MEMO

Aan: werkgroep Edukoppeling

Van: Gerald Groot Roessink

Datum: 2 september 2024

Betreft: Overwegingen DUO bij de introductie Edukoppeling OAuth-profiel

Er zijn goede redenen om OAuth 2.0 te introduceren in Edukoppeling. Het wordt wereldwijd gebruikt daar waar mensen toestemming geven om een resource te benaderen, binnen de Nederlandse overheid gaat het toegepast worden en in het onderwijs, in de Groeifondsprogramma's, zien we de eerste aanzetten tot implementatie. Frameworks die dit ondersteunen zijn goed beschikbaar. De OAuth standaard biedt verschillende profielen (grants/flows) die de basis kunnen vormen voor een toekomstvaste en breed inzetbare manier voor gegevensuitwisseling waar toestemming nodig is.

Er zijn diverse onderwijsketens met gegevensuitwisseling geclassificeerd met een hoge vertrouwelijkheid (typisch, persoonsgegevens). Edukoppeling bestaat als brede onderwijsafspraak daarvoor al zo'n 10 jaar, eerst met een WUS- en later ook een REST-variant. Voor toestemming door een school aan een leverancier is een 'eigen' oplossing gecreëerd, overigens na uitgebreide afstemming met de overheid (de Digikoppeling community). Ondertussen is besloten dat het WUS-profiel einde levenscyclus is, het wordt niet meer doorontwikkeld, en het zal als standaard zal worden uitgefaseerd. De resterende REST variant is relatief eenvoudig te implementeren en wordt bijvoorbeeld toegepast in Facet.

Een 'eigen' oplossing voor toestemming kan op termijn gaan afwijken van het gebruikelijke (inter)nationale standaarden. Met OAuth, nu opgenomen in het Nederlandse standaard profiel NL-GOV en indirect (bijna) in het nieuwe Digikoppeling REST profiel (waarin ook toestemming op basis van Federated Service Connectivity [1] contracten is opgenomen), is het opportuun om een nieuwe toekomstvaste Edukoppeling-variant uit te werken, voorlopig naast Edukoppeling-REST. De werkgroep Edukoppeling heeft dit eerder omarmd als een goed uitgangspunt voor de toekomst van Edukoppeling.

Het voornemen van de werkgroep Edukoppeling is dat de hiermee veranderende uitgangspunten, architectuurkaders en bouwblokken, nu vastgelegd in een Edukoppeling architectuurdocument, worden herzien en onderdeel worden van ROSA (ontwerpgebieden Technische interoperabiliteit en M2M). Een eerste versie van deze requirements is opgesteld door de voorzitter en de standaard-expert vanuit Edustandaard voor bespreking binnen de werkgroep.

In dit memo is uitgewerkt hoe DUO er tegenaan kijkt en wordt aangegeven hoe aan die requirements kan worden voldaan (onder het kopje Overwegingen):

[1] commonground.gitlab.io/standards/fsc/

1. Toestemming verlenen: Introductie van de term contract
   Edukoppeling heeft nu een specifieke oplossing voor het verlenen van toestemming nl. mandateren via een centraal mandateringsregister die nodig wordt geacht i.v.m. met het werken met LAS-leveranciers die gegevens uitwisselen namens een onderwijsorganisatie in een zogenoemde Software-as-a Service (SAAS) constructie.
   *Overweging:*
   Een contract is in de context van het onderwijs kan gezien worden als een overeenkomst over digitale ketensamenwerking tussen een of twee gegevensverantwoordelijken en gecontracteerde dienstverleners. Iets dergelijks wordt door VNG ontwikkeld onder de naam Federatieve Service Connectivity (https://vng.nl/projecten/federatieve-service-connectiviteit-fsc). Er zijn gevorderde plannen om dat in het Digikoppeling REST-profiel te introduceren in combinatie met het NL GOV OAuth-profiel of een specifieke Digikoppeling-afgeleide daarvan. Dat is een mechanisme waarmee op een vergelijkbare vorm van toestemming kan worden bereikt. Het is wenselijk om met Edukoppeling naadloos aan te sluiten op het nieuwe Digikoppeling REST profiel met FSC contracten en het NL GOV profiel. Of dit echt naadloos op elkaar aansluit of dat er wijzigingen op punten nodig zijn zou nog door de Edukoppeling werkgroep onderzocht moeten worden. Met het aansluiten op het nieuwe Digikoppeling REST profiel voldoet Edukoppeling ook op het niveau van toestemming aan een formaliteit, onderwijsinstellingen vallen volgens het Forum Standaardisatie onder de Digikoppeling-verplichting.

