edustandaard

Onderwerp: **Edukoppeling Secure API OAuth profiel / Architectuur v3.0**
Van: **Bureau Edustandaard**
Voor: **Werkgroep Edukoppeling**
Datum: **13-3-2024**

1. Aanleiding

De Edukoppeling werkgroep heeft in 2023 een conceptversie van een OAuth client credentials profiel[1] ontwikkeld en deze in juli 2023 gepubliceerd voor een openbare consultatie. Bij de ontwikkeling is vooral geluisterd naar de wensen vanuit het Groeifondsprogramma Edu-V, omdat in die ketensamenwerking al op korte termijn een conceptversie nodig was voor Proof-of-Concept implementaties. De werkgroep was echter bewust dat hierin ook nog een aantal open punten zaten die na de Edu-V Proof-of-Concepts verder uitgewerkt zouden worden als onderdeel van de nog op te stellen Edukoppeling 3.0 architectuur. Het OAuth-profiel dat als concept nu staat gepubliceerd en ook ter consultatie is aangeboden is derhalve niet geschikt om aan te bieden aan de Architectuurraad ter vaststelling en als een 1.0 versie te publiceren.

Daarnaast heeft SURF recent deze conceptversie in het kader van de openbare consultatie[2] gereviewd[3]. Hieruit kwam min of meer ook naar voren dat deze versie gezien vanuit de internationale standaard en de recente ontwikkelingen in het kader van NL GOV te veel daarvan afwijkt en in hun ogen ongeschikt is om vast te stellen als een 1.0 versie geschikt voor onderwijsbrede toepassingen. De Edu-V Proof-of-Concept implementaties hebben uiteindelijk ook niet plaatsgevonden en zodoende zijn er uit die keten geen ervaringen met de gepubliceerde conceptversie naar voren gekomen.
Edu-V heeft recent wel aangegeven dat er op korte termijn een OAuth-profiel nodig is voor implementaties van een eerste release. Ondertussen is er ook het NL GOV OAuth profiel[4] verder ontwikkeld met daarin ook de vergevorderde voorschriften voor de OAuth client credentials grant. Het zijn deze ontwikkelingen die er toe leiden dat er op korte termijn een Edukoppeling OAuth profiel nodig is terwijl we nog niet toe zijn gekomen om de overkoepelende ROSA architectuurkaders en een nieuwe Edukoppeling architectuur op te stellen en vast te laten stellen.

Deze memo is bedoeld om, vooruitlopend op de verdere uitwerking van de architectuur(kaders), alvast een aantal uitgangspunten vast te stellen die de richting van het Edukoppeling OAuth profiel bepalen en die in lijn zijn met de op te stellen architectuur.
Hiermee hopen we een beter inzicht te geven in de afwegingen die bij de ontwikkeling ervan gaan spelen. We stellen dan ook voor dat een eventueel OAuth-profiel pas opgesteld wordt nadat de in deze memo opgenomen uitgangspunten (en keuzes) zijn vastgesteld in ieder geval in de Edukoppeling-werkgroep en daarna ook in de Architectuurraad van 18 april 2024.

2. Uitgangspunten

1. De API strategie[5] van het Kennisplatform API's de primaire "driver" voor de doorontwikkeling van de Edukoppeling architectuur versie 3.0.
    a. De API strategie is opgesteld door het Kennisplatform API's en beschrijft een nieuwe kijk op gegevensuitwisselingen op basis van API's. Deze worden door zowel de interne organisatie als door ketenpartners gebruikt. Er zijn dus vele verschillende contexten waarin ze gebruikt worden, maar het Kennisplatform speelt in op de wens

[1] https://www.edustandaard.nl/standaard_afspraken/edukoppeling-transactiestandaard/edukoppeling-juli-2023/
[2] Edukoppeling OAuth-profiel gepubliceerd voor openbare consultatie - Edukoppeling OAuth-profiel gepubliceerd voor openbare consultatie - Edustandaard - Edustandaard
[3] Reactie SURF
[4] NL GOV Assurance profile for OAuth 2.0 (logius-standaarden.github.io) (werkversie)
[5] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Inleiding/ (werkversie)

van veel partijen om identificatie, authenticatie en autorisatie voor verschillende use cases zoveel mogelijk uniform in te richten.

