ROSA Architectuurscan/advies: Uniforme Beveiligingsvoorschriften (UBV) TLS

edustandaard

Voor	Architectuurraad
Van	Bureau Edustandaard
Scan uitgevoerd door	
Versie	2e concept
Datum	
Versiehistorie	1e concept: opgesteld door BES 2e concept: afgestemd met de indiener en direct betrokkenen definitief: behandeld door Architectuurraad
Aanleiding	
Betreft	Uniforme Beveiligingsvoorschriften (UBV) TLS
Brondocument(en)	Uniforme-Beveiligingsvoorschriften TLS versie 0.5
Begeleidende documenten	De website: https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/uniforme-beveiligingsvoorschriften-0-2-2/ Gesprekken met Jordy van den Elshout, Erwin Reinhoud, Dirk Linden

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 UBV. 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. de UBV. Deze adviezen zijn direct gericht aan de project(deel)groep die zich met de totstandkoming van de UBV bezighoudt. De CONTEXT-adviezen hebben betrekking op de context waarbinnen de UBV 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 UBV, 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: Uniforme Beveiligingsvoorschriften

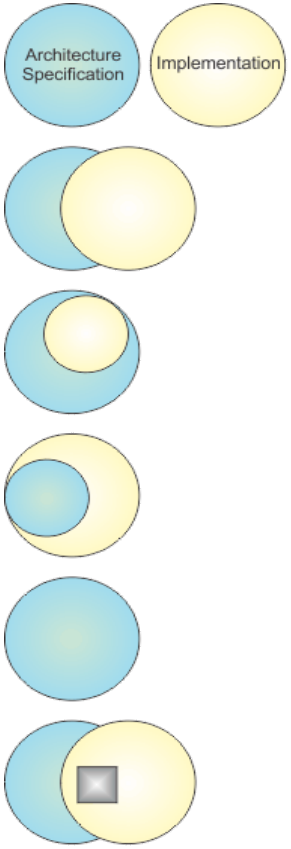
ROSA-onderdeel	Bevindingen uit project: UBV	Relatie met ROSA (blauw: ROSA, geel: UBV)	Voorgesteld advies aan project	Voorgesteld advies aan AR voor plaatsing onderwerpen op de architectuurbacklog ROSA
Werkings-gebied	Volgens §1.3 van de Uniforme Beveiligingsvoorschriften, heeft de afspraak betrekking op de gehele onderwijssector.	 **Fully conformant -** bestrijkt het volledige werkingsgebied van de ROSA.	**PRODUCT:** Overweeg een openbare consultatie / brede review. **CONTEXT:** We raden partijen binnen het werkingsgebied van de ROSA aan om de UBV te vergelijken met de huidige gehanteerde beveiligingsvoorschriften, en deel te nemen aan een eventuele openbare consultatie / brede review.	Ondersteun een openbare consultatie / brede review door de achterban te betrekken.
Toepassings-gebied	Doel van de afspraak is het onderhouden van een eenduidige set van beveiligingsvoorschriften waarmee de veiligheid, interoperabiliteit en efficiëntie in de onderwijsketen wordt bevorderd. De voorschriften gelden voor alle M2M-gegevensuitwisselingen binnen het onderwijs, zowel voor uitwisselingen via Edukoppeling als voor gegevensuitwisselingen die eigen afspraken hebben zoals de Overstap Service Onderwijs (OSO). De afspraken zijn ook van toepassing voor alle H2M-uitwisselingen via websites en webdiensten die binnen het onderwijs gebruikt worden, aangezien die doorgaans ook een beveiligde verbinding bieden.	 **Compliant -** De UBV hebben betrekking op het Informatiebeveiliging en Privacy toepassingsgebied van de ROSA.	**PRODUCT:** **CONTEXT:**	

