Reactie SURF op het voorgestelde Edukoppeling Secure API OAuth Client Credentials-profiel
Peter Leijnse, Bart Geesink, Patrick van der Veer – 19 februari 2024

Op verzoek van Edustandaard heeft SURF (als expert en als beheerder van de HO-sectorarchitectuur) kritisch gekeken naar het concept-profiel voor Secure API OAuth Client Credentials binnen de Edukoppeling-standaard. Dit profiel is tot stand gekomen binnen de context van Edu-V. Om een generiek profiel binnen Edustandaard te kunnen opnemen is toepasbaarheid buiten de context waarin het tot stand is gekomen een randvoorwaarde. Daarom hebben we vooral gekeken naar de samenhang met andere standaarden en profielen, naar de toepasbaarheid in de context waar SURF werkt (HO en MBO; onderwijs én onderzoek).

Hieronder puntsgewijs de verschillende bevindingen.

Consistentie met de andere onderdelen van de Edukoppeling-standaard

- Er komen diverse rollen en begrippen voor die niet gerelateerd kunnen worden aan de Edukoppeling-architectuur
- De alignment met andere Edukoppeling-documenten zoals 'Identificatie en authenticatie' is onduidelijk
- De koppeling van gegevensclassificaties aan specifieke beveiligingsprofielen komt niet voor in andere onderdelen van Edukoppeling. Hier lopen de technische implementatievoorschriften en de juridische en beveiligingsoverwegingen door elkaar heen.

'Vervuiling' met begrippen en concepten die alleen binnen Edu-V betekenis hebben

- 'leverancier' als (kennelijke) verbijzondering van 'ketenpartner'. Hiermee wordt onduidelijk wat er gebeurt als een ander soort ketenpartner (DUO, SURF, …) client credentials gaat ondersteunen. Het risico ontstaat hier dat onderwijsinstellingen voor verschillende toepassingen toch met meerdere profielen te maken krijgen.
- 'Gegevensclassificaties zoals gedefinieerd in Edu-V'. Deze worden niet herkend buiten de context van Edu-V.
- De specifieke inrichting van consent management wordt niet gebruikt buiten de context van Edu-V, en is op andere plekken heel anders ingericht, met onder andere terminologie (denk aan 'Trust anchors' in federatieve architecturen).
- Gebruik van een onbekend en niet nader gespecifeerd eu_org_id, waar Edukoppeling een OIN voorschrijft.

Onduidelijkheden in technische uitwerkingen

- Onduidelijk welke instanties Autorisatie Servers gaan hosten, en welke eisen daar aan worden gesteld zodat trust geregeld is
- Er wordt niet uitgelegd waar het consent management voor dient
- Naast eerdere genoemde onbekendheid met eu_org_id wordt ook niet genoemd hoe de verificatie hierop plaats vindt.
- De vier profielen komen voor een groot gedeelte overeen. Dezelfde onderdelen worden vaak opnieuw toegelicht. Dat komt de leesbaarheid niet ten goede
- Er wordt niet gespecificeerd hoe verificatie van het token door de resource server (bijvoorbeeld door introspectie) wordt gedaan
- Interoperabilteit is essentieel voor adoptie. Er mist een uitleg over hoe dit gewaarborgd wordt.

Samenhang met andere standaarden in Nederland

- Het profiel verwijst naar Digikoppeling, naar de API Design Rules, (zijdelings) naar het NL-Gov OAuth Assurance-profiel. Soms worden zaken overgenomen, soms wordt er verwezen. Soms is de overname direct, vaak indirect (via bijv. andere Edustandaarden). Dat maakt het geheel een zoekplaatje, waardoor niet duidelijk wordt waar elementen zijn weggelaten, toegevoegd of gewijzigd. Een helderder stellingname over wanneer, waarom en hoe wordt afgeweken van genoemde standaarden is wenselijk.

Specifieke Nederlandse invulling hindert internationale aansluiting.

- Met OINs en voorschriften om te beveiligen op basis van PKIoverheid kan niet worden aangesloten op internationale ontwikkelingen. Datzelfde geldt voor de beveiligingsprotocollen op de transportlaag (TLS vs. VPN). Voor veel toepassings- en werkingsgebieden is dat ook niet aan de orde, en kunnen dergelijke nationale afspraken werken. Voor een groot deel van de use cases die in het ho van belang zijn (samenwerkende europese universiteiten, gebruik van open leermaterialen) is dat niet zo. Voor het onderzoeksdomein geldt dat voor vrijwel alle use cases nationaal georiënteerde afspraken niet zullen werken.
- Let wel: dit is dus geen reden om geen NL-profiel te ontwikkelen, maar wel een 'explain' waarom SURF en de hoger onderwijsinstellingen doorgaans zullen kiezen voor een internationaal profiel buiten Edustandaard.

Het onderwijsdomein is te klein voor een eigen profiel op OAuth client credentials

- In de praktijk is het uitwisselingsdomein van een (hoger) onderwijsinstelling veel breder dan het onderwijsveld zelf. Scoping van een *technische* standaard op alleen het onderwijsveld werkt hierbij beperkend. Er zijn immers veel toepassingen die generiek van aard zijn, waar OAuth client credentials nuttig kunnen zijn. Een specifieke onderwijsinvulling past hier niet bij. Een specifiek OAuth-profiel vereist extra werk voor de leveranciers / ontwikkelaars van software die het profiel moet implementeren en onderhouden.
- Toekomstvastheid en onderhoudbaarheid van een onderwijsspecifieke standaard oogt kwetsbaar. De echte expertise is schaars, de inzet van de beschikbare experts moet verdeeld worden over verschillende werkgroepen, het is een domein waar de nodige ontwikkelingen zijn te verwachten.

Waar zou je OAuth client credentials profielen dan wel moeten ontwikkelen?
Wij zien hiervoor twee parallelle contexten:

- Voor een context waarin partijen met name binnen de Nederlandse publieke context opereren: het NL GOV assurance profile for OAuth 2.0 [iGov-NL]
- Voor een context waarin partijen in een belangrijke mate ook internationaal opereren in onderwijs- en onderzoekscontext: een profiel dat in afstemming met de internationale onderwijs- en onderzoeksgemeenschap tot stand is gekomen [dus binnen Géant/REFEDS/EduGain/… community]

In beide contexten is activiteit t.a.v. het ontwikkelen van profielen/standaarden rondom OAuth. Vanuit SURF wordt hier actief aan meegewerkt. Edustandaard/Kennisnet is ook vertegenwoordigd in de iGov-NL-groep. Voor (met name) het hoger onderwijs is de internationale context essentieel. Daarvoor is nodig dat specifieke Nederlandse invullingen kunnen worden 'losgelaten'.

Gezien het werkings- en toepassingsgebied van het beoogde OAuth client credentials-profiel is de Nederlandse publieke context de voornaamste om naar te kijken, en te streven naar samenhang. SURF blijft daarnaast ook actief meewerken aan de internationale context.