edustandaard

Agenda Edustandaard werkgroep Edukoppeling

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

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

Agenda en stukken staan op:
2024-11-06 Werkgroep Edukoppeling bijeenkomst – november

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

1. Opening / mededelingen / verslag

MBO Digitaal zal toch niet een deelnemer in de werkgroep afvaardigen. Ze geven het volgende hierbij aan:

- We vertrouwen op de expertise van de werkgroep en de consensus die daar ontstaat.
- Andersom hebben we niet de expertise om deze in te brengen.
- We nemen de resultaten over voor onze sector.
- Als er een nieuwe versie komt van de standaard dan passeert deze de Edustandaard architectuurraad en standaardisatieraad waardoor we alsnog op de hoogte blijven.

Zij zullen wel als agendalid betrokken zijn.

2. RFC Edu-V

Afgelopen werkgroepen hebben we het vaak gehad om voor het onderwijs al een striktere keuze te maken in datgene wat binnen NL-GOV nu is opgesteld. We hebben daarin de keuze tussen een flexibele architectuur en opties of 1 strikt M2M-profiel. Bij Digikoppeling OAuth profiel zien we ontwikkelingen rond meerdere scenario's en profielen die hierop te mappen zijn en op elkaar voortbouwen. Voor de korte termijn geeft de Best Practice die we hebben opgesteld en gepubliceerd invulling aan dat laatste. Ons advies (dus van de standaardisatie-expert en de voorzitter) is voor dit moment:

- Werk een flexibele architectuur uit (met daarin opties) zoals dat ook gebeurt in het bredere overheidsdomein (NL GOV/Digikoppeling).
- Stel Best Practices op tbv toepassingsgebieden (leermiddelenketen/Edu-V is daar nu 1 van) waarin striktere keuzes worden gemaakt.

Ad2a
Vanuit Edu-V is de volgende RFC ingediend: *20240927 - RFCs M2M IAA en NL GOV*
De RFC is ook voorzien een reactie van de Architectenraad Edu-V.

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 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.*" Dit laatste is nog niet overgenomen in de Best Practice.
NL GOV stelt bij paragraaf 2.3.4 Client Keys: "I*n 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.*" We bespreken graag wat wenselijk is, aansluiten op Edu-V of NL GOV.

Ad2b
Op basis van de RFC en de afstemming die hierover is geweest met ook Erwin en Brian, is door Erwin een nieuwe versie van de Edukoppeling OAuth Best Practices opgesteld (versie 1.1) die recht doet aan de RFC.

Gevraagde acties werkgroep:
- Bespreken en beoordelen RFC
- Beoordelen en mogelijk vaststellen van Edukoppeling OAuth Best Practices v1.1.

Ad2c
Naast AS/RS vraagstuk heeft Edwin Verwoerd het eerder gehad over een PKIo vraagstuk dat speelt bij een Hub/intermediair in de Edu-V context. Edwin zou deze use case nog nader toelichten.

3. 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'. In elk geval moet dat niet minder worden. 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).

Ik vond het in elk geval een interessante exercitie 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.

4. Wvttk

De volgende werkgroepsessie is al gepland:
4 december 2024, 10-12:30