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
27 mei 2020, 10.00-12.30 uur
Locatie: Telefonisch

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Edukoppeling Architectuur 2.0
4. Edukoppeling REST/SaaS-profiel versie 0.4
5. Uniforme beveiligingsvoorschriften Onderwijs
6. Testen services
7. Terugkoppeling TO DK
8. Rondvraag / Sluiting

Ad 3 Edukoppeling Architectuur 2.0
De architectuur is vorige keer voorlopig vastgesteld, maar is nog wel aangepast. Bij de beschrijving va het SaaS profiel is de registratie van de mandatering in meer detail beschreven. Bij de bouwstenen is het functioneel model van het OSR opgenomen.

Ad 4 Edukoppeling REST/SaaS-profiel versie 0.4
Ook voor het REST/SaaS-profiel is er een nieuwe conceptversie opgesteld en er zijn nog verschillende besluiten te nemen. Het belangrijkste besluit dat komend overleg genomen moet worden is hoe we de routeringskenmerken voor de eindorganisatie in het request gaan opnemen. Ter ondersteuning hiervan is een notitie opgesteld. Voor de verplichte routeringskenmerken moeten we tevens besluiten of we hiervoor specifieke foutmeldingen voor definiëren of dat er alleen met HTTP status codes gewerkt wordt.

Ad 5 Edustandaard Uniforme beveiligingsvoorschriften (UBV)
Het REST/SaaS-profiel verwijst al naar UBV, maar UBV is nog in ontwikkeling. De huidige conceptversie is te vinden op https://docs.google.com/document/d/1RX6hoSpuujl4JdKHqW4MpFyQy5uZqcPSbnT8e2oqCKo/edit. Hierin is als bijlage een profiel speciaal voor Edukoppeling opgenomen. We willen graag bespreken of dit voldoet. We constateren voorlopig het volgende:

1. In het UBV Edukoppeling profiel staat dat ook OCSP vereist wordt, maar bij PKIo is dat in principe optioneel (CRL is wel verplicht), daarnaast worden er aanvullende eisen gesteld als OCSP toegepast wordt (zie hieronder PvE PKIo). Aangenomen dat dit geldt voor alle typen certificaten (dus ook m2m).
2. In het UBV Edukoppeling profiel staat nog steeds de verplichting voor poort 443.
3. 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

Ketenpartijen testen frequent elkaars services met het doel om vast te stellen of de service beschikbaar is. Men wil zelf een beeld opbouwen van de beschikbaarheid van een dienst. In plaats van echte services/operaties hiervoor te gebruiken zouden dienstaanbieders ook speciale (light weight liveliness/ readyness) operaties kunnen definiëren waarmee een dienst dit testen out-of-the-box kan ondersteunen. We willen bespreken of zoiets ook binnen Edukoppeling deels gestandaardiseerd zou moeten worden.

Bij het testen is het ook wenselijk om onderscheid te maken in test en productieomgevingen. Door op TLS niveau met verschillende certificaten te gaan werken, kunnen we testcertificaten autoriseren voor testomgevingen, en productiecertificaten voor de productieomgevingen. Zo is het risico op kruisverbanden over omgevingen heen geminimaliseerd. Voorstel is nu om de G3 certificaten te gebruiken voor productie, en G1 certificaten voor testdoeleinden. Beide hebben een apart root certificaat wat makkelijk te onderscheiden is. In best practice staat nu nog het gebruik van ODOC-certificaten maar dit willen we dus aanpassen omdat de ODOC-certificaten helemaal gaan verdwijnen.

Ad 7 Digikoppeling

- Logius zoek naar nieuwe vormen van documenteren en publiceren. Momenteel zijn concepten te vinden op https://gitlab.com/logius/digikoppeling

- 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.

- 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 kvknummer, 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.

---

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