b. Digikoppeling, waar we ons met Edukoppeling op gericht hebben, is over de jaren wel aangepast, maar heeft ook nog kenmerken van een Service Gerichte Architectuur met hierin ook standaarden als ebMS[6]. We zien echter dat bij de doorontwikkeling van Digikoppeling ook aansluiting wordt gezocht bij producten van het Kennisplatform API's zoals het gebruik van de API Design Rules. Federated Services Connectivity (FSC, afkomstig vanuit de VNG) wordt als toekomstig onderdeel van het Digikoppeling REST koppelvlak gezien en gaat waarschijnlijk in de basis het NL GOV OAuth profiel gebruiken. Als we door tijdsdruk moeten voorlopen op Digikoppeling dan lijkt aansluiting op API strategie daarom de beste keuze. Bij de ontwikkeling van de Edukoppeling architectuur versie 3.0 zullen we echter ook waar nodig nog naar Digikoppeling kijken.

2. Edukoppeling maakt gebruik van de producten van de API strategie.
   a. Met het volgen van de API strategie maken we gebruik van de betreffende Architectuur[7].
   b. Met het volgen van de API strategie maken we gebruik van het NL GOV OAuth profiel[8].
   c. Met het volgen van de API strategie maken we gebruik van de API Design Rules[9].

3. Het Edukoppeling Secure API OAuth profiel is (initieel) fully conformant aan het NL GOV OAuth profiel.
   a. Initieel is het Edukoppeling Secure API OAuth profiel fully conformant[10]. Bij de verdere ontwikkeling van de ROSA architectuurkaders en Edukoppeling Architectuur versie 3.0 kunnen we mogelijk naar een conformant profiel (optie b) bewegen.
      i. Fully conformant wil zeggen dat NL GOV OAuth profiel het Edukoppeling Secure API OAuth profiel geheel afdekt en niets van het Edukoppeling Secure API OAuth profiel valt buiten het NL GOV OAuth profiel. Dit is de ideale situatie omdat we hiermee volledig interoperabel en compliant met het overheidsbrede profiel zijn. Er kan feitelijk voor alle scenario's één profiel gebruikt worden.
      ii. Technisch zou het Edukoppeling Secure API OAuth profiel dan alleen een verwijzing zijn naar het NL GOV OAuth profiel. We blijven hiermee in lijn met de (nog op te stellen) bovenliggende Edukoppeling Architectuur versie 3.0 die dan aansluit op de Kennisplatform API's Architectuur.
      iii. In principe wordt interoperabiliteit bereikt door een brede scope van de architectuur en de onderliggende standaarden en componenten die deze standaarden ondersteunen. Deze componenten, zoals een API Gateway, laten bij de implementatie de keuze vrij. Zo kunnen bijvoorbeeld verschillende typen clients zich op dezelfde of verschillende wijze authenticeren zolang de vorm maar door de standaard ondersteund wordt.
   b. Een alternatief uitgangspunt is om (initieel) een conformant Edukoppeling Secure API OAuth profiel op te stellen.
      i. Conformant wil zeggen dat het NL GOV OAuth profiel alleen een deel van het Edukoppeling Secure API OAuth profiel afdekt, maar dat deel is wel in zijn geheel conform het NL GOV OAuth profiel. Hiermee laten we de ruimte voor (optionele) aanvullingen,

[6] Digikoppeling Koppelvlakstandaard ebMS2 (logius-standaarden.github.io) (werkversie)
[7] https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Architectuur/ (werkversie)
[8] NL GOV Assurance profile for OAuth 2.0 (logius-standaarden.github.io) (werkversie)
[99] NLGov REST API Design Rules (logius-standaarden.github.io) (werkversie)
[10] Bijlage C: Compliance

ii. Bij dit alternatief komen er alleen aanvullingen die NIET door het NL GOV OAuth profiel ondersteund worden. Denk bijvoorbeeld aanvullingen rond de aanvraag voor een Access Token en het Access Token zelf. Of het optioneel opnemen van een routeringskenmerk[11] in de uitwisseling zoals we dat nu ook bij de bestaande profielen doen. Het is vervolgens aan een ketensamenwerking om in een ketenafspraak het gebruik van het routeringskenmerk verplicht te stellen.

