Edukoppeling

***MDX OSR protocol***

***M2M gegevensuitwisseling binnen het onderwijs***

Edustandaard

Datum: april 2023

Versie: 0.7

Status: concept

**Inhoudsopgave**

[1. Documenthistorie 3](#_Toc128588443)

[2. Inleiding 4](#_Toc128588444)

[3. High level view 5](#_Toc128588445)

[4. Normatieve voorschriften 5](#_Toc128588446)

[4.1. Algemeen 5](#_Toc128588447)

[4.2. Uitwisseling met mandaten 5](#_Toc128588448)

[4.3. Geldigheidsduur mandaat 6](#_Toc128588449)

[4.4. uitwisselingen ondersteund door eindpunt informatie 6](#_Toc128588450)

[4.5. Geldigheidsduur eindpunt 7](#_Toc128588451)

[4.6. Normatieve voorschriften inrichting van OSR 8](#_Toc128588452)

[1. Bijlage: Rollen 8](#_Toc128588453)

[1.1. Eindorganisaties 8](#_Toc128588454)

[1.2. Verwerkers 8](#_Toc128588455)

[1.3. OSR Beheer 8](#_Toc128588456)

[2. Bijlage: domein modellen 9](#_Toc128588457)

[2.1. Mandaat model 9](#_Toc128588458)

[2.2. EndPoint model 10](#_Toc128588459)

# Documenthistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Auteur | Datum | Opmerking |
| 0.1 | E. Reinhoud | November 2022 | Outlines |
| 0.2, 0.3 | E. Borgers | November 2022 | Invulling met OSR |
| 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 |
| 0.61 | E. Borgers | April 2023 | Aangescherpt wanneer een mandaat verplicht is |

# Inleiding

[volgt later] Bewust buiten scope eerste review gelaten

# High level view



## V2V scenario

Deze afbeelding toont de uitwisseling tussen twee verwerkers

* Het 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 OSR 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 ketenpartner voor beide verwerkers.
* Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat van één of beide verwerkers.
* Het OSR doet een check op geldigheid van het PKI overheidscertificaat van de verwerker bij elke aanroep van OSR.
* Facultatief kan gebruik gemaakt worden van het eindpunt register waarmee URLs kunnen worden beheerd en opgevraagd (eenmalige opslag, meervoudig gebruik).

## V2nietV scenario



Deze afbeelding toont de uitwisseling tussen een verwerker en een niet verwerker (bv DUO)

* Voorwaardelijk voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van de geldigheid van het mandaat van de verwerker voldoende.
* Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat door de verwerkers.
* De niet verwerken kan er voor kiezen het scenario V2V te kiezen

# Normatieve voorschriften

## Algemeen

MUST: Dit protocol is verplicht bij de toepassing van het Secure API REST, WUS en/of OAuth profiel.

1. MUST: Er is een centraal landelijk register genaamd OSR met daarin verplicht alle mandaten en optioneel eindpunten van de betreffende partijen.
2. MUST: Implementatie van het protocol (autorisatie voor een uitwisseling door verwerkers) geschiedt inclusief raadpleging van het OSR (real-time of op andere wijze) voor hiertoe uitgereikte mandaten door een eindorganisatie
3. MUST: Onderliggend aan de implementatie is een ketensamenwerkingsafspraak waarin benodigde informatie voor de inrichting en gebruik zijn vastgelegd

## Registratie mandaten

MUST: Een eindorganisatie registreert de mandaten voor betreffende verwerkers actief in een ketensamenwerking voordat de verwerkers vertrouwelijke gegevens mogen uitwisselen onder elkaar, met andere verwerkers van andere eindorganisaties of met organisaties die wel gegevens verwerken, maar juridisch geen verwerker zijn (zie AVG).

Onder een mandaat vallen alle crud functies (HTTP verbs). Het hoeft dus niet per definitie een verstrekking (bevraging) te betreffen

* 1. MUST: Het OSR 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 gemachtigd is door de eindorganisatie om in het OSR mandaten te registreren.
	2. MUST: De verwerker heeft de voor mandatering benodigde systeemconfiguratie informatie en leverancier gegevens aangereikt aan de beheerder van OSR

## Uitwisseling met mandaten

MUST: Verwerkers in een uitwisseling moeten als voorwaarde voor een geslaagde uitwisseling het mandaat van de ander verifiëren

