edustandaard

Agenda ES-werkgroep Edukoppeling

Datum en locatie
14 januari 2021, 13:00-15:30
Locatie: MS Teams-meeting

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

Ad 3 Vaststellen WUS/SaaS-profiel (wijzigingen issuelijst en generieke voorschriften SaaS)
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.

Verwerkte issues:
- Issue #42 Nieuwe foutcodes WUS/SaaS-profiel
- Issue #43 Aan foutcodes voorloopnullen toevoegen (Bijvoorbeeld EK0020)
- Issue #46 Voorschrift SNI (zie ook actiepunt #82 en #85, opgelost via UBV)
- Issue #47 Toestaan van pushberichten opnemen in best practice, is afwijking op DK WB013

Ad 4 Terugkoppeling ervaringen in Eindtoetsketen en vaststellen REST/SaaS-profiel
Bespreken van mogelijke wijzigingsvoorstellen voortkomend uit de implementatie-ervaringen in de Eindtoetsketen.

Ad 5 Update Edukoppeling docs
- **Identificatie en Authenticatie (versie 1.1)**
  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 6 Technisch Overleg Digikoppeling

- **PKIo Public en Private root certificaten**
  Naar aanleiding van het advies van PKIo om voor M2M verkeer PKIo private root certificaten te gebruiken had Logius voor de Digikoppeling beveiligingsvoorschriften een voorstel uitgewerkt om voor M2M alleen deze certificaten toe te staan. Dit stuitte toch op wat weerstand omdat partijen servers inrichten voor de H2M/M2M combi. We hebben dergelijke overwegingen ook al vanuit UBV gehoord. De verwachting is verder dat met API's hier nog meer sprake van gaat zijn. We moeten er rekening mee houden dat er niet meer specifieke Digikoppeling/Edukoppeling gateways ingericht worden. Er is nog geen besluit genomen, maar naar verwachting wordt het slechts een advies (geen eis) om voor M2M private root te gebruiken. Daar waar men dan naast M2M ook via browsers communiceert kunnen PKIo public root (EV Root CA) certificaten gebruikt worden.

- **Roadmap 2020-2021 Digikoppeling Standaard**
  Dit zijn deels items die dus al uitgevoerd zijn:
  - Update Grote berichten standaard met Push-variant (uitgevoerd)
  - Toevoegen RESTful API profiel aan Digikoppeling (openbare consultatie)
  - Revisie Digikoppeling Architectuur (openbare consultatie)
  - Update OIN-beleid, o.a. t.a.v. SubOIN's[1] (openbare consultatie)
  - Digikoppeling zal een nieuwe tactische en strategische laag inrichten om
  - Herinrichting drie lagen governance (loopt).
  - Nieuwe wijze van Publiceren (op github) (loopt)
  - Knelpunten Routering en Intermediairs (moet nog starten)
  - Verkennen mogelijk gebruik ebMS3/AS4 (moet nog starten)

- **Nieuwe AR en REST profiel**
  Logius past voor de ontwikkeling van de nieuwe Architectuur en REST-profiel een nieuwe vorm van documenteren en publiceren toe. Momenteel zijn versies van deze documenten te vinden op https://github.com/centrumvoorstandaarden/Architectuur2.0-metRestfulAPI en https://github.com/centrumvoorstandaarden/DigikoppelingRestfulApiProfiel. Het REST-profiel is vergelijkbaar met het Edukoppeling REST/SaaS-profiel (beide zijn gebaseerd op de API design rules).

- **Nieuwe versies van de Digikoppeling beveiligingsvoorschriften.**
  Deze sluiten aan op de nieuwe NCSC transportbeveiligingsrichtlijnen (v1.2[2]) en er is nog een nieuwe versie met wijziging t.b.v. private root certificaten (v1.3). Mogelijk volgt nog een aanpassing rond PKIo private root certificaten.

[1] Private partijen met een publieke taak kunnen SubOIN's kunnen aanvragen en private partijen ten behoeve van (SAAS-)dienstverlening aan hun publieke klanten kunnen SubOIN's aanvragen.

[2] 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

- **Besluit SNI**
  Dit wordt mogelijk opgenomen als best practice maar niet in voorschriften. Dit betekent dat Edukoppeling hiervoor een eigen voorschrift moet opstellen. UBV schrijft het gebruik wel voor en Edukoppeling maakt gebruik van dit UBV profiel. Er is op dit punt dus wel een verschil tussen Edukoppeling en Digikoppeling.

- **'Digikoppeling Bevraging' en 'Digikoppeling Melding'**
  In de nieuwe AR wordt hier nader op ingegaan. 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.

- **Online toets van het OIN bij COR**
  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 7 Scenario's gebruik SaaS-profiel

Het Edukoppeling SaaS-profiel bestaat nu grofweg uit de volgende onderdelen;

1. mTLS koppeling tussen twee gegevensverwerkers obv PKI-Overheid certificaten
2. identificatie van beide eindorganisaties middels To en From parameters (in SOAP of URI, afhankelijk van het profiel)
3. bevragen van mandaten bij het OSR: mag verwerken X leveren namens eindorganisatie Y
4. bevragen van de endpoints bij het OSR om gegevens op de juiste plek(URL) bij de verwerker af te kunnen leveren

We willen bespreken hoe hier invulling aan te geven bij verschillende scenario's (partijen kunnen namens zichzelf als eindorganisatie en verwerker communiceren of via verwerker, dus 1:1, 1:n en n:m). We kunnen dan deze keuzes ook expliciet documenteren zodat hierover duidelijkheid is wat er in een bepaald scenario verwacht wordt.