Edukoppeling

Secure API protocol

M2M gegevensuitwisseling binnen het onderwijs

Edustandaard
Datum: maart 2023
Versie: 0.6
Status: concept

edustandaard

Inhoudsopgave

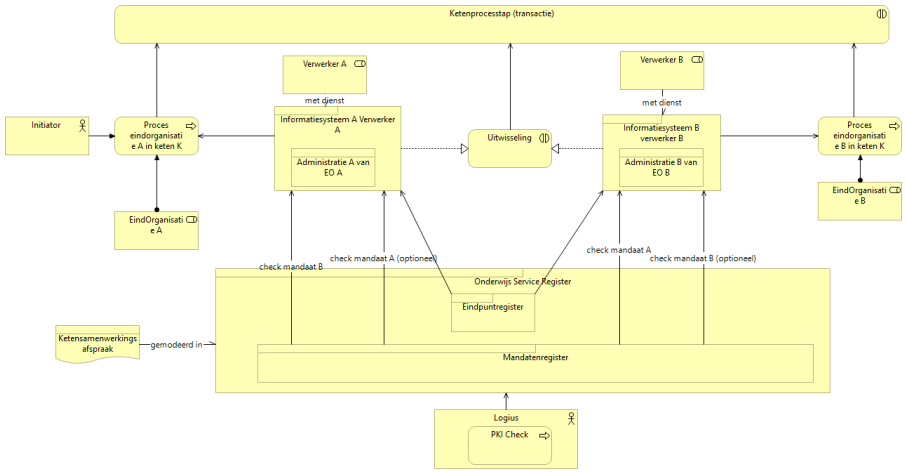
1. Documenthistorie

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

2. Inleiding

[volgt later] Bewust buiten scope eerste review gelaten

3. High level view



Deze afbeelding toont

- 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).

4. Normatieve voorschriften

4.1. Algemeen

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

a) 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
b) MUST: Onderliggend aan de implementatie is een ketensamenwerkingsafspraak waarin benodigde informatie voor de inrichting en gebruik zijn vastgelegd

4.2. Uitwisseling met mandaten

MUST: Een eindorganisatie registreert de mandaten voor betreffende verwerkers actief in een ketensamenwerking voordat de verwerkers vertrouwelijke gegevens mogen uitwisselen. Onder een mandaat vallen alle crud functies (HTTP verbs). Het hoeft dus niet per definitie een verstrekking (bevraging) te betreffen

a. 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.
b. MUST: De verwerker heeft de voor mandatering benodigde systeemconfiguratie informatie en leverancier gegevens aangereikt aan de beheerder van OSR

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

c. MUST: Het OSR biedt verwerkers (M2M) binnen een bepaalde ketensamenwerking de mogelijkheid om mandaten van zichzelf en van de andere verwerker te verifiëren.
d. MUST: Alvorens uitgewisselde informatie te verwerken heeft verificatie van de mandaten van beide verwerkers plaatsgevonden met behulp van het OSR
e. COULD: Alvorens uitgewisselde informatie te verwerken heeft verificatie van de eigen mandaten van beide verwerkers plaatsgevonden met behulp van het OSR
f. COULD: Een verwerker kan gebruik maken van een mandaat mits deze verwerker deel uitmaakt van dezelfde verwerkersgroep[1]
g. 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].
h. 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]
i. MUST: De authenticatie van de digitale identiteit van de verwerker die een verificatie uitvoert geschiedt met een PKI certificaat.
j. COULD: De verificatie van een verwerker op een mandaat van een andere verwerker kan alleen plaatsvinden door verwerkers binnen dezelfde ketensamenwerking[4]

4.3. Geldigheidsduur mandaat

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

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

4.4. uitwisselingen ondersteund 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]. Dit heeft als doel het verminderen van de administratieve last van het beheer en communiceren van eindpunt informatie (eenmalige opslag, meervoudig gebruik).

Met opmerkingen [KR1]: Kan zijn dat dit later nog terugkomt maar om het niet te vergeten: als de verwerker ook de eindorganisatie is (zoals bij DUO) is een mandatenregistratie dan noodzakelijk/gewenst?

