

Architectuurscan Edukoppeling REST/SaaS-profiel



*Remco de Boer, Joeri van Es
Bureau Edustandaard / Kennisnet*

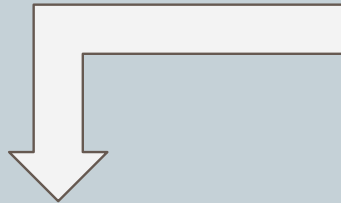
*Architectuurraad
29 oktober 2020*



Architectuurscan



Advies aan project



Advies aan ROSA



ROSA-onderdeel	Bevindingen uit project: Certificeringsschema	Relatie met ROSA (blauw: ROSA, geel: Certificeringsschema)	Voorgesteld advies van AR aan project	Voorgesteld advies voor AR voor plaatsing onderwerpen op de architectuurlandkaart ROSA
Werkingsgebied	ps, vs, mbo	Compliant: De verknipgebieden vallen geheel binnen ROSA.	Beschrijf raakvlak voor de andere RO en Certificeringsschema in lijn te brengen.	-
Toepassingsgebied	Informatiebeveiliging met betrekking tot alle door trekkende, geleverde diensten in de ondersteunende	Consistent: het certificeringsschema is een verknip die volledig past binnen het ROSA-ruimte (BP).	Verander het specifieke begrip (dienst, mbo, private partij, aangehouden voorwaarde).	Definieer van het begrip 'Voorwaarde' spreken. Maak onderscheid in eigenschap van voorwaarde door publiek en door private partijen. Bred de lijst van opgenomen bouwstenen uit, door rode van een stuk van het architectuurlandchap.
Principes en ontbrekende: Samenwerking	Er wordt niet expliciet gerefereerd aan principes en ontbrekende voor de certificeringsschema van de ROSA.	Relevant: deze principes zijn relevant voor de ROSA-geef, en worden lange andere thema's (zoals BP) doorvertaald naar concrete onderwerpen.	-	-

Adviesdeel
Architectuurscan



Te scannen onderwerp
(e.g., projectresultaten)



Traceerbaar naar
brondocumentatie



Bevindingendeel
Architectuurscan



Samenvatting Pitch



Edukoppeling REST/SaaS-profiel

Om welke afspraak gaat het?	Edukoppeling REST/SaaS-profiel en Edukoppeling Architectuur 2.0
Doel van de afspraak	M2M gegevensuitwisseling binnen het onderwijs
Aanleiding voor de afspraak	Toepassing van RESTful standaarden in ketens waar sprake is van m2m uitwisseling van gevoelige gegevens

Samenvatting Pitch



Edukoppeling REST/SaaS-profiel

Scan aangevraagd door	Werkgroep Edukoppeling
Doel van de scan	Onderdeel van de openbare consultatie die door de Architectuurraad is gefiatteerd, ROSA-scan is een van de onderdelen die in de consultatiefase wordt ingezet om de standaard te “harden”.
Wat gaat er nu gebeuren?	Input uit consultatie wordt verwerkt door werkgroep Edukoppeling en leidt tot vast te stellen versie. Besluitvorming (kandidaat)standaard via Architectuurraad
Onderkende risico's	Ontwikkelingen op nationaal niveau rondom REST-strategie en het al of niet onderbrengen onder Digikoppeling kunnen leiden tot vertraging van de definitieve vaststelling. Mitigatie door vaststelling kandidaatstandaard voordat definitieve vaststelling van 1.0-versie begin 2021 plaatsvindt. In sommige ketens en bij sommige voorzieningen kan er weerstand zijn tegen de onderliggende beveiligingseisen (UBV Edukoppeling profiel) die aan dit profiel gekoppeld zijn. Met name de verplichting tot toepassen van Tweezijdige TLS met PKI-overheid certificaten ligt gevoelig in de leermiddelenketen.

