MEMO

Aan: werkgroep Edukoppeling

Van: Gerald Groot Roesink, Dienst Uivoering Onderwijs

Datum: 28 oktober 2024

Betreft: Overzicht toestemming voor M2M

Inleiding

Op het gebied van toestemming voor beveiligde[1] M2M- uitwisselingen gebeurt veel in standaardisatiekringen. Het is lastig te overzien. Maar OAUTH is wel in opkomst, eerst in H2M en nu ook voor M2M, en wordt goed ondersteund in de markt. Daar zijn inmiddels twee profielen van bekend. En ook Edukoppeling heeft toestemming (met zogenaamde SAAS-leveranciers) het in het REST-profiel geregeld. Daarom zijn drie manieren om toestemming, ook wel mandatering en delegatie, te regelen naast elkaar te zetten.

- Edukoppeling-REST
- EDU-V
- Digikoppeling-FSC

Dit zijn eigenlijk geen standaarden maar bouwwerken van standaarden met als prominente standaard NL-GOV waarin is beschreven hoe om te gaan met OAUTH.

Kernmerken van deze bouwwerken werk zijn hieronder uitgewerkt langs de drie fasen van toestemming:

- Contractfase
- Aanvraag token
- Aanvraag resource

En daarna wordt voorlopig afgesloten met een paragraaf over overeenkomsten en verschillen.

[1] Het gaat in dit memo niet over uitwisselingen voor lichte vertrouwelijkheidsclassificaties omdat de urgentie ligt bij uitwisselingen over personen.

Edukoppeling-REST

Dit is de huidige manier van werken binnen Edukoppeling. Dit is een uitbreiding van Digikoppeling waarbij specifiek een oplossing is geformuleerd voor leveranciers in de cloud. Er wordt geen OAUTH gebruikt.

De koppeling is functioneel tussen twee gegevensverantwoordelijken, bijvoorbeeld een onderwijsaanbieder en DUO. In de praktijk maken onderwijsaanbieders meestal gebruik van een leverancier/gegevensverwerker die ook de technische koppeling doet. DUO daarentegen doet zelf de technische koppelng.

Contractfase.

Deelname aan een ketenafspraak krijgt vorm door een wettelijke regeling of door middel van een contractuele verbintenis. Als er sprake is van een leverancier, is er een gegevensverwerkingsovereenkomst en een certificeringsschema voor leveranciers.

Toestemmingsinformatie (zoals wie roept welke service aan namens wie) kan worden opgenomen in het centraal OSR-register en lokaal worden bewaard zodat de gateway van de verwerker de volgende stap kan doen.

Aanvraag Token/Resource

In de huidige Edukoppeling zijn toestemmingsvalidatie en opvraag van een resource gecombineerd. De gateway van DUO valideert de toestemming én levert. De aanvraag gebeurt met mTLS (meerzijdig TLS). Het is mogelijk om daarmee het publieke certificaat uit te lezen en OIN van de client kan daarmee onomstotelijk vastgesteld. Dit kan zonder publieke sleutel.

In Edukoppeling-REST geldt de afspraak dat de client in de from-parameter het OIN doorgeeft namens wie de uitwisseling, bijvoorbeeld een raadpleging of een melding, wordt geïnitieerd.

Andersom gebruikt DUO de to-parameter om door te geven voor welke OIN een uitwisseling (met name een bevestiging van verwerking is bedoeld. Dit is een kwaliteitscontrole voordat het de deur uitgaat.

Commentaar DUO: DUO wisselt ook regelmatig uit in Digikoppeling en streeft ernaar om Edukoppeling daaraan gelijk te houden. Overigens moeten onderwijsaanbieders dat formeel ook. Edukoppeling snelt soms vooruit, maar wel altijd in overleg.

EDU-V

EDU-V is een nationaal groeifonds dat de betrekking heeft op de “leermiddelenketen”. De toestemming tussen gegevensverantwoordelijken én verwerkingsverantwoordelijken wordt geregeld met OAUTH.

Contractfase.

In de context van EDU-V begint de contractfase bij de leveranciers. Zij worden deelnemers van de ketenafspraak EDU-V en regelen onderling een technische koppeling. Daartoe wisselen ze onderling informatie met elkaar uit:

- OIN en naw
- Gegevensdiensten (scope)
- Endpoints ketentest en productie.
- jwks-URI (waar het publieke certificaat staat)

De leverancier aan serverzijde bepaalt het client-id niet zijnde het OIN. Het resultaat is dat er technische tests uitgevoerd kunnen worden. Hierbij zijn geen gegevensverantwoorelijken (c.q. onderwijsaanbieders) betrokken.

