edustandaard

# Verslag Edustandaard werkgroep Edukoppeling

Aanwezig: Patrick van der Veer (SURF), Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)
Gastleden: H.P. Köhler (Edu-V), Piter Blom (Edu-V)
Afwezig
Agendalid: Ernst-Jan van Heuseveldt (Rovict/VDOD), Joël de Bruin (MBO Digitaal)

**Datum en locatie**
6 november, 10:00-12:30 uur
Locatie: Bar Beton, Perron 4/5, Amersfoort CS

Agenda:

1. Opening / mededelingen / Verslag van 3 oktober 2024
2. RFC Edu-V:
    a. RFC toelichten (door Edu-V)
    b. Beoordelen voorgestelde aanpassingen in de OAuth Best Practice (conceptversie 1.1) op basis van die RFC
3. Mogelijke issue met PKIoverheid certs op een intermediair/hub (Edwin)
4. Vergelijking toekstemmingsvarianten (nav actiepunt #132: Voorstel tav de toestemmingsclaim in het access token) (Gerald)
5. wvttk

## 1. Opening, mededelingen en verslag van 3 oktober 2024

- Maarten Kok (SBB) meldt dat een dienstverlener bezwaar maakt op het gebruik van PKIo omdat zij in de door hun gekozen inrichting deze niet kunnen toepassen. Zij gebruiken Microsoft Dynamics 365 (cloud deployment) en deze staat niet toe om een PKIo hiërarchie in de truststore op te nemen. Piter Blom (Edu-V) geeft aan dat er bij Logius voorzieningen zijn die bij Digikoppeling implementaties op de transportlaag (TLS) ook geen PKIo toepassen. Er wordt met ondertekening van payload gewerkt met toepassing van een PKIo-certificaat. Er wordt besloten dat Maarten een memo opstelt en daarin de use case beschrijft. We zullen deze vervolgens met Logius (beheer Digikoppeling) delen omdat we verwachten dat deze problematiek dus ook bij Digikoppeling speelt. Zelf zien we voor de korte termijn hiervoor geen oplossing.

- Itt wat in de agenda staat heeft Hans Swart namens MBO Digitaal aangegeven dat zij voor de werkgroep Edukoppeling Patrick Doomen (SURF) zullen gaan afvaardigen. Patrick is betrokken bij de implementatie van OKE en kan inschatten welke implicaties de keuzes die we in de werkgroep gezamenlijk willen maken kunnen hebben op OKE-uitwisselingen. Deze werkgroepbijeenkomst lukte het nog niet om aan te schuiven.

- Het verslag van de vorige bijeenkomst wordt zonder wijzigingen vastgesteld

## 2. RFC Edu-V

### 2.1. RFC toelichten (door Edu-V) en beoordelen voorgestelde aanpassingen in de OAuth Best Practice versie 1.1

Er wordt besloten om agendapunten 2a en 2b gecombineerd te bespreken. Piter geeft per RFC een toelichting en er wordt gelijk ook besloten of deze adequaat is verwerkt in de OAuth Best Practice.

**RFC008 Het client_id identificeert een referentiecomponent en niet een organisatie.**
NL GOV (en de Edukoppeling OAuth Best Practice v1.0) schrijven niet voor waarmee een Authorization Server (AS) een client_id moet vullen bij registratie van een client. Er wordt dus niet gesteld dat deze met een OIN moet worden gevuld, maar in de Edu-V RFC komt de aanscherping dat het gebruik van een OIN niet de voorkeur heeft. Op de Edu-V site zijn de RFC's verwerkt en deze zijn zoveel mogelijk overgenomen in de Edukoppeling OAuth Best Practices. Deze teksten konden niet 1-op-1 overgenomen worden omdat de structuur van de Edu-V site niet overeenkomt met die van NL GOV OAuth. De Edukoppeling Best Practices zijn gebaseerd op de structuur van het NL GOV Oauth-profiel

Op de Edu-V site staat hierover het volgende:

- *MUST Client registration met een unieke client_id voor iedere applicatie.*
  - *MUST De client_id wordt bepaald door de leverancier die de autorisatieserver aanbiedt.*
  - *SHOULD NOT client_id is bij voorkeur niet gelijk aan het OIN. Het OIN wordt gehanteerd om de organisatie vast te stellen. Het client_id is gericht op de identificatie en de authenticatie van de applicatie van de leverancier.*

Deze tekst is in de Edukoppeling OAuth Best Practices met name aangepast bij de paragraaf '3.1.3. Client Registration'.

