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 (Arlande, OKE), Hans Swart (Alfa College, OKE), Niels van Duijn (SURF), Peter Leijnse (SURF, Npuls), Dennis Grootendorst (Studielink)
Agendalid: Joël de Bruin (MBO Digitaal), Noor Ferket (VDOD), HP Köhler (Edu-V)

Datum en locatie
17 december 2025, 14:00-16:30
Locatie: Bar Beton, Machinistenkamer, Perron 4/5, Amersfoort CS

Agenda en stukken staan op: 2025-12-17 Werkgroepbijeenkomst december

1. Opening / mededelingen / Verslag van 4 november 2025
2. Bespreken werkdocument OAuth client credentials profiel voor RESTful API
3. Identificatie onderwijsorganisaties
4. Nieuwe versie UBV TLS
5. Ontwikkelingen bij Digikoppeling / Logius
6. wvttk

1. Opening / mededelingen / verslag

2. Bespreken werkdocument OAuth client credentials profiel

Er is door Edustandaard een werkdocument opgesteld met zaken die relevant worden geacht voor het opstellen van een nieuwe Edukoppeling profiel(en). Op basis van de uitkomsten van de vorige bijeenkomst is besloten om de verschillende keuzes die bestaan in één document te vatten. Een ketensamenwerking kan zo een keuze maken die bij de betreffende context passen. Dit is wat we ook voor ogen hebben voor het uiteindelijke profiel. Verder is er (nog) niets over mandatering opgenomen, omdat we hiervoor de ervaringen van DUO uit de PoC afwachten.

We vragen alle leden om het document vooraf aan de bijeenkomst goed door te nemen. We bespreken het document graag op twee niveaus. Ten eerste of de structuur, vorm en inhoud in algemene zin een goede basis biedt en of er onderdelen ontbreken. Hiervoor kunnen opmerkingen in het document worden geplaatst. Ten tweede bespreken we graag of het document in detail de juiste informatie bevat en/of dat er inconsistenties of onjuistheden in zijn geslopen. De onderliggende standaarden waarop we ons baseren beschrijven zaken in veel meer detail. Het document focust zich alleen op bepaalde zaken. Zijn dit de juiste en voor ons relevante zaken? Hiervoor graag de tekst in het document naar wens aanpassen met tekstsuggesties aan.

3. Identificatie onderwijsentiteiten

De huidige Edukoppeling-architectuur en profielen gaan uit van de onderwijsinstellingserkenning (beheerd door DUO 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. De Instellingscode (aka BRIN-

nummer) is de identifier van de onderwijsentiteit (dus op het niveau van de onderwijsinstellingserkenning) en wordt gebruikt om de rechtmatigheid van de uitwisseling te kunnen vaststellen.

Voor de Kennisnet Dienst Verwerkersovereenkomsten (DV) moeten dienstverleners 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 van de onderliggende instellingserkenningen die onder dat onderwijsbestuur vallen. 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*).

4. 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

5. 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.

6. Wvttk