Onderwijs Service Register (OSR) ondersteunt de autorisatie op een uitwisseling voor alle profielen en alle soorten patronen (waaronder notificatie, synchroon en asynchrone uitwisseling) door informatiesystemen.
* Het register ondersteunt zo verwerkers in het realiseren van ketenprocesstappen (zie ROSA) voor eindorganisaties.
* Voorwaardelijk voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van de geldigheid van het mandaat van de andere ketenpartner, uitgevoerd door beide verwerkers.
* Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat.
* Het register doet een check op geldigheid van het PKI overheidscertificaat van de verwerker bij elke aanroep van het register.
* Het register gebruikt RIO voor validatie van onderwijsorganisatiegegevens indien eindorganisaties of verwerkers onderwijsorganisaties zijn
* Het register voorziet zo in eenmalige opslag en meervoudig gebruik van mandaten voor het onderwijs.

## Uitwisseling met niet-mandaatplichtige verwerker

Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

In de ketensamenwerking kan zijn afgesproken dat een mandaatcheck niet nodig is voor bepaalde uitwisselingen voor éen of beide verwerkers, bijvoorbeeld op basis van een wettelijke grondslag. Deze afbeelding toont de uitwisseling met en een niet-mandaatplichtige verwerker. In aanvulling op de vorige paragraaf geldt

* Voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van de geldigheid van het mandaat van enkel de mandaatplichtige verwerker voldoende.
* Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat door de verwerker.

## Uitwisseling met gebruik van endpoints

Afbeelding met tekst, diagram, schermopname, Plan

Automatisch gegenereerde beschrijving

Het register biedt de optie om “virtuele endpoints” van administraties of andere “ruimtes” ingericht voor onderwijsorganisaties in systemen op te slaan en her te gebruiken binnen ketens. Deze endpoints zijn gekoppeld aan een mandaat, wat betekent dat na succesvol opvragen van een endpoint geen aparte mandaatcheck meer nodig is, wat gebruik van het register nog praktischer maakt.

* Voorwaardelijk voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde opvraag van het endpoint van de andere ketenpartner, uitgevoerd door beide verwerkers.
* Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat (of endpoint).
* Het register voorziet zo in eenmalige opslag en meervoudig gebruik van endpoints voor het onderwijs.

# Normatieve voorschriften

## Algemeen

1. MUST: Dit protocol is verplicht bij alle MDX profielen, dus de profielen met gebruik van REST, WUS en/of OAuth technologie.
2. MUST: Er is een centraal landelijk mandaterings en endpoint register met daarin verplicht alle mandaten en optioneel endpoints van de betreffende partijen.
3. MUST: Implementatie van het protocol (autorisatie voor een uitwisseling door verwerkers) geschiedt inclusief raadpleging van het register (real-time of op andere wijze) voor hiertoe uitgereikte mandaten door een eindorganisatie.
4. MUST: Onderliggend aan de implementatie is een ketensamenwerkingsafspraak waarin benodigde informatie voor de inrichting en gebruik zijn vastgelegd.
5. SHOULD: Een implementatie van MDX OSR is benaderbaar met alle door EduKoppeling ondersteunde profielen.

## Mandateringsregister functie

Afbeelding met tekst, schermopname, diagram, Lettertype

Automatisch gegenereerde beschrijving

Registeren mandaten

1. MUST: De eindorganisatie registreert actief in het register een mandaat waarmee wordt aangegeven dat een verwerker in een bepaalde ketensamenwerking vertrouwelijke gegevens mag uitwisselen namens een eindorganisatie.
2. MUST: Het register kan verifiëren dat de H2M registratie van het mandaat namens een eindorganisatie wordt gedaan. De digitale identiteit kan herleid worden naar de eindorganisatie en verificatie is mogelijk of deze persoon gemachtigd is door de eindorganisatie om in het register mandaten te registreren.
3. MUST: De schoolbeheerder identificeert de verwerker op basis van in het register bekende systemen. Dit voor het verkrijgen van meta informatie over het mandaat en voor het optioneel registreren van gemandateerde endpoints voor dit systeem met behulp van een mandaattoken.
4. MUST: De datum waarop het mandaat geldig is wordt vastgelegd door de eindorganisatie. Een mandaat wordt per direct geldig op de ingestelde datum. De verandering van geldig naar ongeldig op de vervaldatum valt samen met de datum overgang (24 uurs grens).

