edustandaard

Verslag Edustandaard werkgroep Edukoppeling

Aanwezig:	Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Erik Borgers (Kennisnet, OSR), Koen Voermans (Edu-v), Patrick van der Veer (SURF), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)
Gastlid:	Peter Leijnse (SURF)
Afwezig:	Edwin Verwoerd (Iddink/VDOD)
Agendalid:	Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie

18 maart 2024, 10:00-12:30 uur
Locatie: Seats2Meet Amersfoort CS

1. Opening, mededelingen en vaststellen agenda
2. Openbare consultatie Edukoppeling OAuth profiel: Review toegelicht door SURF
3. Memo Edukoppeling Secure API OAuth profiel: Vaststellen uitgangspunten
4. Voorstel publicatie van nieuw compliance document: Uitfasering WUS profiel
5. Rondvraag / Sluiting

Reviewbare stukken voor werkgroepleden te vinden op de Teams-omgeving van de bijeenkomst van 18 maart 2024
Openbare stukken te vinden op: https://www.edustandaard.nl/standaard_bijeenkomsten/werkgroep-edukoppeling-18-maart-2024/

1. Opening, mededelingen en vaststellen agenda

Edwin Verwoerd heeft zich vanwege ziekte af moeten melden. Hij heeft wel van tevoren mondeling commentaar geleverd op de stukken met name op de uitgangspunten-memo. Dat commentaar zal daar waar nodig ingebracht worden door de voorzitter.
Robert Kars kan melden dat het Edukoppeling REST-profiel is voorgesteld in de gegevensuitwisseling tussen DUO en gemeenten in zake verzuimmeldingen. Daar is dat met veel enthousiasme ontvangen en zal ook geïmplementeerd gaan worden.
De voorzitter geeft aan dat we deze meeting vooral in zullen gaan op de doorstart van het specificeren van een OAuth-profiel voor het onderwijs, maar dat dit wel op basis van een aantal uitgangspunten wort gedaan waarover eerst een besluit wordt genomen in de werkgroep. Uitgangspunten die in later instantie onderdeel van genoemde kaders en architectuur zullen worden opgenomen. Het uitwerken van die kaders en architectuur zal naar verwachting heel 2024 in beslag nemen.

2. Openbare consultatie Edukoppeling OAuth profiel

Afgelopen zomer is het Edukoppeling OAuth profiel als concept gepubliceerd ter consultatie. Recent heeft SURF een review hierop gedaan[1]. Peter Leijnse licht het reviewcommentaar toe in de werkgroep. Hij geeft daarbij aan dat SURF vooral vanuit het perspectief van de eigen diensten en koppelvlakken heeft gekeken en niet vanuit het perspectief van de leermiddelenketen in het funderend onderwijs.

Peter verwacht dat er in het Nederlandse onderwijs- en onderzoeksdomein er ruimte zal moeten zijn voor minimaal (en liefst ook maximaal) 2 profielen:

- Voor een context waarin partijen met name binnen de Nederlandse publieke context opereren: het NL GOV assurance profile for OAuth 2.0 [iGov-NL]
- Voor een context waarin partijen in een belangrijke mate ook internationaal opereren in onderwijs- en onderzoekscontext: een profiel dat in afstemming met de internationale onderwijs- en

[1] https://www.edustandaard.nl/app/uploads/2024/03/Edukoppeling-OAuth-client-credentials-reactie-SURF.pdf

onderzoeksgemeenschap tot stand is gekomen. Voor (met name) het hoger onderwijs is deze internationale context essentieel. Daarvoor is nodig dat specifieke Nederlandse invullingen kunnen worden ‘losgelaten’.

SURF werkt in beide contexten mee aan de ontwikkeling. Edustandaard/Kennisnet zorgt ervoor dat de Edukoppeling werkgroep wordt geïnformeerd over (door)ontwikkeling van het NL GOV Assurance profile for OAuth 2.0 (werkversie[2]) door deelname aan de Kennisplatform API’s[3] beveiliging werkgroep. SURF blijft daarnaast ook actief meewerken aan de internationale context.

De meeste punten uit het reviewcommentaar worden door de werkgroepleden herkend en ook onderschreven. Veel punten zijn al geadresseerd om in de ROSA Architectuurkaders en de Edukoppeling Architectuur 3.0 verwerkt te worden. Dit is reeds onderschreven in de Architectuurraad van Edustandaard en ook de aanpak die de werkgroep wil gaan hanteren is daar goedgekeurd. Het uitgangspuntendocument dat als agendapunt 3 staat geagendeerd geeft verder invulling in aan die aanpak en veel van de door SURF geconstateerde punten.

