edustandaard

Verslag Edustandaard werkgroep Edukoppeling

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

Datum en locatie
22 april 2024, 09:00-11:00 uur
Locatie: Teams

1. Opening, mededelingen en vaststellen agenda
2. Voorstel publicatie conceptversie met compliance document (uitfasering WUS-profiel)
3. Bespreking Edukoppeling Secure API OAuth profiel
4. Rondvraag / Sluiting

1. Opening, mededelingen en vaststellen agenda

Gerald stelt voor om met agendapunt 3 te beginnen omdat hij om 10:30 het overleg moet verlaten. Omdat Edwin pas om 09:30 kan aanschuiven wordt besloten om toch met agendapunt 2 te starten omdat dit waarschijnlijk niet te veel tijd in beslag neemt.

Maarten meldt dat hij vanuit SBB nog geen input heeft gegeven en wil alvast melden dat in SBB-ketens er private partijen zijn die niet over een PKIo (met OIN) willen/kunnen beschikken. Dit wordt verder bij agendapunt #3 besproken.

2. Voorstel publicatie conceptversie met compliance document

We hebben eerder afgesproken dat we in een nieuwe versie van het *Overzicht actuele documentatie en compliance* willen gaan aangeven tot welke datum (naar verwachting) een (normatief) document (specificatie van een profiel, architectuurdocument etc.) in beheer blijft. In het bijzonder willen we aangeven dat we naar REST-standaarden bewegen en als driver de API-strategie hebben gekozen waardoor we WUS (SOAP/WSDL) feitelijk niet meer past daarbinnen en dat we stoppen met het actief beheren van dit profiel. Alle leden zijn het erover eens dat met name rond WUS het wenselijk is om aan te geven dat die aan het einde van zijn “levenscyclus” als afspraak binnen het onderwijs is en dat het niet raadzaam meer is om nieuwe implementaties ermee te starten.
Vanuit DUO wordt aangegeven dat zo’n signaal vanuit Edustandaard door hen een trigger is om in het life cycle management van hun voorzieningen de uitfasering te gaan opnemen.

Over het moment wordt gesteld dat het goed is om dit te doen als er een alternatief is en dat het e.e.a. onder architectuur geborgd is. Momenteel is er in principe al een alternatief met de aanwezigheid van een REST-profiel. Er is echter nog geen nieuwe architectuur. Er wordt besloten om alle nieuwe en aan te passen normatieve documenten als bundel te publiceren waaronder de nieuwe Edukoppeling architectuur (3.0). De huidige planning is dat dit januari 2025 wordt. Derhalve zal het WUS-profiel vanaf januari 2025 niet meer worden ondersteund (status: ”Einde ondersteuning”). Aankondiging hiervan zal wel al via de webpagina (bij Ontwikkelingen) worden opgenomen inclusief het advies om niet meer nieuwe implementaties te starten.
In de volgende releases van Edukoppeling (Architectuur versie 3.0) zal dus ook geen WUS-profiel meer opgenomen worden. Welke profielen onderdeel vormen van de architectuur

versie 3.0 gaan we de komende periode vaststellen. Naar verwachting is dit in ieder geval een Secure API OAuth profiel.

Besluit:

- De voorgestelde datums in het compliance-document worden geaccepteerd (met de kanttekening dat we die periodiek moeten behandelen en bepalen of daar aanpassingen in nodig zijn)
- 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 plus een advies om geen nieuwe implementaties te starten met dit profiel.

3. Bespreking Edukoppeling Secure API OAuth profiel

Tijdens het afgelopen overleg is er geen besluit genomen in hoeverre een Edukoppeling Secure API OAuth profiel (initieel) compliant moet zijn aan het NL GOV OAuth profiel. De leden hebben de achterban geconsulteerd en er wordt besproken welke inperkingen nu noodzakelijk worden geacht en of we daar consensus over kunnen bereiken.

