edustandaard

Verslag Edustandaard werkgroep Edukoppeling

Aanwezig: Edwin Verwoerd (Edu-V), Gerald Groot Roessink (DUO), Robert Kars (DUO), Patrick van der Veer (SURF, OOAPI), Kees van Ginkel (Topicus, OKE), René Rutte (Paragin, OKE), Dennis Grootendorst (Studielink), Maarten Kok (SBB), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, Bureau Edustandaard (BES))
Afwezig: Peter Leijnse (SURF, Npuls), Tom Kirchjunger (Topicus, VDOD),
Agendaleden: Joël de Bruin (MBO Digitaal), Jan Weggemans (Topicus, VDOD), Noor Ferket (VDOD)

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

Agenda:
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

Stukken staan in:
2026-02-11 Werkgroepbijeenkomst februari

1. Opening, mededelingen en verslag vorige keer

Dennis Grootendorst gaat namens Studielink bij dit overleg aanschuiven. Dennis is solutions architect en zit volop in de ontwikkeling en implementatie van de nieuwe voorziening(en) die Studielink onder haar hoede heeft en heeft enerzijds veel behoefte aan een goede OAuth-standaard voor het onderwijs maar kan anderzijds ook veel (praktijk)ervaring inbrengen ten aanzien van het opstellen van een profiel.

Er zijn een aantal opmerkingen over het verslag van 4 november 2025:

- Bij agendapunt 2: Mandaten worden nu nog niet als onderdeel van het OAuth-profiel besproken, maar kunnen op termijn weer op de agenda komen zodra DUO een PoC heeft gedaan met de token exchange standaard (RFC8693). Voor DUO is dit een belangrijk onderwerp en eist mandaatcontrole voor alle uitwisselingen met de eigen voorzieningen. We moeten t.z.t ook duidelijk hebben wat tot de architectuur behoort en wat eventueel in een profiel dat mandaatgebruik ondersteunt moet worden opgenomen.
- Bij agendapunt 2: token exchange standaard (RFC8693) maakt gebruik van de optie ‘Extension Grants’ en kent een eigen grant type (token-exchange) en is dus geen client_credentials. Robert Kars van DUO vraagt zich af of dit zo is. Eea staat beschreven in betreffende RFC’s https://datatracker.ietf.org/doc/html/rfc6749#section-4.4.2 en https://datatracker.ietf.org/doc/html/rfc8693#name-request.0

Na verwerking van de gevraagde wijzigingen wordt het verslag vastgesteld.

2. Bespreken werkdocument OAuth client credentials profiel voor RESTful API's

Op hoofdlijnen is de nieuwe versie een goede stap maar er zijn op hoofdlijnen een aantal zaken die anders moeten.

