edustandaard

Agenda Edustandaard werkgroep Edukoppeling

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

Datum en locatie
4 december 2024, 10:00-13:00
Locatie: Bar Beton, Machinistenkamer, Perron 4/5, Amersfoort CS

Agenda en stukken staan op:
2024-12-04 Werkgroepbijeenkomst december

1. Opening / mededelingen / Verslag van 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 de Authorization Server/Resource Server
4. wvttk

1. Opening / mededelingen / verslag

Erik Borgers is vanwege andere werkzaamheden bij Kennisnet niet meer actief bij OSR betrokken en daarmee ook niet meer actief bij Edukoppeling-aangelegenheden. Erik heeft zich derhalve teruggetrokken uit de werkgroep Edukoppeling.

2. Vergelijking toestemmingsvarianten

Naar aanleiding van actiepunt 132 heeft Gerald een vergelijking opgesteld van de drie bekende manieren in het onderwijsdomein om toestemming te verlenen en dat kenbaar te maken, waarvan twee met OAuth. Zijn toelichting hierbij is de volgende:
In deze vergelijking vormen Edukoppeling-WUS en -REST de norm van wat we met OAuth zouden moeten kunnen. Overigens is het memo beperkt tot de scope van vertrouwelijkheidsclassificatie ‘middel’ of ‘hoog’. Dat betekent onder andere dat de gateway van verwerkers de bekende validaties kan uitvoeren:

- De verwerkingsverantwoordelijke aan clientzijde wordt onomstotelijk met PKIO geïdentificeerd (=OIN)
- De client is gemandateerd door gespecificeerd FROM-OIN om een endpoint te gebruiken (inkomend)
- De server is gemandateerd door gespecificeerd TO-OIN om een endpoint aan te bieden (uitgaand).

Het is een interessante exercitie geweest en ik ben eerlijk gezegd ook opgeschoven. Na dit werk zou ik willen vervolgen met het bedenken van scenario’s voor een toekomstvaste onderwijsbrede standaard. Maar het is best mogelijk dat ik dingen verkeerd heb ingeschat

Gevraagde actie werkgroep:

- Ik nodig een iedereen uit om het te lezen, denkfouten eruit te halen en ook na te denken over scenario’s.

3. RFC Edu-V en Edukoppeling OAuth Best Practice

Vorige keer zijn een aantal RFC's vanuit Edu-V op de Edukoppeling OAuth Best Practice besproken. Dat heeft geleid tot een aantal aanpassingen in de Best Practice.

Ten aanzien van RFC011 (zie ook *20240927 - RFCs M2M IAA en NL GOV)* is er nog geen definitief standpunt ingenomen. In het verslag van de werkgroepmeeting van 6 november is het volgende daarover genoteerd:
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 het niet toepassen van PKIo bij RS en AS endpoints waarmee de client communiceert. 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 tussen client en AS/RS 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 endpoints waarmee client communiceert is nog niet overgenomen in de Edukoppeling OAuth Best Practices. Vanuit beheer NL GOV OAuth[1] wordt begin volgend jaar met de NL GOV OAuth werkgroep een voorstel besproken om alleen tokens met PKIo te ondertekenen als de betreffende rol niet onder controle staat van dezelfde partij als waarmee gecommuniceerd wordt (beheerder client is niet die van AS en private_key_jwt wordt ondertekend met PKIo, AS en RS vallen wel onder beheer zelfde partij dus Access Token kan met een eigen certificaat ondertekend worden. Vanuit beheer Edukoppeling is er een voorkeur om ook de endpoints waar client mee communiceerd van PKIo te voorzien voor TLS verbinding. Zo kan de client betrouwbaar het OIN vaststellen van partij waarmee gecommuniceerd wordt. Nadeel kan zijn dat de AS in bredere context dan alleen Edukoppeling verkeer wordt gebruikt. Wat handig is lijkt dan ook samen te hangen met bredere architectuur vraag. De stelling vanuit beheer Edukoppeling is dat een bredere toepassing van een AS wenselijk is, maar heeft wel de consequentie dat ook de client (bij registratie) betrouwbaar moet kunnen vaststellen dat AS/RS endpoints correct zijn en onder beheer van bepaalde OIN vallen. Het toepassen van PKIo op AS en RS endpoints is dus nog een open punt en we willen komende werkgroep hierover een besluit nemen voor de Edukoppeling OAuth Best Practices versie 1.1. Wat de NL GOV werkgroep definitief besluit weten we pas in het nieuwe jaar.

We moeten dus in onze werkgroep (voorlopig) zelfstandig een besluit nemen.

Gevraagd besluit werkgroep:

- In de Best Practice uitsluiten (of in ieder geval niet verplichten) dat PKIo ook nodig is op de AS/RS endpoints waarmee de client communiceert als de AS en RS niet onder dezelfde partij vallen als de client,
- of dat we dit in de BP nog openlaten totdat NL GOV hier een ei over heeft gelegd.

We willen graag consensus over deze punten zodat we daarna de OAuth BP 1.1 definitief op Edustandaard.nl publiceren. Als ketensamenwerkingen (DUO uitwisselingen met ROD/RIO, Edu-V, OKE...) hier verschillende beelden bij hebben moeten we besluiten hoe we hiermee om willen gaan.

[1] 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."

edustandaard

4. Wvttk

Werkgroepsessies in 2025 plannen.