edustandaard

Agenda ES-werkgroep Edukoppeling

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

Datum en locatie
16 juni 2021, 10.00-12.00 uur
Locatie: MS Teams-meeting

1. Opening, mededelingen, vaststellen agenda
2. Doornemen verslag en actielijst
3. Ontwikkelingen Digikoppeling
4. Impact wijzigingen Digikoppeling
5. Ontwikkelingen OSR
6. Rondvraag / Sluiting

Ad 3 Ontwikkelingen Digikoppeling
De vorige bijeenkomst is alweer een tijd geleden (januari) en daarvoor is de prioriteit aan het REST profiel gegeven. Ondertussen heeft Logius met Digikoppeling ook een aantal belangrijke stappen gemaakt. De grootste stappen zijn een nieuw architectuurdocument en een REST-profiel dat hetzelfde toepassingsgebied heeft als het Digikoppeling WUS profiel. Hoe de documentatie ontsloten wordt is ook opnieuw ingericht. Er wordt hierbij gebruik gemaakt van het Github platform (geen PDF's meer die via de communicatieafdeling online werden gezet op de Logius website). Om te bespreken wat dit mogelijk betekent voor Edukoppeling willen we jullie vragen de documenten door te nemen. De documenten zijn te vinden op Digikoppeling Architectuur (centrumvoorstandaarden.nl) en Digikoppeling Restful API Profiel (centrumvoorstandaarden.nl)[1].

Een aantal wijzigingen die we al eerder hadden willen bespreken zijn in Digikoppeling-documenten verwerkt. Een aantal worden hieronder kort toegelicht, maar zijn dus nu ook al in de verschillende Digikoppeling-documenten verwerkt.

Digikoppeling architectuur
De architectuur is op de volgende punten aangepast:

1. 'Digikoppeling Bevraging' en 'Digikoppeling Melding'
   In de nieuwe architectuur wordt hier nader op ingegaan. In de nieuwe versie wordt vrij gelaten wanneer men WUS of ebMS toepast. WUS kan dus voor melding (push-bericht) en bevraging (pull-bericht) gebruikt worden. Hiermee komt Digikoppeling meer in lijn met wat we binnen Edukoppeling al deden.
2. Met de komst van een REST-profiel wordt er niet meer gesproken van 'uitwisseling van gestructureerde berichten' maar van 'gestructureerde gegevensuitwisseling'.

[1] Beide zijn nog ter vaststelling, maar zijn reeds bij het TO Digikoppeling van maart 2021 vastgesteld.

Digikoppeling beveiligingsvoorschriften[2]
De beveiligingsvoorschriften zijn op de volgende punten aangepast:

1. Er zijn tekstuele aanpassingen gedaan n.a.v. het toevoegen van het nieuwe API profiel.
2. Er wordt verwezen naar de nieuwste versie van de NCSC TLS richtlijnen (versie 2.1*).
3. Er is een aangepaste bepaling opgenomen m.b.t. de toepassing van PKIo certificaten. Eerder was voorgesteld om voor M2M-verkeer vanaf 1-1-2021 alleen nog 'PKIo private root' certificaten te gebruiken. Dit houdt geen rekening met de praktijk waarin een server voor zowel M2M-verkeer als bijvoorbeeld een publieke webserver wordt ingezet. In dat geval ligt het gebruik van een 'public root' certificaat voor de hand. In de Digikoppeling beveiligingsvoorschriften is daarom opgenomen dat, in de beschreven situatie, het toepassen van een 'public root' certificaat nog toegestaan is tot 1-12-2022**.

* Ook het Edustandaard UBV M2M profiel is hierop aangepast. *De belangrijkste wijzigingen zijn:*

- *afwaardering TLS 1.2 van 'Goed' naar 'Voldoende',*
- *volgorde cipher suites niet verplicht bij ciphers 'Goed' , de server hoeft niet langer de eigen volgorde af te dwingen.*
- *ondersteuning van 'Client-initiated renegotation' is niet langer 'Onvoldoende', maar 'Voldoende'.*

De wijzigingen hebben geen invloed op de voorschriften van UBV TLS zelf. Waar verwezen of geciteerd wordt naar NCSC, is de tekst aangepast. Ook zijn de profielen geüpdatet (nieuwe versie) op basis van de wijzigingen van NCSC.

** Het certificaat moet zijn van het type PKIoverheid private root. Uitzondering is wanneer er in het kader van certificaatbeheer op 1 server reden is om PKIo public root certificaten te gebruiken voor zowel koppeling als voor webserver. Hier dienen dan bilateraal afspraken over te worden gemaakt tussen de partijen (bij gebruik van PKIO public root certificaten is een specifieke eis en aandachtspunt dat deze vanwege externe regelgeving altijd binnen drie tot vijf dagen vervangen moeten kunnen worden). Deze uitzondering is toegestaan tot 01-12-2022.

