ROSA Architectuurscan/advies: Entree Federatie 2.0

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	Remco de Boer & Joeri van Es
Versie	2e concept
Datum	12 april 2021
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding	Een toets vanwege de voorgenomen vernieuwing van de Entree Federatie.
Betreft	Entree Federatie 2.0
Brondocument(en)	Een technische verkenning en Toekomst Entree Federatie Een verkenning van de markt en een duurzaam platform - v1.0. KNF:Hoofdpagina - Kennisnet Developers Documentatie Pitch-Architectuurscan-Entree Federatie Attribute Release in de nieuwe Entree Federatie.pptx
Begeleidende documenten	Vernieuwing Entree Federatie- MT SURFconext: overal veilige toegang met 1 set credentials | SURF.nl Entree Federatie - ROSA Wiki

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 **Entree Federatie 2.0**. 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 **Entree Federatie 2.0**. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van het **Entree Federatie 2.0** bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen het **Entree Federatie 2.0** 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 **Entree Federatie 2.0**, 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: Entree Federatie 2.0

ROSA-onderdeel	Bevindingen uit project: Entree Federatie 2.0	Relatie met ROSA (blauw: ROSA, geel: Entree Federatie 2.0)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkings-gebied		 **Compliant** - De Entree Federatie heeft betrekking op het PO, VO en MBO. Daarnaast bestaat er ook een relatie met software leveranciers. In het bijzonder softwareleveranciers die opereren als Identity en Service Providers. (Bron: Pitch (4))	**PRODUCT:** **CONTEXT:**	
Toepassings-gebied		 **Compliant** - De Entree Federatie heeft een relatie met de toepassingsgebieden Identificatie en toegang en IBP.	**PRODUCT:** **CONTEXT:**	
Ontwerpgebied **Bovensectorale samenwerking**	**Koppelen - niet kantelen** *"Entree Federatie zorgt ervoor dat digitale identificatie en authenticatie zo min mogelijk het onderwijsproces onderbreken."* Deze doelstelling uit H2 van de Marktverkenning (2), sluit aan bij het ROSA Basisprincipe Koppelen - niet kantelen. **Een gezamenlijke basisinfrastructuur:** Het ROSA basisprincipe Koppelen - niet kantelen, wordt verder ingevuld door het leveren van een gezamenlijke basisinfrastructuur. Deze basisinfrastructuur realiseert de Entree Federatie door online authenticatie van gebruikers te centraliseren; "*waarbij onderwijsinstellingen en dienstaanbieders met elkaar gekoppeld worden via een centrale voorziening"* (Bron:	 **Compliant** - De Entree Federatie heeft raakvlakken met het ROSA basisprincipe Koppelen - niet kantelen. De implementatie van dit principe leidt tot een relatie met het afgeleide ROSA principe Een gezamenlijke basisinfrastructuur. Deze relatie wordt versterkt door de keuze om de nieuwe versie van de Entree Federatie te baseren op software die binnen het HO wordt toegepast.	**PRODUCT:** **CONTEXT:**	

	H2 Marktverkenning (2)) **Samenwerking met SURFconext:** SURFConext wordt in §4.3.2 van de Marktverkenning (2) genoemd als vergelijkbare partij met een andere doelgroep. In §6.3.1 van de Marktverkenning wordt OpenConext genoemd als de meest kansrijke optie om de vernieuwde Entree Federatie op te baseren. Dit is dezelfde open source software waar SURFConext op gebaseerd is. Uit de gesprekken met de Entree Federatie (5) bleek dat direct gebruik van SURFConext niet mogelijk is, omdat de Zeggenschappen te veel verschillen. In het bijzonder speelt daarbij de rol van instellingen in het ho als eigen ID-provider ten opzichte van scholen in het po en vo die in de regel het LAS c.q. de LAS-leverancier als ID-provider gebruiken. De samenwerking tussen Kennisnet en SURF wordt aangemerkt als gemakkelijk te organiseren. Daarnaast, wordt erkend dat wanneer Kennisnet en SURF OpenConext doorontwikkelen, dit ook van waarde is voor een bredere doelgroep.			
Ontwerpgebied **Informatie-beveiliging en privacy (IBP)**	**AVG is drijfveer voor verbeteringen aan Architectuur:** In §2.2.2 van de Marktverkenning (2) wordt de AVG genoemd als één van de redenen waarom vernieuwing van de Entree Federatie (EF) nodig is. De AVG biedt gebruikers het recht op meer inzicht in en controle over hun gegevens. Met het huidige platform gaat dit lastig en is innoveren duur, aangezien deze gebaseerd is op verouderde technologie. Daarnaast speelt ook mee dat leerlingen tot 14 jaar zelf niet de verantwoordelijkheid over hun eigen identiteit dragen, waardoor de onderwijsinstelling daarvoor verantwoordelijk is.	 **Consistent -** Op pagina 14 van de technische verkenning (1) worden continuïteit, performance en betrouwbaarheid genoemd als de focuspunten om de architectuur te verbeteren. Deze focuspunten hebben veel raakvlakken met het ROSA ontwerpgebied IBP. Het Attribute release policy heeft een relatie met ROSA ontwerpkader Duidelijke eisen en verwachtingen. De uitgangspunten op p.14 van de technische verkenning (1) hebben een	**PRODUCT:** Onderzoek in hoeverre de scope van een ARP past op het ‘dienst’begrip uit het OSR, en welke rol het OSR zou kunnen spelen bij het registreren van ARPs (één bron waar alle mandateringen/toestemmingen rondom een dienst zijn vastgelegd) **CONTEXT:**	Verrijk het ROSA ontwerpkader Continuïteit van de dienstverlening met voorbeeld maatregelen uit de technische verkenning (1) p.15.

