Edukoppeling

Secure API protocol

M2M gegevensuitwisseling binnen het onderwijs

Edustandaard
Datum: november 2022
Versie: 0.4
Status: concept

heeft verwijderd: 1

edustandaard

Inhoudsopgave

1. Documenthistorie

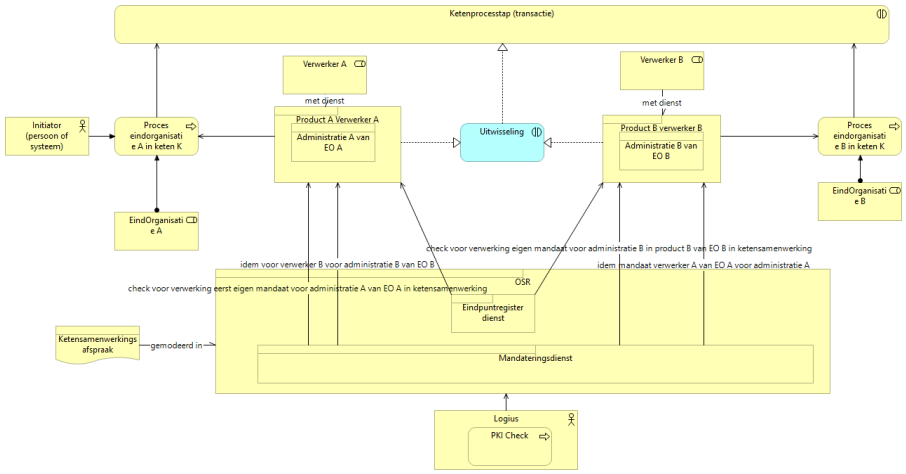
Versie	Auteur	Datum	Opmerking
0.1	E. Reinhoud	November 2022	Outlines
0.2, 0.3	E. Borgers	November 2022	Invulling met OSR
0.4	E. Borgers	November 2022	Verspreid ter review aan de edukoppeling werkgroep

heeft verwijderd: 11

2. Inleiding

[volgt later] Bewust buiten scope eerste review gelaten

3. High level view



Deze afbeelding toont

- OSR ondersteunt de autorisatie op een uitwisseling voor alle profielen en alle soorten patronen (waaronder notificatie, synchroon en asynchrone uitwisseling)
- OSR ondersteunt zo verwerkers in het realiseren van ketenprocesstappen (zie ROSA) voor eindorganisaties.
- OSR doet **geen** uitspraak over de content van het uitgewisselde. Hiervoor kunnen indien gewenst aanvullende maatregelen getroffen te worden, maar OSR faciliteert hier niet in en legt geen restricties op.
- OSR vraagt **niet** om bewijs van aanvullende afspraken/contracten tussen de partijen, maar enkel om mandatering. Dergelijke afspraken zijn buiten scope van OSR. Deze verschillen bij voorbeeld per type uitgewisselde informatie (privacy, vertrouwelijk, vrij), soort organisatie (leverancier, onderwijsorganisatie, aanbieder, vestiging, landelijke partij, etc.) en mogelijk op andere punten.
- Voorwaardelijk voor een geslaagde ketenprocesstap (uitwisseling) is een voorafgaande geslaagde mandaat check van het eigen mandaat en dat van de ander, aan beide zijden van de uitwisseling (beide ketenpartners).
- Er dienen hiertoe geldige mandaten in OSR te zijn. Deze worden versterkt door de eindorganisatie *aan* de verwerker voor deelname in een specifieke ketensamenwerking betreffende de administraties van de eindorganisatie binnen een aangewezen product van de verwerker. Voor elke ketensamenwerking dient er voor elke administratie een mandaat te zijn. OSR heeft één mandaat voor alle administraties binnen een product. [1]
- OSR legt geen restricties op aan het aantal partijen. Er moet wel een ketenafspraak zijn met daarin minimaal de (unieke) naam van de ketensamenwerking. De partijen die deel kunnen nemen (verwerkers en eindorganisaties) worden gemodelleerd in OSR.
- OSR doet een check op geldigheid van het PKI van de verwerker bij elke aanroep van OSR.
- Facultatief kan gebruik gemaakt worden van de eindpunt functionaliteit waarmee URLs kunnen worden beheerd en opgevraagd (eenmalige opslag, meervoudig gebruik).