Complexiteit en risico's



Edukoppeling REST/SaaS-profiel

Projectfase	Afgerond / inbeheername	Al even op weg	Prille begin
Werkinggebied	Eén werkinggebied	Meerdere werkinggebieden	Gehele onderwijsdomein
Processcope	Beperkt aantal ketenprocessen	Meerdere ketenprocessen	(Vrijwel) alle ketenprocessen
Privacy	Geen persoonsgegevens	Enkele persoonsgegevens	Veel / bijzondere persoonsgeg.
Informatiebeveiliging	Geen BIV-eisen	Enkele BIV-eisen	Strikte BIV-eisen
Toegang	Openbaar / publiek	Obv groepslidmaatschap / rol	Obv identiteit
Gegevensuitwisseling	Geen m2m-koppelingen	Enkele koppelingen, meerdere gelijksoortige partijen	Veel koppelingen, veel verschillende partijen
Realisatie / impl. / uitrol	Triviaal	Gemiddeld	Complex
Beheer en doorontw.	Beheer en doorontwikkeling is belegd	Beoogde beheerpartij bekend, nadere afspraken maken	Nog onduidelijk / onbekend

Brondocumentatie



- Edukoppeling REST/SaaS-profiel voor M2M gegevensuitwisseling binnen het onderwijs (Concept), v0.5, juni 2020

Begeleidende documenten:

- Edukoppeling Architectuur 2.0 (Concept, vastgesteld door WG 27 mei 2020), v2.0, 27 mei 2020

Samenvatting scan



Hoofdpijnen:

1. Uitbreiding Edukoppeling

- a. Toevoeging gestandaardiseerde werkwijze voor gebruik REST-APIs aan Edukoppeling-architectuur
- b. Gemeenschappelijkheid in RESTful gegevensuitwisseling
- c. Sluit aan bij bestaande methoden en voorzieningen (OIN, PKI, OSR)

2. Impact op de omgeving

- a. (Verplichte) toepassing OSR bij meerdere gelijkwaardige ketenpartijen stelt aanvullende eisen aan OSR.
- b. Generieke Edukoppeling bedrijfstransactiepatronen als basis voor complexe RESTful interactiepatronen
- c. Impact op bestaande REST-uitwisselingen? (bijv. OO-API)

Samenvatting scan



Hoofdpijnen:

3. Uitbreidingen op specificatie

- a. Afhandeling van authenticatie obv OIN verwerker en/of from-OIN, incl. standaardfoutcodes
- b. Uitwerking foutafhandeling
- c. Uitleg en afweging bij verplichting van niet-normatieve voorschriften uit de API-strategie
- d. Houd rekening met mogelijkheid XML over REST

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Backlog kandidaten (ROSA)

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

- Geen backlog

Adviezen (1/2)

Edukoppeling REST/SaaS-profiel



Product

1. Benadruk het nemen van passende maatregelen t.a.v. vertrouwelijke gegevens in GET-parameters, met een aantal voorbeeldmaatregelen waaronder het gebruik van betekenisloze identifiers.
2. Werk de afhandeling van authenticatie obv OIN verwerker uit PKI en/of from-OIN uit, analoog aan hoe dat in de bijlage is gedaan voor API-keys
3. Verhelder de mogelijke impact van (toekomstig) gebruik van OAuth op het gebruik van de OSR. Wordt dat een (volwaardig) alternatief?
4. Toelichting ontbreekt nog bij een deel van de voorschriften
5. Uitwerken foutafhandeling
 - a. Foutcategorieën irt voorschrift API-47 en

IAA

Context

1. (Verplichte) toepassing OSR voor RESTful-gegevensuitwisseling tussen meerdere gelijkwaardige ketenpartijen stelt aanvullende eisen aan registratie en werking OSR.
2. Baseer complexe interactiepatronen voor RESTful uitwisseling op de generieke Edukoppeling bedrijfstransactiepatronen
3. OO-API: onderzoek mogelijke toepassing van / congruentie met REST/SaaS-profiel

Adviezen (2/2)

Edukoppeling REST/SaaS-profiel



Product

Context

6. Voorzie, waar dat nog niet is gedaan, niet-normatieve voorschriften uit de API-strategie die in het REST-profiel als MUST (i.e., normatief) worden aangemerkt van een toelichting en beargumenteer de afwijking. (API-09, API-21, API-22 (irt API-24), API-25 t/m API-33, API-42, API-44, API-45).
7. Houd rekening met situaties waarin XML over REST wenselijk zou kunnen zijn (tekst, p.6). Overweeg om API-24 als 'SHOULD' te markeren, om zo aan te geven dat JSON over REST de voorkeur zou moeten hebben.
8. Verduidelijk de opmerkingen t.a.v. de toepassing van SCIM. Is de implicatie dat gebruik hiervan wordt ontraden of zelfs 'verboden'?

