edustandaard

Verslag Edustandaard werkgroep Edukoppeling

Aanwezig:	Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)
Gastleden:	-
Afwezig	Erik Borgers (Kennisnet, OSR), Joël de Bruijn (MBO Digitaal), Patrick van der Veer (SURF)
Agendalid:	Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie
2 oktober, 10:00-13:00 uur
Locatie: Bar Beton, Perron 4/5, Amersfoort CS

Agenda:

1. Opening / mededelingen / Verslag van 3 september 2024
2. Terugkoppeling requirements iz toestemming verlenen
3. Uitgangspunten voor nieuwe Edukoppeling architectuur
    a. Te maken keuzes ten aanzien van de architectuur en profielen
    b. Actiepunt #131: overzicht OAuth-initiatieven en hun karakteristieken
4. wvttk

1. Opening, mededelingen en verslag van 3 september 2024

Mededelingen:

- Brian meldt dat BES een RFC vanuit Edu-V heeft ontvangen om de Edukoppeling OAuth Best Practices aan te passen. Deze RFC en een daarop aangepaste 1.1 conceptversie van de OAuth Best Practice worden tijdens de bijeenkomst in november besproken.

Verslag vorige bijeenkomst:

- Gerald heeft in het verslag een opmerking geplaatst bij requirement #0. Of toestemming expliciet nodig is in alle scenario's moet nog besproken worden. Gerald geeft aan dat DUO dit nu administratief (impliciet) heeft geregeld. Bij de uitwerking van de architectuur, de ROSA ontwerpkaders en IV-domein M2M moet duidelijk worden of expliciete toestemming voor alle scenario's gaat gelden.
- Bij vervolgacties heeft Gerald het volgende opgenomen: "*Niet aan toegekomen: De kwestie van de claim-definitie van het Access Token. Bijvoorbeeld doen we dat als FSC? Daar is al een claim-definitie gemaakt waarin alle contractpartners (verantwoordelijk en verwerker, client- en serverzijde) opgenomen kunnen worden*". Dit zien we inderdaad als een vervolgactie, maar kan als onderdeel worden gezien van de doorontwikkeling van de nieuwe architectuur en profielen.
- Bij agendapunt #5[1] wordt aangegeven de tekst te wijzigen: *DUO streeft echter naar verdere standaardisatie en een eenduidig profiel met bijvoorbeeld een keuze door de werkgroep voor één bepaalde vorm van client authenticatie (mTLS of private-key-jwt)*. Het gaat erom dat het duidelijk is dat dit een keuze van de werkgroep is. Niet een keuze bij implementatie.

[1] Overwegingen DUO bij verlenen toestemming ihkv Edukoppeling

Het verslag wordt op betreffende punten aangepast.

Patrick van der Veer heeft een suggestie voor een tekstaanpassing gedaan:

- OKE/OKX gaat voor de integratielaag aansluiten op het nieuwe afsprakenstelsel van Edukoppeling.

Veranderen in:

- OKE/OKX gaat voor de integratielaag aansluiten op de OOAPI standaard (die hier niets over voorschrijft). Voor implementaties van de OKE standaard zal OKE - buiten de standaard om - een leidraad beschrijven voor de integratielaag.

NB hierover zal nog nader contact zijn tussen MBO Digitaal en Patrick.

2. Terugkoppeling requirements iz toestemming verlenen

Er wordt aangegeven dat een (ROSA/Edukoppeling) kerngroep de eerder besproken requirements verder gaat uitwerken als onderdeel van de doorontwikkeling van ROSA ontwerpgebieden en IV-domeinen. Daarnaast gaan ze gelden als kader voor de nieuwe Edukoppeling architectuur.

Een aantal requirements worden inhoudelijk besproken. Een belangrijke basis voor de requirements zijn eenduidige definities. Zo is nu niet duidelijk wat onder ‘uitwisselen’ wordt verstaan. Het voornemen is om bij definities zoveel mogelijk aan te sluiten bij de NORA, GDI en ROSA. Als daar geen passend begrip beschikbaar is definiëren we die zelf en laten die dan opnemen in het ROSA Begrippenkader. Het kan ook zijn dat we een iets andere definitie willen toekennen aan een bestaand begrip. Ook dat leggen we terug bij het begrippenkader waar we ons op gebaseerd hebben.

Over requirement #0 wordt gevraagd of dit, informatieclassificatie/dataclassificatie, relevant is. Gaan we er niet vanuit dat het altijd om vertrouwelijke gegevens gaat en dat toestemming altijd nodig is? Er wordt aangegeven dat dit onderdeel van de discussie is. Ter ondersteuning van deze discussie is ook een memo opgesteld (volgende agendapunt). Vooralsnog lijken de leden consensus te hebben dat er altijd sprake is van vertrouwelijke gegevens en dat toestemming altijd nodig is. Als we hierop uitkomen dan kan bij de impact opgenomen worden dat het profiel (of profielen) altijd er vanuit gaan dat vertrouwelijke gegevens uitgewisseld worden.

