Edukoppeling

Secure API protocol

M2M gegevensuitwisseling binnen het onderwijs

Edustandaard
Datum: november 2022
Versie: 0.5
Status: concept

edustandaard

Inhoudsopgave

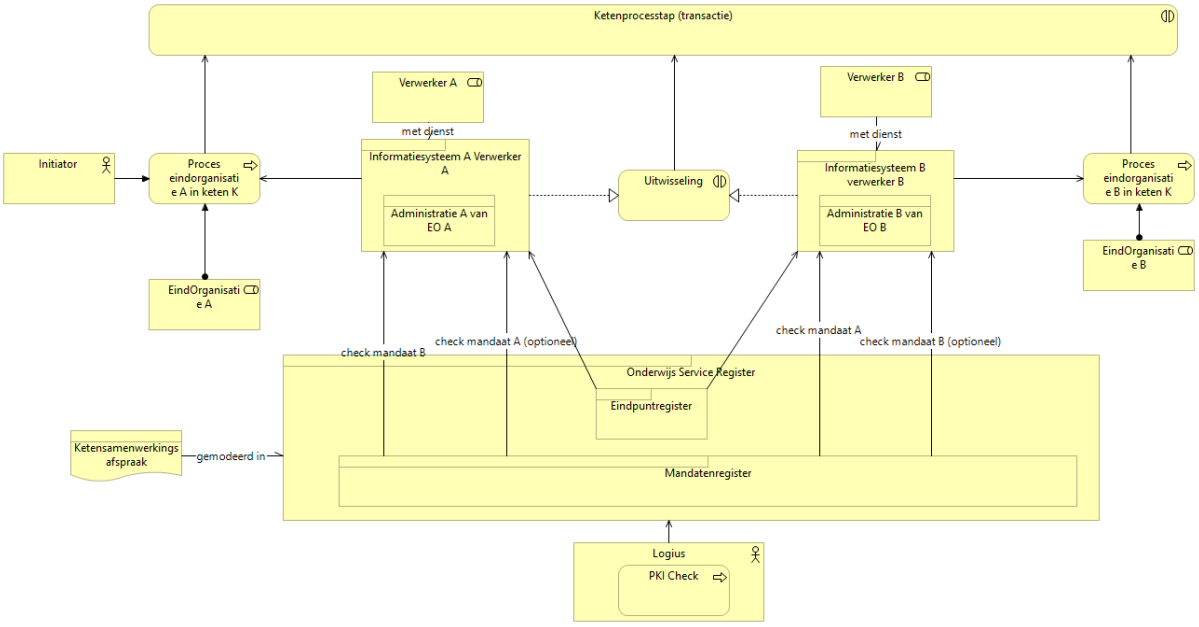
1. Documenthistorie

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

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 mandaat check van de ketenpartner.
- Optioneel voor een geslaagde ketenprocesstap (uitwisseling) is een geslaagde check van het eigen mandaat.
- 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 gebruik protocol 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

5. Normatieve voorschriften 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. SHOULD: Raadplegen van OSR heeft een minimale impact op kwalitatieve aspecten van de uitwisseling buiten die van autorisatie[4]
k. COULD: De verificatie van een verwerker op een mandaat van een andere verwerker kan alleen plaatsvinden door verwerkers binnen dezelfde ketensamenwerking[5]

6. Normatieve voorschriften uitwisselingen ondersteund door 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 elkaar en het verminderen van administratieve lasten (eenmalige opslag, meervoudig gebruik)

a. MUST: Verwerkers kunnen eindpunten configureren op een systeem als ze kunnen aantonen dat ze daartoe geautoriseerd zijn met behulp van een door OSR uitgereikt token aan de verwerker
b. COULD: In de ketensamenwerkingsafspraak voor het benaderen van eindpunten aanvullende informatie opgenomen welke naamruimtes gewenst zijn[6]
c. MUST: Eindpunten zijn opvraagbaar op basis van 1) ketensamenwerkingen, 2) de OIN van een eindverwerker of routeringskenmerken van administraties en 3) optioneel gefilterd met naamruimtes[7]
d. MUST: De authenticatie van de digitale identiteit van de verwerker die registreert en beheert of opvraagt geschiedt met een PKI certificaat.
e. COULD: Het registreren en/of opvragen van eindpunten beperkt zich tot verwerkers die een mandaat hebben voor de ketensamenwerking[8]

---

[1] In OSR 2 is dit altijd het geval om geen extra administratieve lasten te laten ontstaan als de organisatie van leveranciers verandert

[2] In OSR 2 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] Denk hierbij met name aan performance en implementatie effort (ook bij wijzigingen van OSR buiten dit protocol)

[5] Dit betekent bijvoorbeeld dat een verwerker geen mandaat kan opvragen van een ketensamenwerking waarin deze niet participeert (überhaupt of voor een eindorganisatie)

[6] 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.

[7] Een nameruimte onderscheid typen van eindpunten, zoals bijvoorbeeld verschillende soorten onderliggende services.