In detail



Bevindingen en adviezen

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Compliant - Het SaaS/REST-profiel brengt gemeenschappelijkheid in RESTful gegevensuitwisseling in het onderwijsdomein.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Compliant - Het SaaS/REST-profiel brengt gemeenschappelijkheid in RESTful gegevensuitwisseling in het onderwijsdomein

De opmerkingen in de tekst over vertrouwelijke gegevens in GET-parameters zijn in kennelijke tegenspraak.

- ‘Vertrouwelijk’ is breder dan ‘persoonsgegevens’
- Specifiek voor persoonsgegevens geldt AVG (‘passende maatregelen’)
- Pseudonimisering als specifieke maatregel is mogelijk niet in alle situaties toepasbaar. (Uit toelichtende gesprekken blijkt overigens dat ‘pseudonimisering’ hier gelezen moet worden als het gebruiken van betekenisloze identifiers.)

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Compliant - Toepassing voor zowel bevestigingen als meldingen, gebruikmakend van generieke bedrijfstransactiepatronen uit Edukoppeling architectuur. Deze 'atomaire' patronen kunnen worden gecombineerd tot complexe, toepassingsspecifieke interactiepatronen.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Fully conformant - Het REST/SaaS-profiel valt binnen de Edukoppeling architectuur waarvan het werkingsgebied het gehele onderwijsdomein betreft.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Consistent - Het REST-SaaS-profiel voegt een gestandaardiseerde werkwijze voor het gebruik van REST-APIs toe aan de Edukoppeling-architectuur.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Consistent - de invulling van IAA sluit aan bij bestaande methoden en voorzieningen (OIN, PKI, OSR).

(Verplichte) toepassing van het OSR voor RESTful-gegevensuitwisseling tussen meerdere gelijkwaardige ketenpartijen stelt aanvullende eisen aan registratie van diensten in en de werking van het OSR.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Consistent - Het REST-profiel wordt duidelijk gepositioneerd t.o.v. de bestaande WUS-profielen.

De tekst is onduidelijk over of XML over REST 'verboden' is, of ontraden wordt. Er zijn scenario's waarin XML over REST wenselijk kan zijn, m.n. De overgang van WUS naar REST, waarbij bestaande XML-gegevensstructuren tijdelijk gehandhaafd blijven.

Afwijkingen op nationale afspraken zijn grotendeels beargumenteerd en niet in fundamentele tegenspraak.

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Irrelevant

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Irrelevant

Overzicht scanresultaten

Edukoppeling REST/SaaS-profiel



Relatie met ROSA

Relatie met ROSA

Compliant:

- 3. Bovensectorale samenwerking
- 4. IBP
- 6. Gegevensuitwisseling in de keten

Fully conformant

- 1. Werkingsgebied

Consistent:

- 2. Toepassingsgebied
- 5. IAA
- 7. Governance

Irrelevant:

- 8. Ketenprocessen
- 9. Zeggenschappen
- 10. Referentiecomponenten en applicaties

Irrelevant

Ontwerpgebied Bovensectorale Samenwerking

Edukoppeling REST/SaaS-profiel



Gemeenschappelijkheid in informatiehuishouding

Binnen het onderwijs zijn al veel ketenpartijen die gebruik maken van RESTful gegevensuitwisseling. Deze maken nu zelfstandige keuzes hoe transport, logistiek en beveiliging ingericht moeten worden. Het profiel beoogt hier meer standaardisatie in door te voeren, waarbij met name invulling gegeven wordt aan het kunnen routeren tussen de rollen die in Edukoppeling t.b.v. SaaS worden onderscheiden.

Ontwerpgebied IBP

Edukoppeling REST/SaaS-profiel



TLS (wordt verwezen naar UBV)

Vertrouwelijke gegevens in GET-parameters

- P.13: 'dienen gepseudonimiseerd te zijn'
- P.18: igv persoonsgegevens 'kunnen aanvullende beveiligingsmaatregelen toegepast worden, zoals adequaat versleutelen en/of voorkomen ongewenste logging dmv filter'.