c. Een ander alternatief is dat er (initieel) een consistant Edukoppeling Secure API OAuth profiel wordt opgesteld.
   i. Consistant wil zeggen dat er overlap is tussen het Edukoppeling Secure API OAuth profiel en het NL GOV OAuth profiel, en binnen die overlap is het Edukoppeling Secure API OAuth profiel conform het Secure API OAuth profiel, de overlap is echter niet volledig. Sommige specificaties van het NL GOV OAuth profiel zijn niet overgenomen, en het Edukoppeling Secure API OAuth profiel bevat onderdelen die niet door het NL GOV OAuth profiel worden gedekt.
   ii. Bij dit alternatief gaan we het NL GOV OAuth profiel beperken. Logischerwijs gaat dan ook de Edukoppeling Architectuur versie 3.0 afwijken van de Kennisplatform API's architectuur. Het is in deze fase, denken we, onwenselijk om een dergelijke keuze te baseren vanuit wensen voor enkel het OAuth profiel zonder het bredere perspectief van de architectuur te beschouwen. Verder geeft het NL GOV OAuth profiel aan dat een dergelijk Edukoppeling profiel tot implementaties leidt die niet compliant[12] zijn. Daarnaast heeft Digikoppeling in de roadmap[13] het opstellen van Best Practices voor het NL GOV OAuth profiel staan. Er is een kans dat daarin uiteindelijk andere keuzes worden gemaakt. Als wij deze stap nu toch willen maken zouden we de volgende onderdelen kunnen uitsluiten:
      - Use case authorization code flow[14] en betreffende clients uitsluiten. Hiermee wordt in het Edukoppeling Secure API OAuth profiel dan alleen de use case client credentials[15] en bijbehorende direct acces clients[16] ondersteund.
      - Client authenticatie[17] op basis van enkel mTLS/X.509[18] of op basis van private_key_jwt method.
      - Het toepassen van enkel X.509 (self-signed) certificaten of PKIo certificaat. Het nog niet vastgestelde wijzigingsvoorstel[19] heeft het over een X.509 certificaat, maar over het algemeen stelt[20] 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

[11] Het is overigens wenselijk om het begrip en de functie van het routeringskenmerk binnen de Edukoppeling Architectuur versie 3.0 opnieuw te definiëren.
[12] Impact van een consistant Edukoppeling Secure API OAuth profiel
[13] Bijlage B: Roadmap Digikoppeling
[14] https://logius-standaarden.github.io/OAuth-NL-profiel/#use-case-authorization-code-flow
[15] https://logius-standaarden.github.io/OAuth-NL-profiel/#use-case-client-credentials-flow
[16] https://logius-standaarden.github.io/OAuth-NL-profiel/#direct-access-client
[17] https://logius-standaarden.github.io/OAuth-NL-profiel/#requests-to-the-token-endpoint
[18] De optie van mTLS/X.509 is nog niet in de werkversie (24 februari 2024) verwerkt (Het NL GOV OAuth profiel is nog in ontwikkeling).
[19] Het NL GOV OAuth profiel is nog in ontwikkeling
[20] Client keys: "*In case the Authorization Server, Resource Server and client are not operated under responsibility of the same organisation, each party MUST use PKIoverheid certificates with OIN*." en bij Connections with protected resources: "*In case the Authorization Server, Resource Server and client are not operated under responsibility of the same organisation, each party MUST use PKIoverheid certificates with OIN for encryption*."

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.
    - Self-signed X.509 certificaten bieden flexibiliteit en zijn beter interoperabel met RFC8705. PKIo biedt een betrouwbare identiteit waarmee alle ketenpartners een bepaalde ketenpartij kunnen identificeren.