1. Er moet een compact overzicht komen met de eisen die gelden. Er komt een apart hoofdstuk met een toelichting rond de OAuth-standaard en de eisen. Verder gebruiken we niet meer het begrip 'vertrouwelijke gegevens' maar 'gesloten data' om het type gegevens te beschrijven dat via de RESTful API's ontsloten wordt.
2. We hebben bij een aantal eisen een keuze, bijvoorbeeld bij clientauthenticatie. Er wordt gevraagd om de keuzes duidelijker naar voren te laten komen. De keuzes leiden niet tot meer OAuth-profielen, het blijft één document, maar we gaan bepaalde eisen combineren. We zien een set maatregelen voor een laag risicoprofiel, een complexere maar veiligere set maatregelen voor een verhoogd risicoprofiel en het overheidsdomein waar naast maatregelen voor verhoogd risicoprofiel ook overheidsstandaarden gebruikt worden. Een ketensamenwerking kan zo een keuze maken uit een set maatregelen die bij de betreffende context passen. Een beschrijving hiervan is wat we ook voor ogen hebben voor het uiteindelijke OAuth-profiel.
3. Het OAuh-profiel is nu gebaseerd op internationale open (industrie) standaarden en niet specifiek op overheidsstandaarden. In de nieuwe versie moet er een toelichting opgenomen worden. Het is echter ook een besluit[1] dat ook aan de Architectuurraad moet worden gemeld omdat we hiermee niet de harde lijn naar Digikoppeling meer volgen.
4. Verder zijn de Edukoppeling-documenten op zichzelf staande documenten. De lezer hoeft (buiten de internationale open standaarden en relevante Edustandaard standaarden) niet allerlei externe bronnen te raadplegen. We voorkomen hiermee ook een extra beheerlast en documentatie-uitdaging zoals we bij de OAuth Best practices hebben gezien waar het NL GOV OAuth profiel als basis werd gebruikt. Het resultaat daarvan was dat het voor ontwikkelaars en andere betrokkenen lastig te lezen en te hanteren is.
5. Er is nu nog niets over mandatering opgenomen, omdat we hiervoor de ervaringen van DUO uit de PoC afwachten. We moeten dan ook besluiten wat op architectuurniveau moet worden beschreven hierover en of er zaken zijn ten aanzien van mandatering die in een nieuw of bestaand profiel moeten worden opgenomen.
6. Inhoudelijk zijn er ook een aantal belangrijke zaken besproken. mTLS zou als authenticatiemethode opgenomen kunnen worden, maar zoals ook al in de expertgroep-bijeenkomsten is besloten is er een uitdrukkelijke wens om niet mTLS te gebruiken. Er wordt besloten dat de verbinding tussen client en Resource Server wel via mTLS kan verlopen. Verder is er wat discussie over het toestaan van basic authentication. Dit is ook eerder in de expertgroep besproken, we moeten dit nu opnemen om ketens te kunnen laten confirmeren aan het profiel. We geven echter aan dat dit toegepast wordt voor een laag risicoprofiel. Verder wordt benoemd dat het de bedoeling is dat men op termijn migreert naar de eisen voor een hoog risicoprofiel. De regelgeving en eisen zullen in de toekomst alleen maar toenemen.

3. 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

[1] Zie besluit #21

verifiëren bij een M2M-uitwisseling. Het zogeheten BRIN-nummer (onderwijsinstellingscode) is de identifier van de onderwijsentiteit (erkende onderwijsinstelling) en wordt gebruikt om de rechtmatigheid van de uitwisseling te kunnen vaststellen.

Voor de Kennisnet-dienst Verwerkersovereenkomsten (DV) moeten leveranciers informatie rond verwerkersovereenkomsten van onderwijsbesturen (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 onderwijsinstelling die onder dat onderwijsbestuur valt en erkend is. 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).

Vanuit SURF heeft Peter Leijnse aangegeven dat hij voor de architectuur o.a. de onderstaand concerns relevant acht. De precieze inhoud van het mandaat is geen concern voor de Edukoppeling-standaard, want dan importeer je business logica in de transportprotocollen. De verschillende voorbeelden (instelling, bestuur etc) zijn use cases. Maar houd er rekening mee dat de architectuur bestand moet zijn tegen meer en meer gevarieerde use cases (denk: mandaat van ouder om gegevens van lerende in te zien; mandaat van onderwijsprofessional om gegevens lerende in te zien), waarbij de variabelen het te raadplegen bronregister en de inhoud/scope van het mandaat zijn.
Overigens zit je hier ook op het terrein van de werkgroep toegang, en zou een mandaat idempotent moeten zijn. Via M2M of via H2M moet de uitwerking van het mandaat hetzelfde zijn.

- het raadplegen van een bronregister voor mandaten/bevoegdheden
- het opstellen van een verklaring over mandaat
- het transporteren van zo'n mandaatverklaring
- het verifiëren van de mandaatverklaring
- het geven van de juiste toegangsrechten op basis van het mandaat

Verder wordt gesteld dat voor identiteiten van onderwijsorganisatie gerelateerde eenheden vooral de gegevens uit RIO moeten worden gebruikt.

Een volgende keer hopen we de thema's voor de architectuur te kunnen bespreken

4. Nieuwe versie UBV TLS

Het NCSC heeft vorig jaar een nieuwe versie van TLS voorschriften gepubliceerd (Ict beveiligingsrichtlijnen voor transport layer security 2025-05 | Publicatie | Nationaal Cyber Security Centrum).

