Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

CONCEPT
Aan Brian Dommisse, Erwin Reinhoud
Werkgroep Edukoppeling
Edustandaard

memo

Afstemming Edukoppeling voor OAUTH

Directie
R&E

Afdeling
Dataoffice

Contactpersoon
Gerald Groot Roessink
Informatiearchitect

Datum
15-04-2024

Bijlagen
-

Beste Brian en Erwin,

Als reactie op het verzoek om namens DUO schriftelijk een standpunt in te nemen over het toepassen van OAUTH binnen Edukoppeling hierbij een memo met de intentie om dit te bespreken in de werkgroep Edukoppeling die staat gepland voor 22 april a.s..

DUO streeft na om voor wettelijke uitvoering in het onderwijs te werken met afspraken die zijn bekrachtigd in de Standaardisatieraad van Edustandaard en we zijn blij met de rond Edukoppeling gevormde community. Dat faciliteert in aanzienlijke mate de realisatie van wettelijke uitvoeringsregelingen. In de loop der tijd heeft de werkgroep Edukoppeling niet geaarzeld om na overleg een specifieke invulling te geven voor het onderwijs aan de pas-toe-of-leg-uit standaard Digikoppeling. Meermalen bleek Edukoppeling daarmee voorop te lopen op het origineel.

Het lijkt erop dat Edustandaard nu weer zo'n moment heeft dat Edukoppeling zelf een afweging moet maken. Nu is dat ingegeven door technologische ontwikkelingen op het gebied van toestemmingsverlening met OAUTH gecombineerd met de groeifondsen als business driver. In eerste instantie leek DUO geen belanghebbende, maar bleek dat gaande weg toch te zijn met het systeem Facet. Positie van DUO daarin, wij willen wel opschuiven naar OAUTH, op voorwaarde dat die versie is bekrachtigd door de Standaardisatieraad.

In de laatste werkgroep zijn een paar goede uitgangspunten gekozen:

- We volgen de API-strategie van het Kennisplatform API's
- We hanteren NL-GOV voor OAUTH, de werkversie[1]

Daarmee hebben we echter nog geen volledig werkzaam protocol voor Edukoppeling. Er zullen nog aanvullende afspraken nodig zijn. Een aantal daarvan zijn geïdentificeerd in het laatste werkgroepoverleg, maar keuzes zijn nog niet gemaakt. Daarvoor is een volgende werkgroep gepland.

Hieronder de inzet van DUO voor dat overleg:

1 mTLS of private-key-jwt

De keuze tussen deze twee is relevant op twee plekken:

1. Van client naar RS
   In NL-GOV staat dat proof-of-possession (POP) als geavanceerde security wordt ingezet om te voorkomen dat iemand een token steelt en gebruikt voor illegale dingen. Daarbij genoemd staan mTLS en private-key-jwt als opties. De rechtmatigheid kun je controleren. In het ene geval door de request (met token) te beveiligen met mTLS en in het andere geval doordat de requester het token met PKI (mede?) ondertekend.

   DUO: laat proof-of-possession maar even zitten tot het moment dat NL-GOV een conclusie trekt. De kans op een gestolen token achten we in de tussentijd klein als de geldigheidsduur wordt beperkt tot een kwartier.

2. Van client naar AS

   In paragraaf 2.3.3. van NL-GOV, werkversie en standaardversie, staat dat private_key_jwt verplicht is, MUST, ook voor direct access clients relevant in Edukoppeling. Dit kan nog veranderen ten gunste van mTLS of iets anders, maar hoe en wanneer weten we niet.

   DUO: Wij zien geen nadelen van private-key-jwt die het interessant maken om iets anders te introduceren. Daarom is het voorstel om de huidige tekst te volgen en niet zelf iets anders te verzinnen.

[1] De werkversie die op dit moment in ontwikkeling is, omdat in eerdere versie geen client credentials (2 legged of M2M) was opgenomen.

Anders gezegd, wij kunnen langere tijd uit te voeten met de huidige teksten in NL-GOV en wat DUO betreft verandert er op dit punt niks in de concept werkversie.

2 Hoe zit het met OSR

Bij OAUTH client credentials wordt het geven van toestemming niet expliciet voorgeschreven. Het moet er wel zijn, natuurlijk, maar niet dynamisch door de gebruiker verstrekt zoals uitgewerkt in OAUTH code grant.

Bij DUO zoekt voor deze vorm een mandaatverificatie die vergelijkbaar is met de huidige manier van werken. Deze manier van werken geeft zekerheid over de gegevensverantwoordelijke.

In het huidige Edukoppeling worden mandaten (leverancier x handelt voor school y inzake dienst z) beheert in het OSR. DUO gebruikt dat bijvoorbeeld bij Facet om al of niet toegang te verlenen. Vereenvoudigd gaat dat zo: leverancier x die een dienst aanroept is geïdentificeerd met PKI-overheid, in de berichtheader is school y vermeld in de from-parameter en DUO controleert bij de ontvangst in OSR of die combinatie bestaat voor dienst z.

Met OAUTH client credentials draait de verificatie min of meer om. Om hetzelfde niveau van beveiliging te halen kunnen we drie scenario’s volgen:

1. Leverancier x geeft bij AS aan dienst z voor school y te willen uitvoeren.
2. De AS meldt in de claim alle mandaten voor dienst z die leverancier x heeft ontvangen van scholen
3. De AS beperkt zich tot een algemene claim voor dienst z door leverancier x. De fijnmazige controle tot op schoolniveau wordt door de RS gedaan door uitvragen van de OSR.

In de handshake wordt expliciet gemaakt voor welke school een dienst wordt aangeroepen. Dit is wat DUO zoekt, maar we hebben er begrip voor dat dat niet altijd zinvol is. Bijvoorbeeld bij EDU-V zien we dat de uitwisseling tussen las en uitgever geen betrekking heeft op 1 school, maar op een groep scholen.

DUO: laten we uitzoeken of we beide smaken kunnen bedienen met optie 3.

3 PKI-overheid of iets anders

De Digikoppeling standaard hanteert verplicht PKI-overheid. Dat betreft door de overheid uitgegeven certificaten daarin (ssn-parameter) met een OIN als organisatie-id. Wat DUO betreft wijken we daar niet vanaf. Dat OIN is namelijk de identiteit in het mandaat van leverancier x en school y.

Enkele opmerkingen:

- De client die een PKI-overheidscertificaat nodig heeft is degene die fysiek een API-call uitvoert.
- Dit zijn bijvoorbeeld las-leveranciers in de cloud, uitgevers, DUO en SBB.
- In het algemeen zijn deze partijen te vinden in het NHR. Het OIN is daarop gebaseerd zoals gespecificeerd door Digikoppeling.
- Voor buitenlandse organisaties kun je PKI-overheid niet verplicht stellen. Een vergelijkbaar alternatief bij ons niet bekend.

Hiermee in lijn, DUO ziet niks in dynamic registration. Wij wisselen alleen uit met partijen die al kennen en afspraken mee hebben gemaakt.