4. Het Edukoppeling Secure API REST profiel wordt fully conformant aan de API Design Rules.
    a. In het bestaande Edukoppeling REST/SaaS-profiel 1.0 staat de eerdere gepubliceerde versie van de API Design Rules[21] centraal. Als onderdeel van de Edukoppeling Architectuur versie 3.0 zal er echter wel een nieuwe versie van het REST profiel moeten komen. Zoals al eerder besproken in de werkgroep krijgt het profiel een nieuwe naam, Secure API REST profiel. Daarnaast zal het nieuwe Edukoppeling Secure API REST profiel refereren naar de Digikoppeling Koppelvlakstandaard REST-API[22] die ondertussen beschikbaar is gekomen met hierin de nieuwe versie van de API Design Rules. Het Edukoppeling Secure API REST profiel wordt hiermee fully compliant aan de API Design Rules. Verder is het Digikoppeling Koppelvlakstandaard REST-API in ontwikkeling (zie Digikoppeling roadmap[23]) en het is de verwachting dat de Digikoppeling OAuth Best Practices en Federated Services Connectivity[24] een (verplicht) onderdeel worden van dit profiel. Het Digikoppeling REST profiel migreert dus mogelijk naar een OAuth profiel.

[21] REST-API Design Rules (Nederlandse API Strategie IIa) 1.0 (logius.nl)
[22] Digikoppeling Koppelvlakstandaard REST-API (logius-standaarden.github.io) (werkversie)
[23] Bijlage B: Roadmap Digikoppeling
[24] Federated Services Connectivity wordt waarschijnlijk verplicht bij toepassing van het Digikoppeling Koppelvlakstandaard REST-API.

3. Bijlage A: NL GOV OAuth profiel

3.1. Het NL GOV OAuth profiel ondersteund de Authorization code grant en client credentials grant

In lijn met de architectuur van de API strategie is het NL GOV OAuth profiel vanuit het perspectief van een Authorizationserver (API Gateway) opgesteld. Hiermee kunnen verschillende use cases worden ondersteund. Het NL GOV OAuth profiel ondersteund de authorization code grant en het client credentials grant. Voor deze verschillende flows wordt er naar zoveel mogelijk naar uniformiteit en eenduidigheid gestreefd. Men gaat zelfs zo ver dat er naast de specifieke OAuth opties soms ook naar onderdelen (private_key_jwt method) verwezen die de OIDC standaard biedt. Dit ook om vanuit het perspectief van de Authorizationserver een flexibele implementatie te kunnen bereiken die meerdere opties en use cases ondersteund. Zo ondersteunt het profiel verschillende typen clients welke dynamisch of out of band geregistreerd kunnen worden, kunnen self-signed of PKIo certificaten gebruikt worden en kan de client zich authenticeren op basis van een X.509 certificaat of met de private_key_jwt method.

3.2. Het NL GOV OAuth profiel is nog in ontwikkeling

Het NL GOV OAuth profiel dat op 9 juli 2020 is gepubliceerd op de website van Logius is te vinden op https://gitdocumentatie.logius.nl/publicatie/api/oauth/. Sindsdien is het profiel doorontwikkeld en de meest recente werkversie van 24 februari 2024 is te vinden op https://logius-standaarden.github.io/OAuth-NL-profiel/. In deze nieuwe werkversie is ook client credentials grant uitgewerkt[25].

Een wijziging[26] die in deze werkversie waarschijnlijk opgenomen gaat worden mogelijk is het pull request hieronder. Hiermee kan naast het gebruik van een private-key-jwt voor client authenticatie ook een X.509 certificaat (mTLS) gebruikt worden. Het profiel laat verder vrij of het X.509 certificaat een PKIo of ander certificaat is. Met het gebruik van PKIo certificaten wordt het zo mogelijk om een rechtspersoon op basis van een OIN (subject.serial van het certificaat) te identificeren en authenticeren. Het client-id zou dan gebruikt kunnen worden voor identificatie van een referentiecomponent dat de betreffende rechtspersoon gebruikt.

