edustandaard

Agenda Edustandaard werkgroep Edukoppeling

Leden:	Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Erik Borgers (Kennisnet, OSR), Brian Dommisse (Bureau Edustandaard, voorzitter), Erwin Reinhoud (Bureau Edustandaard, standaardisatie-expert)
Gastleden:	Edwin Kense (Basispoort), Koen Voermans (Edu-v)
Agendalid:	Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie
Woensdag 24 mei 2023, 13:00-15:00 uur
Locatie: online

1. Opening, mededelingen, vaststellen agenda
2. Toelichting op uitkomsten afstemming Architectenraad Edu-v (door Koen Voermans)
3. Globale opzet van de uit te werken profielen (op basis van discussie 8 mei en input vanuit Edu-v)
4. Afronden MDX Secure API OAuth profiel versie 0.3 (zie map van de bijeenkomst)
5. Afronden MDX OSR protocol versie 0.8 (zie map van de bijeenkomst)
6. Discussie over de uit te werken extra profielen en de te nemen vervolgstappen
7. Rondvraag / Sluiting

Alle stukken staan in de MS-teams omgeving van Edukoppeling en wel in: 2023-05-24 bijeenkomst mei (2).

Ad 1 Opening/vaststellen agenda
Vorige keer zijn we vooral ingegaan op de input en requirements die vanuit Edu-v en Basispoort waren ingebracht. Aan het eind hebben we toen het volgende afgesproken:

- We maken het OAuth MDX-profiel nu zover mogelijk af en publiceren dit als concept voor openbare review. Uiteraard hoort hier ook een aanpassing van de overkoepelende Edukoppeling-architectuur.
- We verzamelen de functionele behoeften voor een niet-MDX-profiel en gaan als werkgroep hier ook een uitwerking voor maken. Formeel zal hier wel een go vanuit de Architectuurraad voor nodig zijn, maar dat is een formaliteit, dat we de werkgroep Edukoppeling hier het beste handen en voeten aan kan geven was voor alle aanwezigen maandag wel duidelijk.
- We gaan parallel onderzoeken of er naast het werken met certificaten ook een invulling van het veilig m2m-verkeer is dat op een andere wijze aan dezelfde betrouwbaarheidseisen voldoet.

Deze meeting van 24 mei gaat in op het zover mogelijk afronden van het MDX OAuth-profiel en het MDX OSR-protocol enerzijds en het verkennen welke profielen en andere zaken verder nog dienen te worden uitgewerkt. Uiteraard zal daarna (liefst tegelijkertijd) ook de overkoepelende architectuur nog aangepakt moet worden.

In de tussentijd is de Architectenraad van Edu-v bij elkaar gekomen en dat heeft geleid tot aanvullende wensen en besluiten die in agendapunt 2 zullen worden toegelicht en die voor de vervolgstappen waardevolle input vormen.

Ad 2 Toelichting op uitkomsten afstemming Architectenraad Edu-v
Koen Voermans neemt de werkgroep mee in de uitkomsten van de behandeling n de architectenraad van Edu-v ten aanzien van de uitgangspunten en wensen voor het uitwerken van profielen.
De uitkomsten van de discussie in de werkgroep Edukoppeling op 8 mei waren helder. Op basis daarvan is besloten in de Architectenraad Edu-v dat ze het PKI overheidscertificaat en mTLS voor de identificatie en authenticatie ook overnemen in het architectuurkader. Edu-v gaat in de POC ervaring hiermee op doen en ervaren of er zwaarwegende argumenten zijn vanuit leveranciers om hier vanaf te wijken.

Dit betekent dat wat Edu-v betreft nu geen prioriteit hoeft te liggen op het verrichten van onderzoek naar een alternatief voor certificaten. Ook zelf uitgegeven certificaten zijn voor Edu-v als optie afgevallen.
Wel is er een uitdrukkelijke wens om profielen te ontwikkelen voor uitwisselingen van gegevens die niet vertrouwelijk zijn, zowel gegevens die namens een onderwijsbestuur (“school”) worden uitgewisseld als tussen leveranciers onderling.
Bovendien zijn er nog vragen over mandateren (vanuit een bestuur) in relatie tot het geven van consent (vanuit een onderwijsaanbieder).

Ad 3 Opzet van de uit te werken profielen
Op basis van de input die verkregen is uit de architectenraad Edu-v zal Erwin Reinhoud een poging doen om een uitwerking voor profielen op een hoogover niveau te schetsen. Als we het op hoofdlijnen eens hierover zijn, dan kunnen we starten met de benodigde vervolgstappen. Die zijn als agendapunt 6 geagendeerd, omdat we eerst de inhoudelijke bespreking van het MDX-profiel en -protocol willen afronden.