Ontwerpgebied **Bovensectorale samenwerking**	"Doel van de afspraak is het onderhouden van een eenduidige set van beveiligingsvoorschriften waarmee de veiligheid, interoperabiliteit en efficiëntie in de onderwijsketen wordt bevorderd." (UBV §1.2),	 **Compliant -** De doelstelling van UBV draagt bij aan het ROSA-principe "Een gezamenlijke basisinfrastructuur". Door ketenbreed gelijke technische afspraken te hanteren, wordt interoperabiliteit in de keten ondersteund.	**PRODUCT:** **CONTEXT:**	
Ontwerpgebied **Informatie-beveiliging en privacy (IBP)**	**Ketenpartijen conformeren zich aan de 'Code voor informatiebeveiliging'** Sommige voorschriften gelden op basis van BIV classificatie, hierbij wordt gebruik gemaakt van het "Certificeringsschema informatiebeveiliging en privacy ROSA". (UBV §1.4) Voor de Uniforme beveiligingsvoorschriften wordt waar mogelijk gebruik gemaakt van 'hoger gelegen' afspraken. Bij voorkeur internationale afspraken (zoals van INAN), indien nodig nationale afspraken (zoals van Forum Standaardisatie en NCSC) en alleen als die niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Afwijken van bovenliggende afspraken wordt onderbouwd.	 **Compliant -** de Uniforme Beveiligingsvoorschriften omvatten gezamenlijke afspraken op het gebied van Communicatiebeveiliging uit de Code voor Informatiebeveilging (ISO27001/27002)	**PRODUCT:** Maak expliciet wat de scope van de UBV is ten opzichte van ISO27001/27002: beperkt die zich inderdaad tot (aspecten van) communicatiebeveiliging, of is het (op termijn) de bedoeling deze afspraak uit te breiden met afspraken op andere vlakken? **CONTEXT:**	Coördineer de inhoudelijke samenhang tussen (de scope van) verschillende afspraken; Edukoppeling richt zich bijvoorbeeld ook op Communicatiebeveiliging, maar dan meer specifiek op (M2M) Elektronische berichten. Neem een verwijzing naar UBV op in het ROSA-ontwerpgebied IBP.
Ontwerpgebied **IAA**	-	 **Irrelevant** - de uniforme beveiligingsvoorschriften hebben niet direct een relatie met Identificatie, Authenticatie en Autorisatie, maar zorgen op een lager technisch niveau wel dat deze processen veilig kunnen verlopen.	**PRODUCT:** **CONTEXT:**	

Ontwerpgebied **Gegevens-uitwisseling in de keten**	-	 **Irrelevant -** de uniforme beveiligingsvoorschriften ondersteunen (beveiliging en interoperabiliteit van) H2M en M2M-gegevensuitwisseling, maar gaan niet direct over die gegevensuitwisseling.	**PRODUCT:** **CONTEXT:**	
Keten-processen	-	 **Irrelevant -** De Uniforme Beveiligingsvoorschriften zijn dusdanig fundamenteel/technisch dat ze indirect alle ketenprocessen raken. De voorschriften zelf gaan echter niet over (de inrichting / beveiliging van) processen.	**PRODUCT:** **CONTEXT:**	
Zeggen-schappen en gegevens-soorten	-	 **Irrelevant -** De UBV bevat geen voorschriften die direct in relatie staan met Zeggenschappen.	**PRODUCT:** **CONTEXT:**	
Referentiecom ponenten en applicaties	(zie toepassingsgebied)	 **Compliant -** De UBV raken alle referentiecomponenten en applicaties die H2M of M2M gegevens/informatie uitwisselen.	**PRODUCT:** **CONTEXT:**	
Architecturele randvoor-waarden	Bestaande standaarden en uitwisseldiensten moeten naar de UBV-voorschriften verwijzen en niet (meer) zelf definiëren. Edukoppeling, UWLR, ECK DT en OSO worden hierbij met name genoemd.	Een beperkt aantal standaarden en uitwisseldiensten wordt met name genoemd, maar heeft dit niet ook impact op federaties, Entree /SURFConnext en vele online diensten binnen het onderwijs?	**PRODUCT:** Verhelder waarom juist deze standaarden en uitwisseldiensten bij naam worden genoemd, en wat de UBV betekenen voor andere, niet bij naam genoemde uitwisselingen. **CONTEXT:** Bestaande standaarden en uitwisseldiensten moeten gaan verwijzen naar / gebruik maken van de Uniforme Beveiligingsvoorschriften	

Governance	Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van de voorschriften besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep Uniforme beveiligingsvoorschriften en vanuit Edu-K. In de Ketenregie-overleggen wordt nu gesproken over de inrichting van de governance van de UBV. Aangezien het belangrijk is dat alle ROSA ketenorganisaties de UBV gaan volgen wordt het als een belangrijk punt gezien dat alle belanghebbende worden betrokken. Momenteel is nog niet van iedere organisatie binnen de keten vertegenwoordiging binnen deze overleggen.	 **Onbepaald** - Belanghebbenden zijn in beeld, maar nog niet allemaal aangehaakt; governancestructuur is nog in opbouw.	**PRODUCT:** **CONTEXT:**	
Implementatie	Er wordt gewerkt met profielen per standaard, waarin bij elke eis is aangeven waarom deze gevolgd moet worden. In de bijlage van het UBV-document is een profiel voor Edukoppeling uitgewerkt. De profielen worden beheerd door de werkgroep UBV. Wijzigingen kunnen door de desbetreffende werkgroep van het profiel aangemeld worden. Bijvoorbeeld wanneer gerelateerde voorschriften veranderen. Een nieuw profiel wordt door beide werkgroepen vastgesteld.	Op dit moment is alleen een profiel voor Edukoppeling uitgewerkt. Het uitwerken van een profiel incl.vaststelling in twee werkgroepen als voorwaarde om aan te sluiten bij de UBV betekent voor andere implementaties dat het niet makkelijk is om snel in te stappen	**PRODUCT:** Overweeg een ‘basisprofiel’ uit te werken dat direct kan worden geadopteerd, waardoor alleen bij afwijkingen van het basisprofiel een toepassingsspecifiek profiel hoeft te worden uitgewerkt. **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