Met opmerkingen [EB2R1]: We bespraken eerder dat uit oogpunt van uniformiteit/simpliciteit van de standaard/protocol, we geen onderscheid maken tussen commerciele of overheidsorganisaties. Anderzijds kan ik mij voorstellen dat OSR zo slim is, dat bv DUO niet in OSR mandaten per dienst/ketensamenwerking hoeft te registreren, omdat de business logica van OSR herkent dat de bevraging DUO betreft (OIN=DUO) en dat er voor DUO een vinkje staat om altijd OK terug te geven. Dat scheelt DUO administratieve lasten. Dit issue hoort dan niet in de standaard, maar komt in de requirements van OSR 3.0

Met opmerkingen [EB3R2]: Anderzijds is het erg weinig werk en kan DUO het ook juist prettig vinden om een overzicht te hebben van eigen mandaten = ketens waarin ze actief is

Met opmerkingen [EB4R1]: Hetzelfde geldt voor Ketenpartners die in OSR in potentie kunnen opvragen wie in de keten zit.

Met opmerkingen [EB5R1]: Ik besef wel: als partijen het mandaat bij DUO opvragen (of nog sterker, DUO zijn eigen mandaat checkt terwijl dat altijd OK is, roomser dan de paus), dan kost dit soms code aanpassen in systemen, CPU en vertragingstijd. Ik kan mij voorstellen dat sommige ketens dan in hun afspraak vastleggen dit na te laten. Maar het kan dus ook zo zijn dat in andere ketens het juist fijn is in code geen IF-THENs te hoeven inbouwen voor alle partijen.

Met opmerkingen [EB6R1]: Kort antwoord: ja. Maar we kunnen het wel makkelijk maken zonder de standaard geweld aan te doen.

Met opmerkingen [EB7R1]: Opgelost?

Met opmerkingen [EB8]: Commentaar Robert Kas is in de bewerking helaas verdwenen (zie v0.5). Maar het kunnen configureren is vervallen. Er geldt een minimum duur om cashen mogelijk te maken. Dit is nu de daggrens. Er geldt een in te stellen maximum duur voor vervallen voor vermindering lasten en voorkomen van vergeten autorisaties. In een OSR implementatie zou dat eventueel optioneel op "nooit" gezet kunnen worden.

[1] In OSR v2 is dit altijd het geval om geen extra administratieve lasten te laten ontstaan als de organisatie van leveranciers verandert
[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.
[3] Een OSR Systeem Id, de URL of een routeringskenmerk kunnen gebruikt worden als identificerend attribuut.
[4] Dit betekent bijvoorbeeld dat een verwerker geen mandaat kan opvragen van een ketensamenwerking waarin deze niet participeert (überhaupt of voor een eindorganisatie)
[5] Een administratie is hier bedoeld in ruime zin: als een plek in een (SaaS) systeem dat is ingericht voor (een deel van) de organisatie van de Eindverantwoordelijke. Dat kan bijvoorbeeld zijn de administratie zijn van een school, van een onderwijsaanbieder, van alle HBOs in nederland gevoerd door een agentschap of van een groep in een leersysteem.

a. 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
b. MUST: De authenticatie van de digitale identiteit van de verwerker die M2M eindpunten opvraagt of beheert (CRUD) gebeurt met een PKI certificaat.
c. MUST: Voor een eindpunt is opvraagbaar de url van het eindpunt, het routeringskenmerk van de administratie, de identifier van de ketensamenwerking en de namespace.
d. COULD: Het beheren van eindpunten beperkt zich tot verwerkers die een mandaat hebben voor de ketensamenwerking[6]
e. COULD: Het opvragen van eindpunten beperkt zich tot verwerkers die een mandaat hebben voor de ketensamenwerking
f. SHOULD: Het routeringskenmerk voor hetzelfde eindpunt is gelijk over alle ketensamenwerkingen.
g. MUST: In de ketensamenwerkingsafspraak voor het benaderen van eindpunten wordt informatie opgenomen welke namespaces gewenst zijn[7]
h. 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

Met opmerkingen [KR9]: Even voor mij:dit is dus enkel M2M? Anders ook via e<Herkenning?

