ROSA Architectuurscan/advies: OO API

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Jeroen Hamers, Laura Braam
Versie	v2
Datum	18 januari 2018
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met indieners en voorzitter werkgroep IBP Definitief: afgestemd met Architectuurraad
Aanleiding	Standaard is ter beheer aangeboden bij Edustandaard
Betreft	OO API versie 2
Brondocument(en)	Edustandaard Aanmeldformulier https://openonderwijsapi.nl/ https://github.com/open-education-api/specification https://rawgit.com/open-education-api/specification/v2/docs.html
Begeleidende documenten	

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 de OO API. De OO API is ter onderhoud aangeboden bij Edustandaard. Voor de Architectuurraad dient een uitgevoerde architectuurscan als basis voor haar advies aan de Standaardisatieraad. 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. Dit formulier (het adviesdeel) wordt samen met het uitgebreidere “bevindingdeel” geleverd, maar kan eigenstandig gelezen worden (zie de toelichting hieronder). 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. de OO API. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van de OO API bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen de OO API 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 OO API, 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:

- **Edustandaard aanmeldformulier**: in geval van een aanmelding of registratie, is er sprake van een Edustandaard aanmeldformulier[3]. In dit geval worden zowel het aanmeldformulier als de architectuurscan aan de Architectuurraad aangeboden. Het verband tussen de twee is dat het aanmeldformulier de bredere, ook niet-architecturele, context van het ingebrachte beschrijft. De architectuurscan gaat alleen, en dieper, in op de architectuuraspecten. Aangeraden wordt om de twee in samenhang te lezen, het aanmeldformulier eerst.[4]
- **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.

[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.
[3] Een ROSA architectuurscan speelt naar verwachting niet in alle gevallen een rol in een aanmelding bij Edustandaard. Dit proces moet nog geformaliseerd worden.
[4] Op dit moment is er nog sprake van enige overlap tussen de twee formulieren. Deze wordt binnenkort geadresseerd, maar is niet bezwaarlijk voor het begrijpen van beide formulieren.

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 toepassing 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.

ROSA Architectuurscan/advies: OO API

ROSA-onderdeel	**Bevindingen uit project:** OO API	**Relatie met ROSA (blauw: ROSA, geel: OO API)**	**Voorgesteld advies aan project**	**Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA**
Werkings-gebied	Hoger onderwijs (ho)	 **Compliant** - Het werkingsgebied van de OO API valt volledig in het onderwijsdomein c.q. ROSA	**PRODUCT:** Het project ziet potentie om in de toekomst de standaard uit te breiden voor andere sectoren en ook internationaal. Zorg dat bij het maken van ontwerpkeuzes rekening wordt gehouden met eventuele uitbreidingen **CONTEXT:**	
Toepassings-gebied	De OO API ondersteunt administratieve- en onderwijsprocessen, door informatie van onderwijsinstellingen beschikbaar te stellen over: onderwijsafdelingen, onderwijsplannen, cursusgroepen, cursussen, cursusresultaten, toetsresultaten, gebouwen, ruimtes, roostergegevens, nieuwskanalen en nieuwsitems.	 **Compliant** - De OO API geeft invulling aan de volgende ketenfuncties: Onderwijsuitvoering; Personeel en organisatie; Onderwijshuisvesting; Toetsen, examinering en oefening; Informatieverwerking Informatiestandaardisatie.	**PRODUCT:** Zorg voor een goede invulling van de ketenfuncties: Identificatie en toegang; Informatiebeveiliging en privacy. Zie ook thema's: IAA en IBP **CONTEXT:**	
Bovensectorale samenwerking	De OO API beperkt zich tot de ho-sector	 **Irrelevant** - De OO API bestrijkt geen bovensectorale samenwerking	**PRODUCT:** **CONTEXT:**	