Gerald Groot Roessink stelt dat de ontwikkeling van een nieuw OAuth-profiel verleden jaar gericht was op de implementatie in het groeifondsprogramma Edu-V en dat daarbij geconstateerd is geworden dat er een interoperabiliteitsprobleem zou kunnen ontstaan omdat in een ander groeifondsprogramma, Npulse, de intentie was uitgesproken om OOAPI te gebruiken, waar een ander invulling van het OAuth-profiel waarschijnlijk aan de orde was. Bij DUO botst met de bestaande uitwisseling van Facet dat is gebaseerd op Edukoppeling/REST (zonder OAUTH). Gerald geeft aan dat DUO graag wil opschuiven naar OAuth zolang dat maar onder de paraplu van Edustandaard en Edukoppeling valt.

3. Uitgangspunten Edukoppeling Secure API OAuth profiel

In de memo[4] bij dit agendapunt wordt kort de aanleiding beschreven voor de noodzaak van een nieuw Edukoppeling Secure API OAuth profiel. Daarbij wordt ook naar de review van het vorige agendapunt gerefereerd. Er wordt in de memo gesteld dat de Edukoppeling conceptversie[5] met Secure API OAuth Client Credentials profielen v0.8 (concept) niet aangeboden wordt aan Architectuurraad voor vaststelling en publicatie. In plaats daarvan wordt er (mede op basis van nieuwe ontwikkelingen) gewerkt aan een nieuw Edukoppeling Secure API OAuth profiel waarbij het NL GOV Assurance profile for OAuth 2.0 (werkversie[6]) als een belangrijke basis wordt gezien.

Besluit: De werkgroep trekt de huidige Edukoppeling conceptversie[7] van de Secure API OAuth Client Credentials profielen v0.8 (concept) terug. De publicatie van deze versie op Edustandaard gaat hiermee vervallen.

In de memo zijn een aantal uitgangspunten opgenomen waar de werkgroep deels uit moet kiezen om de ontwikkeling van de Edukoppeling architectuur versie 3.0 en het Edukoppeling Secure API OAuth profiel te kaderen. Dit is noodzakelijk gezien het nu nog ontbreken van duidelijke bovenliggende (ROSA) kaders. Omdat er verschillende ontwikkelingen op dit terrein spelen en van invloed kunnen zijn op de standaardisatie binnen het Nederlandse onderwijs op dit vlak, is het vooruitlopen op een aantal van die kaders nodig om de verdere invulling van het profiel te kunnen maken.

3.1. Uitgangspunt 1: De API strategie[8] van het Kennisplatform API’s de primaire “driver" voor de doorontwikkeling van de Edukoppeling architectuur versie 3.0

Deze strategie introduceert een ander perspectief, namelijk dat gegevens tussen (web)applicaties uitgewisseld worden met API's. Ze maken het onder andere mogelijk om heel gericht specifieke gegevens op te vragen, en

[2] https://logius-standaarden.github.io/OAuth-NL-profiel/
[3] Kennisplatform API's | Geonovum
[4] https://www.edustandaard.nl/app/uploads/2024/03/2024-03-13-Memo-Edukoppeling-Secure-API-OAuth-profiel-Edukoppeling-Architectuur-v3.0.pdf
[5] Edukoppeling - Edukoppeling - juli 2023 - Edustandaard
[6] De werkversie bevat nu ook een OAuth Client Credentials grant dat een belangrijk onderdeel is van het Edukoppeling Secure API Oauth profiel.
[7] Edukoppeling - Edukoppeling - juli 2023 - Edustandaard
[8] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Inleiding/ (werkversie)

faciliteren daarmee dataminimalisatie. We zien de API strategie als een belangrijke stap om Edukoppeling te innoveren en zijn hierin efficiënt doordat we gebruik maken van wat er al bij de overheid is ontwikkeld. Onder andere “API first” zal als architectuurprincipe worden opgenomen in de ROSA architectuurkaders. Een andere consequentie is dat we “afscheid gaan nemen” van meer service gerichte architecturen en daarmee ook van het WUS-profiel dat nog onderdeel vormt van Edukoppeling. Die consequentie wordt onderkend, er zal een einddatum voor dit profiel moeten worden gekozen, de datum waarop er geen ondersteuning vanuit Edustandaard meer op dit profiel wordt gegeven met daarbij het advies aan de partijen die dit geïmplementeerd hebben om een planning voor uitfasering en vervanging op te stellen (dit zal onderdeel zijn van agendapunt 4). Gerald Groot Roessink geeft aan dat DUO hier zeker handen en voeten aan zal gaan geven (in de koppelvlakken met ROD en RIO) maar dat dit in nauwe samenspraak met de (voornamelijk LAS- en SIS-)leveranciers moet gebeuren, die misschien niet zitten te wachten dat een op zich goed draaiend koppelvlak aangepast moet gaan worden. Brian Dommisse kan melden dat met name leveranciers die overstappen op nieuwe ontwikkelplatforms dit heel graag zien gebeuren want die nieuwe platforms ondersteunen WUS niet meer zodat maatwerk vereist is met extra beheerlasten. Bovendien is de kennis bij developers over SOAP etc. steeds schaarser aan te worden. Peter Leijnse verwacht wel dat het uitfaseren en overstappen zeker 2 tot 3 jaar in beslag zal nemen.