EDU-V werkt met een expliciet ‘consent’. Een applicatiebeheerder van de onderwijsaanbieder activeert een uitwisseling tussen twee leveranciers. Dit wordt vastgelegd in een instantie van “Consentmanagement” en bij elke uitwisseling wordt gevalideerd of het geactiveerd is. Zie volgende.

Aanvraag Token

De Autorisatieserver wordt aangeboden door de dezelfde leverancier als de Resourceserver. De client ID is te vinden in de client_jwt_assertion. Als dit klopt met de clientregistratie uit de contractfase en de publieke PKIO, dan wordt een Access Token (bearer-token) geleverd.

EDU-V specifieert het niet nader, maar conform NL-GOV bevat de client_jwt_assertion standaard de volgende claims:

iss	the client ID of the client creating the token
sub	the client ID of the client creating the token
aud	the URL of the authorization server's token endpoint
iat	the time that the token was created by the client
exp	the expiration time, after which the token *MUST* be considered invalid
jti	a unique identifier generated by the client for this authentication. This identifier *MUST* contain at least 128 bits of entropy and *MUST NOT* be re-used by any subsequent authentication token

Het resulterende Access Token wordt niet nader beschreven in EDU-V. Aanname, dat bevat dezelfde attributen, maar dan ondertekend door de Autorization Server.

Aanvraag Resource

De client vraagt een resource aan bij de Resource Server. Als de ondertekening van het Access Token klopt, de geldigheid niet is verstreken (max. 1 uur) wordt de gegevensdienst geleverd.

In de http-gets en -posts wordt het organisatie ID (primair=OIN) van de betrokken onderwijsaanbieder doorgegeven in de requestbody. Het is mogelijk dat het Access Token binnen de termijn van een uur wordt gebruikt voor meerdere onderwijsaanbieders.

De Resource Server controleert of er daadwerkelijk mandaat/delegatie is afgegeven. Dat verloopt niet via attributen in het Access Token, maar in met aan aparte consent-API geleverd door de AS. Deze wordt aangeroepen voor dat de feitelijke uitwisseling plaats vindt.

Bevinding DUO:

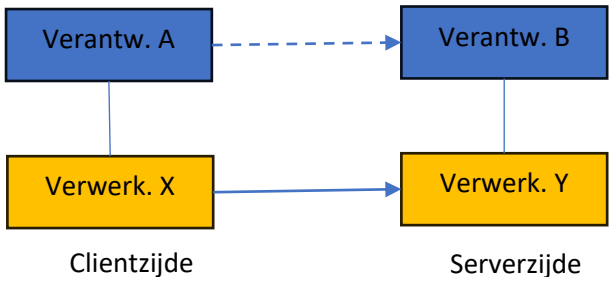
- De keuze voor private-key-jwt, in tegenstelling tot mTLS, betekent het beschikbaar maken van het publieke certificaat van de client. mTLS is eenvoudiger en misschien ook welk meer toekomstvast. DUO kan niet helemaal inschatten of het een blijvertje is in (inter)nationale ontwikkelingen. Maar kan er eventueel wel mee werken.

Digikoppeling met FSC

Federated Service Connectivity (FSC) is ontwikkeld door VNG voor standaardisatie in de gemeentewereld. Het is een oplossing voor in de cloud. Het concept is in aanleg Ests en algemeen en het voornemen van het overheidsprogramma GDI is om dit te integreren in Digikoppeling.

Contractfase.

In FSC worden contracten gesloten tussen peers die allen een 'contractmanager' hebben. Dit is als open source beschikbaar gemaakt. De eenvoudigste vorm is twee peers, één aan clientzijde en één aan serverzijde. Ze kunnen ook acteren namens (gedelegeerd/gemandateerd door) een andere peer. Elke peer accepteert zijn deel van het contract in de contractmanager en zendt dat naar de anderen ondertekend met zijn PKIO-certificaat in het mTLS-mechanisme.



Een grant beschrijft een interactie tussen peers en zijn onderdeel van een contract. FSC kent vier soorten:

- autorisatie om een service te publiceren (Y)
- autorisatie om een service te publiceren namens een ander (Y namens B)
- autorisatie om een service af te nemen (X)
- autorisatie om een service af te nemen namens een ander (X namens A)

Nota bene, omdat FSC tokens laat aanvragen met mTLS is er geen mechanisme nodig om het publieke certificaat te delen.

