edustandaard

Agenda Edustandaard werkgroep Edukoppeling

Leden: Edwin Verwoerd (Edu-V), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Patrick van der Veer (SURF, OOAPI), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES), Kees van Ginkel (Topicus, OKE), René Rutte (Paragin, OKE), Tom Kirchjunger (Topicus, VDOD), Ruud Martin en Niek Derksen (Arlande, OKE), Hans Swart (Alfa College, OKE), Niels van Duin (SURF), Peter Leijnse (SURF, Npuls)
Agendalid: Joël de Bruin (MBO Digitaal), Noor Ferket (VDOD), HP Köhler (Edu-V)

Datum en locatie
4 november 2025, 13:00-15:30
Locatie: Bar Beton, De Sprinter, Perron 4/5, Amersfoort CS

Agenda en stukken staan op: 2025-11-04 Werkgroepbijeenkomst november

1. Opening / mededelingen / Verslag van 26 februari 2025
2. Terugkoppeling vanuit groeifondsen over specificaties en implementaties
3. Discussie uniform profiel of profielvarianten
4. Edukoppeling Architectuur
5. Identificatie onderwijsorganisaties
6. Nieuwe versie UBV TLS
7. Ontwikkelingen bij Digikoppeling / Logius
8. wvttk

1. Opening / mededelingen / verslag

Na een uitstapje te hebben gemaakt met de Expertgroep OAuth, hebben we in augustus in die expertgroep besloten dat de verdere uitwerking van het OAuth-profiel en de architectuur weer in de overleggen van de Edukoppeling-werkgroep plaats gaan vinden. Voor de geïnteresseerde: een kort verslag van de Expertgroep bijeenkomst van 19 augustus is hier te vinden: 2025-08-19 Verslag en actiepunten Edukoppeling-Expertgroep OAuth.docx.

Als randvoorwaarde werd gesteld dat alle relevante implementerende partijen vertegenwoordigd en aanwezig zijn in de werkgroep Edukoppeling: DUO, Edu-V, OKE, SURF (Npuls/OOAPI) naast de andere vaste leden van de werkgroep (SBB, VDOD).

Peter Leijnse (SURF) wijst op een tweetal ontwikkelingen die mogelijk het werk van de werkgroep Edukoppeling kunnen raken:

- SURF heeft een open vraag vanuit het TIP-netwerk gehad over mogelijkheden om meer samen te werken. Vooral in context van dataspaces, credentials en wallets, maar er is zeker raakvlak/overlap met onderwerpen die binnen de werkgroep Edukoppeling spelen. Hier is meer informatie te vinden: Publicaties – Trusted Information Partners
- In de Architectuurdag van de Groeifondsprogramma's georganiseerd door Edustandaard van maandag 27 oktober 2025 is uitgebreid stilgestaan bij het topic datadelen/ 'dataspaces'.

Beide zaken zullen niet inhoudelijk nu besproken worden maar zullen voor een volgende keer op de agenda kunnen terugkomen.

2. Terugkoppeling vanuit groeifondsen over specificaties en implementaties

Tijdens de laatste Edukoppeling werkgroep is besloten dat we binnen een expertgroep een stap terug maken om te kijken of we niet alleen tot een uniform OAuth profiel kunnen komen, maar ook wat er rond mandatering (toestemming/consent) nodig is. We hebben hierom destijds ook besloten om de 1.1 versie van de Edukoppeling Oauth best practices nog niet te publiceren. De expertgroep heeft de afgelopen periode met name over OAuth specificaties gesproken en er lijkt met betrekking tot toegang tot een REST API (client credentials grant) over de meeste punten consensus te zijn. We vragen bij dit agendapunt de vertegenwoordigers van de implementerende partijen (OKE/OKx, Npuls/OOAPI, Edu-V en DUO) om de voor hun belangrijkste keuzes toe te lichten. We denken hierbij aan punten als:

1. grant_type;
2. gegevens die worden vastgelegd bij registratie van een client;
3. vorm van client authenticatie bij token endpoint;
4. claims in acces token;
5. PKI vertrouwensanker;
6. TLS versie & ciphers.

Achtergrondinformatie is te vinden in:

Specificatie Edu-V: M2M identificatie, authenticatie en autorisatie - Afsprakenstelsel Edu-V - Confluence

Specificatie OKE: Update volgt nog van het document *Voorstel aanpak REST OAuth2 profielen*

Specificatie DUO (OKE-Facet): Zie het document in de map van deze bijeenkomst: *Memo Expertgroep OAuth - Protocol en mandaten (1.0)*
Toelichting vanuit DUO: Dit document is een aanzet om te gaan oefenen met rfc 8693 voor implementatie van Facet in OKE. Deze rfc moet kunnen werken met mandaten (on behalf of), is een industriestandaard en wordt ondersteund door vooraanstaande tools op de markt.