Er wordt nog gevraagd of het gebruik van de Logius Centrale OIN Raadpleegvoorziening (COR) vereist moet worden. Hiermee zou er een centrale voorziening binnen het Edu-V stelsel gebruikt worden. Daarnaast vraagt men zich af wat toegevoegde waarde zou zijn en of Logius een dergelijk gebruik wenselijk vindt. Het OIN wordt al geverifieerd bij opname in een PKIo certificaat. Wel is onduidelijk of PKIo actief (basis)registers bevraagt om eventueel certificaten in te trekken als het OIN hoofdnummer niet meer actief/ingetrokken is. We verwachten dat dit laatste niet het geval is. Een CA is wel in staat om bij bepaalde omstandigheden een certificaat in te trekken. Welke dit zijn weten we niet. Over het algemeen is degene die het certificaat heeft aangevraagd tekeningsbevoegd (geweest) en verantwoordelijk voor het intrekken van het certificaat. Er wordt besloten om het gebruik van COR niet verplicht te stellen.

**RFC009 (registratie client jwks_uri), RFC010 (registratie client public key) & RFC011 (PKIo certificaten dienen alleen gebruikt te worden door clients).**
Bij Edu-V wordt verwacht dat er tientallen tot misschien wel honderd clients per Authorization Server gemanaged gaan worden. RFC009 stelt het gebruik van een jwks_uri verplicht (MUST, niet aanbevolen). Met de private_key_jwt authenticatiemethode moet verder een publieke sleutel gebruikt worden om de ondertekening te verifiëren. Het was nog niet duidelijk hoe de AS over de publieke sleutel kan beschikken. RFC010 stelt de JWK set (en hiermee de locatie van publieke sleutel) bij registratie wordt vastgelegd. Zoals RFC009 aangeeft MOET hiervoor een jwks_uri vastgelegd worden. Bij de private_key_jwt methode wordt de toepassing van een PKIo certificaat verplicht gesteld. Het OIN in het certificaat is bedoeld om de organisatie (rechtspersoon) van client te identificeren, niet om een client zelf

te identificeren. RFC011 stelt dat de client een eigen identifier heeft en wordt geauthentiseerd met de private_key_jwt.

Op de Edu-V site staat hierover het volgende:

- *MUST De Client beschikt over een PKIoverheid certificaat met Client keys bestaande uit een publieke en een private key.*
- *MUST De publieke key wordt door de Client beschikbaar gesteld middels een jwks_uri.*
    - *De private key wordt door de Client gehanteerd om in de private_key_jwt flow de Client_jwt te signeren.*
    - *De autorisatieserver kan met de publieke key vervolgens de Client_jwt ontcijferen. De publieke key verkrijgt de autorisatieserver via de jwks_uri.*

En bij Laag 2 – Registratie staat het volgende:

*Leveranciers delen de noodzakelijke gegevens met elkaar:*

- *Leverancier A die met Applicatie A wil koppelen aan Applicatie B van Leverancier B deelt de volgende informatie:*
    - *MUST Naam van Applicatie A*
    - *SHOULD Omschrijving van Applicatie A*
    - *COULD Icon van Applicatie A om te tonen in de Consent UI van Leverancier B.*
    - *MUST Gewenste scopes*
    - *MUST Naam van leverancier A*
    - *MUST OIN van leverancier A*
    - *MUST wks_uri van leverancier A*

