Uitgangspunten uitwerken architectuur ROSA-Edukoppeling en opstellen OAuth-profiel

Voor:	Architectuurraad Edustandaard
Van:	Brian Dommisse
Datum	18 april 2024
Betreft	Uitgangspunten uitwerken architectuur ROSA-Edukoppeling en opstellen OAuth-profiel

Inleiding
In de AR is er nav een ingebrachte memo van de werkgroep Edukoppeling op 25 januari de volgende besluiten genomen:

- Accordering van uitgangspunten en aanpak (*voor het opstellen van de architectuur in de ROSA en daarmee in samenhang voor Edukoppeling*): De Architectuurraad onderschrijft de uitgangspunten en aanpak van de werkgroep Edukoppeling.
- Behoefte aan update van architectuur: Er is een duidelijke behoefte geïdentificeerd voor het updaten van de overkoepelende architectuur van de profielen, vooral met de introductie van het OAuth-profiel op twee plekken in het onderwijs.

Op basis van die opdracht heeft de werkgroep Edukoppeling op 18 maart een start gemaakt met het uitwerken van de architectuur en de opzet van het OAuth-profiel. Die uitkomsten van deze werkgroep zijn hieronder op hoofdlijnen beschreven. De nadere details zijn te vinden in het verslag van de werkgroepbijeenkomst: https://www.edustandaard.nl/app/uploads/2024/04/2024-03-18-Verslag-Edustandaard-Werkgroep-Edukoppeling.pdf

Gevraagd besluit

- Kan de Architectuurraad de uitgangspunten en de vervolgstappen onderschrijven?

Uitgangspunten
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[1] 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

[1] Zie bijlage A : TOGAF Conformance

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. Dit heeft ook een relatie met de discussie rond uitgangspunt #3.

Over het volgende uitgangspunt is er nog geen consensus:

- Uitgangspunt 3: Het Edukoppeling Secure API OAuth profiel is (initieel) fully conformant aan het NL GOV OAuth profiel.

Binnen de werkgroep was er nog geen consensus rond de (initiële[3]) mate van compliance. Er wordt afgesproken dat de leden de achterban consulteren of en welke inperkingen nu noodzakelijk worden geacht. Een verkenning welke keuzes* (inperkingen op het NL GOV profiel) voor het Nederlandse onderwijsveld mogelijk relevant zijn wordt op korte termijn uitgevoerd door Edu-V, DUO en Npuls/SURF (OOAPI/OKE). Als hier (nog) geen unaniem besluit kan worden genomen, dan zal binnen de Edu-V ketensamenwerking met het oog op de implementaties in het najaar zelf al een keuze maken. Voor Edukoppeling zou dit betekenen dat een fully conformant Secure API Oauth profiel ons vertrekpunt wordt voor het opstellen van de specificaties voor het onderwijs.

** Keuzes kunnen onder meer gemaakt worden op de volgende vlakken:*

- *Use case authorization code flow en betreffende clients uitsluiten. Hiermee wordt in het Edukoppeling Secure API OAuth profiel dan alleen de use case client credentials en bijbehorende direct acces clients ondersteund.*
- *Client authenticatie op basis van enkel mTLS/X.509/RFC8705[4] of op basis van private_key_jwt method. Het toepassen van enkel X.509 (self-signed) certificaten of PKIo certificaat. Over het algemeen stelt het NL GOV profiel dat als de rollen niet in beheer zijn bij dezelfde organisatie dat er dan PKIo certificaten gebruikt moeten worden. In de Edukoppeling architectuur gaan we uit van een ketensamenwerking en gaan we er dus vanuit dat NL GOV OAuth voor onze context de toepassing van PKIo vereist.*

De volgende kanttekeningen zijn hierbij te maken:

- Het NL GOV OAuth (werkversie) is nog in beweging en dat geldt ook voor het Digikoppeling REST-API profiel. Dit kan dus betekenen dat nu keuzes maken mogelijk een grotere delta met betreffende standaarden op termijn betekent. We kunnen dan alsnog besluiten weer aan te sluiten wat vanuit het oogpunt van standaardisatie van beperkte impact is. De impact zal groter zijn bij implementaties.
- Tot nu toe is de strategie binnen Edustandaard geweest dat Edukoppeling zoveel mogelijk de overheidsstandaard Digikoppeling volgt als het gaat om het overnemen van vergelijkbare profielen[5]. Het NL GOV OAuth profiel wordt door een Digikoppeling OAuth werkgroep formeel vastgesteld en er loopt nu een voorstel om dit ook op te laten gelden (via Federatieve Service

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

[3] Initieel omdat de werkgroep heeft besloten later de architectuur en ROSA M2M kaders uit te werken. Mogelijk kunnen keuzes hierin later nog impact hebben op het Edukoppeling Secure API OAuth profiel.

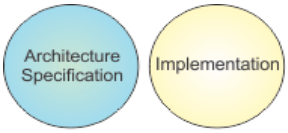
[4] Het lijkt er nu sterk op dat Digikoppeling dit gaat voorschrijven voor client authenticatie bij een volgende versie van het Digikoppeling Koppelvlakstandaard REST-API profiel. Daarnaast is het waarschijnlijk dat een volgende versie van het NL GOV OAuth profiel ook de ondersteuning van een proof-of-possession token (*token bound to the client that requested the token*) gaat ondersteunen op basis van RFC8705.

[5] Dat wil niet zeggen dat alle profielen uit Digikoppeling ook voor het onderwijs van toepassing zijn. Zo is het ebMS-profiel toentertijd niet onderdeel geworden van Edukoppeling. Bij de ontwikkeling van een REST-profiel waren we met Edukoppeling eerder en hebben in afstemming met Digikoppeling ervoor gezorgd dat dit profiel ook in Digikoppeling is opgenomen.

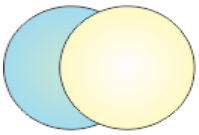
connectiviteit standaard[6]) voor het Digikoppeling REST-API profiel. Welke keuzes er uiteindelijk allemaal gemaakt gaan worden is nu nog niet te zeggen.

[6] Overleg/Digikoppeling/2024-05-29/Wijzigingsvoorstel_FSC/FSC_Discussie_Onderwerpen_Q&A.md at main · Logius-standaarden/Overleg (github.com) en Federatieve Service Connectiviteit opnemen in het Digikoppeling voor REST API's profiel · Issue #26 · Logius-standaarden/Digikoppeling-Koppelvlakstandaard-REST-API (github.com)

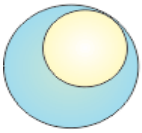
Bijlage **A**: **Conformance**



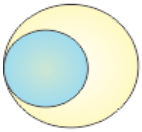
Irrelevant:
The implementation has no features in common with the architecture specification (so the question of conformance does not arise).



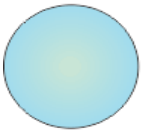
Consistent:
The implementation has some features in common with the architecture specification, and those common features are implemented in accordance with the specification. However, some features in the architecture specification are not implemented, and the implementation has other features that are not covered by the specification.



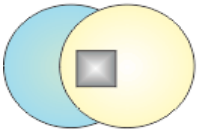
Compliant:
Some features in the architecture specification are not implemented, but all features implemented are covered by the specification, and in accordance with it.



Conformant:
All the features in the architecture specification are implemented in accordance with the specification, but some more features are implemented that are not in accordance with it.



Fully Conformant:
There is full correspondence between architecture specification and implementation. All specified features are implemented in accordance with the specification, and there are no features implemented that are not covered by the specification.



Non-conformant:
Any of the above in which some features in the architecture specification are implemented not in accordance with the specification.