Besluit: De werkgroep is unaniem in het onderschrijven van dit uitgangspunt.

3.2. Uitgangspunt 2: Edukoppeling maakt gebruik van de producten van de API strategie.

Concreet hebben we het dan over:
- gebruikmaken van de betreffende Architectuur[9],
- gebruikmaken van het NL GOV OAuth profiel[10],
- gebruikmaken van de API Design Rules[11].

Erwin Reinhoud geeft aan dat de architectuur een belangrijk kader is voor de Edukoppeling architectuur en profielen. Vanuit het Kennisplatform en de API Strategie wordt er geredeneerd vanuit een flexibele architectuur, eentje die meerdere use cases kan ondersteunen waarbij API’s bevraagd worden. Ook bij Digikoppeling worden de ontwikkelingen bij het Kennisplatform gevolgd, maar zoals ook eerder met het Edukoppeling REST profiel willen wij binnen de Edukoppeling werkgroep wat sneller kunnen doorontwikkelen. De consequentie is wel dat bij Digikoppeling, die we als Edukoppeling tot nu toe gevolgd hebben, er op termijn andere keuzes gemaakt kunnen worden. Hoe verhouden we ons daartoe?
Voorstel is om als dat duidelijker wordt, dit dan in de werkgroep op tafel komt, maar dat we niet gaan wachten op waarmee Digikoppeling gaat komen. Bovendien wordt vanuit de Edukoppeling-werkgroep ook geparticipeerd in het Technisch Overleg Digikoppeling zodat er zaken daar ingebracht kunnen worden.

Besluit: De werkgroep is unaniem in het onderschrijven van dit uitgangspunt en de consequenties daarvan.

3.3. Uitgangspunt 3: Het Edukoppeling Secure API OAuth profiel is (initieel) fully conformant aan het NL GOV OAuth profiel.

Fully conformant betekent dus dat we in het onderwijs geen afwijkingen hebben tov het NL GOV profiel en we ons qua documentatie kunnen beperken tot een verwijzing. Maar “initieel” staat er niet voor niets. Bij de verdere ontwikkeling van de ROSA architectuurkaders en Edukoppeling Architectuur versie 3.0 kunnen we mogelijk naar een conformant profiel bewegen. De verwachting is namelijk dat er op termijn zaken aan het profiel worden toegevoegd waar in het onderwijs behoefte aan is om die nader te specificeren en te standaardiseren. Denk bijvoorbeeld aan een binding met een toestemmingslaag en varianten die in de laag kunnen spelen. Hiermee wordt het Edukoppeling OAuth-profiel dan “conformant”.
Gerald Groot Roessink merkt op dat in zijn ogen het OAuth-profiel binnen Edukoppeling toegepast wordt op het bestaande toepassingsgebied van Edukoppeling waarbij de user (mens) niet rechtstreeks binnen de flow toestemming geeft. De bredere context van NL GOV leidt niet tot verbreding van hdit toepassingsgebied.

[9] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Architectuur/ (werkversie)
[10] NL GOV Assurance profile for OAuth 2.0 (logius-standaarden.github.io) (werkversie)
[11] NLGov REST API Design Rules (logius-standaarden.github.io) (werkversie)