- *Leverancier B deelt de volgende informatie met Leverancier A:*
    - *MUST Naam van Applicatie A*
    - *SHOULD Omschrijving van Applicatie A*
    - *COULD Icon van Applicatie A om te tonen in de Consent UI van Leverancier B.*
    - *SHOULD Acceptatieomgeving (endpoints voor testdoeleinden)*
    - *MUST Productieomgeving (endpoints)*
    - *SHOULD Technische documentatie*
    - *MUST Client credentials voor M2M identificatie, authenticatie en autorisatie*
        - client_id per applicatie
            - De client_id wordt bepaald door Leverancier B.
            - SHOULD NOT client_id is bij voorkeur niet gelijk aan het OIN. Het OIN wordt gehanteerd om de organisatie vast te stellen. Het client_id is gericht op de identificatie en de authenticatie van de applicatie van de leverancier.
        - Scopes per client_id

Deze tekst is niet volledig overgenomen in de Edukoppeling OAuth Best Practices. In de conceptversie OAuth Best Practices zijn delen overgenomen die volgens de opsteller het beste passen binnen de bredere context[1] van Edukoppeling en de kern van de RFC's vormen. Verder is de Edu-V structuur niet net als bij de Edukoppeling OAuth Best Practice conform het NL GOV OAuth profiel. In huidige situatie zal er waarschijnlijk niet naar de

[1] Onder andere het vereisen van de naam van de applicatie en het toepassen van scopes is aan de betreffende ketensamenwerking dat Edukoppeling OAuth Best Practices wil toepassen om dat in het eigen afsprakenstelsel nader te specificeren.

Edukoppeling OAuth Best Practices gekeken worden maar alleen naar de Edu-V teksten. Deze geven een volledig beeld van Edu-V eisen voor een implementatie.

**RFC012 (stel Kennisplatform API Design Rules niet verplicht)**
Deze RFC is niet door Edu-V geaccepteerd en wordt dus ook niet in de Edukoppeling Best Practices verwerkt.

**RFC013 (sta toepassing van Discovery toe)**
Discovery heeft toegevoegde waarde om (endpoint) metadata uit te wisselen. Het kan ook door clients gebruikt worden om o.a. het token endpoint op te halen.

Op de Edu-V site staat hierover het volgende:

- *COULD Het aanbieden van de discovery endpoints issuer, token_endpoint en jwks_uri. Het authorization_endpoint is niet verplicht. Ook op dit punt wijken we af van de specificatie.*

Het uitsluiten (MUST NOT) van Discovery is eerder op verzoek van Edu-V in de Edukoppeling OAuth Best Practice opgenomen. Dit uitsluiten is nu verwijderd. Het is nu conform Edu-V toegestaan (COULD). Het authorization_endpoint was per definitie niet relevant omdat het een client credentials grant betreft.

**RFC014 (toepassing van mTLS uitsluiten)**
De huidige specificatie is onduidelijkheid over toepassing mTLS.

Deze RFC is niet in de Edu-V specificatie overgenomen en dus ook niet verder verwerkt in de Edukoppeling OAuth Best Practices. mTLS zou dus toegepast kunnen worden, maar niet ten behoeve van authenticatie van client. Voor dit laatste moet private_key_jwt toegepast worden.