[1] Beter is vanuit autorisatie oogpunt om een mandaat per administratie uit te reiken, maar dit betekent extra administratieve lasten voor de eindverwerker en een impediment is dat de eindverwerker geen administraties kan aanwijzen bij een gebrek aan een afgesproken Id voor administraties (de verwerker kan dit wel op basis van een met behulp van OSR vrijgegeven routeringskenmerk). Daarom wijst de eindverwerker in OSR momenteel een product aan bij mandateren.

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[2] voor hiertoe uitgereikte mandaten door een Eindorganisatie
b) MUST: Onderliggend aan de implementatie is een ketensamenwerkingsafspraak waarin minimaal de ketennaam genoteerd is
c) SHOULD: De ketensamenwerking kan desgewenst door OSR ondersteund worden met het centraal registreren en uitvragen van eindpunten van verwerkers door OSR voor minder administratieve lasten en een meer foutloze en beter beheerde M2M communicatie[3].
    a. MUST: In de ketensamenwerkingsafspraak voor het benaderen van eindpunten aanvullende informatie opgenomen welke namespaces gewenst zijn[4]

5. Normatieve voorschriften uitwisseling met mandaten

a. MUST: Een eindorganisatie registreert de mandaten voor betreffende verwerkers actief in een ketensamenwerking voordat de verwerkers vertrouwelijke gegevens mogen uitwisselen[5]
    a. MUST: Het OSR kan verifiëren dat de (H2M) registratie van het mandaat namens een Eindorganisatie wordt gedaan. De digitale identiteit kan herleid naar de eindorganisatie en verificatie is mogelijk dat deze gemachtigd is door de Eindorganisatie om in het OSR mandaten te registreren.
    b. MUST: De verwerker heeft de voor mandatering benodigde systeeminformatie[6], routeringskenmerken en leverancier gegevens aangereikt aan de Kennisnet beheerder
    c. MUST: Het mandaat geldt enkel voor de administraties binnen het product van de verwerker dat de Eindorganisatie heeft gemandateerd.[7]
    d. MUST: Het mandaat geldt enkel voor deelname in de door de eindorganisatie aangewezen ketensamenwerking
    e. COULD: Het mandaat beperkt zich tot bepaalde uitwisselingen tussen systemen of administraties (de zogenaamde paden) in een daaraan toegewezen ketensamenwerking[8]
    f. SHOULD: Het beheer van mandaten door de Eindorganisatie streeft naar minimale administratieve last voor de Eindorganisatie, Leveranciers en Kennisnet[9]
b. MUST: Beide verwerkers in een uitwisseling moeten als voorwaarde voor een geslaagde uitwisselingen eerst het eigen mandaat en dat van de ander verifiëren

---

[2] Voor varianten als cashing en/of het gebruik maken van geldigheidstermijnen zie later in het document.
[3] Zo wordt verminderd dat foute of verouderde URLs worden aangesproken en tevens dat eindpunt informatie moet worden “rondgepompt” tussen de ketenpartners over niet secure kanalen.
[4] 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.
[5] Onder het mandaat vallen alle crud functies (HTTP verbs). Het hoeft dus niet per definitie een verstrekking (bevraging) te betreffen
[6] In OSR is voor het mandateren de systeem informatie nodig omdat de beheerder van de eindorganisatie kiest voor deelname van een product met de daarin opgenomen administraties. Een autorisatie verbetering zou zijn te mandateren op administraties (routeringskenmerken), maar hier is momenteel geen oplossing voor. Dit is een punt van toekomstig onderzoek. Voor het endpoint register is deze informatie in OSR nodig ter authenticatie van de verwerker.
[7] In OSR 2.0 geldt nu dat als een verwerker een mandaat krijgt voor een product, dit geldig is voor *alle* administraties in *alle* producten die de verwerker in de ketensamenwerking voert. Voorstel is de mandatering specifieker te binden op de administraties binnen het door de eindorganisatie aangewezen product. De consequentie hiervan is dan wel dat bij opvragen van een mandaat het routeringskenmerk, de URL of de OSR systeem REST Id in de ketensamenwerking bekend is, daar dit de administratie resp het systeem identificeert. Dit is een punt ter discussie met de werkgroep en stakeholders van OSR.
[8] Dit is in OSR nu niet geïmplementeerd.
[9] Dit is altijd een balans tussen de partijen en wat vanuit autorisatie en authenticatie wenselijk is

