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
30 september 2020, 10.00-12.30 uur
Locatie: Telefonisch

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Terugkoppeling openbare consultatie REST/SaaS-profiel
4. PKIo Public en Private Root Certificaten
5. Edustandaard UBV (v0.7) – impact TLS 1.3, ciphers, SNI verplicht voor client, bij voorkeur poort 443, bij voorkeur PKI OCSP stapeling
6. Update Edukoppeling docs – Compliance en overzicht, REST/SaaS, WUS/SaaS, I&A, Best Practices
7. Terugkoppeling TO Digikoppeling
8. Rondvraag / Sluiting

Ad 3 Terugkoppeling openbare consultatie Edukoppeling REST/SaaS-profiel

Op het Edukoppeling discussieplatform[1] is half juli een post geplaatst met de vraag aan de leden om het REST/SaaS-profiel (0.5 versie) en de Architectuur (versie 2.0, juni 2020) te reviewen die op de Edustandaard[2] website zijn gepubliceerd. De opmerkingen die via het forum en anderszins zijn binnengekomen willen we graag met jullie bespreken. Het is de bedoeling dat we kunnen vaststellen welke wijzigingen nog doorgevoerd moeten worden voordat we het REST-profiel ter vaststelling kunnen aanbieden aan de Edustandaard Architectuurraad (volgende bijeenkomst van de AR is in oktober). Het ontvangen commentaar richt zich niet alleen op nieuwe zaken die met het REST-profiel geïntroduceerd worden. Er zijn bijvoorbeeld ook opmerkingen hoe transportbeveiliging nu is ingericht en dan met name met betrekking tot het gebruik van PKIo-certificaten en het OIN. Voor de vaststelling zijn alleen de opmerkingen relevant die betrekking hebben op REST-profiel (zoals Design rules principes). De opmerkingen die meer betrekking hebben op de fundamenten van het SaaS-profiel (zoals PKIo en OIN) willen we graag apart bespreken.

Ad 4 PKIoverheid private en public root certificaten

Een partij die bij een PKIo TSP een certificaat wilde aanvragen kreeg te horen dat de PKIo public root certificaten niet meer geleverd mogen worden. De melding vanuit de betreffende TSP was: *De overheid heeft besloten dat er vanaf vandaag geen standaard servercertificaten meer mogen worden uitgegeven wanneer zij worden gebruikt voor communicatie met de overheid. Hiervoor is een PRIVATE servercertificaat of een Digipoort PRIVATE servercertificaat nodig. Het standaard servercertificaat zal namelijk niet meer worden ondersteund in de digipoort-omgeving*.

[1] https://groups.google.com/a/kennisnet.nl/g/edukoppeling/c/Tl9iVL6pFjg
[2] https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/edukoppeling-juni-2020/

Na navraag bij Logius wordt duidelijk dat sinds begin juli is begonnen met een onderzoek naar de uitgegeven PKIo certs. Informatie hierover is te vinden op https://logius.nl/actueel/logius-onderzoekt-certificaten-die-niet-voldoen-aan-de-afgesproken-richtlijnen. Een van de consequenties is (of zal zijn) dat er voor M2M verkeer geen public root certs, dus alleen de private root, gebruikt kunnen of mogen worden.
In de Edukoppeling community ontstond hiermee de vraag of private certificaten toegepast mochten worden. Hoewel zowel private als public root certificaat mogen worden gebruikt was deze informatie niet nadrukkelijk gedocumenteerd bij Digikoppeling. Recent zijn documenten gepubliceerd waarin dit nadrukkelijk wordt aangegeven:

https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.3.pdf

https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Gebruik_en_achtergrond_certificaten_v1.6.pdf

https://www.logius.nl/sites/default/files/bestanden/website/20200902_Release_Notes_Wijziging_Digikoppeling_Standaard_documentatie.pdf

Zowel private als public root mogen dus NU NOG gebruikt worden. Het is dus wel de verwachting dat op termijn public certificaten niet meer gebruikt mogen worden. Logius (PKIo) geeft aan dat de prognose is dat het vervangingsproces zes maanden (vanaf juli 2020) zal gaan duren. Belangrijk punt in het actieplan is dat certificaten die gebruikt worden voor machine-to-machine verkeer omgezet moeten worden naar zogeheten private certificaten met een langere geldigheidsduur. We hopen bij het komende TO Digikoppeling definitief duidelijkheid te krijgen over wat dit voor Digikoppeling (en Edukoppeling) betekent.

Ad 5 Openbare consultatie Edustandaard Uniforme beveiligingsvoorschriften (UBV)
De Edukoppeling SaaS-profielen verwijzen voor transportbeveiliging naar UBV. UBV is momenteel nog in ontwikkeling. Voor versie 0.7 loopt nu een openbare consultatie:
https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/uniforme-beveiligingsvoorschriften-0-7/

In UBV is een bijlage opgenomen met een profiel speciaal voor Edukoppeling. We willen jullie vragen om de UBV versie 0.7 door te nemen. We willen bespreken of dit voldoet en een niet te grote impact creëert voor Edukoppeling (zowel voor het REST/SaaS als WUS/SaaS-profiel. Voor het WUS/SaaS-profiel is ons inziens wel een nieuwe minor versie nodig, 1.4). We constateren voorlopig de volgende aandachtspunten:

1. TLS: versie 1.3 en nieuwe ciphers kunnen worden gebruikt
2. Verificatie van het certificaat: Bij UBV heeft OCSP stapeling de voorkeur. Bij PKIo is dat in principe optioneel (vanuit PKIo zijn TSP's verplicht een CRL te ondersteunen), daarnaast worden er aanvullende eisen gesteld als OCSP toegepast wordt (zie hieronder PvE PKIo).
3. Voorkeur voor poort 443, maar niet verplicht (dus in principe geen impact).
4. SNI verplicht voor clients
5. In het UBV Edukoppeling profiel staan voor de items rond Berichtondertekening dat deze verplicht zijn, dat klopt maar alleen bij toepassing van het WUS/SaaS-profiel met ondertekenen (2W-be-S). Hetzelfde geldt voor Berichtversleuteling, dit alleen relevant voor het 2W-be-SE profiel

Ad 6 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 7 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[3]) 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.

---

3 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

- 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.