**Overige besproken (open)punten**
Bij Edu-V is er discussie rond toepassing van PKIoverheid certificaten op RS en AS. Edu-V heeft nu op confluence duidelijk aangegeven dat toepassing van PKIo door client vereist wordt. Dat is nu overgenomen in Edukoppeling OAuth Best Practices v1.1.
Wat nog niet is overgenomen is de toepassing van PKIo bij RS en AS. In Edu-V RFC011 staat “PKIo certificaten dienen alleen gebruikt te worden door clients, niet door de Resource Server of Authorization Server. RS en AS hebben een onderlinge trust door middel van inrichting van een authority uri.” Naast de TLS verbinding kan de AS dus ook voor een Access Token een eigen (niet PKIo) certificaat gebruiken. Bij het Access Token gaat het om vertrouwen tussen AS en RS wat een interne vertrouwensrelatie beschouwd kan worden. De relatie tussen de client en AS/RS is dat echter niet. Het niet toepassen van PKIo bij de AS en RS is nog niet overgenomen in de Edukoppeling OAuth Best Practices. Vanuit NL GOV OAuth[2]/EK OAuth Best Practices wordt aangenomen dat PKIo voor alle partijen van toepassing is. Dit is ook waar DUO de voorkeur aan geeft. Hiermee is het wel of niet toepassen van PKIo op AS en RS nog een open punt. Dit punt zal ook nog bij de NL GOV OAuth werkgroep aangekaart worden.

[2] NL GOV stelt bij paragraaf 2.3.4 Client Keys: “In case the Authorization Server, Resource Server and client are not operated under responsibility of the same organisation, each party MUST use PKIoverheid certificates with OIN.”

2.2. Beoordelen voorgestelde aanpassingen in de OAuth Best Practice (conceptversie 1.1)
Zie vorig agendapunt.

2.3. Mogelijke issue met PKIoverheid certs op een intermediair/hub (Edwin Verwoerd)

Edwin heeft het eerder gehad over een PKIo vraagstuk dat speelt bij een Hub/intermediair in de Edu-V context. Bij de use case gaat het om verschillende uitwisselingen tussen verschillende partijen. De intermediair ontvangt uit een bepaald proces gegevens en levert deze weer door als onderdeel van een ander proces. Hierbij gaat het dus om een niet-transparante intermediair. De intermediair kan dus als een op zichzelf staande partij gezien worden waarvoor dezelfde kaders gelden als bij een point-2-point uitwisseling tussen partijen. Als de partijen in de rol van verwerker de uitwisseling uitvoeren namens een verwerkingsverantwoordelijke geldt dat hierbij dus ook toestemming geregeld moet zijn.

Besloten wordt dat deze use case past binnen de bestaande en nieuwe architectuur en (vooralsnog) niet specifieke aandacht behoeft.

## 3. Vergelijking toekstemmingsvarianten (Gerald)

Wordt volgende keer besproken.

## 4. Wvvtk

Er waren verder geen mededelingen.
De volgende werkgroep is op 4 december 2024, 10-12:30 (met mogelijke uitloop naar 13:00)

Acties

| # | Omschrijving | Status | Eind datum | Actie-houder | Prio |
|---|---|---|---|---|---|
| 94 | Kan de huidige OIN methodiek o.b.v. instellingscode (aka BRIN4) uitgebreid worden met een identiteit van een onderwijsaanbieder zoals nu in RIO is opgenomen? | Voorlopig geen actie tot behoefte beter kenbaar wordt. Dit wordt in Architectuur versie 3.0 verder uitgewerkt | Q4 2024 | BES | 2 |
| 110 | Architectuurraad informeren dat er nu tussen XML en JSON een onderscheid gemaakt kan worden in kwaliteit/ betrouwbaarheid. Het is wenselijk dat (met aanvullende voorschriften) XML en JSON een vergelijkbare kwaliteit/ betrouwbaarheid hebben. Deze moeten dan ook wel nageleefd (kunnen) worden. | Probleemstelling indienen bij AR, vraag is of dit nog speelt | Open | Edwin | 2 |
| 120 | Documentatie ter ondersteuning van REST profiel | Open, in eerste instantie onderdeel versie 3.0 architectuur. Daarna bepalen of meer nodig is. | Q4 2024 | BES | 2 |
| 125 | Werkingsgebied Edukoppeling profielen, keuzes aan AR voorleggen:<br>• G2G irt B2B, en wat verstaan we daaronder.<br>• Koppelingen vanuit NL onderwijs met internationale/ Europese partijen of niet? | Notitie voor AR opstellen | Q4 2024 | Brian | 2 |
| 130 | Edukoppeling FAQ uitbreiden met vragen uit de Edu-V keten en de antwoorden vanuit NL GOV/EK WG | Loopt | | BES | 2 |
| 132 | Voorstel tav de toestemmingsclaim in het access token | Voor werkgroep 6 november ingebracht, wordt op 4 december besproken | Afgerond | Gerald | 1 |

