edustandaard

Agenda ES-werkgroep Edukoppeling

Leden: Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Peter Dam (Cito), Olav Loite (Topicus), Pieter Bruring (Kennisnet/CTO/OSR), Maarten Kok (SBB), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)
Agendalid: Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie
21 oktober 2020, 10.00-12.00 uur
Locatie: MS Teams-meeting

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Vaststellen REST/SaaS-profiel (versie 0.7)
4. Update Edukoppeling docs – Compliance en overzicht, REST/SaaS, WUS/SaaS, I&A, Best Practices
5. Terugkoppeling TO Digikoppeling
6. Bespreken scenario's gebruik SaaS-profiel
7. Rondvraag / Sluiting

Ad 3 Terugkoppeling openbare consultatie Edukoppeling REST/SaaS-profiel

Aanpassingen nav bevindingen ROSA-scan en de bespreking in de werkgroep van 24-9-2020.

Ad 4 Update Edukoppeling docs
Met de komst van het REST/SaaS-profiel hebben we al de Architectuur moeten aanpassen. Deze zijn al eerder besproken. In deze meest recente versie zijn een aantal van de punten uit de openbare consultatie verwerkt (Requirements Notation and Conventions conform RFC2119).

WUS/SaaS-Profiel
Beide SaaS-profielen (WUS/REST) hebben een aantal generieke voorschriften waardoor we voor het WUS/SaaS-profiel een nieuwe versie met tekstuele wijzigingen hebben opgesteld. Hierin zijn tevens de teksten bij paragrafen PKI, PKIoverheid en Identificatie samengevoegd en tekstueel aangepast. Ook is in deze nieuwe versie de verwijzing naar UBV voor transportbeveiliging opgenomen. Met de overgang naar UBV hebben we in principe te maken met een aantal aspecten die van impact variëren. Zo wordt in het UBV profiel TLS versie 1.3 en betreffende ciphers toegestaan (backward compatible wijziging), maar wordt ook SNI voor clients verplicht gesteld (niet backward compatible wijziging). We stellen voor om het nieuwe WUS/SaaS-profiel als een minor release te zien en hebben dus een 1.4 conceptversie opgesteld. We willen jullie vragen deze door te nemen en eventuele opmerkingen in het document aan te geven zodat we dit tijdens het overleg kunnen bespreken.

Identificatie en Authenticatie
Het I&A document is op een aantal tekstuele zaken aangepast. Ook is het plaatje met SOAP header en body verwijderd omdat er nu meerder SaaS-profielen zijn. Verder wordt bij REST ook de query string gebruikt voor logistiek informatie en wordt de grens tussen header en body (payload) wat vager. Verder is de afgelopen periode duidelijk geworden dat het handig is om het HRN (OIN voor private partijen) wat nadrukkelijker te benoemen. Dit heeft ook tot een kleine herstructurering van de tekst geleid om het identiteitskenmerk van een school en private partij te verduidelijken.

Best Practices
Het nieuwe REST/SaaS-profiel heeft ook impact op de best practices. Dit heeft met name geleid tot een herstructurering maar ook een aantal tekstuele wijzigingen.

Compliance en overzicht
Eerder is al besproken (actepunt #92) dat er een Compliance en overzicht document moet komen dat vergelijkbaar is met die van Digikoppeling. We hebben een eerste conceptversie opgesteld waarin ook het

REST/SaaS-profiel in is opgenomen. We hopen met dit document duidelijk te communiceren welke versies van documenten bij elkaar horen om tot een Edukoppeling implementatie te komen. Met dit document kunnen we ook beter sturen op het 'In gebruik' hebben van maximaal 2 versies van een bepaald document. Of ketens zich hier aan houden valt niet te monitoren, maar we hopen ze hiermee in ieder geval handvatten te geven om de gewenste set te gebruiken.

Ad 5 TO Digikoppeling

- Logius zoek naar nieuwe vormen van documenteren en publiceren. Momenteel zijn concepten te vinden op https://github.com/centrumvoorstandaarden/Architectuur2.0-metRestfulAPI. Ook heeft men plannen om een REST profiel te ontwikkelen: https://github.com/centrumvoorstandaarden/DigikoppelingRestfulApiProfiel

- Logius heeft nieuwe versies van de Digikoppeling beveiligingsvoorschriften opgesteld. Deze sluiten aan op de nieuwe NCSC transportbeveiligingsrichtlijnen (v1.2[1]) en er is nog een nieuwe versie met wijziging t.b.v. private root certificaten (v1.3).

- Er is een besluit genomen rond SNI; dit wordt opgenomen als best practice bij Beveiligingsvoorschriften. Dit betekend dat Edukoppeling hiervoor een eigen voorschrift moet opstellen. Het huidige voorstel is om dit op te nemen bij het UBV Edukoppeling profiel (dit is ondertussen opgenomen in UBV profiel).

- Het Architectuurdocument gaat nu uitvoerig in op de begrippen 'Digikoppeling Bevraging' en 'Digikoppeling Melding' en wanneer deze patronen toegepast dienen te worden (ebMS/WUS). In de nieuwe versie wordt vrij gelaten wanneer men WUS of ebMS toepast. WUS kan dus voor melding (push) en bevraging (pull) gebruikt worden, zoals dat binnen Edukoppeling al langer toegepast wordt.

- We zien de ontwikkeling dat partijen naast een gevalideerd OIN in het certificaat ook een online toets van het OIN bij COR willen doen bij het berichtenverkeer. Dit omdat de COR API sinds kort de mogelijkheid biedt om de mapping te maken tussen kvk-nummer, OIN en BGcode (bevoegd gezag gemeente). Logius is bezig om deze toets als aanpassing in het OIN beleid (werktitel OIN Architectuur) op te nemen. Bij Edukoppeling wordt hiervoor een serviceregister (OSR) gebruikt, dit is de authentieke bron van OIN's binnen het onderwijs en OSR beheert mandateringen als onderdeel van het SaaS-profiel.

Ad 6 Scenario's gebruik SaaS-profiel

Partijen kunnen zelf als eindorganisatie en verwerker communiceren of via verwerker (1:1, 1:n en n:m).

---

1 https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.2.pdf
https://www.logius.nl/sites/default/files/bestanden/website/20191217_Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie.pdf
https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Overzicht_Actuele_Documentatie_en_Compliance_v1.4.pdf