Digikoppeling WUS

1. Voorschrift DK WUS WM001 is aangepast. Er stond 'Toepassen MTOM wordt door webservicerequester bepaald' dit is geworden 'Toepassen MTOM wordt door webserviceprovider bepaald'. Concreet betekent dit dat in de toolkit wordt aangegeven dat een webservice een response volgens MTOM verstuurt indien deze een MTOM request heeft ontvangen en een niet geoptimaliseerd bericht verstuurt indien het request ook niet geoptimaliseerd was. De webservicerequester neemt dus het initiatief hierin. Bij het inrichten bepaalt de provider of een koppelvlak wel of geen ondersteuning biedt voor MTOM. Bij een nieuwe koppeling in samenspraak, bij toevoegen van een afnemer aan een bestaande dienst dient deze zich te conformeren aan de bestaande inrichting (en wel of niet gebruik van MTOM).
2. Voorschrift DK WUS – Verplicht gebruik van wsa:to in response vervalt**.

[2] Edukoppeling heeft eigen beveiligingsvoorschriften binnen het UBV M2M profile

Concreet is het voorstel om Mandatory Y* te vervangen door Mandatory N*:

WS-Addresing response headers

Field	*Property*	*Mandatory*	*Description.*
wsa:To	*[destination]*	~~*Y**~~ *N**	*Provides the address of the intended receiver of this message.*

** Sommige platformen wijken op dit punt af van de Web Service Addresing 1.0 – Metadata standaard. Het wsa:To veld wordt bij synchrone SOAP verkeer actief uit het antwoordbericht gefilterd. Om hier vanuit de standaard aan tegemoet te komen mag bij het ontbreken van dit veld in het antwoordbericht door de ontvanger de anonymous waarde (http://www.w3.org/2005/08/addressing/anonymous) worden aangenomen.*

** We hebben in Edukoppeling aangegeven dat WSA:To in response verplicht is. Echter, ook binnen onderwijs blijkt dit lastig omdat het synchroon verkeer is. Willen we conform het REST profiel (en DK) ook het WUS profiel alleen in P2P context beschouwen? De Eindorganisatie in wsa:To request is dan de eindorganisatie From in response en visa versa. Uitzondering is dan mogelijk het gebruik met een intermediair (met tevens ondertekening en versleuteling bericht)

Overige punten

Besluit SNI

Dit is uiteindelijk niet als voorschrift in Digikoppeling opgenomen. Mogelijk wel als best practice. Omdat Edukoppeling ondertussen UBV voorschrijft en deze het gebruik van SNI wel voorschrijft is dit geen probleem. Dit blijft dus wel een verschil tussen Digikoppeling en Edukoppeling.

OIN beleid

Private partijen kunnen ten behoeve van (SAAS-)dienstverlening voor hun publieke klanten SubOINs aanvragen. Het is wenselijk dit te bespreken en te documenteren hoe deze toepassing bij SaaS diensten zich verhoudt tot de huidige oplossing binnen Edukoppeling. In theorie zou via COR de relatie tussen een SubOIN en OIN publieke klanten (scholen) geverifieerd kunnen worden (ook RIO is aan COR gekoppeld).

COR ondersteund OIN verificatie

Bij Digikoppeling willen partijen naast een gevalideerd OIN in het certificaat ook een online verificatie van het OIN bij COR uitvoeren. De COR API kan een mapping maken tussen kvk-nummer, OIN en BGcode (bevoegd gezag gemeente). Logius is bezig om deze toets als aanpassing in het OIN beleid[3]. 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 4 Impact wijzigingen Digikoppeling

De nieuwe Digikoppeling Architectuur en REST-profiel roepen bij ons de vraag op of we weer wat nauwer zouden moeten aansluiten op Digikoppeling. Zo zou de Edukoppeling Architectuur en het SaaS-profiel nog meer beperkt kunnen worden. Er is ook wat voor te zeggen om onze Edukoppeling-documenten te houden zoals ze zijn, we zijn dan flexibeler wat we wel en niet willen binnen het onderwijs. Dit sluit ook beter aan bij de keuze om met eigen UBV-voorschriften te gaan werken. Voor TLS blijven we natuurlijk verwijzen naar UBV. We willen graag jullie mening hierover horen.

[3] OIN Stelsel 2.0.1 (centrumvoorstandaarden.nl)

Ad 5 Ontwikkelingen OSR
We willen graag wat nader gaan kijken hoe Edukoppeling op het terrein van *Identificatie en authenticatie* (dit is ook een apart standaardendocument binnen Edukoppeling) zich verhoudt tot het inmiddels in volle werking zijnde OSR (een belangrijke basisvoorziening voor het onderwijs). Wat zijn de evt. verschillen tussen theorie (Edukoppeling) en praktijk (OSR) en moeten we daar wat mee. Bijv. door de standaard aan te passen of wijzigingsvoorstellen voor OSR mee te geven. Pieter Bruring was als architect bij Kennisnet als liaison tussen Edukoppeling en OSR al voortvarend van start gegaan, maar heeft ons begin 2021 zoals jullie weten verlaten. Zijn opvolger Erik Borgers is ondertussen behoorlijk goed ingewerkt en gaat derhalve onze rangen versterken.