Bureau Edustandaard = BES / Grijs = afgehandeld of vervallen

Besluiten

| # | Omschrijving | datum |
|---|---|---|
| 15 | De werkgroep trekt de huidige Edukoppeling conceptversie (juli 2023) van de Secure API OAuth Client Credentials profielen v0.8 (concept) terug. De publicatie van deze versie op Edustandaard gaat hiermee vervallen. | 18-3-2024 |
| 16 | De volgende uitgangspunten zijn door de werkgroep bekrachtigd voor de uitwerking van de architectuur en als basis voor het OAuth-profiel:<br>Uitgangspunt 1: De API strategie van het Kennisplatform API's de primaire "driver" voor de doorontwikkeling van de Edukoppeling architectuur versie 3.0<br>Uitgangspunt 2: Edukoppeling maakt gebruik van de producten van de API strategie. Concreet hebben we het dan over:<br>• gebruikmaken van de betreffende Architectuur,<br>• gebruikmaken van het NL GOV OAuth profiel,<br>• gebruikmaken van de API Design Rules.<br>Uitgangspunt 4: Het bestaande Edukoppeling Secure API REST profiel wordt fully conformant aan de API Design Rules. Bij voorkeur blijven we aansluiten op Digikoppeling door het Edukoppeling Secure API REST profiel te baseren op de Digikoppeling Koppelvlakstandaard REST-API[3] die ondertussen beschikbaar is gekomen met hierin de nieuwe versie van de API Design Rules. We verwachten echter dat het Digikoppeling Koppelvlakstandaard REST-API profiel op termijn mogelijk migreert waarbij ook (delen) van het NL GOV OAuth profiel van toepassing zal zijn. De werkgroep zal nog moeten besluiten of direct aansluiten op de ADR van het Kennisplatform API's wenselijk is of via Digikoppeling. | 18-3-2024 |
| 17 | Specifiek voor het WUS-profiel stellen we de datum "einde ondersteuning" op januari 2025 (de datum waarop de nieuwe bundel normatieve documenten incl. de nieuwe architectuur opgeleverd gaat worden conform de planning). Op de Edustandaard-webpagina van Edukoppeling wordt reeds hierop gewezen vanaf mei 2024 plus een gebruiksadvies om geen nieuwe implementaties te starten met dit profiel | 22-4-2024 |
| 18 | Voor Edukoppeling zijn best practices voor het NL GOV OAuth profiel vereist ter ondersteuning van de najaarsrelease 2024 van Edu-V is op 22-4-2024 besloten. Het OAuth Best Practices-document is akkoord en kan gepubliceerd worden zodra versie 1.1 van het NL GOV OAuth profiel beschikbaar komt. NB in deze Best Practices wordt de wijze van toestemming verlenen (delegatie) niet opgenomen. De invulling wordt aan de implementerende partijen overgelaten. | 3-7-2024 |
| 19 | De voor (Technische) Interoperabiliteit relevante principes en kaders die vanuit publieke regie zijn aangeleverd zijn relevant en kunnen met enkele aanscherpingen in de ROSA Architectuurkaders worden verwerkt. | 3-7-2024 |
| 20 | Kernteam (Erwin, Brian, Remco de Boer) bereidt de uitwerking voor van de architectuurkaders die in de ROSA worden opgenomen. | 3-7-2024 |
| | | |

NB voor de voorgaande besluiten zie:
https://www.edustandaard.nl/app/uploads/2022/10/2022-06-29-Verslag-Edustandaard-Werkgroep-Edukoppeling.pdf

[3] Digikoppeling Koppelvlakstandaard REST-API (logius-standaarden.github.io) (werkversie)