Zoals we eerder al in de Edukoppeling werkgroep besproken hebben is er ook een standaard voor client authenticatie op basis van mTLS, RFC8705[27]. De NL GOV OAuth werkgroep heeft niet voor de toepassing hiervan gekozen omdat hiermee het gebruik van een client-id hiermee verplicht wordt. Het bezwaar wat wij eerder in de Edukoppeling werkgroep hadden is dat het gebruik van het subject.serial niet standaard ondersteund wordt door RFC8705[28]. Voor de toepassing ervan i.c.m. met PKIo zou eerst onderzocht moeten worden of verschillende platformen hier flexibel mee om kunnen gaan.

```
<!-- iGov-NL : Start of the additional content -->
<aside class=" addition">
<b>iGov-NL : Additional content</b></br>
Direct access clients that are using the client credentials grant type and are not using
```

[25] Deze is dus nog niet vastgesteld en gepubliceerd. Het is een werkversie.
[26] https://github.com/Logius-standaarden/OAuth-NL-profiel/pull/33/files
[27] https://datatracker.ietf.org/doc/html/rfc8705
[28] https://datatracker.ietf.org/doc/html/rfc8705#section-2.1.2

OpenIDConnect are also allowed to use an X.509 certificate to authenticate with the authorization *server's token endpoint. This flow is compatible with OAuth 2.0 due to section 2.3.2 of [[rfc6749]].* *</aside>* *<!-- iGov-NL : End of the additional content -->*

Tabel 1 - Pull request op huidige NL GOV Oauth werkversie

3.3. De status van het NL GOV OAuth profiel bij Forum standaardisatie

De internationale open standaard OAuth[29] is door forum standaardisatie op de lijst van aanbevolen standaarden gezet. Het NL GOV OAuth profiel[30] staat op de ptlu-lijst.

NL GOV OAuth

- Functioneel toepassingsgebied: NL GOV Assurance Profile for OAuth 2.0 moet worden toegepast bij applicaties waarbij gebruikers of 'resource owners' impliciet of expliciet toestemming geven aan een dienst van een derde om namens deze toegang te krijgen tot gegevens via een REST API waarvoor ze recht van toegang hebben.
- Organisatorisch werkingsgebied: Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Het functioneel toepassingsgebied komt met name overeen met de Authorization code grant flow. Deze was ook de eerste flow die het NL GOV OAuth profiel ondersteunde. De client credentials grant flow is anders en kent ook een iets ander functioneel toepassingsgebied. Het is afwachten of bij publicatie van de nieuwe versie van het NL GOV OAuth profiel met daarin de client credentials flow ook het functioneel toepassingsgebied wordt aangepast.

3.4. Impact van een consistant Edukoppeling Secure API OAuth profiel

Het NL GOV OAuth profiel geeft aan dat consistant implementaties niet compliant[31] zullen zijn: "*When an iGov-NL-compliant component is interacting with other iGov-NL-compliant components, in any valid combination, all components MUST fully conform to the features and requirements of this specification."*

3.5. H2M en M2M interacties in relatie tot de API Strategie architectuur en het NL GOV OAuth profiel

In de ROSA staat de volgende definitie voor H2M[32]: "*De gegevensuitwisseling tussen mens en een systeem.*" En M2M[33] heeft de volgende definitie: "*De gegevensuitwisseling tussen systemen onderling zonder menselijke tussenkomst.*"
De API strategie architectuur gaat uit van API's die vanuit verschillende use cases bevraagt worden door verschillende typen clients. In de referentiearchitectuur[34] staat een API gateway hierin centraal.

[29] OAuth | Forum Standaardisatie
[30] NL GOV Assurance profile for OAuth 2.0 | Forum Standaardisatie
[31] NL GOV OAuth: "*When an iGov-NL-compliant component is interacting with other iGov-NL-compliant components, in any valid combination, all components MUST fully conform to the features and requirements of this specification."*
[32] https://rosa.wikixl.nl/index.php/2f69854e-dd3b-41ed-92dd-4377d06be41a
[33] https://rosa.wikixl.nl/index.php/Eba9f611-249a-4dcc-bffd-0ddb489fc87a
[34] https://github.com/Geonovum/KP-APIs/raw/master/overleggen/Werkgroep%20API%20architectuur/uitwerkingen/media/api-security-architecture.png

Vanuit het perspectief van een API Gateway met daarin een Authorizationserver kunnen we stellen dat de interacties tussen client en authorizationserver en tussen de client en de resource server M2M koppelingen betreft. Hiermee willen we benadrukken dat (vanuit BES) er dus niet sprake is van een H2M uitwisselingen in deze interacties, maar enkel M2M. Als we willen blijven stellen dat Edukoppeling alleen over M2M uitwisselingen gaat en toch zowel het OAuth Authorization code grant en client credentials grant willen ondersteunen in het Edukoppeling Secure API OAuth profiel dan hoeft dit niet in tegenspraak met elkaar te zijn. Als er in de werkgroep toch geen consensus is over een deze uitspraak dan kunnen we misschien wel stellen dat we de scope niet moeten baseren op M2M interacties, maar op een referentiearchitectuur.