Een ander alternatief is dat er (initieel) een consistant Edukoppeling Secure API OAuth profiel wordt opgesteld. Consistant wil zeggen dat er overlap is tussen het Edukoppeling Secure API OAuth profiel en het NL GOV OAuth profiel, en binnen die overlap is het Edukoppeling Secure API OAuth profiel conform het Secure API OAuth profiel, de overlap is echter niet volledig. Sommige specificaties van het NL GOV OAuth profiel zijn niet overgenomen, en het Edukoppeling Secure API OAuth profiel bevat onderdelen die niet door het NL GOV OAuth profiel worden gedekt.
Bij dit alternatief gaan we het NL GOV OAuth profiel beperken. Logischerwijs gaat dan ook de Edukoppeling Architectuur versie 3.0 afwijken van de Kennisplatform API's architectuur. Het is in deze fase wellicht onwenselijk om een dergelijke keuze te baseren vanuit wensen voor enkel het OAuth profiel zonder het bredere perspectief van de architectuur te beschouwen. Verder geeft het NL GOV OAuth profiel aan dat een dergelijk Edukoppeling profiel tot implementaties kunnen leiden die niet compliant zijn. Daarnaast heeft Digikoppeling in de roadmap het opstellen van Best Practices voor het NL GOV OAuth profiel staan. Er is een kans dat daarin uiteindelijk andere keuzes worden gemaakt.
Ondanks het architectuurperspectief van het Kennisplatform dat Edukoppeling wil omarmen kan het zijn dat ketensamenwerkingen wel een nadere inperking van het Edukoppeling cq NL GOV OAuth-profiel wordt opgenomen in de afspraken die voor die ketensamenwerkingen worden opgesteld. Het is echter nu nog onduidelijk om welke inperkingen dit allemaal zou gaan en of het mogelijk alleen om een handleiding gaat om ketenpartijen bij implementaties te ondersteunen. Als een ketensamenwerking wel een inperking opneemt in de afspraak dan wordt in een "explain" nader aangegeven welke inperkingen en het waarom ervan uitgelegd. Dit zou naderhand ook weer ingebracht kunnen worden bij de Edukoppeling werkgroep om eventuele impact te bepalen. Bepaalde ketensamenwerkingen (Koen Voermans noemt Edu-V als concreet voorbeeld) zouden inderdaad de keuzes die NL GOV OAuth biedt willen inperken voor implementerende partijen. Grotere partijen zullen met hun integratieplatform veelal geen problemen hebben om meerdere configuraties te ondersteunen. Edwin Verwoerd heeft van tevoren aangegeven dat zij binnen de kaders van NL GOV flexibel willen zijn omdat zij in meerdere ketensamenwerkingen dan alleen Edu-V participeren. Maar dat geldt niet voor veel kleinere partijen.
Koen vraagt zich af of wat hij voorziet voor Edu-V qua keuzes[12] wellicht in het onderwijsveld breder gedragen wordt en of we met het OAuth-profiel niet op het uitgangspunt 3c moeten gaan zitten: (initieel) een consistant Edukoppeling Secure API OAuth profiel. Gerald Groot Roessink geeft aan dat hij dit op zich ook wel als een mogelijk alternatief ziet en dat hij dit vanuit het perspectief van DUO graag zou willen verkennen samen met de twee groeifondsprogramma's Edu-V en Npuls, met als doel een ketensamenwerkingsoverstijgende keuze voor de werkgroep Edukoppeling te maken, zodat ketenpartners in die ketensamenwerkingen zonder keuzestress een implementatie kunnen doen. Erik Borgers geeft aan dat de flexibiliteit van NL GOV OAuth-profiel aan de ene kant prettig is omdat de bredere scope meerdere implementaties toestaat maar hij begrijpt ook de argumenten waar Koen en Gerald mee komen. Brian Dommisse merkt op dat als we als werkgroep op voorhand de keuze voor het inperken van het OAuth-profiel willen omarmen, dat dit een breed gedragen standpunt moet zijn. Ook vanuit het ho (OOAPI) en mbo (OKE) zou hij graag zien dat zij meewerken aan die verkenning. Patrick van der Veer wordt gevraagd of hij mensen kan leveren die hier een bijdrage aan willen leveren.

Besluiten:

1. Binnen de werkgroep kan geen consensus worden gemaakt rond de (initiële) mate van compliance. Er wordt afgesproken dat de leden de achterban consulteren of en welke inperkingen nu noodzakelijk worden geacht. Een verkenning welke keuzes* (inperkingen op het NL GOV profiel) voor het Nederlandse onderwijsveld mogelijk relevant zijn wordt op korte termijn uitgevoerd door Edu-V, DUO en Npuls/SURF (OOAPI/OKE). Als hier (nog) geen unaniem besluit kan worden genomen, dan zal binnen de Edu-V ketensamenwerking met het oog op de implementaties in het najaar zelf al een keuze maken. Voor Edukoppeling zou dit betekenen dat een fully conformant Secure API Oauth profiel ons vertrekpunt wordt voor het opstellen van de specificaties voor het onderwijs.