Bevragen mandateringsregister

1. MUST: Het register biedt verwerkers binnen een bepaalde ketensamenwerking de mogelijkheid om mandaten van zichzelf en van de andere verwerker M2M te verifiëren.
2. MUST: Het register kan verifiëren dat raadpleging van het mandaat namens een verwerker wordt gedaan. De digitale identiteit kan herleid worden naar de verwerker middels een PKI overheidscertificaat.
3. MUST: Verificatie van het mandaat wordt nagegaan op basis van de OIN van de verwerker en de OIN van de eindorganisatie (heeft *deze verwerker* een mandaat van *deze eindorganisatie* voor een willekeurig systeem).
4. COULD: Verificatie van het mandaat wordt nagegaan op basis van de OIN van de verwerker en de OIN van de eindorganisatie en de UUID van een systeem (heeft *deze verwerker* een mandaat van *deze eindorganisatie* voor *dit systeem*).
5. MUST: De verandering van ingaan en vervallen van een mandaat valt samen met een datum overgang (24 uurs grens).
6. MUST: Een verwerker kan met het register inzicht krijgen in de geldigheidsduur van zijn eigen mandaten.
7. MUST: Een verwerker kan met het register inzicht krijgen in het op een bepaald moment geldig zijn van mandaten
8. COULD: Als extra informatie kan bij een mandaat systeem informatie worden opgevraagd, als dit is aangegeven in de ketensamenwerking.

Uitwisseling op basis van mandaten

1. MUST: Alvorens uit te wisselen informatie te verwerken heeft verificatie van het mandaat van de andere verwerker door beide verwerkers plaatsgevonden.
2. COULD: Een verwerker kan gebruik maken van een mandaat van een andere verwerker, mits deze verwerker deel uitmaakt van dezelfde verwerkersgroep
3. COULD: De verificatie van een verwerker op een mandaat van een andere verwerker kan alleen plaatsvinden door verwerkers binnen dezelfde ketensamenwerking

## Endpoint register functie

Eindorganisaties hebben of gebruiken systemen (Lassen, LVSsen, toetssystemen …) met daarop endpoints. Een endpoint verbindt een internet adres (URL) met het systeem. Aangezien meerdere onderwijsorganisaties vaak hetzelfde fysieke systeem en de URL kunnen delen, worden er “virtuele endpoints” gedefinieerd. Hiervoor dienen routeringskenmerken. De combinatie van URL plus routeringskenmerk adresseert de gewenste administratie van een onderwijsorganisatie.

Het register biedt de optie om deze “virtuele endpoints” op te slaan en her te gebruiken binnen ketens. Meestal kent een systeem meerdere endpoints, voor verschillende soorten uitwisselingen, die in een ketensamenwerking niet allemaal gebruikt worden. Keuzes hierin zijn leverancier en ketenspecifiek.

Een centraal endpoint register voorkomt dat (updates op) endpoints via “lijstjes” worden rondgepompt, wat veel werk is en fouten in de hand werkt. Verwerkers *kunnen* gebruik maken van de mogelijkheid endpoints te configureren en op te halen in het register. Dit vermindert administratieve lasten en fouten (eenmalige opslag, meervoudig gebruik).