* 1. MUST: Het OSR biedt verwerkers (M2M) binnen een bepaalde ketensamenwerking de mogelijkheid om mandaten van zichzelf en van de andere verwerker te verifiëren.
	2. MUST: Alvorens uitgewisselde informatie te verwerken heeft verificatie van de mandaten van betrokken verwerkers in de uitwisseling plaatsgevonden met behulp van het OSR
	3. COULD: Alvorens uitgewisselde informatie te verwerken heeft verificatie van de eigen mandaten van beide verwerkers plaatsgevonden met behulp van het OSR
	4. COULD: Een verwerker kan gebruik maken van een mandaat mits deze verwerker deel uitmaakt van dezelfde verwerkersgroep[[1]](#footnote-2)
	5. MUST: Verificatie van het mandaat kan worden nagegaan op basis van de identificerende attributen van een verwerker en een eindorganisatie binnen de ketensamenwerking (heeft *deze verwerker* een mandaat van *deze eindorganisatie*)[[2]](#footnote-3).
	6. COULD: Verificatie van het mandaat kan worden nagegaan op basis van een identificerende attributen van een systeem binnen de ketensamenwerking (is er door *deze eindorganisatie* een mandaat afgegeven voor verwerking met *dit systeem*).[[3]](#footnote-4)
	7. MUST: De authenticatie van de digitale identiteit van de verwerker die een verificatie uitvoert geschiedt met een PKI certificaat.
	8. COULD: De verificatie van een verwerker op een mandaat van een andere verwerker kan alleen plaatsvinden door verwerkers binnen dezelfde ketensamenwerking[[4]](#footnote-5)

## Geldigheidsduur mandaten

MUST: de geldigheidsduur van een mandaat is te configureren en achterhalen

1. MUST: De datum waarop het mandaat moet ingaan en stoppen wordt vastgelegd door de Eindorganisatie.
2. MUST: De verandering van ingaan en vervallen valt samen met een datum overgang (24 uurs grens).
3. MUST: Een verwerker kan met OSR inzicht krijgen in de geldigheidsduur van zijn eigen mandaten.
4. MUST: Een verwerker kan met OSR inzicht krijgen in het op een bepaald moment geldig zijn van mandaten

## Beheren van routeringsadressen van administraties

Eindorganisaties hebben administraties. Deze beheren ze zelf of besteden ze uit aan leveranciers. Administraties hebben in het onderwijs een unieke identifier zoals vastgelegd in edukoppeling middels een routeringskenmerk. Een routeringskenmerk is opgebouwd uit een voorloper die het type organisatie aangeeft, gevolgd door een uniek nummer voor deze organisatie (een KVK nummer, een erkenningsnummer of in de toekomst wellicht een aanbiedersnummer) plus een suffix voor de administratie “binnen” de organisatie. Organisaties kunnen immers meerdere administraties zitten, bv meerdere Lassen. In Edukoppeling heeft een routeringskenmerk het formaat van een OIN, alhoewel er (nu) geen PKI diensten aan worden gekoppeld, dus een ander formaat zou kunnen.

De huidige standaard kent helaas mankementen:

1. Administraties kunnen overlappen, wat niet te duiden is, daar het routeringskenmerk betekenisvol is en daarmee een organisatiegrens zet. In de praktijk is dit nu geen probleem, omdat routeringskenmerken zich beperken tot juridische eenheden en die delen normaal gesproken geen administratie (zijn gescheiden).
2. Een meer praktisch probleem is dat over het suffix geen strikte afspraken zijn gemaakt. Administraties kunnen in principe een ander suffix krijgen per ketenafspraak, terwijl het feitelijk dezelfde administratie betreft. OSR registreert de suffixes en deelt vrije routeringskenmerken uit. OSR beheer streeft hergebruik van dezelfde suffix na over ketensamenwerkingen heen, maar dit is geen garantie. Dit bemoeilijkt beheer van routeringskenmerken voor leveranciers.
3. Het suffix is niet altijd bekend. Het gevolg is dan “broadcasten” waarbij alle administraties van de organisatie het bericht ontvangen. Dit is ongewenst. Daarom wil men liever gerichter adresseren. Een manier om dit te doen is middels onderwijsaanbieders. Een onderwijsaanbieder voert (veel) minder administraties. Edukoppeling voorziet momenteel helaas niet in routeringskenmerken voor onderwijsaanbieders.

MUST: Een administratie dient een binnen een organisatie die onderdeel is van een eindorganisatie en binnen een ketensamenwerking een uniek routeringskenmerk te hebben. Dit is in OSR opgeslagen.