Met opmerkingen [EB10R9]: Inderdaad, in deze MUST/requirement alleen M2M. Ik heb dat verhelderd. Dit is nu ook de praktijk in OSRv2.

Met opmerkingen [EB11R9]: Het is een idee dit ook handmatig te kunnen doen. In OSR v2 kan dat nu niet, maar mogelijk is hier behoefte aan en voegen we dit toe.

Met opmerkingen [KR12]: naamruimtes?? Dan is namespace duidelijker toch?

Met opmerkingen [EB13R12]: Beide mag van de ROSA. Naamruimte staat daar zelfs als geprefereerde term (lekker Hollands). Maar ik verander het met plezier. Ik heb de link gelegd naar de ROSA.

Met opmerkingen [EB14R12]: Opgelost?

Note: Administraties hebben geen unieke identifier in het onderwijs (zijn ook niet opgenomen in RIO). Om een administratie uniek te duiden is een meervoudige sleutel nodig. Deze is opgebouwd uit de ketensamenwerkingscode en een routeringskenmerk. Het routeringskenmerk in EduKoppeling bestaat uit een vaste voorloper, een instellingscode plus een driecijferig volgnummer per administratie binnen de instelling. Tesamen heeft dit het format van een OIN. Een administratie oogt daarmee als (virtueel) organisatieonderdeel. Hetzelfde routeringskenmerk kan echter ook in een andere ketensamenwerking gebruikt worden, terwijl het dus niet om dezelfde administratie gaat. OSR beheer adviseert hergebruik van hetzelfde routeringskenmerk over de ketensamenwerkingen heen, maar kan dit (momenteel) niet afdwingen.
Note: Eindpunten hebben ook geen unieke identifier. De identifier van een eindpunt bestaat uit de meervoudige sleutel van een administratie (ketensamenwerkingscode + routeringskenmerk) plus een URL. Indien een administratie meerdere eindpunten heeft, zullen de URLs hiervan dus verschillen.
Note: Van een routeringskenmerk is (mede door bovenstaande) in de praktijk vaak alleen de instellingscode bekend. Binnen een instelling bevinden zich in potentie veel administraties. Het gevolg is dat eindpunten worden opgehaald van alle administraties en een broadcast plaatsvindt. Een wens is voor routeringskenmerken ook andere opbouwen toe te staan. Een mogelijke vorm is onderwijsaanbieder + volgnummer. Binnen een onderwijsaanbieder zijn er veel minder administraties. Als de Eindverantwoordelijke geen onderwijsinstelling is, maar bijvoorbeeld een agentschap, is weer een andere vorm van routeringskenmerk wenselijk (bv om een RIO eindpunt te duiden).

4.5. Geldigheidsduur eindpunt

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

[6] In OSR v2 is bezit van een mandaat verplicht voor registreren (MUST)
[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.

4.6. Normatieve voorschriften algemeen gebruik van OSR

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

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

1. Bijlage: Rollen

1.1. Eindorganisaties

- Eindorganisatie: eindorganisaties moeten hun administratie duiden met een uniek routeringskenmerk. Dit wordt (momenteel) voor hen gedaan door een Verwerker. De eindorganisatie heeft er zelf geen weet van.
- Machtiging vertrekker eindorganisatie (aan beheerder). Deze machtigt de beheerder van de eindorganisatie voor het mandateren in OSR.
- 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

1.2. Verwerkers

- 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

Met opmerkingen [KR15]: Moet dat niet zijn: OSR beheerder?