a. MUST: Het OSR biedt verwerkers (M2M) binnen een bepaalde ketensamenwerking de mogelijkheid om mandaten van zichzelf en van de andere verwerker te verifiëren.
b. MUST: Alvorens uitgewisselde informatie te verwerken heeft verificatie van de mandaten van beide verwerkers plaatsgevonden met behulp van het OSR[10]
c. MUST: De authenticatie van de digitale identiteit van de verwerker die een verificatie uitvoert geschiedt met een PKI certificaat.
d. SHOULD: Raadplegen van OSR heeft een minimale impact op kwalitatieve aspecten van de uitwisseling buiten die van autorisatie[11]
e. COULD: De verificatie van een verwerker op een mandaat van een andere verwerker kan alleen plaatsvinden als zoiets nodig is nodig is binnen de ketensamenwerking[12]

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. MUST: Eindpunten zijn opvraagbaar op basis van ketensamenwerkingen, routeringskenmerken en namespaces[13]
c. MUST: Eindpunten zijn opvraagbaar op basis van de OIN van een eindverwerker, optioneel gefilterd gegeven een namespace
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 opvragen van eindpunten beperkt zich tot verwerkers die deelnemen aan de ketensamenwerking
f. SHOULD: Registeren van Eindpunten streeft naar minimale lasten te gaan voor verwerkers, eindverwerkers en kennisnet beheerders[14]

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 namespaces

[10] Dit staat los van het hoe. Dit kan when needed, maar ook bijvoorbeeld met cashing of in een event-driven architectuur. Zie voor het hoe de OSR specificaties.
[11] Denk hierbij met name aan performance en implementatie effort (ook bij wijzigingen van OSR buiten dit protocol)
[12] Dit betekent bijvoorbeeld dat een verwerker geen mandaat kan opvragen van een ketensamenwerking waarin deze niet participeert (überhaupt of voor een eindorganisatie)
[13] Een namespace onderscheid typen van eindpunten, zoals bijvoorbeeld verschillende soorten onderliggende services.
[14] Dit is altijd een balans tussen de partijen en wat vanuit autorisatie en authenticatie wenselijk is

e. SHOULD: Inrichten van een ketensamenwerking dient met minimale lasten te gaan voor verwerkers, eindverwerkers en kennisnet beheerders[15]

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, binnen de kaders van de ROSA
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

c. Als bij Mandaten. Voor eigen eindpoints is ook nu meer info beschikbaar (onder andere ook geldigheidsduur en gekoppeld systeem) dan van eindpunten van derden (daarbij minimaal URL, routeringskenmerk(en) van onderliggende administraties, OIN Eindorganisatie, namespaces 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 (onafhankelijk of ze deelnemen) en stemmen dit af met de Kennisnet beheerder.
- De contactpersoon van de verwerkersorganisatie verkrijgt een API-key voor het configureren OSR (eindpunten en routeringskenmerken van administraties) van Kennisnet
- De contactpersoon van de verwerker dient aan te geven welke routeringskenmerken voor een eindorganisatie in de ketensamenwerking zijn opgenomen
- 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.

[15] Dit is een requirement voor onder andere zoveel mogelijk hergebruik van bv systeem, leverancier, eindpunt en routeringskenmerk informatie, alhoewel dat gehinderd wordt door praktische zaken als niet herbruikbare routeringskenmerken en verschillende afspraken in ketensamenwerkingen en mogelijk verplichte rapportages