Thema: **Informatie-beveiliging en privacy (IBP)**	***Ontwerpkaders*** ***Voorkom onrechtmatige toegang of verspreiding*** Uit de website blijkt dat de OO API onderstaande data beschikbaarheidsniveaus kent: 1. *"Data wat beschikbaar is voor iedereen, zoals nieuwsberichten of een overzicht van de verschillende studies."* 2. *"Data wat voor een bepaalde doelgroep beschikbaar is, zoals rooster data wat alleen beschikbaar is voor studenten van een bepaalde instelling of van een bepaalde studierichting. Voordat deze data kan worden vrijgegeven dient het systeem (veelal de API manager) de identiteit van de gebruiker te achterhalen om te kunnen bepalen 'Is dit een student van deze instelling of van deze studierichting?'. De gebruiker zal deze gegevens middels een inlog moeten vrijgeven."* 3. *"Data wat bedoeld is voor een bepaalde gebruiker. Denk hier bijvoorbeeld aan tentamen/examen cijfers. Voordat deze data kan worden vrijgegeven dient het systeem de identiteit van de gebruiker te achterhalen. De gebruiker zal hiervoor moeten inloggen"* Zie: https://openonderwijsapi.nl/community/faq/ In de website van de OO API staat dat de OO API de OAuth 2.0 protocol ondersteunt. De specificatie zelf geeft niet aan hoe OAuth 2.0 precies gebruikt/geïmplementeerd moet	 **Onbepaald** - Verdere ontwerp- en implementatiekeuzes bepalen de mate waarin toegang tot vertrouwelijke gegevens afdoende kan worden beperkt	**PRODUCT:** ***Ontwerpkaders*** ***Voorkom onrechtmatige toegang of verspreiding*** Waarborg dat relaties en identificerende kenmerken op het juiste data beschikbaarheidsniveau vastgelegd zijn, zodat de doelgroepen slechts die gegevens kunnen raadplegen waartoe zij gerechtigd zijn. Licht nader toe wat de criteria achter de ontwerp- en implementatie keuzes zijn voor het filteren van informatie uit de verschillende data beschikbaarheidsniveaus Borg het correcte gebruik van filters zodat vertrouwelijke gegevens op de juiste manier afgeschermd worden. Leg daarbij vast welke criteria gelden om de informatie uit de verschillende beschikbaarheidsniveaus te filteren. ***Voorbeeld:*** *de OO API specificeert de methode "Get Course result" met optionele filters. Wanneer je geen parameters voor de filters opgeeft, mag je in principe alle resultaten verwachten van alle vakken van alle studenten voor alle academische jaren.* Leg vast welke eisen of richtlijnen er gelden voor de verschillende beschreven beschikbaarheidsniveaus.	

	worden. Er is een PoC waarin informatie hierover is opgenomen. ***Transparantie over maatregelen*** In het HO is gekozen voor het vastleggen van afspraken ten aanzien van privacy en security middels het SURF juridisch normenkader. ***De juiste gegevens op het juiste moment op de juiste plaats*** De OO API geeft een goede invulling hieraan Maakt het mogelijk om gegevens op een laagdrempelige manier op te vragen bij de bronnen. Welke gegevens de 'juiste' zijn, kan worden aangegeven via filters (zie hierover de opmerkingen bij *Voorkom onrechtmatige toegang of verspreiding*) ***Handelingen zijn herleidbaar*** Over de traceerbaarheid van opvragingen via de OO API zijn geen besluiten of richtlijnen vastgelegd ***Voorkom ongewenste traceerbaarheid en vindbaarheid*** Over het gebruik van persoonsgegevens (zoals geslacht, tel.nummer, foto,..) zijn geen besluiten of richtlijnen vastgelegd		***Transparantie over maatregelen*** Maak een risicoanalyse van de gegevens in de OO API op basis van een BIV classificatie Leg vast welke informatiebeveiliging en privacy maatregelen van toepassing zijn voor de OO API Het certificeringsschema bevat een classificatie hulpmiddel waar een BIV mee bepaald kan worden. De OO API dient maatregelen te bieden voor de 'zwaarste' BIV die op basis van de gegevens bepaald wordt. Voor maatregelen kan men te rade gaan bij het toetsingskader van het certificeringsschema. Zie ook: Principes voor informatievoorziening HORA -> *Gegevens zijn beveiligd op basis van hun risicoclassificatie* https://www.wikixl.nl/wiki/hora/index.php/Principes_voor_informatievoorziening ***Handelingen zijn herleidbaar*** Leg vast aan welke eisen m.b.t. traceerbaarheid implementaties van de OO-API moeten voldoen ***Voorkom ongewenste traceerbaarheid en vindbaarheid*** Onderbouw besluiten en richtlijnen over het gebruik van persoonsgegevens **CONTEXT:** Het project geeft aan dat informatiebeveiliging geen geen onderdeel uit de specificatie maakt, maar belangrijk is voor het gebruik daarvan. Ze adviseren het gebruik van Surfconext in combinatie met een API Manager/OAuth 2.0,	

