ROSA Architectuurscan/advies: Edukoppeling REST/SaaS-profiel

edustandaard

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Remco de Boer
Versie	1e concept
Datum	28 sep 2020
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding	
Betreft	Edukoppeling REST/SaaS-profiel voor M2M gegevensuitwisseling binnen het onderwijs
Brondocument(en)	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

Inleiding

Met de ROSA Architectuurscan worden op systematische wijze alle architectuuraspecten van een bij Edustandaard ingebracht onderwerp in kaart gebracht en worden knelpunten en kansen gesignaleerd. Niet alleen kan de indiener er zijn voordeel mee doen, ook kan ROSA ermee worden verrijkt. En tot slot stelt het andere ketenpartijen in staat om kennis te nemen van architectuurwijzigingen en het belang hiervan voor de eigen organisatie of achterban te bepalen (transparantie in de keten, informatiepositie).

Dit formulier bevat de uitkomst van een architectuurscan van het Edukoppeling REST/SaaS-profiel. Voor de indiener biedt de scan concrete handvatten voor toepassing van ROSA, en de mogelijkheid om lessen en ervaringen uit het project terug te koppelen aan ROSA. Een architectuurscan wordt in principe uitgevoerd met een hoge mate van betrokkenheid van vertegenwoordigers van de inbrenger. Deze wordt hierbij ondersteund door Bureau Edustandaard, de beheerder van ROSA. De inbrenger zou zich moeten herkennen in de uitkomsten.

Iedere architectuurscan begint met de vraag: welke onderdelen van ROSA zijn relevant voor het ingebrachte onderwerp, en indien relevant, op welke wijze? Vervolgens worden de vragen gesteld hoe het ingebrachte past op wat in ROSA is uitgewerkt, en of het project wellicht inzichten heeft die kunnen leiden tot verbetering of uitbreiding van ROSA. De antwoorden op deze vragen worden verwoord in termen van een advies richting zowel inbrenger, als richting ROSA zelf. De opzet van het advies is dat per onderdeel van ROSA uitspraken worden gedaan over:

1. Bevindingen uit project: *wat zegt het project zelf over het verband met ROSA van het ingebrachte onderwerp?*
2. Relatie met ROSA: *hoe verhoudt het ingebrachte zich tot ROSA[1]?*
3. Voorgesteld advies van de Architectuurraad aan het project: *tips, verbeterpunten, en ook bekrachtiging dat er goed werk is geleverd vanuit het perspectief van ROSA[2]*
   Adviezen in deze kolom zijn, gegroepeerd in 'PRODUCT' en 'CONTEXT'. De PRODUCT-adviezen bestrijken sec het ingediende 'product', d.w.z. het Edukoppeling REST/SaaS-profiel. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van het Edukoppeling REST/SaaS-profiel bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen het Edukoppeling REST/SaaS-profiel toegepast gaat worden. Deze adviezen kunnen gericht zijn aan het project zelf, maar kunnen ook zijn gericht aan partijen die zich in die context bevinden, zoals de project(deel)groep die zich richt op de implementatie van de uiteindelijke Edukoppeling REST/SaaS-profiel, maar ook (sector)organisaties die met de uiteindelijke implementatie te maken gaan krijgen.
4. **Voorgesteld advies voor de Architectuurraad voor plaatsing onderwerpen op de ROSA architectuur backlo**g: *wat kan ROSA doen om in het vervolg een betere ondersteuning te bieden aan dit project, en andere?*

Samenhang met andere formulieren:

- **Pitch Architectuurscan**: Het doel van de architectuurpitch is om een eerste indruk te krijgen van een ketenafspraak . Op basis van de pitch en de aangeleverde documentatie voert Bureau Edustandaard een architectuurscan uit. Voor de leden van de Architectuurraad (en andere geïnteresseerden) verduidelijkt deze pitch de context van de afspraak en de resultaten uit de architectuurscan.
- **ROSA architectuurscan *bevindingen***: aan het invullen van het adviesdeel van een architectuurscan (dit formulier) gaat het verzamelen van feitelijke informatie, en het analyseren daarvan, vooraf. Die informatie, en de analyses, worden vastgelegd in het bevindingendeel van de architectuurscan. De lezer van het adviesdeel kan die erop na slaan als hij wil weten hoe het advies tot stand is gekomen. Het lezen van het bevindingendeel is niet vereist om het adviesdeel te begrijpen. Waar van toepassingen verwijst het bevindingendeel naar specifieke locaties van de brondocumenten die als input dienden voor de architectuurscan. Ook het lezen van de brondocumenten is niet vereist om het adviesdeel te begrijpen.

[1] De verhouding tussen het ingediende en de ROSA wordt per onderdeel uitgedrukt in een 'level of conformance' ontleend aan TOGAF, zie de bijlage.
[2] Dit is een concept advies, de uitkomsten worden eerst door de Architectuurraad besproken.