* Keuzes kunnen onder meer gemaakt worden op de volgende vlakken[13]

[12] https://www.edustandaard.nl/app/uploads/2024/03/20240222-Memo-Architectuurraad-Edu-V-iz-Edukoppeling-REST-OAuth-profielen.pdf
[13] We willen benadrukken dat NL GOV OAuth (werkversie) nog in beweging is en dat de keuzes dus nog kunnen wijzigen

- Use case authorization code flow[14] en betreffende clients uitsluiten. Hiermee wordt in het Edukoppeling Secure API OAuth profiel dan alleen de use case client credentials[15] en bijbehorende direct acces clients[16] ondersteund.
- Client authenticatie[17] op basis van enkel mTLS/X.509[18] of op basis van private_key_jwt method.
- Het toepassen van enkel X.509 (self-signed) certificaten of PKIo certificaat. Het nog niet vastgestelde wijzigingsvoorstel[19] heeft het over een X.509 certificaat, maar over het algemeen stelt[20] het NL GOV profiel dat als de rollen niet in beheer zijn bij dezelfde organisatie dat er dan PKIo certificaten gebruikt moeten worden. In de Edukoppeling architectuur gaan we uit van een ketensamenwerking en gaan we er dus vanuit dat NL GOV OAuth voor onze context de toepassing van PKIo vereist. Afwegingen:
    - Self-signed X.509 certificaten bieden flexibiliteit en lijken[21] beter interoperabel met RFC8705.
    - PKIo biedt een betrouwbare identiteit waarmee alle ketenpartners een bepaalde ketenpartij kunnen identificeren.

3.4. Het Edukoppeling Secure API REST profiel wordt fully conformant aan de API Design Rules.

In het bestaande Edukoppeling REST/SaaS-profiel 1.0 staat de eerdere gepubliceerde versie van de API Design Rules[22] centraal. Als onderdeel van de Edukoppeling Architectuur versie 3.0 zal er echter wel een nieuwe versie van het REST profiel moeten komen. Zoals al eerder besproken in de werkgroep krijgt het profiel een nieuwe naam, Secure API REST profiel. Daarnaast zal het nieuwe Edukoppeling Secure API REST profiel refereren naar de Digikoppeling Koppelvlakstandaard REST-API[23] die ondertussen beschikbaar is gekomen met hierin de nieuwe versie van de API Design Rules. Het Edukoppeling Secure API REST profiel wordt hiermee fully compliant aan de API Design Rules. Verder is het Digikoppeling Koppelvlakstandaard REST-API in ontwikkeling (zie Digikoppeling roadmap[24]) en het is de verwachting dat de Digikoppeling OAuth Best Practices en Federated Services Connectivity[25] een (verplicht) onderdeel worden van dit profiel. Het Digikoppeling REST profiel migreert dus mogelijk naar een OAuth profiel.

Besluit: De werkgroep is unaniem in het onderschrijven van dit uitgangspunt.

4. Voorstel publicatie van nieuw compliance document

Aan dit agendapunt komt de werkgroep niet meer toe. Bij de bespreking van uitgangspunt 1 onder agendapunt 3 is al onderkend dat er een einddatum aan het WUS-profiel wordt toegevoegd. In een volgend overleg moeten we die concreet maken en ook kijken naar de andere profielen en onderdelen van Edukoppeling.
Het WUS-profiel zal in ieder geval op basis blijven van de Edukoppeling architectuur 2.0.

[14] https://logius-standaarden.github.io/OAuth-NL-profiel/#use-case-authorization-code-flow
[15] https://logius-standaarden.github.io/OAuth-NL-profiel/#use-case-client-credentials-flow
[16] https://logius-standaarden.github.io/OAuth-NL-profiel/#direct-access-client
[17] https://logius-standaarden.github.io/OAuth-NL-profiel/#requests-to-the-token-endpoint
[18] De optie van mTLS/X.509 is nog niet in de werkversie van 24 februari 2024 verwerkt (**Fout! Verwijzingsbron niet gevonden.**).
[19] **Fout! Verwijzingsbron niet gevonden.**
[20] 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*." en bij Connections with protected resources: "*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 for encryption*."
[21] Er zijn geen ervaringen bekend met het gebruik van RFC8705 en PKIo. Er lijkt een kans te bestaan dat platformen van de RFC het gebruik van PKIo niet standaard ondersteunen (subject.serial met OIN).
[22] REST-API Design Rules (Nederlandse API Strategie IIa) 1.0 (logius.nl)
[23] Digikoppeling Koppelvlakstandaard REST-API (logius-standaarden.github.io) (werkversie)
[24] **Fout! Verwijzingsbron niet gevonden.**
[25] **Fout! Verwijzingsbron niet gevonden.**