			maar laat instellingen vrij in hun keuze. Op deze wijze is de uitwerking van IBP aspecten verantwoordelijkheid van de implementerende partijen. Gezien er privacygevoelige gegevens ontsloten worden, adviseren we het project om bij dit onderwerp nadere advies in te winnen bij de IBP werkgroep (Edustandaard). De voorzitter van deze werkgroep heeft zich overigens beschikbaar gesteld om het project van advies te voorzien. **Acties opgenomen in de roadmap:** ● API manager PoC wordt geactualiseerd https://github.com/open-education-api/poc-apiman-docs/blob/master/OOAPI%20-%20POC%20beschrijving.docx ● De gegevens BIV classificatie wordt uitgewerkt en opgenomen in de specificatie https://github.com/open-education-api/specification/blob/v2/ROADMAP.md **Aanbevolen acties om op te nemen in roadmap:** ● Eisen m.b.t. traceerbaarheid documenteren ● Besluiten en richtlijnen over het gebruik van persoonsgegevens documenteren	

Thema: **IAA**	***Ontwerpkaders*** ***Gebruik onderwijsidentiteit waar nodig*** Over het gebruik van identiteiten zijn geen besluiten of richtlijnen vastgelegd	 **Onbepaald** - Verdere ontwerp- en implementatiekeuzes bepalen hoe het gebruik van identiteiten afdoende kan worden geborgd	**PRODUCT:** ***Ontwerpkaders*** ***Gebruik onderwijsidentiteit waar nodig*** Leg vast welke identiteit gebruikt wordt in de OO API voor personen (studenten, docenten, andere personeel) **Acties in de roadmap:** ● Identifiers gedocumenteerd in de specificatie. Deze worden overgenomen van SURFconext https://github.com/open-education-api/specification/blob/v2/ROADMAP.md **CONTEXT:**	

