Beste Brian en Erwin,

Zoals afgesproken in de vorige werkgroep Edukoppeling zouden we een achterbanraadpleging doen in de Architectenraad Edu-V en ook bij Topicus. Dit heeft geleid tot de volgende input voor de volgende werkgroep:

We zien mogelijkheden om expliciete keuzes en implicaties helder te maken in het NL GOV profiel:

1. Het NL GOV development profiel heeft alleen de Private Key JWT variant uitgewerkt. mTLS wordt niet genoemd. Wat ons betreft is mTLS dan ook niet meer nodig. Topicus heeft hier nog naar gekeken en geeft het volgende mee:
    a. Voorkeur te hebben voor de Private Key JWT.
    b. mTLS zit nog niet in het profiel en heeft niet de voorkeur omdat de gegevens over de client dan uit het client certificaat gehaald moeten worden. Met Private Key JWT houdt je dit netjes gescheiden.
    c. Het is mogelijk om beiden te ondersteunen als Client. Als autorisatieserver is dit niet wenselijk omdat dit kan leiden tot conflicten in de operatie. Bijvoorbeeld toepassing van beiden. Via het discovery endpoint kan een Client opvragen wat een autorisatieserver ondersteunt.
2. In het NL GOV profiel is het Client Credentials profiel nog niet volledig uitgewerkt. Vooral het voorbeeld van de grant_type is niet conform client_credentials en ook iedere autorisatieserver moet authorization_code ondersteunen. Dat is niet strikt noodzakelijk bij een autorisatieserver die alleen operationeel is voor Direct Access Clients.
3. Dynamic registration wordt genoemd als optie. We stellen voor om dit niet toe te passen.
4. De levensduur van een token is maximaal 6 uur. We denken dat dit te lang is en stellen voor om dit verder in te perken naar 1 uur.
5. Het profiel geeft aan dat het PKI certificaat verplicht is in een situatie waarbij de Client en de Resourceserver van een andere organiastie zijn. Dat is altijd het geval bij een ketensamenwerking. Dus dit betekent dat PKI ook verplicht wordt.

Binnen Edu-V hebben we de pagina's over M2M gegevensuitwisselingen inmiddels aangepast. De verwijzing naar het ingetrokkken Edukoppeling Secure API Oauth profiel is verwijderd. Bovenstaande keuzes op NL GOV zijn hier ook expliciet gemaakt:

https://edu-v.atlassian.net/wiki/spaces/AFSPRAKENS/pages/10846209/M2M+identificatie+authenticatie+en+autorisatie

Mochten jullie vragen hebben over deze input dan weten jullie me te vinden 😊.

Met vriendelijke groet,

Koen Voermans
+31 6 45 79 07 66