Requirement #1 wordt aangepast naar: *Toestemming wordt gegeven via het opstellen en ratificeren van een contract door de betrokken gezagsdrager~~(s)~~ en dienstverlener(s).*

Requirement #4 wordt aangepast naar: ‘*Contractanten zijn in het maatschappelijk verkeer altijd eenduidig herleidbaar naar een rechtspersoon’*

Voor #4 kunnen de volgende requirements als implicatie geclassificeerd worden:

- #8 ‘*Ketenpartners (onderwijsorganisaties, hun dienstverleners én uitvoeringsorganisaties) gebruiken in Nederland hetzelfde identificatieschema: In Digikoppeling en Edukoppeling worden organisaties geïdentificeerd met een OIN (sinds 2017). ’*
- *#9 ‘Ketenpartners (onderwijsorganisaties, hun dienstverleners én uitvoeringsorganisaties) gebruiken in Europa hetzelfde netwerk van identificatieschema's: EU accepteert diverse internationaal gebruikte schema's waaronder OIN in NL. Dat netwerk heet EAS.’*
- *#? Buiten de EU maken ketenpartners een eigen keuze welk identificatieschema gebruikt wordt.*

Er wordt verder aangegeven dat het wenselijk is om inzicht te krijgen in de versie van Edukoppeling die in een bepaalde keten toegepast wordt en gaat worden. Hierover hebben we het in de werkgroep al eerder gehad en is ook al eerder in de Architectuurraad besproken. Het is echter lastig om deze wens binnen de huidige Edustandaard-processen adequaat te ondersteunen. Wel zien we ontwikkelingen hiertoe bij de Groeifondsprogramma's. Het kan dus zijn dat dit uiteindelijk binnen die programma's en de daaruit voortvloeiende gremia geregeld wordt maar de scope van Edukoppeling is groter. Er wordt voorgesteld dat leden de behoeften kenbaar maken bij hun vertegenwoordigers in de Architectuurraad en Standaardisatieraad.

3. Uitgangspunten voor nieuwe Edukoppeling-architectuur

Voor het derde agendapunt is een memo opgesteld: 'Memo kaders voor nieuwe Edukoppeling architectuur'. Naast een overzicht met OAuth-initiatieven en hun karakteristieken (agendapunt 3b) zijn in de memo ook de volgende discussiepunten opgenomen:

1. Biedt het nieuwe informatie-uitwisselingsmodel de juiste aandachtsgebieden om op hoog niveau tot een structuur voor de architectuur te komen?

2. Gaan we uit van een flexibele architectuur die meerdere communicatiekanalen ondersteunt, of een specifiek M2M kanaal waarin andere keuzes kunnen worden gemaakt dan bij andere (bijvoorbeeld H2M) kanalen?

3. Sturen we op één M2M profiel of zijn er verschillende (sub)profielen die toegepast moeten worden voor een bepaalde context?

Als eerste wordt het nieuwe informatie-uitwisselingsmodel besproken. Dit model is bedoeld om structuur te bieden bij de verschillende aandachtsgebieden die in de nieuwe architectuur opgenomen worden. In deze versie wordt benadrukt dat we in de architectuur verschillende aspecten eerst op een abstract niveau functioneel willen beschrijven. Vervolgens kan er dan waar mogelijk verwezen worden naar standaarden die hier (binnen de betreffende versie van de architectuur) invulling aan geven. Zo kunnen we bijvoorbeeld toestemming eerst functioneel beschrijven en verwijzen naar verschillende inrichtingsvarianten zoals OSR mandaten en FSC contracten. Deze opzet lijkt een goede basis voor de nieuwe architectuur. Ook de opname van een Toestemmingslaag in het model lijkt wenselijk. Het is alleen nog niet duidelijk of deze verticaal (haaks op de overige lagen) moet staan. Het uiteindelijke model wordt als onderdeel van de architectuur verder ontwikkeld.

Bij de proceslaag is het concept van een scenario opgenomen vanuit de gedachte dat de ketensamenwerking bepaalde interactiekarakteristieken heeft die te mappen zijn op een interactiemodel. In de gegevenslaag is het concept van een informatieclassificatie opgenomen om aan te geven dat de gegevens die binnen het proces (processtap) uitgewisseld moeten worden geclassificeerd worden om tot de keuze van een passend Edukoppeling-profiel te komen. De bespreking van deze concepten raakt het bovenliggend vraagstuk of we 1 of meerdere profielen onderkennen. Het is tenslotte zo dat als er vanuit 1 profiel geredeneerd wordt, de proceseigenschappen en gegevenstypen dan niet relevant zijn (er is geen beslisboom om tot een profiel te komen). Dit vanuit de gedachte dat dat ene profiel altijd toegepast kan worden en voldoende veilig is.

Het idee achter het memo is om eerste de kaders en functies te benoemen en dan naderhand pas te concluderen hoeveel profielen er nodig zijn. Het nu plat slaan van deze

discussie leidt er toe dat we geen goede onderbouwing hebben hoe we tot dat ene profiel met betreffende beveiligingsmaatregelen zijn gekomen en in hoeverre dat voor het hele onderwijs toegepast kan worden binnen het betreffende functionele toepassingsgebied. Er wordt besloten om deze discussie op een later moment te voeren. De prioriteit wordt gegeven om op korte termijn tot 1 profiel te komen dat ook op korte termijn toegepast kan worden. Er wordt voorgesteld om dan de huidige OAuth Best Practices hiervoor te gebruiken. Deze zullen worden aangepast op de wijzigingsvoorstellen vanuit Edu-V.

Daarnaast wordt volgende keer het voorstel van Gerald rond de toestemmingsclaim in het access token besproken. We verwachten zo voor het einde van het jaar in ieder geval een nieuwe versie van de OAuth Best practices op te kunnen opleveren. Daarna pakken we de ROSA kaders, Edukoppeling Architectuur en profielen weer op.

4. Wvvtk

Er waren verder geen mededelingen.

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
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	Q4 2024	Brian	2
130	Edukoppeling FAQ uitbreiden met vragen uit de Edu-V keten en de antwoorden vanuit NL GOV/EK WG	Loopt		BES	2
131	Overzicht met verschillende (internationale/nationale) initiatieven en hoe deze zich tot elkaar verhouden	Afgerond		BES	1

132	Voorstel tav de toestemmingsclaim in het access token	Voor werkgroep 6 november om te bespreken	Q4	Gerald	1

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

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

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