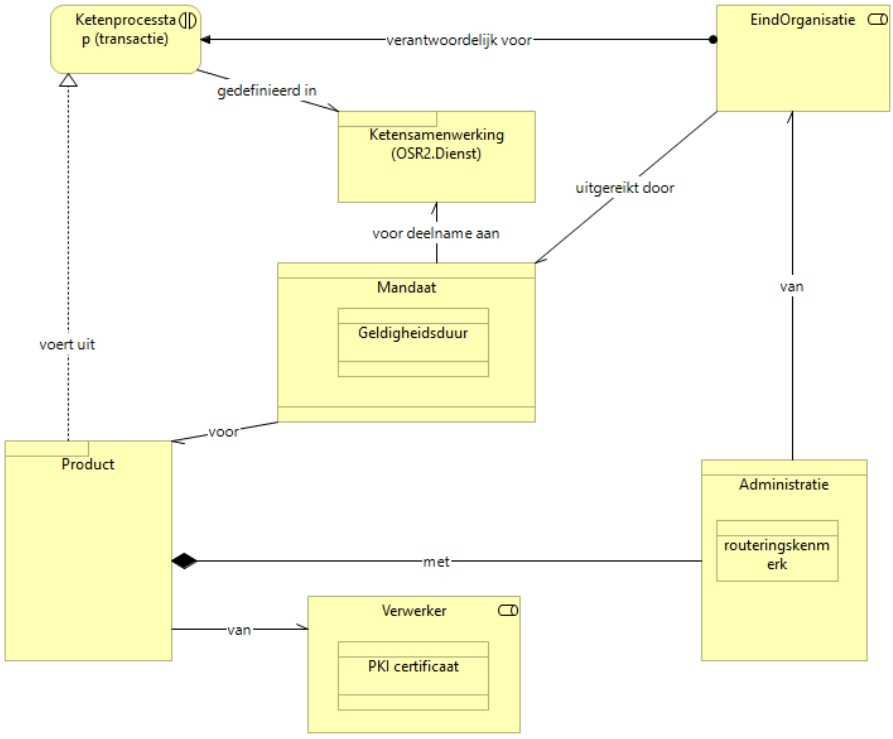
- Vertegenwoordiger verwerker: helpt met het opstellen van een ketensamenwerking

1.3. Kennisnet

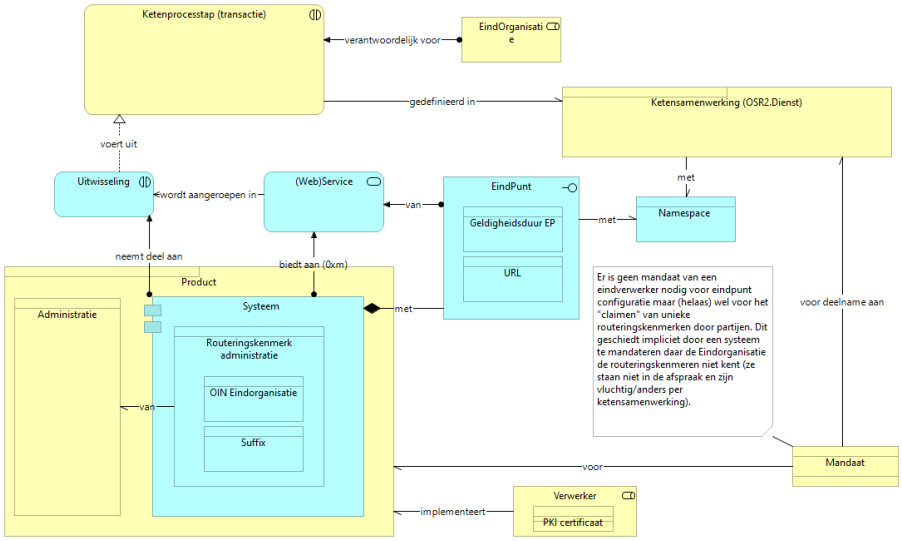
- Kennisnet OSR beheerder: deze staat in contact met de deelnemers aan een ketensamenwerking en helpt bij inrichten en gebruik van OSR. De kennisnet beheerder geeft ook token aan de contactpersoon van de verwerker.
- Kennisnet OSR product management: product management verzamelt wensen aangaande OSR en maakt middelen vrij en prioriteert de wijzigingen op advies van haar stakeholders.
- Kennisnet OSR architect: bewaakt de aansluiting van OSR op edukoppeling, in het bijzonder het secure API protocol en doet gevraagd en ongevraagd voorstellen voor veranderingen van het protocol en OSR.