Specificatie Npuls/OOAPI:

3. Discussie uniform profiel of profielvarianten

Vanuit Bureau Edustandaard hebben we gekeken naar de documenten die zijn verspreid en constateren we dat bij de Oauth-specificaties (client credentials grant) wat verschillende keuzes zijn. We willen op basis van een globale analyse die we in het overleg zullen tonen, bespreken waar deze verschillen volgens ons zitten en of we hier tot een meer uniform besluit kunnen komen. Dit biedt ons de mogelijkheid om vast te stellen of we één profiel kunnen opstellen of dat er verschillende profielen nodig zijn en waarom.

We onderkennen hierbij 2 lagen. De eerste betreft kenmerken van de OAuth specificatie zelf. De tweede gaat over het mandaatbeheer.

Op basis van de discussie rond de twee lagen hopen we meer duidelijkheid te hebben hoe we de komende periode verder willen gaan. Kunnen we tot consensus komen over de specificatie die we tot profiel kunnen verheffen? Of verwachten we dat we voor hetzelfde werkingsgebied en functionele toepassingsgebied meerdere profielen gaan krijgen die (deels) van elkaar verschillen? Of verschillende profielen voor verschillende werkingsgebieden en/of verschillende functionele toepassingsgebieden?

4. Edukoppeling Architectuur

Met meer zicht op de profielen en mandaatbeheer wordt het ook tijd om een nieuwe versie van de Edukoppeling-architectuur te ontwikkelen. We gaan uit van een complete herziening en de huidige versie die nu nog op Edustandaard is gepubliceerd zal dan ook niet als basis worden gebruikt. Daarnaast willen we deze architectuur in lijn brengen met de (nog voor een groot deel op te stellen) bovenliggende ROSA kaders. We stellen voor om hierin gezamenlijk in op te trekken en iedereen uitnodigen hieraan mee te werken.

5. Identificatie onderwijsentiteiten

De huidige Edukoppeling-architectuur en profielen gaan uit van de onderwijsinstellingserkenning (beheerd en ontsloten via RIO register) om enerzijds op basis daarvan gegevens bij een SaaS te kunnen routeren en anderzijds een mandaat te kunnen verifiëren bij een M2M-uitwisseling. Het BRIN-nummer is de identifier van de onderwijsentiteit (instelling) en wordt gebruikt om de rechtmatigheid van de uitwisseling te kunnen vaststellen.

Voor de Kennisnet-dienst Verwerkersovereenkomsten moeten leveranciers informatie rond verwerkersovereenkomsten van schoolbesturen (en tzt van samenwerkingsverbanden Passend Onderwijs) kunnen opvragen via een API. Ook hier wordt vereist dat voordat de gegevensuitwisseling kan plaatsvinden er een mandaat kan worden geverifieerd. Voor dit mandaat is de identificatie van een onderwijsbestuur vereist, dus niet een instelling die onder dat onderwijsbestuur valt. Voor deze use case moet dus een andere onderwijsentiteit (nl. die van het bestuur) geïdentificeerd kunnen worden.

Als onderdeel van de Edukoppeling-architectuur moeten we vaststellen of het mandaatbeheer op onderwijsbestuur binnen scope is, welke scenario's we hierbij onderkennen en tot op welk niveau we dit willen specificeren. Dit heeft dus ook een relatie met het voorstel van DUO rond RFC8693 (zie ook: *Memo Expertgroep OAuth - Protocol en mandaten*).

6. Nieuwe versie UBV TLS

Er is een nieuwe conceptversie van UBV TLS (zie UBV TLS v1.3 Concept 29-10-2025.pdf)

- Bijgewerkt op basis van TLS-voorschriften 2025-05 (NCSC), gezien degradatie van ciphers en TLS-opties; van 'Voldoende' naar 'Uit te faseren'.
- Voor M2M is 1.3 verplicht gesteld incl. een nieuwe selectie van ciphers.
- Profielen zijn bijgewerkt, mede op basis van Digikoppeling beveiligingsvoorschriften v2.x.x

7. Ontwikkelingen bij Digikoppeling / Logius

PKIo G4 certificaten: Wat is er nieuw?
G4 beschikt over 4 Root certificaten in plaats van 2. Ieder voor verschillend gebruik en onderhevig aan eigen (externe) kaders:

- S/MIME (publiek vertrouwd);
- EU-gekwalificeerde digitale handtekeningen;
- Server authenticatie (privaat vertrouwd);
- Overig (privaat vertrouwd; vooral bedoeld voor authenticatiedoeleinden),

Elk type is nog maar voor één doeleinde te gebruiken (dus bijvoorbeeld niet langer zowel voor authenticeren als een digitale handtekening);

G4 bevat een moderner cryptografisch algoritme voor het ondertekenen van alle certificaten: RSASSA-PKCS1-v1_5 is vervangen door RSASSA-PSS. RSASSA-PSS met SHA-256, MGF-1 met SHA-256, en een salt lengte van 32 bytes.;

De naamgeving van zowel de eindgebruikerscertificaten als die van de bovenliggende hiërarchie is aangepast. Hierdoor sluiten ze beter aan bij internationale normen en kaders en is het makkelijker te zien waarvoor een certificaat kan worden gebruikt, wat de doelgroep is, het validatietype en het vertrouwensanker.

8. Wvttk