Vanuit Edu-V wordt aangegeven dat het NL GOV OAuth profiel een bredere context heeft dan enkel M2M uitwisselingen. Het is wenselijk om de context die voor Edu-V geldt nader te specificeren. Het gaat dus niet zozeer om het inperken van de standaard maar beschrijven van de context en voorkeuren. Vanuit BES wordt aangegeven dat er in eerste instantie een best practice opgesteld kan worden die naar de nog te publiceren vastgestelde 1.1 versie van het NL GOV OAuth profiel verwijst en aangeeft welke keuzes er gemaakt zijn rond een M2M uitwisseling binnen Edu-V (en mogelijk ook andere contexten/ketensamenwerkingen). Wat Edu-V betreft gaat het dan om closed data, direct access clients, het gebruik van een private-key-jwt voor client authenticatie, geen dynamic client registration vereisen en PKIo voor identificatie (OIN) en authenticatie van rechtspersonen. Of het uiteindelijk op te stellen Edukoppeling OAuth-profiel ook een vorm van toestemming door de onderwijsorganisatie ondersteunt (zoals bijvoorbeeld mandateren van een verwerker door eindorganisatie dat ook het huidige WUS en REST profiel i.c.m. met een mandaatregister ondersteunen) gaan we de komende periode verder vaststellen, maar de voor Edu-V gewenste OAuth best practice op basis van NL GOV OAuth versie 1.1 zal hier nog geen uitspraken over doen.
Vanuit DUO wordt aangegeven dat er bij hen wel urgentie is rond ook dit vraagstuk. Het is wenselijk dat in de uitwisseling met Facet door mbo-instellingen op basis van OKE de partijen rond dit punt op 1 lijn zitten. Wat de keuzes bij OKE zijn voor zowel de m2m-invulling en voor de wijze waarop toestemming moet worden geregeld is bij geen van de aanwezige werkgroepleden bekend. DUO gaat dit direct met hen opnemen is het advies en kan vanuit de ketenvoorziening Facet hier zelf ook eisen aan stellen die deels bouwen op bijv. de best practice voor het OAuth-profiel en deels op de wijze waarop op dit moment voor deze voorziening (en andere DUO-voorzieningen) de toestemming nu is geregeld.

De huidige werkversie van het NL GOV OAuth profiel ondersteunt nog geen client authenticatie op basis van mTLS. Het is echter de verwachting dat versie 1.1 van het NL GOV OAuth profiel dit wel zal bevatten (op basis van RFC8705). Mede omdat hiermee een access token aan het certificaat dat de client gebruikt “gebonden” kan worden.
Door Gerald wordt aangegeven dat mTLS voor client authenticatie een onwenselijke ontwikkeling is en Gerald gaat proberen hierop bij te sturen. Als mTLS toegepast kan worden bij het client credentials profiel voor client authenticatie dan is de keuze voor private-key-jwt wenselijk omdat men voorziet dat de toepassing van mTLS meer problemen oplevert. Zeker in combinatie met PKIo. De omvang van dit probleem is afhankelijk van de toegepaste architectuur. Zo kan het voor een partij lastig zijn om standaardsoftware te gebruiken als

mTLS en PKIo toegepast wordt. Robert nuanceert dit punt omdat het in de meeste gevallen prima te doen is (DUO doet het nu immers ook) alleen vindt hij wel dat je dit alleen toe moet passen indien nodig.
Bovendien acht hij dat als authenticatie op basis van mTLS nog niet in de standaard (werkversie) staat, we het dan niet zouden moeten toepassen. Vooruitlopen hierop is risicovol.

Verder is het NL GOV OAuth profiel bedoeld voor het publieke domein (G2G). Vindt er namens een school (een publiekrechtelijk orgaan) gegevensuitwisseling plaats dan valt dit onder het werkingsgebied van NL GOV OAuth en het daarvan nog op te stellen afgeleide profiel binnen Edukoppeling. Binnen Edu-V en ook andere ketensamenwerkingen worden ook (bedrijfs)gegevens tussen private ketenpartners uitgewisseld. Het is goed om deze nuance in het werkingsgebied te onderkennen. Het gaat er dan om dat werkingsgebieden expliciet benoemd zijn en dat men hierin ook het mandaat heeft, dat daar waar (bedrijfs)gegevens door ketenpartijen namens zichzelf uitgewisseld worden zij dus een keuze hebben. Waarbij het niet uitgesloten hoeft te zijn dat zij de voorkeur geven ook hiervoor aan te sluiten op nationale onderwijsstandaarden. De randvoorwaarde is dan wel dat hierin de juiste keuzes worden gemaakt.
De internationale context speelt in het hoger onderwijs (bij o.a. de diensten van SURF). De werkgroep bespreekt of een nationaal onderwijsprofiel en een internationaal profiel wenselijk is. Of en hoe zal echter later besproken worden bij de uitwerking van de 3.0 versie van de architectuur. Verder is het wenselijk om de standaardisatieraad en architectuurraad de vraag (actiepunt #125) voor te leggen hoe er naar het werkingsgebied van Edukoppeling gekeken wordt. Gaat dit altijd enkel om koppelingen en gegevensuitwisseling tussen Nederlandse ketenpartners binnen het Nederlands onderwijs of geldt het ook voor koppelingen vanuit het Nederlandse onderwijs met internationale/Europese partners? NB dit punt is wel al ingebracht in de Architectuurraad van 18 april 2024 maar er is toen geen besluit of standpunt geformuleerd (zie de Notulen Architectuurraad 2024-04-18).

