edustandaard

# Agenda Edustandaard werkgroep Edukoppeling

Leden: Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Erik Borgers (Kennisnet, OSR), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)

Agendaleden: Ernst-Jan van Heuseveldt (Rovict/VDOD), Wouter van der Veer (Topicus), Jorim van der Wijngaard (Topicus)

**Datum en locatie**
8 maart 2023, 13:00-15:00 uur
Locatie: Deventer

1. Opening, mededelingen, vaststellen agenda
2. MDX Secure API OAuth profiel 0.2 (in de map van deze bijeenkomst)
3. Secure API protocol 0.6 (in de map van deze bijeenkomst)
4. Rondvraag / Sluiting

**Ad 2 MDX Secure API OAuth profiel v0.2**

1. In deze 0.2 versie van het OAuth-profiel wordt client authenticatie (bij token end point van de authorization server) ondersteund met een JWT. Hiermee sluiten we op dit aan bij de keuze in het iGOV NL OAuth profiel[1]. Het voordeel hiervan is dat we hiermee ook een ontkoppeling hebben met mTLS[2] dat slechts de transportlaag tussen ketenpartijen betreft. Met de JWT kan ook in het achterliggend landschap de client geauthentiseerd en geïdentificeerd worden. In hoeverre dit geldt hangt ook af van de infrastructuur bij betreffende partijen.
2. Om de juiste keuzes te maken (zie 1e punt) zullen we de Edukoppeling (REST) architectuur verder moeten uitdiepen. Hierbij speelt ook de keuze[3] om profielen los van het MDX protocol en/of mTLS-PKIo te gaan ondersteunen een rol. Het OAuth-profiel in deze 0.2 versie is nu een aanvulling op het REST-profiel. Het is dus in essentie geen eigen MDX-profiel maar bovenop het REST-profiel. De gedachte is dat we met deze ontkoppeling dit OAuth-profiel zonder de MDX/mTLS PKio laag ook kunnen gebruiken in andere toepassingsgebieden door de verwijzingen naar het REST-profiel te verwijderen. Het streven is in ieder geval om een breed inzetbaar OAuth-profiel te ontwikkelen.
3. In de vorige versie was een domain_hint parameter opgenomen. Hiermee kon de client aangeven namens[4] welke (onderdeel van een) onderwijsorganisatie het verzoek uitgevoerd wordt. Op basis hiervan kunnen er aanvullende policies ingeregeld worden die autorisaties op dataniveau mogelijk maken. Omdat het een referentie naar een onderwijsorganisatie betreft is de naam in deze versie aangepast naar edu_org_id. Het autorisatiemechanisme op dataniveau oogt te complex om te standaardiseren en er wordt vooralsnog niet in voorzien in het OAuth-profiel. We

[1] Dit betreft wel het code grant profiel, maar waarschijnlijk worden voor het client credentials profiel dezelfde keuzes gemaakt.
[2] In de vorige versie gebruikte we mTLS voor de client authenticatie.
[3] We zien met name in het ho (en ook mbo) dat er andere keuzes worden gemaakt.
[4] SEM: *"…Token aanvragen aanvragen in de context van een School." "Voor het uitwisselen van gegevens waarvoor instemming vanuit de School is vereist is het verplicht om een Token aan te vragen inclusief de schoolidentifier. Op deze manier kan in het endpoint worden gecontroleerd of er een consent is geregistreerd voor uitwisseling van gegevens tussen de beide leveranciers.*"

ondersteunen het scenario echter wel door expliciet te benoemen dat er een edu_org_id[5] opgenomen kan worden in het verzoek naar de authorization server.
4. Er zijn in de 0.2 versie uitgangspunten toegevoegd en deels opnieuw geformuleerd en het document is anders ingedeeld.

**Ad 3 Secure API protocol 0.6**

Op basis van de opmerkingen in de 0.5 versie en de discussie in de werkgroep vorige keer, is een nieuwere versie opgesteld.

[5] Dit is nu opgenomen als een optionele claim in de JWT naar het token endpoint. Net als bij client authenticatie zijn hierin verschillende keuzes te maken. We moeten dus enerzijds de keuze maken of we dit opnemen en als we dat doen dan ook nog besluiten hoe.