	Duidelijke eisen en verwachtingen Op P.11 van de technische verkenning (1) wordt het idee van de Attribute Release Policy service uitgelegd. Uit gesprekken met de EF (5) bleek dat iedere school met iedere service provider een eigen ARP afsluit. De scope van de Attribute Release Policy lijkt te passen bij de scope van Services waarvoor in het OSR mandaten worden vastgelegd. Scholen zullen voor een dienst zowel mandateringen in het OSR als ARPs voor Entree moeten vastleggen.. In de Developer documentatie (3) bestaat een pagina waar aanvullende attributen en richtlijnen op te vinden zijn. Uit brondocument (5) blijkt dat in de nieuwe situatie dit anders zal werken. Bij het aansluiten van een service provider kan de attributenset ingericht worden conform, bijvoorbeeld, het Attributenbeleid van Edu-K of andere relevante afspraken. **Continuïteit van de dienstverlening** De uitgangspunten op p.14 technische verkenning (1) gaan in op een technische implementatie om de continuïteit van de dienstverlening te waarborgen. De maatregelingen om de continuïteit te waarborgen zijn goed uitgewerkt en zouden potentieel van toegevoegde waarde kunnen zijn voor de ROSA om de implicatie binnen het ontwerpkader te verrijken met voorbeelden.	relatie met ROSA ontwerpkader Continuïteit van de dienstverlening.		
Ontwerpgebied **IAA**	Het huidige Entree Federatie platform loopt tegen grens aan van het aantal authenticaties p.22 technische verkenning (1), daarnaast wil Kennisnet nieuwe technologieën op het gebied van Identity Management kunnen ondersteunen zoals SSO voor mobiele devices. [§2.2.2 van de Marktverkenning (2)]	 **Compliant** - Er is een relatie met ROSA ontwerpkader **Meerdere expliciete betrouwbaarheidsniveaus**. Het inrichten van deze betrouwbaarheidsniveaus is niet de	**PRODUCT:** **CONTEXT:**	

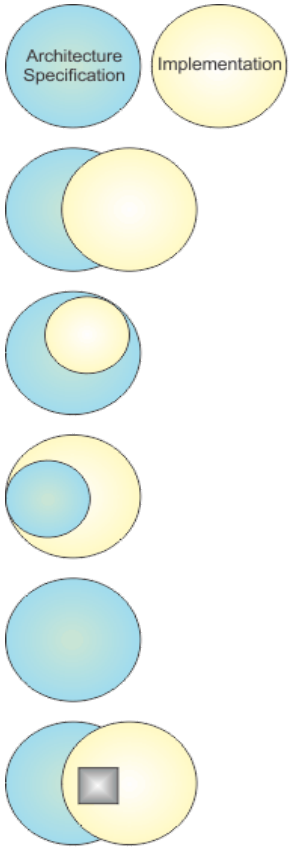
	Marktpartijen kunnen IAA-diensten leveren Volgens p.8 vd technische verkenning (1) maakt de Entree Federatie (EF) gebruik van een Hub-and-spoke model. Dit houd in dat de EF erin voorziet dat meerdere Service providers gebruik kunnen maken van identiteiten vanuit verschillende ID providers via een centrale hub. **Meerdere expliciete betrouwbaarheidsniveaus** Op p.24 van de technische verkenning (1) staat de impact omschreven van het ondersteunen van betrouwbaarheidsniveaus op de Entree Federatie. ID providers zijn verantwoordelijk om deze betrouwbaarheidsniveaus in te stellen. Er zijn momenteel geen attributen ingericht om een betrouwbaarheidsniveau uit te wisselen binnen de Entree Federatie.	verantwoordelijkheid van de EF, maar zal dit wel gaan ondersteunen. Daarnaast is er een relatie met het ontwerpkader **Marktpartijen kunnen IAA-diensten leveren**, aangezien de EF de dienstverlening van ID providers makkelijker maakt.		
Ontwerpgebied **Gegevens-uitwisseling in de keten**	**Behoeftegerichte en doelgebonden gegevensuitwisseling** De EF biedt een manier om identiteit van een gebruiker uit te wisselen op het moment dat die gebruiker zich bij een systeem aanmeldt. Daarvoor wordt gebruik gemaakt van het SAML-protocol of OpenID-connect. De Entree Federatie is zelf geen gegevensbron voor identiteitsgegevens. Ook de attributen die via de Entree Federatie kunnen worden meegestuurd worden niet binnen Entree opgeslagen. De registratie en het gebruik van Attribute Release Policies ondersteunt het behoeftegericht en doelgebonden uitwisselen van deze gegevens.	 **Compliant** - De inrichting van de Entree Federatie is gericht op het minimaliseren van de uit te wisselen attributen, waarmee invulling gegeven wordt aan het basisprincipe **Behoeftegerichte en doelgebonden gegevensuitwisseling**.	**PRODUCT:** **CONTEXT:**	