Aanvraag Token

De contractmanager is tevens de Autorisatie Server. Het heeft een /token endpoint (zie https://gitlab.com/commonground/standards/fsc/-/raw/master/manager.yaml) voor het afgeven van Access Tokens voor de onderliggende services/API's. Dit is door de peer die als client optreedt ondertekend met PKIO in het mTLS-mechanisme. Parameters in de aanvraag:

grant_type	"client_credentials"
Scope	The scope should contain the hash of the Grant that contains the authorization for a connection to a Service
client_id	The Peer ID of the connecting Peer

Aanvraag Resource

De resource wordt aangevraagd met een door de AS ondertekend Access Token. FSC heeft een uitgebreide claim gespecificeerd op basis van standaard en publieke attributen. Hierin zijn alle 'peers' opgenomen. Het Access Token van FSC:

Attribute	Meaning	Zijde	Wie
Gth	The hash of the Grant that serves as basis for the authorization		
Gid	The ID of the Group		
Sub	This should be the ID of the Peer for whom the token is intended	**CLIENT**	**OIN VAN GEGEVENSVERANTWOORDELIJKE A**
Iss	The ID of the Peer who issued the token. I.e. the Peer who is offering the Service	**SERVER**	**OIN VAN GEGEVENSVERWERKER Y**
Svc	Name of the Service		
Aud	The URI is a URL that ***MUST*** contain the scheme and port number used by the Inway		
Exp	Expiration time		
Nbf	Not before		
Cnf	The thumbprint of the certificate that is allowed ot use the access token		
act/sub	The ID of the Peer connecting to the Service on behalf of another Peer.	**CLIENT**	**OIN VAN GEGEVENSVERWERKER X**
Pdi	The ID of the Peer delegating the publication of the Service to another Peer	**SERVER**	**OIN VAN GEGEVENSVERANTWOORDELIJKE B**
Add	An object which can be used to provide additional data		

De Resource Server kan met deze info controleren dat de client, vaak namens een andere verwerkingverantwoordelijke, is geautoriseerd voor het benaderde endpoint. De dienstverlening is daarmee ingeperkt tot een specifieke onderwijsaanbieder.

Commentaar DUO:

- FSC in de huidige vorm gaat niet werken voor onderwijsaanbieders zonder PKIO. De makers van FSC erkennen dat ook. Er zijn meer situaties waarbij een gegevensverantwoordelijke geen PKIO heeft (maar wel een OIN). Daar willen ze graag met het onderwijs verder over nadenken.

Overeenkomsten en verschillen.

Overzicht van de ingrediënten op het gebied van identificatie, authenticatie en autorisatie (mandatering, delegatie) bij de drie beschreven raamwerken.

IAA -fase	Edukoppeling-REST	EDU-V best practice	Digikoppeling-FSC i.o.
Contractfase	administratief/OSR	administratief (w.o. jwks-uri)	mTLS voor /manager endpoints
Aanvraag OAUTH-token	-	private-key-jwt	mTLS voor /token endpoint
Aanvraag resource	mTLS (from/to)	Basis Access Token + (from/to) + Consent-API	Uitgebreid Access Token

Aandachtspunten

1. Gegevensverwerkers eerst
   Bij EDU-V en FSC leidt OAUTH tot een soort omkering van de inrichting. Waar Edukoppeling-REST begint met de functionele afspraak tussen twee verwerkingsverantwoordelijken (vaak onderwijsaanbieder die wettelijk moeten uitwisselen met DUO), begint het in EDU-V en FSC met de technische afspraak tussen twee gegevensverwerkers. Dit sluit aan bij de manier waarop OAUTH wordt ingezet in de H2M wereld. Enkele voorbeelden per keten.

Ketenafspraak	Verwerker X	Verwerker Y	Keteninstantie
Leermiddelenketen	Magister	Leermiddel nn	1
Leermiddelenketen	Magister	Somtoday	2
Digitaal examineren	Magister	Examenspeler nn	3
Digitaal examineren	Magister	Facet	4
Digitaal examineren	Parnassys	Examenspeler nn	5
Digitaal examineren	Parnassys	Facet	6
Registeren onderwijsresultaat	Magister	DUO	7
Registeren onderwijsresultaat	Parnassys	DUO	8
Overstapdossier	Magister	Parnassys	9

De gegevensverwerkers in de kolommen maken afspraken met elkaar en zorgen dat het technisch werkt. Dit is een keteninstantie. Daarna sluiten de onderwijsaanbieders zich bij één of meer keteninstanties[2] aan. In het geval van DUO vloeit dit voort uit een wettelijke verplichting van de onderwijsaanbieders.