Edukoppeling sluit hierop aan via de Edustandaard UBV TLS afspraak. Hiervan is een nieuwe versie van in ontwikkeling (UBV TLS). Kees van Ginkel geeft aan dat de link in de agenda niet werkte. Deze is in dit verslag aangepast.

Wanneer de nieuwe versie wordt gepubliceerd is nog onduidelijk. Deze versie wordt in de Architectuurraad van 5 februari besproken.

Belangrijke wijzigingen staan hieronder.

Changelog UBV TLS v1.3.1 – op hoofdlijnen

- **TLS 1.3 heeft de voorkeur**; bij M2M-koppelingen wordt TLS 1.3 door de ServiceAanbieder aangeboden.
- **Cipher suites zijn opgeschoond en geactualiseerd**.
- **PKIoverheid-certificaten** zijn alleen toegestaan in **productie**; voor **test en acceptatie** wordt **TrialCA** gebruikt.
- **DNSSEC is generiek van toepassing** (niet langer conditioneel).
- **Structureel beheer van TLS-configuraties** is voorgeschreven (periodieke controle).
- **TLS-profielen in de bijlage zijn bijgewerkt** en kunnen worden gebruikt om bestaande configuraties na te lopen (*mag niet / mag / voorkeur*, gebaseerd op UBV, NCSC en Digikoppeling).

Voorschrift	Verandering op hoofdlijnen	Toelichting / impact
TLS-ALG-03	Vervallen	Het expliciet scheiden van legacy TLS op een aparte hostnaam is verwijderd.
TLS-ALG-04	DNSSEC breder toegepast	DNSSEC is niet langer conditioneel (bijv. BIV-afhankelijk), maar generiek opgenomen. DNSSEC kan daardoor in meer situaties verwacht worden.
TLS-ALG-06	Nieuw: beheer en actualiteit TLS	Periodiek scannen en evalueren van TLS-configuraties is voorgeschreven. TLS vraagt structureel beheer.
TLS-M2M-01	TLS 1.3 heeft de voorkeur voor M2M	TLS 1.3 is de voorkeursversie. Het is aan de **ServiceAanbieder** om TLS 1.3 **aan te bieden** bij M2M-koppelingen. Vanaf 1-1-2027 is TLS versie 1.2 niet meer verplicht.
TLS-M2M-02	Cipher suites aangescherpt	Cipher suites die volgens de nieuwe NCSC TLS-richtlijnen als onvoldoende veilig worden beschouwd, zijn verwijderd. Nieuwe TLS-1.3 cipher suites zijn toegevoegd. **Er worden geen minder veilige cipher suites meer voorgeschreven uit legacy-overwegingen.** Dit vraagt actieve opschoning van configuraties.
TLS-M2M-09 / TLS-M2M-10	Samengevoegd	Voorschriften over ingetrokken en verlopen certificaten zijn samengevoegd. **Geen inhoudelijke wijziging**: ongeldige certificaten blijven onacceptabel.
TLS-H2M-01	Nieuw: hybride sleuteluitwisseling	Nieuw advies om hybride (quantumveilige) sleuteluitwisseling te overwegen. Geen verplichting, wel relevant voor toepassingen met lange vertrouwelijkheid.
TLS-H2M-02	Cipher suites aangepast aan TLS 1.3	Beschrijving van cipher suites volgt nu het TLS-1.3-model. H2M-configuraties en documentatie kunnen hierdoor aangepast moeten worden.
TLS-PKI-01	Uitgebreid	Het gebruik van PKIoverheid-certificaten is alleen toegestaan in productieomgevingen. Voor test- en acceptatieomgevingen dient PKIoverheid TrialCA te worden gebruikt.