2. Ondertekenen van contracten
   Het sluiten van contracten in het kader van een uitwisseling met OAuth gaat er anders uitzien dan nu binnen Edukoppeling architectuur is beschreven. Alle contracterende partijen (bijv. onderwijsorganisaties) én hun gedelegeerde dienstverleners spelen daarin een rol.
   *Overweging:*
   FSC introduceert het digitaal ondertekenen van het contract door alle contractanten met een PKIO-certificaat. Dit kent speciale open source software, de contractmanager, die het ondertekenen regelt en het contract distribueert. Dat gaat in het onderwijs niet helemaal werken, omdat een onderwijsorganisatie juist geen PKIO-certificaat heeft, maar wel bijvoorbeeld een middel om in te loggen zoals E-herkenning. Er zijn meer van dit soort situaties. We verwachten dat deze manier van werken ook binnen FSC mogelijk wordt en voor alle voor partijen in het onderwijs soepel en zonder fouten kan verlopen.

3. Introductie van Autorisatie Server
   OAuth beschreven in de NL-GOV standaard, wordt veel toegepast in een 3-legged variant (authorization code grant). Hierbij geeft een mens (resource owner) toestemming in de betreffende oauth-flow. Bijvoorbeeld, iemand geeft toestemming de data van zijn google account te gebruiken voor Github. Maar binnen Edukoppeling gaat het om de 2-legged variant (client credentials) van OAuth. Toestemming moet er zijn, maar er is niet bepaald hoe die toestemming wordt gegevens. De AS kent het contract en levert op basis hiervan wel of niet het gevraagde access token.
   *Overweging:*
   Het OSR van Kennisnet fungeert binnen Edukoppeling ook als een Autorisatie Server avant la lettre. OAuth standaardiseert dit. Het mechanisme bestaat er uit dat een client eerst toestemming vraagt bij de Autorisatie Server en daarbij, indien positief, een access-token krijgt. De levensduur van dit Access Token is instelbaar en altijd tijdelijk. De Resource Server ontvangt het access-token van de client en vertrouwt op de Autorisatie Server met behulp van diens public key waarmee het access-token ondertekend is.

Behalve centraal ingericht zoals OSR kan de Autorisatie Server specifiek voor een gegevensuitwisseling worden ingericht, of bijvoorbeeld door de aanbieder van de resource zelf. Het kan dus op meerdere manieren worden ingericht.

4. Onomstotelijk vaststellen van de identiteit van partij die als client optreedt.
   Het OIN van de partij die als client optreedt moet onomstotelijk worden vastgesteld door de Autorisatie Server. Dit is beschreven in NL-GOV met de toepassing van PKIo certificaten. Dit gebeurt op twee momenten: bij de registratie van de client en bij het aanvragen van een Access Token. NL-GOV beschrijft daarbij twee varianten (private-key-jwt en mTLS). Een enkelvoudig en zo duurzaam mogelijke keuze daartussen is wenselijk voor de hele sector overheid en zelfs de hele (semi-)publieke sector.
   *Overweging:*
   De werkgroep Edukoppeling heeft in conclaaf met Edu-V een provisorische keuze gemaakt voor de private-key-jwt methode uit NL-GOV voor client authenticatie. Het was toen al bekend dat er ook een NL-GOV versie met mTLS zou komen, maar er was nog veel onbekend (bij DUO in elk geval). Ondertussen is er meer informatie beschikbaar en is het nodig om een meer diepgaande analyse te doen of beide varianten (private-key-jwt en mTLS) allebei gelijkwaardig zijn als het gaat om te voldoen aan de requirements die we gaan hanteren. Hierbij Als blijkt dat ze niet gelijkwaardig zijn dan zou DUO de voorlopige keuze van de werkgroep voor private-key-jwt willen heroverwegen.

5. Onomstotelijk vaststellen of de client gemandateerd (FSC gebruikt de term: gedelegeerd) is.
   De Autorisatie Server bepaalt of datgene wat de client wil, rechtmatig gebeurt op basis van een contract. Het contract moet bekend zij bij de Autorisatie Server.
   *Overweging:*
   Bijvoorbeeld, in FSC wordt het contract in gehashte vorm vermeld in het scope-veld van het /token endpoint. Als de autorisatieserver deze hash kan terugleiden tot een contract die bij de client hoort genereert de Autorisatie Server een Access Token waarmee toegang wordt verleend tot de Resource Server. Het Access Token kent standaard claim-attributen waarin de contractanten (met hun OIN) kunnen worden opgenomen. De FSC-standaard heeft deze attributen expliciet uitgewerkt.