Edukoppeling REST/OAuth profielen

Van: Architectenraad Edu-V

Aan: Werkgroep Edukoppeling

Aanleiding

Binnen de werkgroep Edukoppeling is gewerkt aan REST/OAuth profielen waarbij veel input vanuit Edu-V is verwerkt. Tijdens de publieke consultatie is feedback ontvangen van SURF waardoor er naar verwachting wijzigingen zullen volgen in de profielen.

Voor Edu-V is het van belang dat de impact van deze wijzigingen op de technische details op korte termijn duidelijk worden. De reden hiervoor is dat de eerste partijen binnenkort starten met de implementatie van de profielen. We willen voorkomen dat deze partijen rework zodra de profielen wijzigen.

Een oplossing zou kunnen zijn dat er twee profielen naast elkaar bestaan. Een profiel voor het mbo/ho en een profiel voor Edu-V. Dit vinden wij geen wenselijke situatie aangezien dit zal leiden tot een concessie op het vlak van technische interoperabiliteit. We streven er juist naar om binnen Edustandaard deze technische interoperabiliteit te realiseren.

In deze notitie stellen we een aantal oplossingsrichtingen voor om het rework te voorkomen en technische interoperabiliteit te borgen.

Overwegingen

- Binnen Edustandaard werken we in de Edustandaard werkgroepen aan technische interoperabiliteit over alle onderwijssectoren heen. Technische interoperabiliteit op het vlak van de M2M gegevensinteractie is een belangrijk onderwerp.
- De feedback van SURF betreft ook de architectuur van Edukoppeling en is daarmee breder dan het profiel. De feedback is valide maar zit wat ons betreft niet op het kritieke tijdspad van implementatie.
- In de opzet van Edukoppeling zijn de gegevensinteractie en autorisatie op de gegevensinteractie met elkaar verweven. Zowel voor het MDX profiel (OSR) als het REST/OAuth profiel (edu_org_id).
- Forum standaardisatie (NL GOV) heeft een toepassing gemaakt voor de NL overheid. De NL GOV standaarden worden ook gehanteerd in bijvoorbeeld de werkgroep Toegang.
    - Het bestaande NL GOV OAuth 2.0 profiel houdt geen rekening met Direct Access Clients.
    - Het profiel in ontwikkeling wel. Hierbij wordt voor vertrouwelijke gegevens gewerkt met Private Key JWT. Dit verschilt van het huidige Edukoppeling OAuth REST voorstel waarin Mutual TLS wordt toegepast als variant.
    - In het NL GOV profiel worden PKI-overheidscertificaten gehanteerd. Dit zou in alle NL contexten (inclusief het hoger onderwijs) moeten kunnen werken.

- Edu-V heeft een kritiek tijdpad waarin leveranciers op korte termijn starten met de implementatie van het profiel. Als Edu-V zullen we op korte termijn een beslissing moeten nemen over het te implementeren profiel.

Oplossingsrichting

- We richten ons in eerste instantie op de gegevensinteractie en laten de autorisatie op de gegevensinteractie (via mandaten of consent) voor nu buiten beschouwing. Ook de inbedding in de nieuwe architectuur pakken we later op.
- Door het loslaten van consent als onderdeel van het profiel, ontstaan er twee varianten:
    - Profiel voor niet vertrouwelijke gegevens
    - Profiel voor vertrouwelijke gegevens
- We richten ons in eerste instantie op het profiel voor vertrouwelijke gegevens.
- Voor dit profiel bepalen we of het NL GOV OAuth 2.0 profiel dat in ontwikkeling is hiervoor gebruikt kan worden.
- Een quickscan laat zien dat het de volgende toepassing betreft:
    - We hebben te maken met een Direct Access Client.
    - De RFC die is gekozen voor het met hogere betrouwbaarheid kunnen authenticeren bij de autorisatieserver is Private Key JWT (RFC7521 en RFC7523).
    - Dit wijkt af van de RFC die op dit moment in het Edukoppeling REST OAuth profiel staat voor vertrouwelijke gegevens (gegevensclassificaties III en IV). Dit is namelijk Mutual TLS (RFC8705).
    - Voor beide RFC's blijft het PKI-overheidscertificaat van toepassing.
- Voor SURF betekent dat voor M2M gegevensuitwisselingen met een Direct Access Client er ook gebruik kan worden gemaakt van dit profiel, voor Nederlandse partijen hier het PKI-overheidscertificaat gebruikt kan worden. Uiteraard kan SURF in een internationale context bijvoorbeeld met andere certificaten werken. Dit is een pas toe, leg uit.
    - Dit zou bijvoorbeeld van toepassing zijn op de OOAPI en het OKE initiatief.

Vervolgactie

De oplossingsrichting betreft een quickscan door het NL GOV profiel. We stellen voor om ter voorbereiding op de werkgroep Edukoppeling een gedetailleerde vergelijking te maken tussen het NL GOV profiel en het huidige Edukoppeling REST/OAuth profiel. Hierbij lijkt ons de scope gericht op vertrouwelijke gegevens voor nu voldoende.

In de werkgroepbijeenkomst Edukoppeling van 18 maart kunnen we vervolgens met elkaar een afweging maken of we het Edukoppling REST/OAuth profiel al dan niet aanpassen. Voor ons is voornamelijk de oplossingsrichting en de keuze voor de RFC van belang omdat dit de grootste impact is bij de implementatie.