Thema: **Gegevens-uitwisseling in de keten**	***Ontwerpkaders*** ***Ketenpartijen bieden wederzijdse services*** De OO API is weliswaar geen webservicespecificatie, maar biedt desalniettemin een (REST) endpoint voor data consumers om gegevens uit de bron op te halen. Op die manier geeft de OO API een goede invulling hieraan. ***Registreer de betekenis van nieuwe gegevens*** Het is niet duidelijk welke OO API begrippen nieuw zijn. Sommige begrippen zijn niet scherp gedefinieerd ***Serviceinformatie wordt samenhangend openbaar gemaakt*** Het is niet duidelijk hoe een gebruiker of ontwikkelaar weet dat er een endpoint bestaat ***Classificeer alle gegevens- en domeinobjecten met het Kernmodel Onderwijsinformatie*** Het is onbekend hoe de semantiek van de OO API zich tot de semantiek van het KOI verhoudt. Sommige gegevens, attributen en relaties zijn niet scherp gedefinieerd Voorbeelden:: - *Educational departments = The educational departments of an organization.* - *Faculty = The organizational parts of an organization.* Wat is het verschil tussen educational departments en faculty? Waarom is Organization niet gedefinieerd? Hoe weet je over welke organisatie het gaat?	 **Onbepaald** - Verdere ontwerp- en implementatiekeuzes bepalen hoe de gegevensuitwisseling afdoende kan worden geborgd	**PRODUCT:** ***Ontwerpkaders*** ***Registreer de betekenis van nieuwe gegevens*** Zorg voor goede zichzelf verklarende definities van gebruikte begrippen. Definieer gegevens, attributen en relaties scherper ***Serviceinformatie wordt samenhangend openbaar gemaakt*** Ontwikkel een register/pagina waar alle API endpoints staan ***Classificeer alle gegevens- en domeinobjecten met het Kernmodel Onderwijsinformatie*** Analyseer hoe de semantiek van de OO API zich tot de semantiek van het KOI verhoudt Definieer waar mogelijk de OO API begrippen in termen van het KOI. Waar dat niet kan, omdat het nieuwe begrippen betreft, dien een voorstel in voor uitbreiding van het KOI. Het is goed dat de de OO API specifiek is, zolang de relatie met generieke begrippen ook maar duidelijk is. Dit maakt de standaard ook begrijpelijk voor niet ingewijden. Formuleer scherpe definities en controleer de consistentie van de relaties tussen gegevens.	

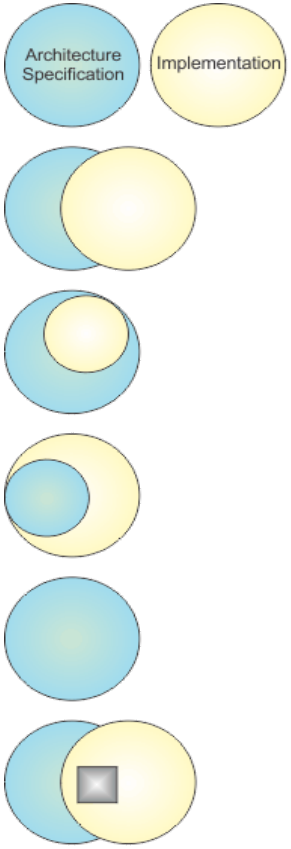
	- *Affiiation:* *description: The affiliations of how this person is associated with the organization* - *Student* - *Employee* - *Staff* - *Member* - *Affiliate* - *Organization* Het verschil tussen employee, staff en member is onduidelijk. Er lijkt ook een, verder niet beschreven, relatie te zijn met filters en autorisatie (Zie ook de bevindingen over filters bij IBP) - *"Building"* Dit gegeven staat los van de rest. Building is een attribuut van "Schedule", maar de verwijzing ontbreekt. Wat is de ontwerpbeslissing hierachter? ***Behoeftegerichte en doelgebonden gegevensuitwisseling*** Het is niet duidelijk hoe de OO API borgt dat er niet meer (maar ook niet minder) informatie dan nodig uitgewisseld wordt.		***Behoeftegerichte en doelgebonden gegevensuitwisseling*** Waarborg dat niet meer (maar ook niet minder) informatie dan nodig uitgewisseld wordt. Maak expliciet waar (evt. op implementatie niveau) nog nader invulling hieraan gegeven moet worden **Acties in de roadmap:** ● Datamodel wordt gedocumenteerd ● Definities van begrippen worden aangescherpt ● Mechanisme voor het actualiseren en bijhouden van instellingen endpoints wordt verbeterd https://github.com/open-education-api/specification/blob/v2/ROADMAP.md **CONTEXT:**	