Afbeelding met tekst, schermopname, diagram, Lettertype

Automatisch gegenereerde beschrijving

Registreren endpoints

1. MUST: Verwerkers kunnen endpoints M2M configureren (CUD) in het register mits ze kunnen aantonen dat ze daartoe geautoriseerd zijn met behulp van een door het endpoint register uitgereikt token aan de verwerker voor het systeem waar de endpoints betrekking op hebben.
2. MUST: Verwerkers kunnen endpoints M2M configureren (CUD) in het register met medegeven van het token behorende bij het mandaat van het betreffende systeem.
3. MUST: De digitale identiteit van de verwerker die M2M endpoints configureert kan herleid worden met een PKI overheid certificaat.
4. MUST: Elk endpoint is gekoppeld aan een (één) namespace.
5. MUST: Het routeringskenmerk van een endpoint bestaat uit de OIN van de eindorganisatie inclusief een driecijferig suffix. Deze OIN inclusief suffix is uniek binnen de namespace.
6. MUST: Het register maakt claimen van een vrij suffix voor een OIN van een eindorganisatie mogelijk binnen een namespace van een ketensamenwerking.
7. MUST: Een namespace heeft de vorm van een binnen het gehele register unieke URL waarin metadata over endpoints kan zijn opgenomen zoals de ketensamenwerkingsnaam, de versie van de ketensamenwerking en het type endpoint.
8. MUST: De datum waarop het endpoint geldig is wordt vastgelegd door de verwerker. Een endpoint wordt per direct geldig op de ingestelde datum. De verandering van geldig naar ongeldig op de vervaldatum valt samen met de datum overgang (24 uurs grens).
9. SHOULD: Het routeringskenmerk voor hetzelfde endpoint is gelijk over alle ketensamenwerkingen.

Opvragen endpoints

1. MUST: Het register kan verifiëren dat de M2M raadpleging van endpoints namens een verwerker wordt gedaan. De digitale identiteit kan herleid worden naar de verwerker
2. MUST: Endpoints in een ketensamenwerking zijn opvraagbaar op basis van
   * het routeringskenmerk of de OIN van de eindorganisatie plus
   * een namespace
3. MUST: Van een endpoint is opvraagbaar de URL, de gekoppelde namespace, de data van geldigheid, het routeringskenmerk van het endpoint.
4. MUST: Bij succesvol opvragen van een endpoint is geen aparte mandaatcheck meer nodig van de verwerker die de endpoints configureerde, want deze voert het register dan zelf uit.
5. COULD: Van een endpoint is systeeminformatie opvraagbaar, als dit is aangegeven als mogelijkheid binnen de ketensamenwerking.
6. COULD: Het kunnen opvragen van endpoints beperkt zich tot verwerkers die een mandaat hebben in dezelfde ketensamenwerking

## Inrichten van het register

Voor het kunnen gaan gebruiken van het register worden afspraken gemaakt met het registerbeheer en de ketensamenwerking gemodelleerd

Afbeelding met tekst, diagram, lijn, Plan

Automatisch gegenereerde beschrijving

1. MUST: Voor gebruik in een ketensamenwerking wordt door de keten met de beheerder van het register een unieke ketensamenwerkingsnaam afgesproken
2. MUST: Informatie over systemen van verwerkers worden door de register beheerder ingebracht.
3. MUST: Het bevoegd gezag machtigt onderwijsmedewerkers voor het beheren van mandaten.
4. MUST: De onderwijsorganisatie beheerders maken mandaten aan voor de verwerkers die deel uitmaken van specifieke ketensamenwerkingen
5. MUST: het register beheer ondersteunt verwerkers en eindorganisaties in het correct gebruik van het register en ziet toe op levering conform de afgesproken SLA.

Afbeelding met tekst, diagram, lijn, schermopname

Automatisch gegenereerde beschrijving

1. MUST: Verwerkers die endpoints opnemen in het register sluiten een aansluitcontract af met de register beheerder voor het gebruik van het register. Voor bevraging is geen aansluitcontract nodig.
2. MUST: Verwerkers die endpoints opnemen in het register ontvangen een token van het de beheerder van het register dat zij dienen te gebruiken voor configureren van hun endpoints op een systeem
3. MUST: Indien in de ketensamenwerking gebruik gemaakt wordt van endpoints, worden met de keten namespaces afgesproken en zorgt de register beheerder voor het configureren hiervan.
4. MUST: Als verwerkers Endpoints willen configureren doen ze dit met hun token bij de onder het mandaat vallende systemen.