[8] In OSR 2 is bezit van een mandaat verplicht voor registreren maar niet voor opvragen

7. Normatieve voorschriften inrichting van OSR

MUST: Er is een afspraak opgesteld door de ketenpartners die in OSR wordt gemodelleerd in samenspraak met de OSR beheerder

a. MUST: Samen met de Kennisnet beheerder wordt een unieke ketensamenwerkingsnaam opgenomen
b. MUST: Potentiële systemen met de benodigde verwerkersgegevens en routeringskenmerken van eindorganisaties voor een bepaalde ketensamenwerking worden ingebracht in samenspraak met de Kennisnet beheerder
c. MUST: Eindorganisaties en verwerkers sluiten een contract af met Kennisnet voor het gebruik van het OSR
d. MUST: In het geval men gebruik wenst te maken van eindpunten worden hiertoe op basis van de ketensamenwerking aanvullende afspraken gemaakt met de Kennisnet beheerder voor unieke naamruimtes

8. Geldigheidsduur mandaat en eindpunten

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

a. MUST: In een ketensamenwerking wordt de minimale en maximale geldigheidsduur van een mandaat vastgelegd[9]
b. MUST: Een eindorganisatie bepaalt de geldigheidsduur van een mandaat binnen de kaders van een afgesproken minimale en/of maximale geldigheidsduur in de ketensamenwerking en beheert deze in OSR
c. MUST: Een verwerker kan met OSR inzicht krijgen in de afgesproken maximale en minimale geldigheidsduur in de ketensamenwerking
d. MUST: Een verwerker kan inzicht krijgen in de geldigheidsduur van zijn eigen mandaten met OSR
e. MUST: Een verwerker kan met OSR inzicht krijgen in het op dat moment wel of niet geldig zijn van het mandaat van een andere verwerker

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

f. Als bij mandaten. Voor eigen eindpunten is ook nu weer meer info beschikbaar (onder andere ook geldigheidsduur en gekoppeld systeem) dan van eindpunten van derden (minimaal URL, routeringskenmerk(en) van onderliggende administraties, OIN eindorganisatie, naamruimtes en systeem informatie)

1. Bijlage: Rollen

1.1. Eindorganisaties

- Eindorganisatie: eindorganisaties moeten een OIN hebben en 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 Kennisnet beheerder.

[9] In OSR 2 betreft de minimale geldigheid de datum van een dag, waarbij een mandaat dus kan vervallen op de 24 uurs grens.

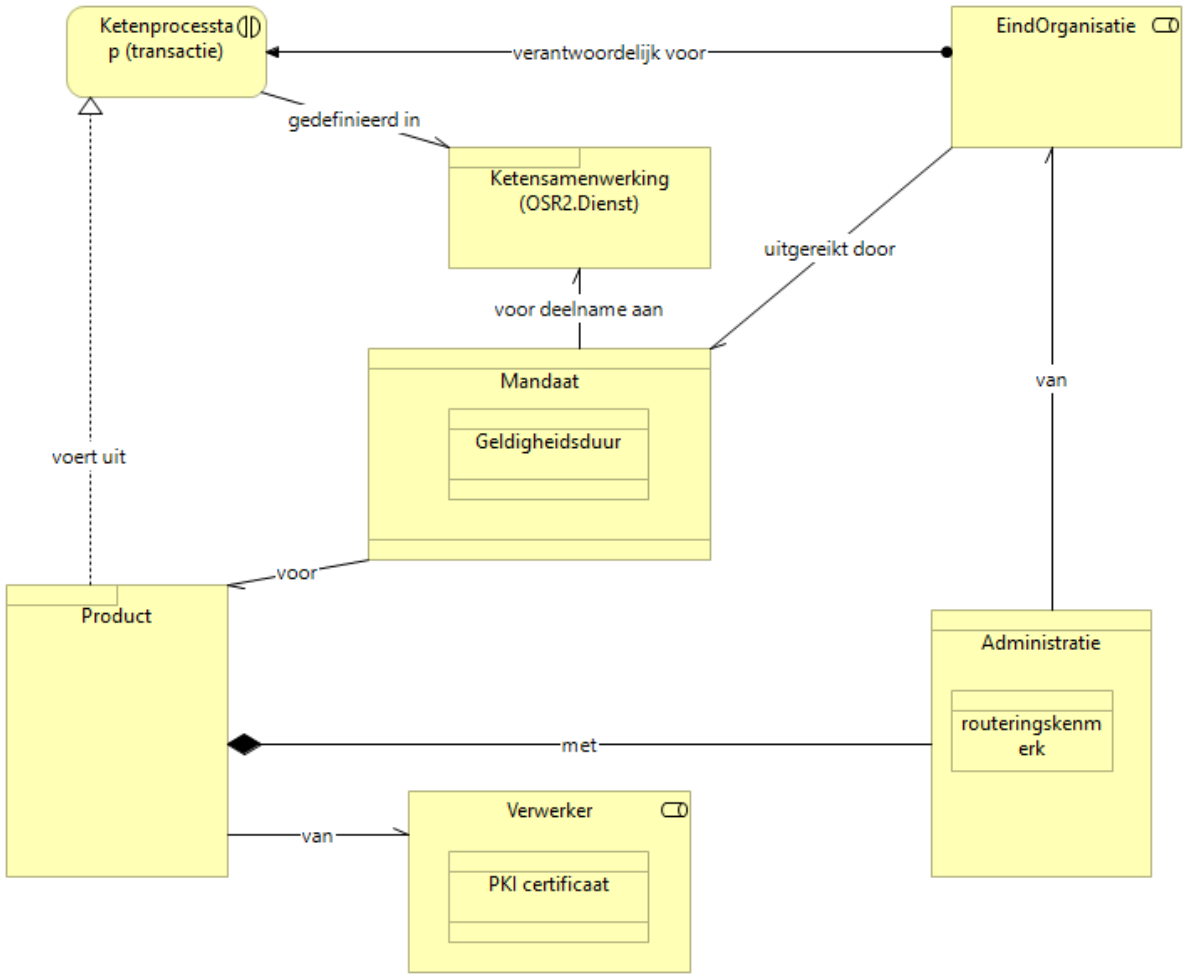
- De contactpersoon van de verwerkersorganisatie verkrijgt een token van Kennisnet voor het beheren van eindpunten en routeringskenmerken van administraties in OSR voor het betreffende systeem
- Een systeem van de verwerker zorgt voor beheer van eindpunt informatie in OSR
- De IT afdeling van de verwerker dient OSR te gebruiken zoals afgesproken in deze standaard en conform de OSR API guidelines.
- Vertegenwoordiger verwerker: helpt met het opstellen van een ketensamenwerking

