Voorstel aanpak REST OAuth2 profielen

Datum: Juni 2025 (bijgewerkt nav expertgroepoverleg 19-08-2025

Afkomstig van: Kerngroep techniek OKE

Betreft: Use-cases en stappenplan voor gebruik van verschillende OAuth2 profielen bij het gebruik van REST.

Onderliggend aan de OAuth profielen zien we de volgende uitgangspunten.

1. Token request en berichtenverkeer gaat altijd over een beveiligde verbinding. Momenteel is de minimale eis daarvoor TLS1.3. Er moet periodiek gevalideerd worden of de minimaal voorgeschreven standaard voor de verbindingslaag nog voldoet. Voorstel is om hierbij de TLS richtlijnen van NCSC te volgen.
2. Voor de verschillende authenticatieprofielen wordt altijd een industry standard implementatie van OAuth2 gekozen. Dit om te voorkomen dat er voor nieuwe/kleine partijen integratiedrempels worden opgeworpen.
3. Partijen/samenwerkingsverbanden zijn vrij in het bepalen van te gebruiken scopes en de validatie daarop zolang deze scopes passen binnen OAuth2.
4. Mtls maakt geen onderdeel uit van het voorstel. Partijen kunnen naast de standaard wel naar eigen inzicht mtls toepassen zolang dit het toepassen van de standaard niet in de weg zit.
5. De autorisatie server zal de check doen of de uitwisseling plaats mag vinden bij het uitdelen van het token. Voor de client is verkrijgen van een token de indicatie dat credentials en mandaat gecontroleerd zijn. Wel kan de server bij gegevensuitwisseling een extra controle uitvoeren of gegevens die opgevraagd worden ook daadwerkelijk verstrekt mogen worden.
6. De partij die een token uitreikt bepaalt of een extra/step-up vereist is als onderdeel van de authenticatie.
   Dit kan ertoe leiden dat er bij gegevensuitwisseling tussen partijen die beide in verschillende flows tokens verstrekken verschillen ontstaan in authenticatieniveau. Dit verschil accepteren we omdat elke partij zelf verantwoordelijk is voor het bepalen van authenticatieniveaus van koppelingen.
7. We scheiden de protocol laag van de beheerlaag. Het REST OAuth2 best practise gaat over protocol. De beheerlaag zoals die onder andere bij EDU-V toegepast wordt valt onder de verantwoordelijkheid van een samenwerkingsverband.

Voor de verschillende OAuth2 profielen gaan we uit van een basisprofiel en twee profielen met ieder een zwaardere beveiligingslaag. Uitgangspunt hierbij is dat het basisprofiel in de meeste situaties voldoet en dat waar nodig tussen partijen (leveranciers/onderwijsinstellingen/samenwerkingsverbanden) gekozen kan worden voor één van de step up profielen. Hierbij moeten de profielen wel logisch oplopen in zwaarte van authenticatie.

Door voor dit model te kiezen bieden we een toekomstpad waarbij uitgegaan wordt van het ondersteunen van het het binnen OKE al toegepast Basisprofiel waarna een van de twee

Met opmerkingen [PL1]: Toevoegen principe/uitgangspunt: Scheiden van protocollaag en beheerlaag - hier hebben we het over protocollaag.

Met opmerkingen [PL2R1]: Dit betekent ook dat je de industrie-standaard X.509 volgt, en dat het een beheervraag is welke trust root (bijv. PKIo) je toelaat.

Met opmerkingen [PL3]: Best practice is het volgen van de TLS richtlijnen van NCSC (actuele versie: TLS-Richtlijnen-2025-05.pdf)

Met opmerkingen [GG4]: Wat DUO betreft is dit een goed uitgangspunt en we realiseren ons dat de FSC oplossing die eerder door ons is voorgesteld, afvalt. Dit voorstel werd gedaan om net als in het huidige vanuit het huidige Edukoppeling alleen partijen op het interne netwerk toe te laten met een geverifieerd mandaat. Maar dat principe blijft. Daarom stellen we voor te bewegen naar rfc 8693 dat is de industriestandaard voor token-delegation. Zie ons andere document.

Met opmerkingen [PL5]: Is het niet omgekeerd? Want er zijn heel erg goede redenen om zeker bij system-to-system wél mTLS toe te passen. Of je het wel of niet toepast is niet 'vrijblijvend', maar de uitkomst van een risicoanalyse voor de desbetreffende koppeling.