Ontwerpgebied Gegevensuitwisseling in de keten

Edukoppeling REST/SaaS-profiel



Must: Gebruik van openbare internet

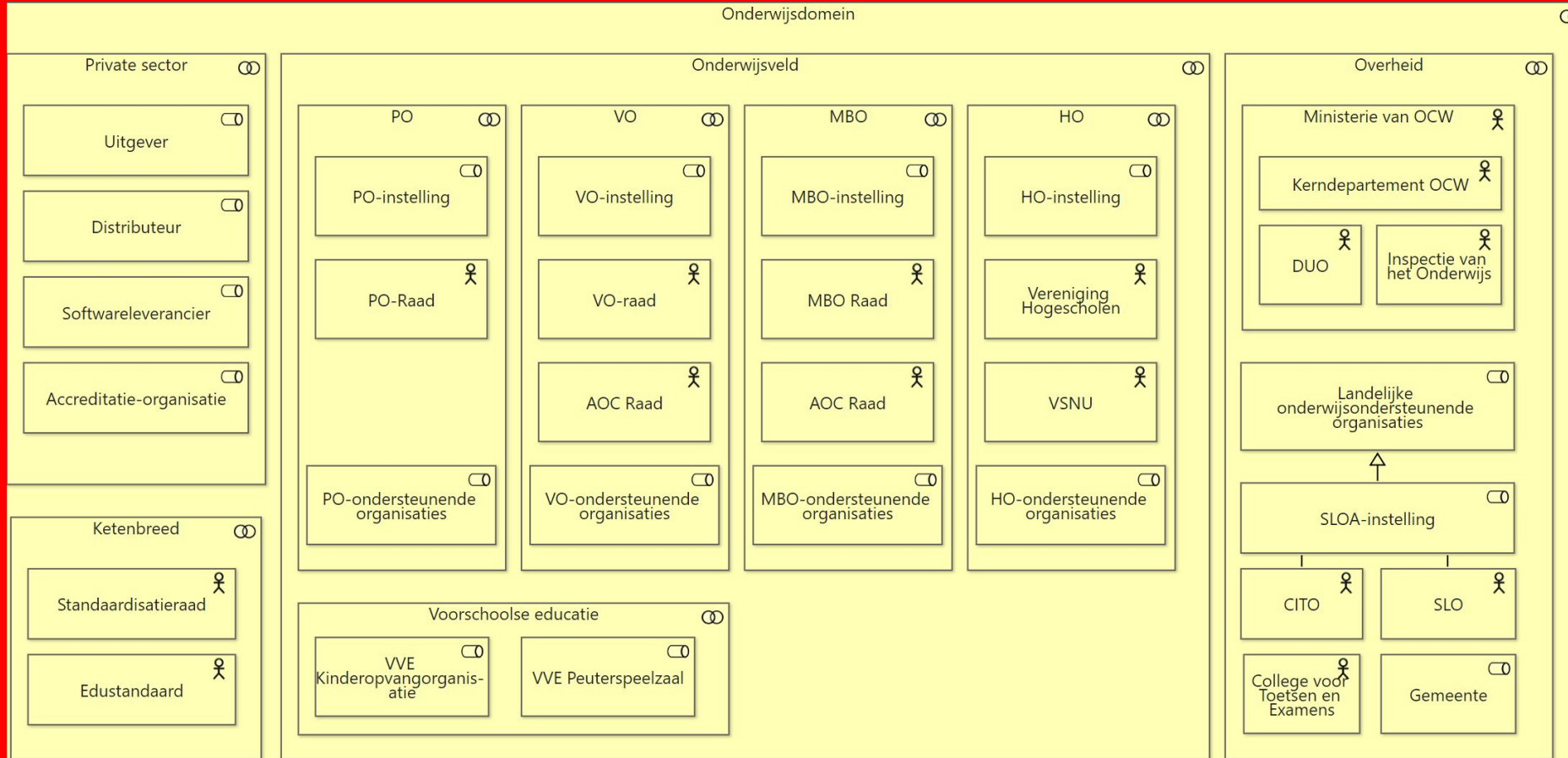
“Overigens kan Edukoppeling ook toegepast worden in gesloten netwerken.”. Tegenspraak? Hoe ‘must’ te lezen?

Foutafhandeling:

- Architectuur definieert categorieën A t/m E In 3.1.8 alleen foutmeldingen voor cat. A t.a.v. syntax to/from-routeringskenmerken.
→ hoe passen de andere categorieën op HTTP statuscodes?