2. Asynchrone transacties
   In veel gevallen zullen binnen keteninstanties uitwisselingspatronen voorkomen samengesteld uit meerdere API-calls. Hierbij kunnen de rollen van client en server omdraaien. Bijvoorbeeld het melden van een onderwijsresultaat bij DUO en de verwerkingsbevestiging terug of het aanmelden van kandidaten aan een examenspeler en het rapporteren van de resultaten terug aan het LAS.

   Relevant is daarom dat beide verwerkers moeten kunnen beschikken over de lijst met aangesloten onderwijsaanbieders. Bij FSC is dit geregeld door middels van verkeer tussen lokale contractmanagers van verwerkers en verantwoordelijken. In Edukoppeling-REST is het register RIO leidend omdat door de overheid erkende aanbieders wettelijke verplichtingen hebben rond ROD. In EDU-V ligt relevante toestemmingsinformatie altijd aan de serverzijde, maar wordt niet expliciet gemaakt hoe om te gaan met wisseling van zijde (@Koen: klopt da?)

3. Doorgifte gegevensverantwoordelijke
   De manier waarop verwerkingsverantwoordelijke wordt doorgegeven in de resource-aanvraag verschilt nogal.

   a. Bij Edukoppeling-REST zijn het queryparameters from en to, zodat de gateway van de verwerkers validaties kan doen zonder de payload te openen.:
      - Dat de client gemandateerd/gedelegeerd is door genoemde from-OIN (met name in OSR) om een endpoint te gebruiken.
      - Dat de server gemandateerd/gedelegeerd is om namens genoemde to-OIN het endpoint aan te bieden.
   b. Bij EDU-V geeft het Access Token alleen aan wat de (technische) client-id (niet OIN) is en verder is de gegevensverantwoordelijke (de onderwijsaanbieder) waar nodig in de payload vermeld van het requestbericht. De hierboven genoemde validaties gebeuren feitelijk op applicatieniveau. Daartoe is er een aparte consent-API in EDU-V ingericht.
   c. En bij FSC zijn de OIN's van alle peers opgenomen in het Access Token. De resource server kan daarmee in principe bij de ontvangst van een aanvraag de mandatering/delegatie valideren.

4. Access Token als in FSC

[2] Onderwijsaanbieders ook zelf een keteninstantie inrichten, bijvoorbeeld omdat het LAS on premise is.

Met een Access Token als in FSC wordt op een krachtige manier gebruik gemaakt van OAUTH. Maar dat lijkt er op neer kunnen komen dat elke aanvraag van een resource vooraf wordt gegaan door de aanvraag van een token. Als dat zo is, dan schiet het behoorlijk zijn doel voorbij. Vermoedelijk is dat de reden achter de consent-API van EDU-V (zie aandachtspunt 3). Hier zijn er ook twee calls achter elkaar (bij vertrouwelijksheids-classificatie midden/hoog) maar de truc is dat voor de consent-API de RS en AS vlak bij elkaar staan en beter kan performen.

Eigenlijk liggen EDU-V en Edukoppeling-REST helemaal niet zover uit elkaar als in eerste instantie lijkt. In feite gebeurt deze 'truc' in Edukoppeling-REST ook, in elk geval bij DUO, maar die is niet expliciet beschreven als onderdeel van de standaard.

5. Private-key-jwt of mTLS

Edukoppeling is gewend om met mTLS te werken en dat doet FSC ook. Dit heeft als voordeel dat het OIN van de verwerker aan client-zijde onomstotelijk vastgesteld kan worden zonder het publieke PKIO te kennen. Dat heeft daarom de voorkeur. Maar EDU-V werkt met private-key-jwt vermoedelijk omdat dat tot op heden gebruikelijk was in OAUTH-H2M. Het is niet goed in te schatten of private-key-jwt (inter)nationaal een blijvertje is voor M2M. Maar er kan eventueel wel mee gewerkt worden.

Voorgesteld vervolg

Scenario's voor de Edukoppeling standaard.