	‘Mijn Entree’ biedt een aantal APIs voor metadata en rapportage. Via de Mijn Entree APIs kunnen alleen publieke gegevens worden ontsloten. Toepassing van de UBV-TLS afspraak wordt als vanzelfsprekend gezien.			
Ontwerpgebied **Governance**	Volgens de Pitch (4) blijft het beheer van de Entree Federatie belegd bij Kennisnet. **Alle belangen in kaart** H4 van de Marktverkenning (2) beschrijft de positie van alle groepen belanghebbende waaronder kennisnet zelf, verschillende groepen gebruikers concurrenten en leveranciers. **Betrokken belanghebbenden** In H4 van de Marktverkenning (2) worden de groepen belanghebbenden benoemd. Uit de gesprekken met de EF blijkt dat via programma start schooljaar SEM de communicatie verloopt. Scholen worden geïnformeerd via de nieuwsbrief van Kennisnet en later ook via de raden. **Bewaak relaties met andere afspraken** Het governanceproces rondom de Entree Federatie haakt aan bij bestaande governance- en opverlegstructuren met overlappende doelstellingen. Dit governanceproces is vanuit de Entree Federatie zelf lastig te sturen. **Aanvullend** Het onderwijsdomein kent geen stelselconformiteit als eis of randvoorwaarde. Hoewel dit strikt genomen buiten de scope van de ROSA-governanceparagraaf valt, onderkennen we dat gebrek aan een	 **Compliant** - H4 van de Marktverkenning (2) beschrijft de positie van alle groepen belanghebbenden en heeft daarom een relatie met ontwerpkader **Alle belangen in kaart**. Er is een relatie met **Betrokken belanghebbenden.** Er is bekend hoe de groepen belanghebbende betrokken zullen worden bij het beheer/doorontwikkelproces. Relaties met andere afspraken worden bewaakt door bijvoorbeeld aan te sluiten bij werkgroepen met overlappende doelstellingen. Daarom wordt voldaan aan het ontwerpkader **Bewaak relaties met andere afspraken.**		

	overkoepelend stelsel hier wel als risico. De werking van de federatie is uiteindelijk afhankelijk van de op intenties gebaseerde samenwerking tussen ketenpartijen.			
Keten-processen		**Compliant** - Volgens het stuk Context uit H2 van de Marktverkenning (2) is de Entree Federatie een aanmelddienst. Daarom heeft het een relatie met het ketenproces **aanmelden en inschrijven**.	**PRODUCT:** **CONTEXT:**	
Zeggen-schappen en gegevens-soorten	Zie bijlage 2	**Compliant** - Entree is zelf ook idP, maar daar is een aparte dienst voor gemaakt. Er zitten geen identiteiten in de Entree federatie zelf (alleen bij Idps). Uit gesprekken blijkt dat de EF de uitwisseling van attributen en het goed vastleggen van zeggenschappen op attributen faciliteert. Entree is daarin geen verantwoordelijke partij. Rollen en verantwoordelijkheden zijn (juridisch) geregeld in een contract voor aansluiting.	**PRODUCT:** **CONTEXT:**	
Referentie-componenten en landelijke voorzieningen		**Compliant** - Uit de ROSA Wiki (7) wordt duidelijk dat er een relatie is met het referentiecomponent Toegangsdienst educatieve content.	**PRODUCT:** **CONTEXT:**	
Architecturele randvoor-waarden			**PRODUCT:** **CONTEXT:**	

Beheer en (door)ont-wikkeling			**PRODUCT:** **CONTEXT:**	
Implementatie	Het project omvat een stevige infrastructurele vernieuwing die veel partijen raakt.		**PRODUCT:** ● Zorg ervoor dat alle relevante partijen vroegtijdig betrokken zijn en weten welke (implementatie)last de vernieuwing voor hen betekent. ● Zorg dat de Entree Federatie goed wordt ingepast t.o.v. andere ketenvoorzieningen en -ontwikkelingen **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

Bijlage 2: **ZEGGENSCHAPPEN**