Uitgangspunten en voortgang OAuth-profiel Edukoppeling

Voor:	Architectuurraad Edustandaard
Van:	Brian Dommisse, namens Werkgroep Edukoppeling
Datum	20 april 2023
Betreft	Uitgangspunten en voortgang van nieuw profiel OAuth en aanpassingen in andere profielen en architectuur van Edukoppeling

Inleiding
De werkgroep Edukoppeling is ver gevorderd met het opstellen van een nieuw profiel, MDX Secure API OAuth-profiel, als onderdeel van de Edukoppeling-afspraak. De aanleiding voor deze uitbreiding op de afspraak was een wens vanuit de deelnemers aan de afspraak FDE-set voor fijndistributie om de beveiliging van de FDE REST API met een OAuth-profiel te ondersteunen.
Behalve een nieuw profiel zal ook de Edukoppeling-architectuur worden aangepast. Dit was overigens al voorzien voor 2022, maar in de werkgroep is besloten om de architectuur in 1 keer aan te passen samen met het opleveren van het nieuwe profiel. Oplevering van concepten ter review was gepland voor Q1-Q2 2023. De werkgroep verwacht nu in juni-juli zover te zijn. Het tussenconcept van de specificatie (gepubliceerd bij de stukken van de werkgroep-sessie) is echter al geschikt om te bestuderen, op te reflecteren en om voor partijen impact te bepalen.
Met deze notitie wil de werkgroep alvast de Architectuurraad meenemen in de uitgangspunten die zijn opgesteld en vastgesteld in de werkgroep, waarbij ook afstemming is geweest met Topicus, die reeds een eigen implementatie heeft draaien op basis van OAuth.

Gevraagd besluit
Kan de Architectuurraad de uitgangspunten onderschrijven? Zo nee, waar zitten volgens de AR nog vragen en/of knelpunten?

Uitgangspunten

1. De Edukoppeling afspraak is van toepassing verklaard op het uitwisselen van vertrouwelijke informatie, waaronder privacygevoelige informatie.
2. In plaats van de huidige aanduiding SaaS-profiel (dienst, leverancier) wordt de term Mandated Data eXchange (MDX) Secure API profiel gehanteerd, omdat de afspraak niet alleen SaaS-diensten betreft.
3. Het MDX Secure API OAuth profiel is toegevoegd aan Edukoppeling, naast de al bestaande profielen voor REST en WUS. OAuth wordt in de praktijk gebruikt als aanvullende maatregel voor beveiligen van informatie, iets wat we vanuit Edustandaard graag willen ondersteunen.
4. Het MDX secure API OAuth profiel werkt met 3 partijen: een client die resources wil opvragen, een authorisation server die tokens voor toegang (access-token) verstrekt en een resource server die de eigenlijke resources bevat. Als de client toegang wil hebben tot een resource van de resourceserver, dan vraagt die bij de authorisation server een acces-token aan. Met een geldig access-token kan de client vervolgens de API op de resource server aanroepen om toegang te krijgen tot de resource.

5. Het OAuth profiel beschrijft mogelijkheden hoe autorisatie op attribuutniveau uitgevoerd kan worden met behulp van dit protocol. Ketens maken eigen keuzes of en hoe ze hier invulling aan geven.
6. De autorisatiecontrole door een authorisation server met OAuth en het op basis daarvan uitgeven van een toegangstoken kan volgens dit OAuth profiel zowel centraal als decentraal worden ingericht. Ketenpartijen kunnen er dus voor kiezen om dit zelf te doen met een eigen OAuth authorisation server, maar ook om dit over te laten aan een centrale partij. Bij een centrale inrichting zitten de resource- (de te benaderen API) en authorisation server in verschillende security domeinen. Ter voorkoming van mogelijke verschillende interpretaties wat scopes en resources etc zijn, dienen deze dan ook centraal gedefinieerd te worden.
7. Het OAuth profiel is enkel toepasbaar voor REST APIs. Vanwege de (optioneel) decentrale opzet moeten per dienst/leverancier afspraken gemaakt worden.
8. Alle profielen (WUS, REST, OAUTH) gaan uit van een verplichte mandaatcheck zoals beschreven in het nieuwe MDX OSR protocol als voorwaarde voor een geslaagde uitwisseling. Een mandaat bepaalt of een gegevensverwerker namens een eindorganisatie deel mag nemen aan een specifieke ketensamenwerking. Aanvullend hierop kunnen nog andere beperkende maatregelen worden getroffen met de WUS, REST en OAuth profielen.
9. De standaard beschrijft in het nieuwe MDX OSR protocol nu normatief hoe het Onderwijs Service Register (OSR) het proces van mandateren voor alle ketensamenwerkingen in het onderwijs ondersteunt. Een mandaat geeft een verwerker recht op deelname aan een ketensamenwerking en de daarin onderkende ketenprocessen.
10. Door het centrale register karakter van het OSR biedt het de eindorganisatie en eventuele gemachtigde derden overzicht op ketenniveau over deelnemende partijen. OSR voorziet in centraal beheer door een door het bestuur gemachtigd persoon (personen).