edustandaard

Verslag Edustandaard werkgroep Edukoppeling

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

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

Agenda:

1. Opening / mededelingen / Verslag van 6 november 2024
2. Vergelijking toestemmingsvarianten (nav actiepunt #132: Voorstel tav de toestemmingsclaim in het access token)
3. RFC 011 Edu-V:
    a. Wel of niet PKIo bij end points Authorization Server/Resource Server
4. MEMO vertrouwen PKI-overheidscertificaten
5. wvttk

1. Opening, mededelingen en verslag van 6 november 2024

- Patrick Doomen is werkzaam bij SURF, maar neemt deel namens het GF Npuls. Hij sluit aan vanwege zijn betrokkenheid bij OKE koppelingen.
- Robert heeft een opmerking bij het verslag van november. Hij vraagt zich af of bij de eisen rond jwks_uri niet moet staan dat authorization server “de Client_jwt valideert” (ipv ontcijferen). Er wordt aangegeven dat de teksten overgenomen zijn uit de Edu-V afspraak[1]. Edu-V kan eventueel de tekst aanpassen. Het verslag hoeft op dit punt dus niet aangepast te worden.
    - *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.*

- Verslag wordt zonder wijzigingen vastgesteld

- Maarten heeft een memo (MEMO vertrouwen PKI-overheidscertificaten) opgesteld dat wordt toegevoegd als agendapunt.

[1] M2M identificatie, authenticatie en autorisatie - Afsprakenstelsel Edu-V - Confluence

2. Vergelijking toekstemmingsvarianten (Gerald)

Naar aanleiding van actiepunt 132 geeft Gerald een presentatie[2] van drie manieren om toestemming te verlenen in een SaaS context[3]. Het uiteindelijke voorstel is om met betrekking tot het OAuth Access Token op een aantal punten aan te sluiten op de invulling van FSC[4]. Er is consensus om in de Edukoppeling OAuth Best Practices versie 1.1 de claims van het voorstel over te nemen.

Attribute	Meaning	Zijde	Wie
iss*	The ID of the Peer who issued the token. I.e. the Peer who is offering the Service	Server	OIN van gegevensverwerker Y
azp*[5]	The client id of the client to whom this token was issued		
exp*	Expiration time		
jti*[6]	A unique JWT Token ID value with at least 128 bits of entropy. This value MUST NOT be re-used in another token. Clients MUST check for reuse of jti values and reject all tokens issued with duplicate jti values.		
aud**	The URI is a URL that MUST contain the scheme and port number used by the Inway		
sub**	This should be the ID of the Peer for whom the token is intended	Client	OIN van gegevensverantwoordelijke A
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

* Verplichte claims voor JWT AT volgens NL GOV OAuth standaard[7]
** Optioneel in NL GOV OAuth, verplicht in voorstel
*** Nieuwe[8] optionele claims in voorstel

[2] Edukoppeling-OAUTH.ppt
[3] Een verwerker (leverancier) verwerkt persoonsgegevens in systemen waar de verwerkingsverantwoordelijke (onderwijsorganisatie) gebruik van maakt.
[4] De claims komen niet volledig overeen met FSC AT https://commonground.gitlab.io/standards/fsc/core/draft-fsc-core-00.html#jwt-payload
[5] Waarschijnlijk toegevoegd voor interoperabiliteit met OIDC, in die context wordt sub claim gevuld met referentie naar geauthentiseerd subject (RO in OAuth context).
[6] Verplicht in NL GOV maar ontbrak nog in besproken voorstel
[7] https://logius-standaarden.github.io/OAuth-NL-profiel/#jwt-bearer-tokens
[8] Vanuit FSC overgenomen claims