Met opmerkingen [GG6R5]: Eens. Het risico bijvoorbeeld dat iemand anders bij DUO de toegang claimt die is voorbehouden aan Magister,

verzwaringsprofielen beschreven en toegepast kan worden, zonder daarbij de weg af te sluiten naar het andere verzwaringsprofiel

De verschillende profielen worden hieronder kort toegelicht:

Basisprofiel (OAuth2 client credentials)

Dit profiel is de standaard OAuth2 client credentials flow met gebruikmaking van een client secret (zoals nu in gebruik bij OKE)

Verzwaring 1 (client credentials met signed private-key-jwt i.p.v. secret)

Dit authenticatieprofiel dat ook door EDU-V wordt gebruikt kan toegepast worden in situaties dat zowel de aanvrager (de onderwijsinstelling) als de partij die technisch de koppeling verzorgt (leverancier) geïdentificeerd moeten worden.

Aandachtspunten hierbij zijn:

- Applicatie in gebruik door een organisatie wordt geïdentificeerd door client credential en private-key-jwt.
- Leverancier signed binnen de NL-context het private-key-jwt met het eigen pki overheidcertificaat)
- Partijen kunnen op basis van de informatie die is meegegeven bij de token aanvraag eigen autorisatie/mandateringsfunctionaliteiten aanbieden (zoals EDU-V nu al doet bijvoorbeeld) zolang de authenticatie door de tokenserver in overeenstemming met de standaard plaatsvindt.
- In OAuth2 termen moet deze step up voor de tokenserver duidelijk herkenbaar zijn als een andere flow dan het basisprofiel.
- Het heeft de voorkeur om partijen in het onderwijsveld die al een eigen implementatie hebben waarin zowel onderwijsinstelling als de leverancier bij de authenticatie een rol spelen overstappen op dit profiel.

Verzwaring 2 (OAuth conform RFC 8693)

Voorstel van DUO om met dit profiel RFC 8693: OAuth 2.0 Token Exchange het eerder voorgestelde FSC profiel te vervangen. Er zijn nog genoeg vragen over de attributen en gedrag van de auth server om in detail uit te werken. Ook de vragen rond welke attributen bij de aanvraag moeten zijn en meegegeven in het nieuwe token. Hiervoor verwachten we een concreter voorstel vanuit DUO die de volgende dingen bevat: voortborduren op de verzwaring 1, toevoegen welke partij het bericht stuurt en namens wie dit gebeurd. (het 4 partijen plaatje) . En zie uitgangspunt 6

Vervolgstappen binnen EDUkoppeling

We stellen voor om eerst het verzwaringsprofiel 1 profiel uit te werken. Ook omdat daar al ervaring vanuit EDU-V mee is. Daarnaast is dit profiel vereist voor situaties waarin zowel onderwijsinstelling als leverancier geauthentiseerd moeten worden.

Daarnaast kan verzwaringsprofiel 2 verder uitgewerkt en gespecifieerd worden. Dit kan in het kader van OKE voor de uitwisseling van gegevens tussen Facet en leveranciers als Topicus en Paragin.

Met opmerkingen [PL7]: Let op dat er twee partijen zijn die zich kunnen/moeten authenticeren: de partij die de verbinding opzet resp. de persoon die achter de verbinding zit. 'Step up' wordt vooral met de laaatste geassocieerd.

Met opmerkingen [KG8]: onderwijs instelling vervangen door applicatie van de leverancier. Dit kan per school een andere applicatie zijn

Met opmerkingen [PB9]: client credential bestaat (bij Edu-V) alleen uit een client-id. de client is namelijk een direct access client, dwz. het systeem van de leverancier dat door de school is gemandateerd bij registratie.

Met opmerkingen [PL10]: Of ander x509-certificaat mits in een door beide partijen vertrouwde root?

Met opmerkingen [PL11]: (dit is conform best practice OOAPI 6)

Met opmerkingen [PB12]: authenticatie en autorisatie vindt (bij edu-v) plaats op de koppeling. autorisatie zit in de token in de hoedanigheid van scopes. mandatering (consent bij Edu-V) gebeurd op de inhoud, nl. aan de hand van identifiers in het bericht.

Met opmerkingen [PL13]: Step-up 2 (volgens FSC) vereist een contract? Kun je/wil je dan verder gaan dan 'er is een geldig contract' of 'ik zie dat het contract is opgesteld door een vertrouwde partij'? Hoe het contract is gevuld, met de juiste attributen is 'out of band' voor de transport/berichtlaag.?

Onderdeel van dit proces zou ook een richtlijn kunnen zijn voor partijen waarin voorgeschreven wordt bij welke berichtinhoud welk profiel voldoet. Dit bijvoorbeeld voor bijzondere persoonsgegevens en/of het delen van informatie met andere juridische entiteiten.

Vervolgstappen rond EDUKoppeling

Partijen en/of samenwerkingsverbanden kunnen rond de authenticatieprofielen bijvoorbeeld:

- Authorisatieprofielen definiëren (EDU-V)
- (Centrale) registraties van mandateringen (PO/VO)
- Richtlijnen voor gebruik verschillende profielen (bv SBB BPV-API voor al dan niet mogen ophalen contactpersonen bij leerbedrijven)