Een ander punt van discussie is dat gegevensuitwisselingen steeds internationaler worden en dat het gebruik van PKIo hier gaat wringen. Nog los van het feit dat partijen het als lastig ervaren om een PKIo-certificaat aan te vragen zoals ook al eerder door SBB is aangegeven. PKIo heeft het voordeel dat het proces rond de aanvraag van het certificaat zo georganiseerd is dat het OIN een betrouwbare en gestandaardiseerde identifier voor rechtspersonen vormt. In hoeverre dat voordelen oplevert hangt samen met hoe een bepaalde ketenpartij deze processen zelf al heeft georganiseerd voor de eigen dienstverlening. Bij dergelijk “beperkt” gebruik levert PKIo dan ook minder voordelen op. In complexe ketensamenwerkingen echter (waarvan Edu-V er eentje is) is het alternatief dat ketenpartners zelf dergelijke processen moeten inrichten voor als er geen PKIo wordt gebruikt. Voor ketenpartners die in meerdere ketensamenwerkingen opereren is de meerwaarde van een overkoepelend PKIo zelfs nog groter. De kosten voor het aanschaffen worden door diverse werkgroepleden als niet blokkerend ervaren (600 euro voor 3 jaar). PKIo levert wel extra kosten op als men voor de hele OTAP-straat verschillende certificaten wil aanschaffen. Dat hier mogelijk wijzigingen op gaan komen hoe hier mee om te gaan is wel onderwerp van gesprek, maar zeker nog niet praktijk.

Besluiten:

- Voor Edukoppeling zijn best practices voor het NL GOV OAuth profiel vereist. De best practices worden opgesteld op basis van de nog te publiceren NL GOV OAuth 1.1 versie.
- Als de 1.1 versie niet voor de volgende werkgroepbijeenkomst beschikbaar is kan er wel een eerste conceptversie van de best practices worden besproken die aansluit op de keuzes die nu door de werkgroepleden als plausibel zijn beschouwd. Het idee is dat we dan sneller tot een conceptpublicatie kunnen overgaan van deze best

practices als eenmaal versie 1.1 van het NL GOV OAuth profiel beschikbaar komt, zonder te wachten tot de hele bundel gereed is.

Onderwerpen voor de volgende keer:

- Best practice op basis van NL GOV OAuth profiel.
- Eerste aanzet voor de uitwerking van de ROSA architectuurkaders rond ontwerpgebieden technische interoperabiliteit en M2M i.c.m. versie 3.0 van de Edukoppeling architectuur.

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	Q4 2024	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.	Q4 2024	BES	2
121	Besluiten of we Architectuur 1.2.2, I&A 1.0 en WUS 1.3 verlengen of niet meer ondersteunen. Daarna opstellen nieuw compliancedocument.	Agendapunt #2, 22 april 2024, afgerond	Q2 2024	WG	2
123	Wat betekent API-strategie voor Edukoppeling (en AR)	Afgerond (uitgangspunt feb 2024)	Q2 2024	WG	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	Q3 2024	Brian	2
126	Onderbouwing voor opname onderwijsaanbieder in het I&A document	Actie samenvoegen met #94,	Q4 2024	Gerald / Brian	2
127	Logius verzoeken Onderwijsaanbieder met prefix op te laten opnemen in de OIN matrix	Actie samenvoegen met #94,	Q4 2024	Gerald / Erwin	2
128	Opstellen Best practice op basis van NL GOV OAuth profiel 1.1	Voor de volgende werkgroepbijeenkomst	Q2 2024	BES	1

BES = Bureau Edustandaard
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[1] 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. De best practices worden opgesteld op basis van de nog te publiceren NL GOV OAuth 1.1 versie. Als de 1.1 versie niet voor de volgende werkgroepbijeenkomst (juni 2024) beschikbaar is kan er wel een eerste conceptversie van de best practices worden besproken die aansluit op de keuzes die door de werkgroepleden als plausibel zijn beschouwd. Die best practice kan gepubliceerd worden als versie 1.1 van het NL GOV OAuth profiel beschikbaar komt, zonder te wachten tot de hele bundel gereed is.	22-4-2024

NB voor de voorgaande besluiten zie:
https://www.edustandaard.nl/app/uploads/2022/10/2022-06-29-Verslag-Edustandaard-Werkgroep-Edukoppeling.pdf

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