edustandaard

Agenda Edustandaard werkgroep Edukoppeling

Datum en locatie
30 januari 2023, 10:00-12:30 uur
Locatie: Amersfoort

1. Opening, mededelingen, vaststellen agenda
2. MDX Secure API OAuth profiel
3. Secure API protocol
4. Rondvraag / Sluiting

Ad 2 Initiële versie Secure API OAuth profiel
Op basis van het discussiestuk is een eerste conceptversie van het OAuth-profiel opgesteld.

- **Een aantal uitgangspunten zijn gewijzigd**
  Op basis van de uitgangspunten in versie 0.3 van het discussiestuk is een eerste versie van het OAuth-profiel opgesteld. Op basis van voortschrijdend inzicht zijn hierin toch een aantal andere keuzes gemaakt. Dit betreft o.a. het onderstaande.
  - We sluiten zoveel mogelijk aan op het REST-profiel. OAuth is een extra beveiliging bovenop dit profiel. Hiermee maken we (vooralsnog) gebruik van een querystring voor het doorgeven van het routeringskenmerk en gaan we uit van een point-2-point verbinding waarbij de eindorganisatie in respons hetzelfde is als in het request.
  - We passen RFC8705 nog niet toe. Deze RFC ondersteunt client authenticatie op basis van mTLS en binding van het Access Token aan het client certificaat. Bij nadere uitwerking blijkt dat de standaard het DN van het certificaat gebruikt voor token binding. We onderzoeken nog met andere gremia wat mogelijke stappen zijn om hier het subject.serial aan toe te voegen. We gebruiken echter wel mTLS voor client authenticatie, maar dat deden we al.

- **Nieuwe naam voor SaaS context**
  We hebben vorige keer besloten dat we mogelijk op termijn ook profielen voor andere contexten willen opstellen. Hiermee moeten we de huidige (SaaS) profielen kunnen onderscheiden van deze nieuwe. In het nieuwe OAuth-profiel wordt de naam Mandated Data eXchange (MDX) gebruikt. De volledige naam wordt bijvoorbeeld het Edukoppeling MDX Secure API OAuth profiel. We moeten hierin een keuze gaan maken om dit in de nieuwe versie van de documenten mee te kunnen nemen. We hebben het graag ook over eventuele alternatieven.

- **OAuth-profiel vormt een eigen identificatie- en autorisatielaag**
  Authenticatie van de client wordt via transportbeveiliging op basis van mTLS ondersteund. Binnen het OAuth profiel wordt de client bij de AS geregistreerd en daarbij krijgt de client een eigen identifier die intern naar een OIN herleid kan worden. Deze meer fijnmazige identificatie is nodig omdat het OIN (incl. suffix[1]) niet voldoende opties biedt om de mogelijk vele clients te identificeren.

Ad 3 Nieuwe versie Secure API protocol
Er is een nieuwe versie van het Secure API protocol opgesteld. Hierin is commentaar verwerkt zoals gegeven in de comments en tijdens de bespreking. De belangrijkste hiervan zijn:

[1] Een alternatief zou de suffix van het OIN kunnen zijn, maar naast het beperkte bereik maakt de ontkoppeling van het OIN (en PKIo) het gebruik van het profiel ook bruikbaar in andere contexten (anders dan MDX).

- Het niet verplicht stellen van de check van het eigen mandaat
- Het (optioneel) kunnen binden van een mandaat op een systeem (doet OSR nu niet, kan technisch wel makkelijk)
- Het (optioneel) kunnen binden van een mandaat op een hele groep van leveranciers (is nu standaard in OSR)
- Het (optioneel) verplicht stellen van een mandaat voor registratie van een eindpunt (is nu standaard in OSR)