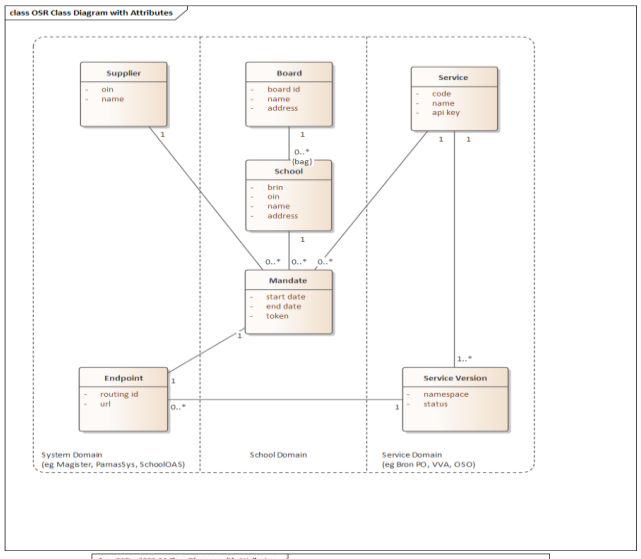
2. Bijlage: domein modellen

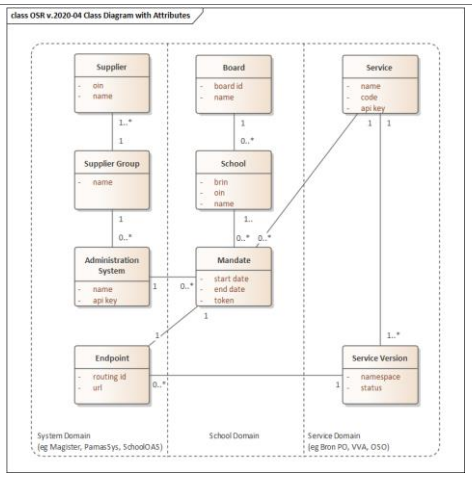
2.1. Mandaat model

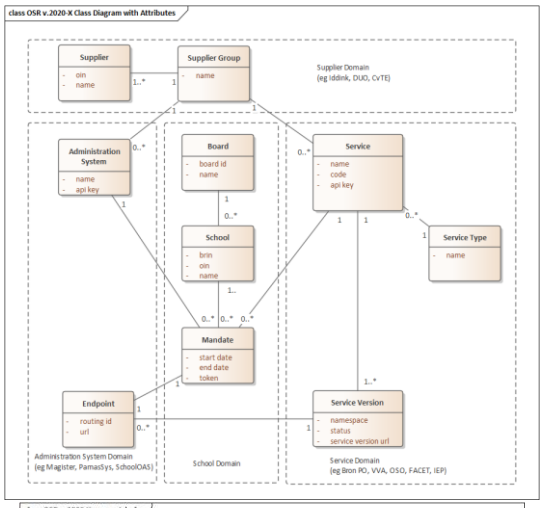


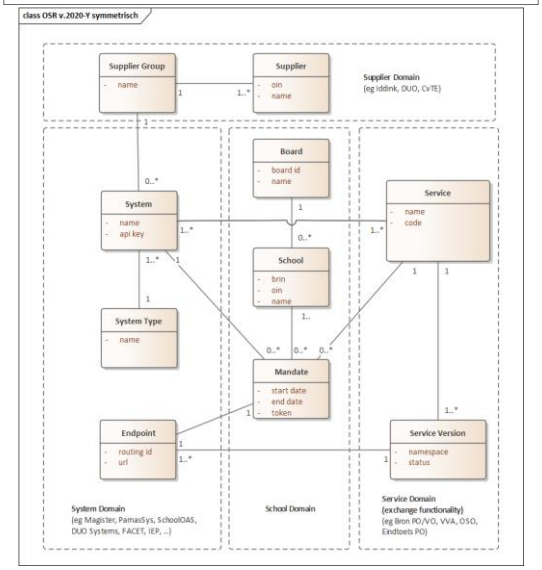
2.2. EndPoint model

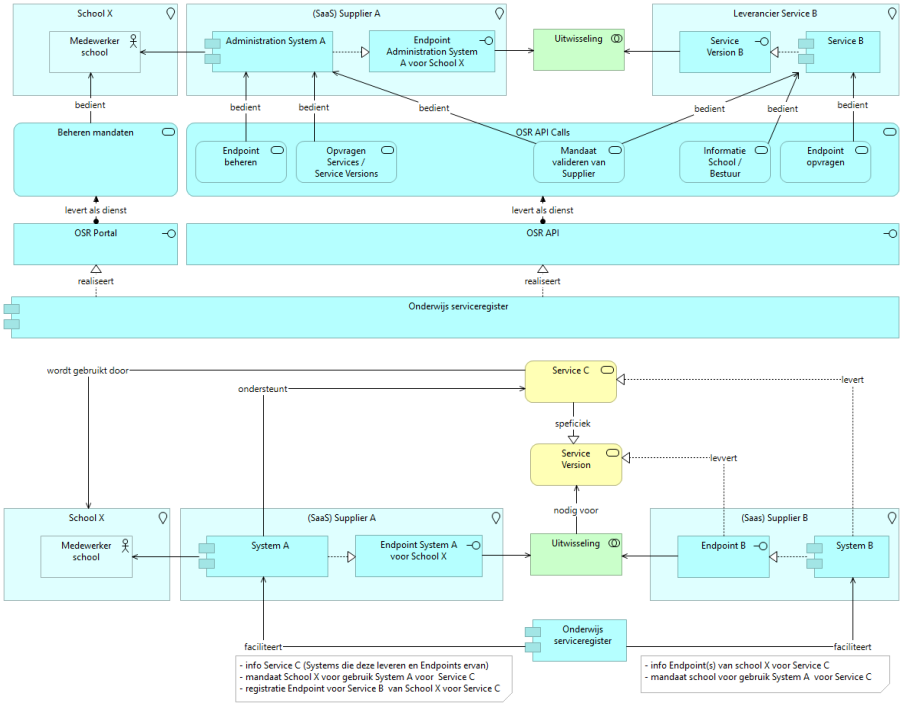



class OSR Class Diagram with Attributes
Supplier
- oin
- name
Board
- board id
- name
- address
Service
- code
- name
- api key
(bag)
School
- brin
- oin
- name
- address
Mandate
- start date
- end date
- token
Endpoint
- routing id
- url
Service Version
- namespace
- status
System Domain
(eg Magister, PamasSys, SchoolOAS)
School Domain
Service Domain
(eg Bron PO, VVA, OSO)


class OSR v.2020-04 Class Diagram with Attributes
Supplier
- oin
- name
Board
- board id
- name
Service
- name
- code
- api key
Supplier Group
- name
School
- brin
- oin
- name
Administration System
- name
- api key
Mandate
- start date
- end date
- token
Endpoint
- routing id
- url
Service Version
- namespace
- status
System Domain
(eg Magister, PamasSys, SchoolOAS)
School Domain
Service Domain
(eg Bron PO, VVA, OSO)


class OSR v.2020-X Class Diagram with Attributes
Supplier
- oin
- name
Supplier Group
- name
Supplier Domain
(eg Iddink, DUO, CvTE)
Administration System
- name
- api key
Board
- board id
- name
Service
- name
- code
- api key
School
- brin
- oin
- name
Service Type
- name
Mandate
- start date
- end date
- token
Endpoint
- routing id
- url
Service Version
- namespace
- status
- service version url
Administration System Domain