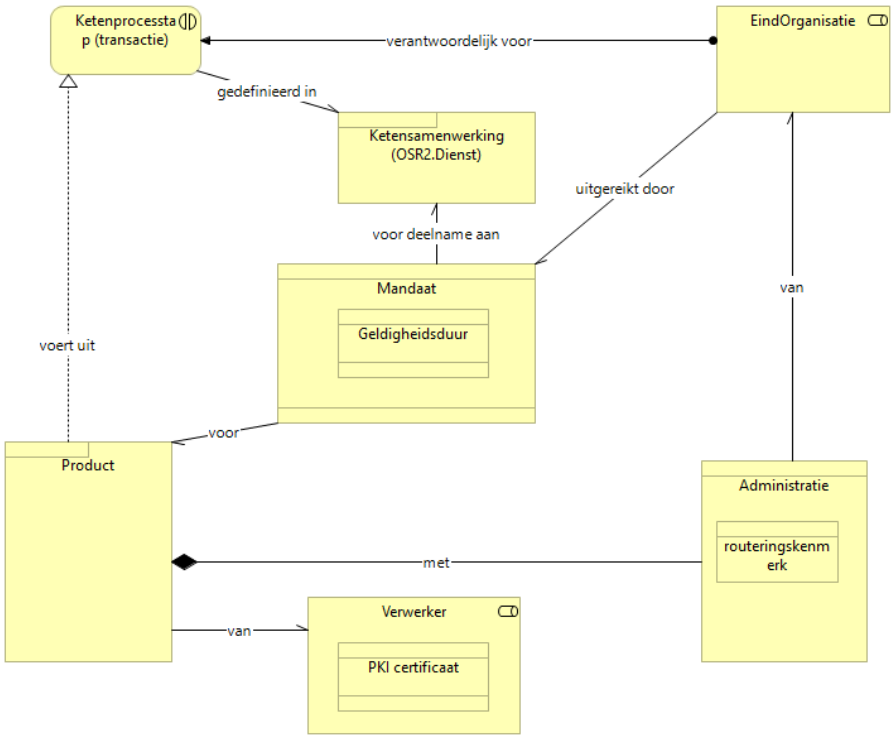
Met opmerkingen [EB16R15]: Check

1.3. OSR Beheer

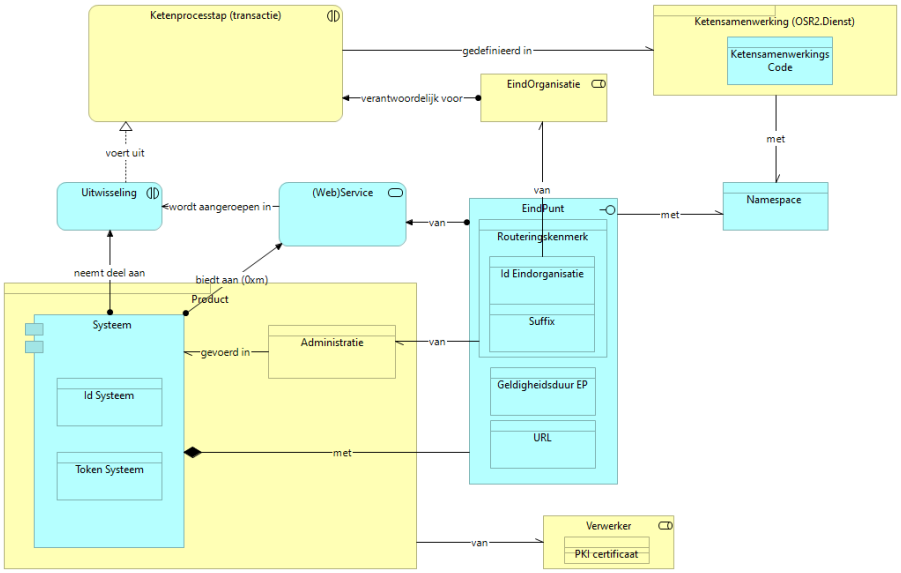
- De OSR functioneel beheerder ondersteunt verwerkers bij het inrichten van OSR.
- De OSR functioneel beheerder verstrekt OSR API tokens aan verwerkers.
- OSR product management verzamelt wensen aangaande OSR, vertaalt deze naar requirements en prioriteert deze op advies van haar stakeholders.
- De OSR 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.

2. Bijlage: domein modellen

2.1. Mandaat model



2.2. 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].

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.

[8] In OSR2 is een mandaat een noodzakelijke voorwaarde