# Bijlage: Rollen

## Mogelijke eindorganisaties in het onderwijs

Afbeelding met diagram

Automatisch gegenereerde beschrijving

Elke organisatie met een OIN kan in principe ingevoerd worden als eindorganisatie in het register. Daarbij dient dan wel authenticatie mogelijk te zijn.

Als onderwijsorganisatie kan volgens RIO dienen

* Een bestuur
* Een onderwijsaanbieder
* Een onderwijsaanbiedersgroep

Aangezien BRIN jarenlang de duiding was van organisatie wordt in de praktijk ook een onderwijsinstelling met een instellingserkenning als optie geboden om te gebruiken als eindorganisatie in het onderwijs.

Daar waar Edukoppeling voorziet in een OIN voor deze organisaties kunnen deze in principe als eindorganisatie dienen. De beheerder van deze eindorganisatie dient daartoe gemachtigd te zijn door een het bestuur.

## Mogelijke routeringskenmerken in het onderwijs

Routeringskenmerken die in EduKoppeling beschreven worden kunnen worden opgenomen in het register. Dit is momenteel een nummering of basis van een HRN of onderwijsinstellingserkenning (BRIN4).

De huidige Edukoppeling standaard kent een aantal restricties wat betreft het duiden van een endpoints op systemen met behulp van een routeringskenmerk:

1. Hetzelfde endpoint voor een eindorganisatie kan een ander suffix krijgen in een andere ketensamenwerking. De beheerder van het register streeft hergebruik van hetzelfde routeringskenmerk na, maar dit is geen garantie. Dit bemoeilijkt beheer van routeringskenmerken voor leveranciers.
2. Edukoppeling kent als mogelijke OIN vulling een HRN of een onderwijsinstellingserkenning code (voorheen BRIN4). Dit is echter een juridische indeling op basis van licenties, die de administratieve werkelijkheid slecht volgt. In de praktijk zijn administraties veel vaker ingedeeld op onderwijsaanbieders. Daarom is het wenselijk (ook) te kunnen adresseren op basis van onderwijsaanbieder. Een manier om dit te doen is als organisatie in de OIN de onderwijsaanbiederscode te gebruiken. Dit is punt van onderzoek.
3. Het suffix is niet altijd bekend in een uitwisseling. In de praktijk gaat men dan “broadcasten” naar alle endpoints van de eindorganisatie in de ketensamenwerking (bv meerdere LASsen). Berichten komen dan aan op meerdere systemen, mogelijk zelfs op systemen van verschillende verwerkers, en/of adresseren meerdere administraties binnen een systeem. De systemen moeten dan zelf nagaan of het bericht voor hen bedoeld is. Dit is uiteraard zeer ongewenst. Een mitigatie is te filteren op de namespace. In de namespace kan bijvoorbeeld het type systeem of het type bewerking worden opgenomen.

## Mogelijke verwerkers

Afbeelding met diagram

Automatisch gegenereerde beschrijving

Een verwerkersorganisatie moet een OIN hebben en een daaraan gekoppeld PKI overheidscertificaat.

## Beheerorganisatie van het register

Het register product management verzamelt wensen aangaande het register, vertaalt deze naar requirements en prioriteert deze op advies van haar stakeholders. Het productmanagement is het eerste aanspreekpunt voor partijen die aangesloten willen worden op het register.

De register architect adviseert en ondersteunt het register product management bij van de requirements op Edukoppeling, in het bijzonder het MDX OSR protocol. De architect neemt deel aan de EduKoppeling werkgroep.

De register systeem architect (technisch specialist) bewaakt de realisatie en operatie van het register conform requirements.

De register beheerder ondersteunt eindorganisaties en verwerkers bij het inrichten en gebruik van het register. De register beheerder verstrekt API tokens aan verwerkers.

1. <https://www.logius.nl/diensten/digikoppeling> [↑](#footnote-ref-3)
2. **Fout! De hyperlinkverwijzing is ongeldig.** <https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/> [↑](#footnote-ref-5)
3. https://tools.ietf.org/html/rfc2119 [↑](#footnote-ref-6)