(eg Magister, PamasSys, SchoolOAS)
School Domain
Service Domain
(eg Bron PO, VVA, OSO, FACET, IEP)


class OSR v.2020-Y symmetrisch
Supplier Group
- name
Supplier
- oin
- name
Supplier Domain
(eg Iddink, DUO, CvTE)
Board
- board id
- name
System
- name
- api key
Service
- name
- code
School
- brin
- oin
- name
System Type
- name
Mandate
- start date
- end date
- token
Endpoint
- routing id
- url
Service Version
- namespace
- status
System Domain
(eg Magister, PamasSys, SchoolOAS,
DUO Systems, FACET, IEP, ...)
School Domain
Service Domain
(exchange functionality)
(eg Bron PO/VO, VVA, OSO,
Eindtoets PO)


School X
Medewerker school
(SaaS) Supplier A
Administration System A
Endpoint Administration System A voor School X
Uitwisseling
Leverancier Service B
Service Version B
Service B
bedient
Beheren mandaten
OSR API Calls
Endpoint beheren
Opvragen Services / Service Versions
Mandaat valideren van Supplier
Informatie School / Bestuur
Endpoint opvragen
levert als dienst
OSR Portal
OSR API
realiseert
Onderwijs serviceregister
wordt gebruikt door
ondersteunt
Service C
levert
speficiek
Service Version
levvert
nodig voor
(Saas) Supplier B
System A
Endpoint System A voor School X
Endpoint B
System B
faciliteert
Onderwijs servicesregister
- info Service C (Systems die deze leveren en Endpoints ervan)
- mandaat School X voor gebruik System A voor Service C
- registratie Endpoint voor Service B van School X voor Service C
- info Endpoint(s) van school X voor Service C
- mandaat school voor gebruik System A voor Service C