Ad 4 Afronden MDX Secure API OAuth profiel v0.3
Het afronden van het MDX-profiel is een van de vervolgstappen. De 0.3 versie van het OAuth-profiel hebben we vorige keer niet inhoudelijk doorgelopen. Dat zullen we dit keer wel moeten doen zodat we een volgende versie kunnen opleveren die we idealiter als concpet ook op Edustandaard gaan publiceren voor openbare consultatie. Er zitten de volgende belangrijke wijzigingen ten opzichte van versie 0.2[1]:

1. Client authenticatie (bij token endpoint van de authorization server) wordt nog steeds ondersteund met een JWT. Met de JWT kan ook in het achterliggend landschap de client geauthenticeerd en geïdentificeerd worden. In hoeverre dit noodzakelijk is hangt ook af van de infra bij betreffende partijen.
2. Deze versie verwijst niet meer naar het Edukoppeling REST-profiel, maar bevat zelf de voorschriften die deels overeenkomen met de voorschriften uit het REST-profiel (en WUS-profiel) en staat nu op zichzelf.
3. De reden om niet meer voort te bouwen op het hele REST-profiel is omdat we in deze versie een duidelijk onderscheid maken in het koppelvlak naar het token endpoint van de AS (STAP #1) en het koppelvlak naar de protected resource (STAP#3). Bij de interactie tussen client en protected resource heeft de client alleen een Access Token nodig en levert deze over een TLS verbinding. Deze verbinding vereist dus geen mTLS en PKIo. Het token volstaat. Deze TLS verbinding moet voldoen aan het UBV TLS basisprofiel. Het request naar het token endpoint van de AS voldoet wel aan alle (MDX) eisen die we ook bij het REST en WUS profiel onderkennen. Dit betekent naast het toepassen van mTLS/PKIO/OIN ook het routeringskenmerk in de query string en toepassing van het MDX OSR protocol.
4. Verduidelijken van de uitgangspunten en opgenomen in eigen hoofdstuk

[1] Zie documentatie voor details

Ad 5 Afronden MDX OSR protocol v0.8
In deze versie zitten nog een aantal niet doorgesproken comments van versie 0.7, omdat we agenda-technisch hier niet aan toe kwamen de vorige keer, plus een aantal toevoegingen/aanscherpingen. Belangrijke wijzigingen ten opzichte van versie 0.7 en 0.6 zijn:

1. Inleidende tekst en plaat, overgenomen uit het architectuurdocument (0.8)
2. Verplicht koppelen van een mandaat aan een systeem (in 0.7 nog optioneel genoemd), daarmee
    a. Een simpeler protocol en ontwerp.
    b. Nauwer aansluitend op de huidige praktijk in administratieve en toetsketensamenwerkingen.
    c. Overeenkomend met de privacybijsluiter waar het bijbehorend gemandateerde systeem genoemd wordt.
3. Antwoord op openstaande en nog niet besproken vragen (vanaf 0.7)
4. Aanscherping wanneer een mandaatcheck verplicht is (niet voor bv agentschappen met een juridische plicht gegevens te verwerken). (vanaf 0.7)
5. Een sectie toegevoegd over OSR als landelijk register. (vanaf 0.7)
6. Centrale landelijke functie van het register beschreven. (vanaf 0.7)

Ad 6 Discussie over de uit te werken extra profielen en de te nemen vervolgstappen
Het gaat om een passend antwoord te vinden op de constatering dat binnen Edu-v er varianten van gegevensuitwisselingen zijn te onderkennen:

- Gegevensuitwisselingen die van een onderwijsorganisatie of een leverancier zijn.
- Gegevensuitwisselingen van gegevens van een onderwijsorganisatie waar al dan niet een verwerkersovereenkomst voor vereist is, en dus wel mandaat of geen mandaat.
- Gegevensuitwisselingen met vertrouwelijke en niet vertrouwelijke gegevens.

Door deze varianten af te doen met het meest strikte profiel (MDX-profiel) is de keten mogelijk niet flexibel genoeg voor de andere gegevensuitwisselingen die voorzien zijn in het Edu-v ecosysteem. De vraag is of de profielen opgebouwd kunnen worden, dus niet van strikt naar minder strikt, maar juist van het laagste niveau op te bouwen naar het hoogste niveau.