MEMO

Aan: werkgroep Edukoppeling

Van: Gerald Groot Roessink

Datum: 1 juli 2024

Betreft: Digikoppeling, FSC, NL-GOV

Binnen de overheid gebeuren op dit moment twee verschillende maar samenhangende ontwikkelingen op het gebied van Digikoppeling. Het een heeft te maken met een vernieuwingsvoorstel van VNG en het ander met het uitbreiden van NL-GOV. Hierover is nu twee keer gesproken in het technisch overleg (TO) van Digikoppeling en om de vergelijking te trekken met het onderwijs is nu twee keer overlegd door VNG, kennisplatform API’s, Kennisnet en DUO. De laatste keer op 29 juni 2024.

De stand van zaken:

1. FSC

Het technisch overleg (TO) van Digikoppeling heeft het voorstel geaccepteerd om FSC op te nemen in Digikoppeling. FSC staat voor Federated Service Connectivity en is ontwikkeld door VNG in combinatie met RINIS. Het bestaat uit drie onderdelen:

* Het sluiten van een (uitwisselings)contract tussen ketenpartners. Hierbij is nadrukkelijk rekening gehouden met delegatie. Dat komt overeen met wat we in Edukoppeling mandatering van SAAS leveranciers noemen. Het sluiten van een contract in FSC gebeurt in de backoffic met een serie van API’s. Een contract wordt met PKIO ondertekend door leverancier (de verwerker) én de gemeente (de gegevensverantwoordelijke).
* Om toestemming te verkrijgen hasht de client het uit te voeren contract en zendt dit naar het token-endpoint van de autorisatieserver. De client ondertekent dit met PKIO middels mTLS en als alles klopt ontvangt de client een access token met claimattributen over de details van het contract.
* Vervolgens wordt de resourceserver conform NL-GOV aangeroepen met dit access token. Het bezit van het token is voldoende om de resource te mogen benaderen[[1]](#footnote-2).

Deze vorm van FSC is voor het onderwijs geen werkbare oplossing is. Een belangrijk verschil is dat de onderwijsaanbieder, in tegenstelling tot een gemeente, niet een PKIO-certificaat heeft. Een medewerker van de onderwijsaanbieder geeft wel formeel akkoord door met een vertrouwd middel als E-herkenning in te loggen op een autorisatieportaal, mogelijk zelfs met OAUTH code grant.

Bij VNG erkennen ze dat dit een valide use case is, generieker dan het onderwijs ook. Het staat nu op de backlog om uit te werken als onderdeel van het opnemen van FSC in Digikoppeling.

1. NL-GOV

NL-GOV heeft recent een consultatieversie opgeleverd voor NL-GOV client credentials, met een specifieke uitbreiding voor backoffice verkeer. De kern van de wijziging is dat mTLS is opgenomen als optie om de identiteit van de direct access client vast te stellen. Dit is gedaan om FSC te faciliteren. De vorige versie van NL-GOV had alleen code grant met een met DigiD of E-herkenning geautoriseerde natuurlijke persoon en kende alleen private-key-jwt. Dat is een met PKIO ondertekende standaard claim, om de identiteit van de client vast te stellen.

Nu is mTLS niet per se een probleem in het onderwijs, want dat doen we nu ook bij Edukoppeling-WUS en -REST. Dat heeft wel restricties:

* mTLS werkt alleen bij point-to-point verbindingen. Het is misschien vermijdbaar, maar als er een hub in de keten zit werkt het niet.
* Internationale voorschriften (iGOV) kennen op dit moment alleen een private-key-jwt.
* Omdat het onderwijs werkt met een geautoriseerde vertegenwoordiger van de onderwijsaanbieder ligt private-key-jwt voor de hand.

Maar zoals ze benadrukken bij FSC, mTLS heeft ook een voordeel. Op deze manier wordt de client onweerlegbaar geïdentificeerd (het OIN) en kan direct worden gecontroleerd dat die beperkt tot zijn eigen contracten. In theorie althans kan de client met private-key-jwt ook een contract van een andere client proberen. Om dat te voorkomen moet de combinatie van OIN en public key op één of andere manier geverifieerd kunnen worden door de autorisatieserver.

Het contract van FSC bevat alle relevante informatie, onder meer namens wie het contract wordt uitgevoerd. Dit contract wordt opgenomen in het scope-attribuut van token-endpoint van de autorisatieserver. Queryparameters zoals in Edukoppeling-WUS en -REST zijn daardoor niet nodig. Echter, om hetzelfde te kunnen met private-key-jwt zou in NL-GOV in de claim voor de autorisatieserver ook een scope-attribuut moeten worden opgenomen. Dat zit er nu nog niet in. Een lopende consultatieopmerking is dat mTLS en private-key-jwt daardoor geen volwaardige alternatieven zijn.

Betrokkenen in beide overheidstrajecten is er veel aan gelegen om een generieke oplossing te formuleren die ook werkt voor het Nederlandse onderwijs. Ze zijn ook benieuwd naar de vorderingen van de werkgroep Edukoppeling en zouden daar verder aan willen werken. Ter verkenning van mogelijke samenwerking een paar vragen aan de werkgroep Edukoppeling:

* Zien we in de nieuwe versie van NL-GOV reden om het eerder door de werkgroep ingenomen uitgangspunt private-key-jwt te wijzigen naar mTLS?
* Zo nee:
  + zullen we toch qua systematiek aansluiten bij FSC door de grant hash van het contract te vermelden in de claim van private-key-jwt en onderdeel te laten zijn van NL-GOV?
  + vinden we het dan nodig om ten behoeve van validatie de combinatie van OIN en public key beschikbaar te hebben en hoe dan?
* Zo ja:
  + Wat betekent dit voor Edu-v, Npulse en anderen?
* Zien we er heil in op het niveau van Digikoppeling een generieke werkwijze uit te werken om een uitwisselingscontract op te stellen en te ondertekenen, met dien verstande dat gegevensverantwoordelijken zoals onderwijsaanbieders niet worden verplicht tot PKIO.

En tenslotte, zullen we als werkgroep Edukoppeling NL-GOV en FSC uitnodigen voor een volgende bijeenkomst?

1. NL-GOV oppert de mogelijkheid om het rechtmatig bezit van het token te controleren maar dat is optioneel. [↑](#footnote-ref-2)