1.3. OSR Beheer (Kennisnet)

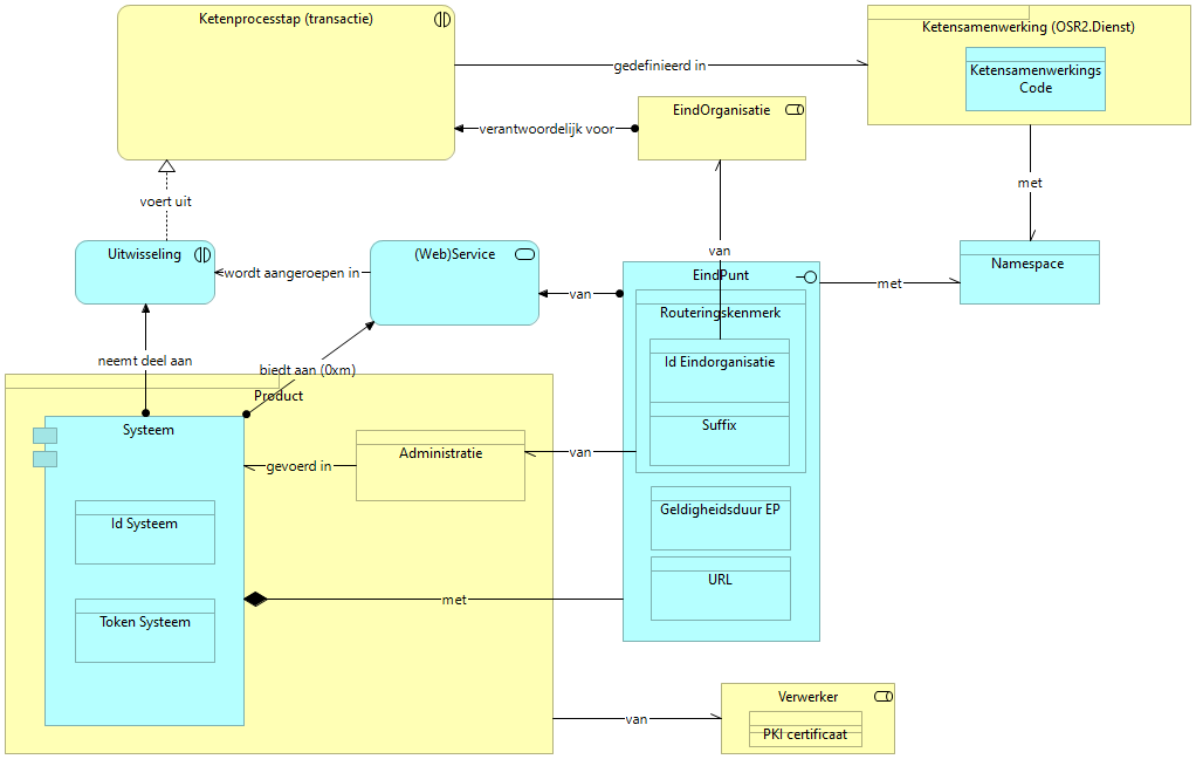
- De OSR functioneel beheerder ondersteunt verwerkers bij het inrichten van OSR.
- De OSR functioneel beheerder verstrekt OSR API tokens aan verwerkers.
- OSR product management verzamelt wensen aangaande OSR, vertaalt deze naar requirements en prioriteert deze op advies van haar stakeholders.
- De OSR 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 kunnen in de praktijk specifiek zijn voor een administratie. Zo kan de naam van de URL eindorganisatie specifiek zijn 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[10].

[10] In OSR2 is een mandaat een noodzakelijke voorwaarde