Keten-processen	De ketenprocessen zijn niet gedefinieerd in de OO API specificatie	 **Onbepaald** - bij gebrek aan informatie is niet goed te bepalen voor welke processen de OO API wel of niet is bedoeld.	**PRODUCT:** Leg vast voor welke (keten)processen de OO API wel en voor welke expliciet niet bedoeld is. **Aanbevolen acties om op te nemen in roadmap:** ● Processen documenteren (als onderdeel van de architectuur documentatie) **CONTEXT:**	
Zeggen-schappen en gegevens-soorten	De zeggenschappen bij de gegevenssoorten (wat wel en wat niet door welke partij mag worden uitgewisseld, opgeslagen, ingezien, bewerkt) zijn niet gedefinieerd in de OO API specificatie. Deze zouden wel gedefinieerd moeten worden worden, mede als opmaat naar verdere uitwerking van security-aspecten als autorisatie en filtering (cf. IBP)	 **Onbepaald** - omdat de zeggenschappen niet zijn uitgewerkt.	**PRODUCT:** Werk de zeggenschappen uit in de specificatie **Aanbevolen acties om op te nemen in roadmap:** ● Zeggenschappen uitwerken en documenteren in de specificatie **CONTEXT:**	
Referentie componenten en applicaties	Het is niet vastgelegd welke referentiecomponenten en/of applicaties via de OO API ontsloten (moeten) kunnen worden. In de website wordt er gerefereerd aan een ‘API Manager’. Dit lijkt een referentiecomponent (bouwblok) dat bij de OO API hoort. Over deze referentiecomponent is echter maar weinig vastgelegd.	 **Onbepaald** - bij gebrek aan informatie is niet goed te bepalen voor ontsluiting vanuit welke referentiecomponenten de OO API is bedoeld, noch welke referentiecomponenten rechtstreeks bij (de implementatie van) de OO API zijn betrokken.	**PRODUCT:** Neem een goede (functionele) beschrijving op van de bij (de implementatie van) de OO API betrokken referentiecomponenten, zoals de API Manager. Beschrijf welke referentiecomponenten ontsloten dienen te worden via de OO API. **Aanbevolen acties om op te nemen in roadmap:** ● Referentiecomponenten en/of applicaties die via de OO API ontsloten (moeten) kunnen worden documenteren (als onderdeel van de architectuur documentatie)	

			CONTEXT:	
Architecturele randvoor-waarden	De ontwikkeling van de OO API is nog niet onder architectuur gebracht		Positioneer de OO API ten opzichte van de bestaande (keten) architectuur en documenteer de criteria achter de ontwerp- en implementatiekeuzes.	
Beheer en (door)ont-wikkeling	**Versiebeheer:** Het is niet duidelijk wat de status is van V1 en V2. De lezer van de website c.q. gebruiker van de OO API specificatie zal zich afvragen: - Is V1 (nog) in gebruik? - Wordt V1 uitgefaseerd/vervangen door V2? - Is er een roadmap? - Hoe ga je van een versie naar de volgende versie (als ontwikkelaar en als gebruiker)?		Zorg voor een goede communicatie over zaken zoals: - Binnen welke periode ontwikkelaars de gelegenheid krijgen om hun code aan te passen aan de nieuwe versie (deprecation period). - Migratieplan om over te stappen naar de nieuwe versie (als ontwikkelaar en als gebruiker); - Welke features er toegevoegd, gewijzigd of verwijderd worden; - Welke wijzigingen de huidige implementaties kunnen breken; - Contactmogelijkheid om een verlenging van de deprecation periode aan te vragen **Aanbevolen acties om op te nemen in roadmap:** ● Versiebeheer uitwerken en documenteren (zie bovenstaande advies)	
Implementatie	De OO API bevat geen implementatiehandleiding		Ondersteun instellingen en leveranciers bij de implementatie van de OO API, door bijvoorbeeld een implementatiehandleiding op te nemen als onderdeel van de specificatie	

Overig	De naam OO API kan voor verwarring zorgen. De naam OO API suggereert dat het om een (geïmplementeerde) API gaat. Maar de OO API is de standaard waaraan zo'n API moet voldoen. Daarnaast heeft DUO een API met nagenoeg dezelfde naam (open onderwijsdata API), maar die bedoeld is voor andere doelgroep en andere gegevenssoorten ontsluit.		Overweeg een andere naam voor de OO API die de lading dekt en deze herkenbaar maakt als standaard c.q. API specificatie.	

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