1. MUST: Het OSR dient als centraal register voor routeringskenmerk uitgave en bevraging
2. MUST: Het routeringskenmerk heeft het format van een OIN (met een suffix ipv 000?)
3. MUST: OSR maakt claimen van een vrij routeringskenmerk mogelijk binnen een ketensamenwerking op basis van een OIN (zonder suffix?), zodat een routeringskenmerk gekozen kan worden door een verwerker dat uniek is voor een organisatieonderdeel van de eindorganisatie
4. SHOULD: Het routeringskenmerk van een administratie dient hetzelfde te zijn voor alle ketensamenwerkingen (over ketensamenwerkingen heen)
5. COULD: Het routeringskenmerk kan ook gebruikt worden voor adresseren van administraties van onderwijsaanbieders

## Uitwisselingen ondersteunen met eindpunt informatie

COULD: Eén of beide verwerkers betrokken bij een uitwisseling kunnen gebruik maken van de mogelijkheid gegevens over Eindpunten (zie ROSA) op te halen in OSR voor het correct adresseren van administraties[[5]](#footnote-6). Dit heeft als doel het verminderen van de administratieve last van het beheer en communiceren van eindpunt informatie (eenmalige opslag, meervoudig gebruik).

* 1. MUST: Verwerkers kunnen eindpunten configureren (CUD) in OSR als ze kunnen aantonen dat ze daartoe geautoriseerd zijn met behulp van een door OSR uitgereikt token aan de verwerker
	2. MUST: De authenticatie van de digitale identiteit van de verwerker die M2M eindpunten opvraagt of beheert (CRUD) gebeurt met een PKI certificaat.
	3. MUST: Voor een eindpunt is opvraagbaar de url van het eindpunt, het routeringskenmerk van de administratie, de identifier van de ketensamenwerking en de namespace.
	4. COULD: Het beheren van eindpunten beperkt zich tot verwerkers die een mandaat hebben voor de ketensamenwerking[[6]](#footnote-7)
	5. COULD: Het opvragen van eindpunten beperkt zich tot verwerkers die een mandaat hebben voor de ketensamenwerking
	6. SHOULD: Het routeringskenmerk voor hetzelfde eindpunt is gelijk over alle ketensamenwerkingen.
	7. MUST: In de ketensamenwerkingsafspraak voor het benaderen van eindpunten wordt informatie opgenomen welke [namespaces](https://rosa.wikixl.nl/index.php/F662c02f-0c2d-4457-9746-1fd8e617e037) gewenst zijn[[7]](#footnote-8)
	8. MUST: Eindpunten zijn opvraagbaar op basis van 1) ketensamenwerkingen, 2) de OIN van een eindverwerker of identifiers van administraties, in alle gevallen 3) optioneel gefilterd met namespaces

## Geldigheidsduur eindpunten

MUST: de opvraagbaarheid van eindpunt informatie is te configureren en deze datum is te achterhalen

1. MUST: De datum waarop informatie over het eindpunt beschikbaar komt en wanneer deze niet meer opvraagbaar is, wordt vastgelegd door de Verwerker.
2. MUST: De verandering van beschikbaar komen en vervallen valt samen met een datum overgang (24 uurs grens).
3. MUST: Een verwerker kan met OSR inzicht krijgen in de ingangs- en eind data van zijn eigen eindpunten.
4. MUST: Een verwerker kan met OSR inzicht krijgen in het op een bepaald moment opvraagbaar zijn van eindpunten

## Normatieve voorschriften beheerorganisatie OSR

MUST: Voor het kunnen gebruiken van OSR worden algemene afspraken gemaakt met OSR

* 1. MUST: Eindorganisaties en verwerkers sluiten een aansluitcontract af met de OSR beheerder voor het gebruik van het OSR
	2. MUST: Informatie over systemen van verwerkers worden ingebracht in samenspraak met de OSR beheerder
	3. MUST OSR beheer ondersteunt verwerkers en eindorganisaties in het correct gebruik van OSR en levert conform contract

# Bijlage: Rollen

## Tekenbevoegde en beheerder van een eindorganisaties

* Eindorganisatie: als eindorganisatie geldt een juridische eenheid. Deze heeft een KVK nummer. Dit is doorgaans een bestuur of een agentschap. Een leverancier kan ook als eindorganisatie optreden, maar dan is sprake van een constructie met subverwerkers.
* Machtiging tot CRUD acties op mandaten worden verstrekt door een tekenbevoegde (bestuurder) van eindorganisatie aan de mandaat beheerder.
* Beheerder eindorganisatie: Deze moet zich kunnen identificeren en beschikken over de autorisatie zoals verkregen van de eindorganisatie en gevalideerd door OSR
* Vertegenwoordiger eindorganisatie: helpt met het opstellen van een ketensamenwerking