Werkinggebied

Edukoppeling REST/SaaS-profiel

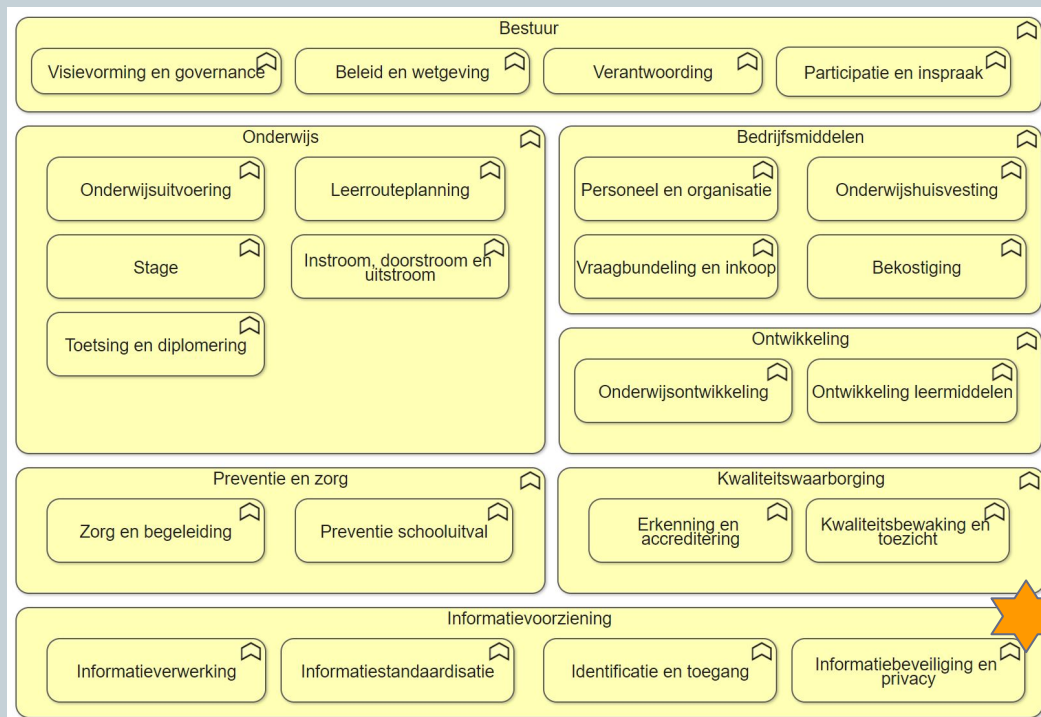


Toepassingsgebied

Edukoppeling REST/SaaS-profiel



M2M-gegevensuitwisseling via een beveiligde point-to-pointverbinding waarbij RESTful standaarden voor gesloten (access-restricted en purpose-limited) APIs worden toegepast (zowel pull als push).



Ontwerpgebied IAA

Edukoppeling REST/SaaS-profiel



- Identificatie/authenticatie verwerker obv OIN / PKI-infrastructuur (P2P).
- Eindorganisaties worden geïdentificeerd via routeringskenmerken (TO, FROM)
- Inzet van transparante dienstverleners wordt (nog) niet ondersteund (daarvoor: WUS)
- Verplicht gebruik Onderwijsserviceregister
- Verwijzing naar ontwikkelingen OAuth in bijlage A.
- Gebruik van API-sleutels geen onderdeel van het profiel, maar wel toegestaan
 - Voor API-key (geen onderdeel profiel) stroomschema's en mogelijke 401/403-foutcodes. Zoiets mist voor afhandeling van 'from-OIN' en OIN verwerker (P2P) .

Governance

Edukoppeling REST/SaaS-profiel



Relaties met andere standaarden

- UBV (zie ook onderdeel IBP)
- Voor transparante intermediair, onweerlegbaarheid, en/of uitwisseling obv XML: toepassen Edukoppeling WUS-profiel
- OOAPI: onduidelijk of Edukoppeling-rollen hierin onderkend worden
- Inbedding in nationale (overheidsbrede) standaarden. Basis wordt gevormd door afspraken en voorschriften uit de landelijke API-strategie. Enige mate van ontkoppeling via MoSCoW-classificering.
- Op p.6 wordt XML over REST niet toegestaan, volgens API-24 is het een eigen afweging (COULD).