5. Ontwikkelingen bij Digikoppeling / Logius

Met de introductie van de vierde generatie PKIoverheid certificaten (G4) zijn er meerdere private roots beschikbaar gekomen. Afhankelijk van het beoogd gebruik, zal een certificaat van een andere private root gebruikt moeten worden (zie https://www.logius.nl/onze-dienstverlening/toegang/pkioverheid/wees-voorbereid-de-nieuwe-generatie-pkioverheidcertificaten-komen-eraan);

Het "Programma van Eisen" is inmiddels uitsluitend in het Engels beschikbaar is daarom hernoemt naar "Programme of Requirements" (PoR). De meest recente versie is beschikbaar op https://cp.pkioverheid.nl/.

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.

Client-authenticatie

Uitsluitend SAML of mTLS te gebruiken bij SBR, Digipoort, DigiD, etc.

G3/G1 certificaat	G4-certificaat
G1 Private Services Server certificaat (OID: 2.16.528.1.1003.1.2.8.6) zonder domeinnamen G3 Organisatie Services Authenticiteit certificaat (OID: 2.16.528.1.1003.1.2.5.4)	G4 Private Other Generic Legal Persons Organization Validated Authentication (OID: 2.16.528.1.1003.1.2.44.16.25.8)

Server-authenticatie

Webserver, kan ook gebruikt worden voor SBR, Digipoort, DigiD, etc.

G3/G1 certificaat	G4-certificaat
G1 Private Services Server certificaat (OID: 2.16.528.1.1003.1.2.8.6) met domeinnamen	G4 Private TLS Generic Devices Organization Validated Server (OID: 2.16.528.1.1003.1.2.44.15.35.11) *

EU-gekwalificeerde digitale handtekening

eIDAS eSeal

G3/G1 certificaat	G4-certificaat
G3 Organisatie Services Onweerlegbaarheid certificaat (OID 2.16.528.1.1003.1.2.5.7)	G4 EUTL Organization Validated eSeal (OID: 2.16.528.1.1003.1.2.44.14.25.5)

Certificaten voor individuen

EU-gekwalificeerde digitale handtekening

Individuen in hoedanigheid van beroepsbeoefenaar (eIdas e-signature)

G3/G1 certificaat	G4-certificaat
G3 Organisatie Persoon Onweerlegbaarheid certificaat (OID: 2.16.528.1.1003.1.2.5.2)	G4 EUTL Regulated Profession eSignature (OID: 2.16.528.1.1003.1.2.44.14.12.5)

Individuen (algemeen)

G3/G1 certificaat	G4-certificaat
G3 Burger Onweerlegbaarheid certificaat (OID: 2.16.528.1.1003.1.2.3.2)	G4 EUTL Individual Validated eSignature (OID: 2.16.528.1.1003.1.2.44.14.11.5)

Op de volgende sites is meer informatie te vinden:

- Logius | Wees voorbereid, de nieuwe generatie PKIoverheidcertificaten komen eraan!
- PKIoverheid G4-certificaten: belangrijke data en het laatste nieuws

6. Wvttk

Geen onderwerpen

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	Q2 2026	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.	Q2 2026	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	Q2 2026	Brian	2
130	Edukoppeling FAQ uitbreiden met vragen uit de Edu-V keten en de antwoorden vanuit NL GOV/EK WG	Open	Q2 2026	BES	2
131	Opstellen werkdocument om afspraken rond het OAuth protocol scherper te krijgen	Afgerond	Voor de werkgroep sessie in december 2025	BES, leden reviewen vooraf aan de meeting	1
132	Aanpassen compliance document op pagina met conceptversie juni 2024 Edukoppeling - Edukoppeling - juni 2024 - Edustandaard	Open	Q1 2026	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[2] 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
21	Loslaten van directe koppeling met Digikoppeling. We volgen waar dat relevant is, onderdelen van overheidsstandaarden. De werkgroep bepaalt wat wel en niet overgenomen wordt. De specificaties zijn zelfbeschrijvend en waar we het nodig achten worden relevante referenties opgenomen.	4-11-2025
	NB voor de voorgaande besluiten zie: https://www.edustandaard.nl/app/uploads/2022/10/2022-06-29-Verslag-Edustandaard-Werkgroep-Edukoppeling.pdf	

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