ROSA Architectuurscan/advies: Edukoppeling REST/SaaS-profiel

ROSA-onderdeel	Bevindingen uit project: Edukoppeling REST/SaaS-profiel	Relatie met ROSA (blauw: ROSA, geel: Edukoppeling REST/SaaS-profiel)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkings-gebied	Gehele onderwijsdomein (cf. organisatorisch werkingsgebied zoals beschreven in Edukoppeling architectuur).	 **Fully conformant -** Het REST/SaaS-profiel valt binnen de Edukoppeling architectuur waarvan het werkingsgebied het gehele onderwijsdomein betreft.	**PRODUCT:** **CONTEXT:**	
Toepassings-gebied	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).	 **Consistent -** Het REST-SaaS-profiel voegt een gestandaardiseerde werkwijze voor het gebruik van REST-APIs toe aan de Edukoppeling-architectuur.	**PRODUCT:** **CONTEXT:**	
Ontwerpgebied **Bovensectorale samenwerking**	**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.	 **Compliant** - Het SaaS/REST-profiel brengt gemeenschappelijkheid in RESTful gegevensuitwisseling in het onderwijsdomein.	**PRODUCT:** **CONTEXT:**	

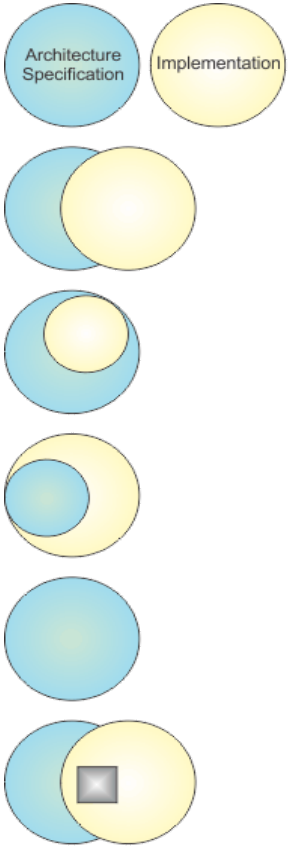
Ontwerpgebied **Informatie-beveiliging en privacy (IBP)**	• TLS (wordt verwezen naar UBV) Vertrouwelijke gegevens in GET-parameters • P.13: 'dienen gepseudonimiseerd te zijn' • P.18: igv persoonsgegevens 'kunnen aanvullende beveiligingsmaatregelen toegepast worden, zoals adequaat versleutelen en/of voorkomen ongewenste logging dmv filter'.	 **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.)	**PRODUCT:** • Benadruk het nemen van passende maatregelen t.a.v. vertrouwelijke gegevens in GET-parameters, met een aantal voorbeeldmaatregelen waaronder het gebruik van betekenisloze identifiers. **CONTEXT:**	
Ontwerpgebied **IAA**	• 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)	 **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.	**PRODUCT:** • 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 • Verhelder de mogelijke impact van (toekomstig) gebruik van OAuth op het gebruik van de OSR. Wordt dat een (volwaardig) alternatief? **CONTEXT:** • (Verplichte) toepassing OSR voor RESTful-gegevensuitwisseling tussen meerdere gelijkwaardige	

	stroomschema's en mogelijke 401/403-foutcodes. Zoiets mist voor afhandeling van 'from-OIN' en OIN verwerker (P2P) . ○		ketenpartijen stelt aanvullende eisen aan registratie en werking OSR.	
Ontwerpgebied **Gegevens-uitwisseling in de keten**	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?	**Compliant -** Toepassing voor zowel bevragingen als meldingen, gebruikmakend van generieke bedrijfstransactiepatronen uit Edukoppeling architectuur. Deze 'atomaire' patronen kunnen worden gecombineerd tot complexe, toepassingsspecifieke interactiepatronen.	**PRODUCT:** ● Toelichting ontbreekt nog bij een deel van de voorschriften ● Uitwerken foutafhandeling ○ Foutcategorieën irt voorschrift API-47 en IAA **CONTEXT:** ● Baseer complexe interactiepatronen voor RESTful uitwisseling op de generieke Edukoppeling bedrijfstransactiepatronen	

Ontwerpgebied **Governance**	**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).	 **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.	**PRODUCT:** ● 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). ● 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. ● Verduidelijk de opmerkingen t.a.v. de toepassing van SCIM. Is de implicatie dat gebruik hiervan wordt wordt ontraden of zelfs 'verboden'? **CONTEXT:** ● OO-API: onderzoek mogelijke toepassing van / congruentie met REST/SaaS-profiel	
Keten-processen			**PRODUCT:** **CONTEXT:**	
Zeggen-schappen en gegevens-soorten			**PRODUCT:** **CONTEXT:**	
Referentie-componenten en landelijke voorzieningen			**PRODUCT:** **CONTEXT:**	

Architecturele randvoor-waarden		*Afhankelijkheid van OSR*	**PRODUCT:** **CONTEXT:**	
Implementatie			**PRODUCT:** **CONTEXT:**	

Bijlage 1: **ARCHITECTURE COMPLIANCE (TOGAF)**



Irrelevant:
The implementation has no features in common with the architecture specification (so the question of conformance does not arise).

Consistent:
The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.

Compliant:
Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.

Conformant:
All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.

Fully Conformant:
There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.

Non-conformant:
Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.

Bron: http://pubs.opengroup.org/architecture/togaf9-doc/arch/Figures/48_conformance.png

Een Nederlandse vertaling van de beschrijving van de TOGAF-categorieen:

a. **irrelevant** = er is geen relatie tussen het ingebrachte en ROSA
b. **consistent** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is het ingebrachte conform ROSA gerealiseerd, de overlap is echter niet **volledig** = sommige specificaties van ROSA zijn niet overgenomen, en het ingebrachte heeft onderdelen die niet door ROSA worden gedekt.
c. **compliant** = het ingebrachte valt volledig binnen ROSA (subset) en is conform ROSA gerealiseerd
d. **conformant** = ROSA dekt alleen een deel van het ingebrachte, maar dat deel is wel conform ROSA gerealiseerd
e. **fully conformant** = ROSA dekt het geheel van het ingebrachte, en niets van het ingebrachte valt buiten ROSA
f. **non-conformant** = er is overlap tussen het ingebrachte en ROSA, en binnen die overlap is er iets van het ingebrachte *niet* conform ROSA gerealiseerd