Hierbij stellen we dat de bredere context (betekenis van de claims en hoe deze te vullen) (voorlopig) aan ketensamenwerkingen wordt overgelaten. Zo geeft Edu-V aan dat zij de toegevoegde optionele claims waarschijnlijk niet gaan gebruiken, maar gaan dit nog onderzoeken. Voor de ketensamenwerking mbo-examens (waartoe ook DUO met Facet behoort) waar men OKE gaat gebruiken als standaard, geldt dat zij deze onder andere de nieuwe optionele claims waarschijnlijk wel willen gebruiken. Over het hoe en waarom rond de claims gaan de ketensamenwerkingen in een volgende Edukoppeling-bijeenkomst terugkoppeling geven. Na bespreking hiervan zal als er voldoende consensus is, een OAuth Best Practices versie 1.2 opgesteld worden. We verwachten dat dit in de loop van Q1 2025 zal plaatsvinden.
We verwachten dan ook meer zicht te hebben over de ontwikkeling van een Digikoppeling OAuth Best Practice en de nieuwe versie van het Digikoppeling REST-profiel waar de FSC afspraak in opgenomen wordt. Zie hiervoor ook de Digikoppeling stukken[9]. Ook het NL GOV OAuth profiel is nog in ontwikkeling. Mogelijk dat ook het Access Token aangepast zal worden, zoals bij uitbreiding rond Proof of Possession[10] tokens. Bovendien zijn we als werkgroep ook bezig om de nieuwe architectuurkaders op te stellen zowel voor de ROSA als voor de Edukoppeling-architectuur.
Pas als al deze ontwikkelingen definitief genoeg zijn, lijkt het voor het onderwijs een mooi moment om dan de standaard Edukoppeling uit te breiden met een OAuth-profiel. Tot dan werken we dus met de genoemde Best Practices.

3. RFC Edu-V PKIo certificaten

Een open punt in de Edukoppeling OAuth Best Practices is het gebruik van PKIo certificaten. De NL GOV OAuth standaard is hier niet heel duidelijk over. Dit met name bij connection with protected resource[11]: "*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 for encryption*.".

Er is vanuit onze werkgroep Edukoppeling met de beheerders van NL GOV OAuth gesproken om tot een voorstel voor verduidelijking te komen. Hierbij is met name gevraagd om duidelijkheid te geven of PKIo relevant is voor een access token. Voor het access token is de tekst aangepast naar "*In case the Authorization Server and Resource Server are not operated under responsibility of the same organisation, the bearer token MUST be signed with the use of a PKIoverheid certificates with OIN*."

Dit maakt de weg dus vrij om in het geval van het Access Token een eigen certificaat (geen PKIo) te gebruiken voor ondertekening als de AS en RS onder de controle vallen van dezelfde partij. Er wordt echter niets gesteld over de endpoints die een client van een andere organisatie gebruikt in communicatie met AS (token endpoint) en AS (resource(s)). Moeten deze endpoints TLS met een PKIo certificaat toepassen als de client niet onder de controle van dezelfde partij valt als AS/RS?
Van oudsher gebruiken Digikoppeling en Edukoppeling PKIo als vertrouwensanker. Hiermee hebben ketens een gestandaardiseerd proces rond de identiteitsverificatie van rechtspersonen en uitgifte van een certificaat met een identiteit uit een basisregistratie.

---

[9] Federatieve Service Connectiviteit opnemen in het Digikoppeling voor REST API's profiel · Issue #26 · Logius-standaarden/Digikoppeling-Koppelvlakstandaard-REST-API · GitHub en Digikoppeling-Algemeen/Digikoppeling_Roadmap_2024_2025.md at roadmap_2024-2026 · Logius-standaarden/Digikoppeling-Algemeen · GitHub
[10] https://logius-standaarden.github.io/OAuth-NL-profiel/#proof-of-possession-tokens
[11] https://logius-standaarden.github.io/OAuth-NL-profiel/#connections-with-protected-resources

Hiermee kunnen clients en servers elkaar identificeren en authenticeren. Met het voorstel van NL GOV OAuth beheerders kan het zijn dat de client bij gebruik van AS/RS endpoints deze niet kan identificeren en authenticeren als deze geen TLS met PKIo toepassen. Het voorstel wordt ergens in Q1 2025 in de NL GOV OAuth werkgroep besproken. Er zal dan duidelijk worden of de werkgroep hierin meegaat. Er zal dan ook duidelijk worden of dit een wijziging is die in versie 1.1 meegaat of de volgende 1.2 versie.