## Beheerder van een verwerker

* Een verwerkersorganisatie moet een OIN hebben en een daaraan gekoppeld PKI certificaat
* De verwerkersorganisatie geeft aan welke systemen potentieel gebruikt kunnen worden voor welke ketensamenwerkingen en stemmen dit af met de OSR beheerder.
* De contactpersoon van de verwerkersorganisatie verkrijgt een token van de OSR beheerder voor het beheren van eindpunten en routeringskenmerken van administraties in OSR voor het betreffende systeem
* Een systeem van de verwerker zorgt voor M2M beheer van eindpunt informatie in OSR
* De IT afdeling van de verwerker dient OSR te gebruiken zoals afgesproken in deze standaard en conform de OSR API guidelines.
* Vertegenwoordiger verwerker: helpt met het opstellen van een ketensamenwerking

## OSR Beheerder

* De OSR functioneel beheerder ondersteunt verwerkers bij het inrichten van OSR.
* De OSR functioneel beheerder verstrekt OSR API tokens aan verwerkers.
* OSR product management verzamelt wensen aangaande OSR, vertaalt deze naar requirements en prioriteert deze op advies van haar stakeholders.
* De OSR Systeem architect (technisch specialist) bewaakt de realisatie en operatie van OSR conform requirements.
* De OSR architect ondersteunt bij de aansluiting van de requirements van OSR op Edukoppeling, in het bijzonder het secure API protocol.

# Bijlage: domein modellen

## Mandaat model



## EndPoint model



Notes

* EindPunten zijn specifiek voor een administratie. De naam van een URL kan meerdere administraties duiden. Zo kan de naam van de URL eindorganisatie of onderwijsaanbieder specifiek zijn. Dit is zeker het geval als de administraties fysiek gescheiden zijn door de verwerker.
* Binnen een ketensamenwerking dient een uniek suffix per eindorganisatie en administratie te worden gebruikt.
* Een mandaat is in dit model niet nodig. Wel kan het als voorwaarde worden gesteld[[8]](#footnote-9).

Note: Dit model is nog niet zoals ik het wil. De Id Eindorganisatie is namelijk niet persé onderdeel van het routeringskenmerk. De Id Eindorganisatie is het bestuur, maar Bij het routeringskenmerk gebruiken we in Edukoppeling nu een BRIN4 (erkenningscode van een onderwijsinstelling). Daarnaast is het de wens om een Onderwijsaanbiederscode te kunnen gebruiken

In OSR v2 en Edukoppeling wordt het routeringskenmerk gebruikt, opgebouwd uit een onderwijsinstellingserkenning nummer (voorheen BRIN4) plus een uniek random gekozen volgnummer binnen de ketensamenwerking. Echter in principe kan een administratie ook anders geduid worden, bijvoorbeeld als behorende bij een onderwijsaanbieder of een vestiging/locatie.

1. In OSR v2 is dit altijd het geval om geen extra administratieve lasten te laten ontstaan als de organisatie van leveranciers verandert [↑](#footnote-ref-2)
2. In OSR v2 geldt dat als een verwerker een mandaat krijgt voor een informatiesysteem van de verwerker, dit mandaat ook geldig is voor *alle* andere informatiesystemen van die verwerker. [↑](#footnote-ref-3)
3. Een OSR Systeem Id, de URL of een routeringskenmerk kunnen gebruikt worden als identificerend attribuut. [↑](#footnote-ref-4)
4. Dit betekent bijvoorbeeld dat een verwerker geen mandaat kan opvragen van een ketensamenwerking waarin deze niet participeert (überhaupt of voor een eindorganisatie) [↑](#footnote-ref-5)
5. Een administratie is hier bedoeld in ruime zin: als een plek in een (SaaS) systeem dat is ingericht voor (een deel van) de Eindorganisatie. Dat kan bijvoorbeeld zijn de administratie zijn van een bestuur, een onderwijsinstelling (met een erkenning), van een onderwijsaanbieder of van alle onderwijsinstellingen beheerd door een agentschap. [↑](#footnote-ref-6)
6. In OSR v2 is bezit van een mandaat verplicht voor registreren (MUST) [↑](#footnote-ref-7)
7. Dit om verschillende soorten eindpunten te kunnen onderscheiden bijvoorbeeld omdat er meerdere webservices zijn. OSR dringt geen classificaties op en laat dit puur aan de ketensamenwerking. [↑](#footnote-ref-8)
8. In OSR2 is een mandaat een noodzakelijke voorwaarde [↑](#footnote-ref-9)