

Agenda ES-werkgroep Edukoppeling

Leden: Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Peter Dam (Cito), Don de Lange (Kennisset/OSR), Maarten Kok (SBB), Brian Dommissie (Kennisset, voorzitter), Erwin Reinhoud (Kennisset, BES)
Agendalid: Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie

29 april 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 0.3
5. Uniforme beveiligingsvoorschriften Onderwijs
6. Testen services
7. Terugkoppeling TO DK
8. Rondvraag / Sluiting

Ad 3 Edukoppeling Architectuur 2.0

Vorige keer hebben we de 2.0 conceptversie al besproken. Op basis van de gemaakte opmerkingen is er een nieuwe conceptversie opgesteld. De meeste aspecten rond deze nieuwe versie zijn vorige keer vastgesteld, maar er zijn nog een aantal punten die aandacht vragen, zoals de theorie rond een serviceregister en OSR als bouwsteen.

Ad 4 Edukoppeling REST/SaaS-profiel versie 0.3

Ook voor het REST/SaaS-profiel is er een nieuwe conceptversie opgesteld. Vorige keer is niet het hele document besproken. Daarnaast zijn er in de tussentijd wel een aantal keuzes gemaakt, zoals het gebruik van HTTP headers om te kunnen routeren. Verder zijn er een aantal andere zaken die we nog wat concreter willen specificeren, zoals endpoints, resources en diensten en de registratie van de benodigde gegevens in een serviceregister.

De voorschriften rond GEO-informatie (GeoJSON / RFC-7946 en coördinaatreferentiesysteem CRS) zijn in het huidige concept niet overgenomen, tenzij we verwachten dat dit binnen het gedefinieerde werkingsgebied en functionele toepassingsgebied dit toegepast gaat worden (we willen nl. een specifiek profiel definiëren, maar mogelijk is dit een ongewenste beperking).

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://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/uniforme-beveiligingsvoorschriften-v0-2/. Hierin is als bijlage een profiel speciaal voor Edukoppeling opgenomen. We willen graag bespreken of dit voldoet.

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 dienstverleners ook speciale (light weight liveliness/ readiness) operaties kunnen definiëren waarmee een dienst dit testen out-of-the-box kan ondersteunen. We willen bespreken of zo iets 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 (v1.2¹) 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 betekent 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_voorschrift_en_v1.2.pdf

https://www.logius.nl/sites/default/files/bestanden/website/20191217_Release_Notes_Wijziging_Digikoppeling_Stand_aard_documentatie.pdf

https://www.logius.nl/sites/default/files/bestanden/website/Digikoppeling_Overzicht_Actuele_Documentatie_en_C_ompliance_v1.4.pdf