Momenteel sluit Edu-V het gebruik van PKIo voor AS en RS uit: "*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.*" Hiermee kiezen zij er dus ook voor dat alleen de partij met AS/RS de client runtime met PKIo kan authenticeren en met OIN kan identificeren. De client kan de endpoints van AS/RS niet op basis van PKIo authenticeren.

De werkgroep besluit om in de Edukoppeling OAuth Best Practices 1.1 op te nemen dat ook voor het AS token endpoint en de Resource endpoints TLS met PKIo toegepast moet worden. Dit zal nog binnen Edu-V besproken worden maar het is waarschijnlijk dat zij dit punt niet zullen opvolgen. Of dat voorlopig is of blijvend hangt mede af van de uitkomsten van de standaardisatieprocessen binnen de overheid en het onderwijs.

4. MEMO vertrouwen PKI-overheidscertificaten

Maarten heeft een memo opgesteld m.b.t. problemen rond Microsoft Dynamics Business Central bij het gebruik van PKIo certificaten. Business Central is een SaaS-product. Afnemers hebben geen toegang tot de certificate store van het onderliggende besturingssysteem en kunnen hierin geen private root (PKIo hiërarchie) opnemen. Er is zo geen gebruiksvriendelijke manier om dit pakket als SaaS te gebruiken in een M2M communicatie met PKIo certificaten. De afnemer van SBB heeft nu een proxy geplaatst voor de HTTP-client van Business Central om met de API van SBB te kunnen communiceren. Hiermee voldoet de communicatie tussen de proxyserver en Business Central niet aan de Edukoppeling standaard.

Het is duidelijk dat Microsoft Dynamics Business Central in de SaaS-vorm het voor klanten niet makkelijk maakt om M2M-koppeling met private root certificaten in te richten (focus H2M /browser). Verder is de verwachting dat meer en meer SaaS-leveranciers deze mogelijkheid niet meer aanbieden en het kan in de toekomst vaker gaan voorkomen. Helaas is er voor Edukoppeling (en Digikoppeling) niet mogelijk om over te stappen naar een public root gezien PKIo hier een aantal jaar geleden juist mee gestopt is.

Voor de nieuwe Edukoppeling architectuur is het eerder besproken uitgangspunt rond een flexibele infrastructuur ook voor dit punt relevant. Gaat de architectuur uit van bijvoorbeeld een AS die vele verschillende communicatiekanalen ondersteunt (niet alleen M2M maar ook H2M) of gaan we uit van een specifiek M2M koppelvlak. Op de korte termijn is er aan het gestelde probleem weinig te doen. Ook in de OAuth Best Practices zien we PKIo nog als een belangrijke basis voor vertrouwen in de onderwijsketens.

5. Wvvtk

Werkgroepsessies 2025 moeten ingepland worden. Voorlopig gaan we weer online verder en bepalen we of een fysieke sessie nodig is op basis van de verwachte agenda. Eerstvolgende zal in ieder geval in februari worden gepland.

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: • G2G irt B2B, en wat verstaan we daaronder. • 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

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: Uitgangspunt 1: De API strategie van het Kennisplatform API's de primaire "driver" voor de doorontwikkeling van de Edukoppeling architectuur versie 3.0 Uitgangspunt 2: Edukoppeling maakt gebruik van de producten van de API strategie. Concreet hebben we het dan over: • gebruikmaken van de betreffende Architectuur, • gebruikmaken van het NL GOV OAuth profiel, • gebruikmaken van de API Design Rules. 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[12] 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

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