Ons vertrekpunt voor de discussie is dat een Edukoppeling Architectuur versie 3.0 ook vanuit een dergelijke context beschouwd moet worden. Voor de bespreking van 18 maart staat de architectuur niet op de agenda, maar hoe we naar de architectuur kijken heeft consequenties voor andere onderdelen zoals de Edukoppeling profielen.

4. Bijlage B: Roadmap Digikoppeling

4.1. Digikoppeling roadmap

Belangrijke ontwikkelen in de Roadmap Digikoppeling zijn de komst van de FSC standaard en Best practices voor het gebruik van het NL GOV OAuth profiel icm het Digikoppeling Koppelvlakstandaard REST-API.

Tijdlijn Roadmap Digikoppeling Standaarden

Activiteit	Q1 2024	Q2 2024	Q3 2024	Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
Digikoppeling REST API profiel baseren op ADR 2.0	X	X						
Signing & Encryptie toevoegen aan RESTful API profiel	X	X	X					
Aansluiting Digikoppeling op Federatief Data Stelsel (FDS)	X	X	X	X	X	X	X	X
Implementatie invoering ebMS3/AS4 (*)	X	X	X	X	X	X	X	X
Aansluiting FSC standaard op Digikoppeling (*)	X	X	X	X	X	X	X	X
Best practice Gebruik OAuth icm Digikoppeling REST_API			X	X				
Periodiek actualiseren architectuur		X				X		
Periodiek actualiseren beveiligingsvoorschriften			X				X	

(*) Deze onderwerpen zijn afhankelijk van besluitvorming in het MIDO, bij goedkeuring wordt in 2025 vooral een accent op ondersteuning van de implementatie van de standaard verwacht

4.2. Federated Services Connectivity wordt waarschijnlijk verplicht bij toepassing van het Digikoppeling Koppelvlakstandaard REST-API.

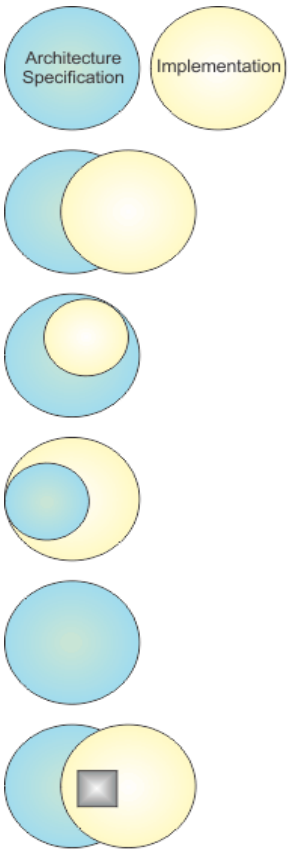
Federated Services Connectivity[35] (FSC) vindt zijn oorsprong in de NLX software. De implementatie is omgeschreven naar een standaard. Het bestaat uit een core[36], delegation[37] en logging[38]. De aanleiding voor FSC waren o.a. Common Ground, Applicatie silo's doorbreken door processen en data te scheiden, Data bij de bron principe, Behoefte aan technische interoperabiliteit, Ver-API-ficering en de resulterende Explosie aan koppelingen.

Met de FSC core wil men interoperabel M2M uitwisselingen organiseren. De inrichting is op netwerkniveau wat vergelijkbaar is met ons begrip ketensamenwerking. Binnen een netwerk bestaat een directory met metadata. De peers die de M2M uitiwsseling ondersteunen zijn de technische systemen die partijen gebruiken. Deze worden niet apart geïdentificeerd en geauthentiseerd. Het vertrouwensmodel is gebaseerd op een CA als trustanchor. Voor overheidsnetwerken wordt aangenomen dat PKIo wordt gebruikt maar binnen de standaard is dit een vrije keuze.

De FSC delegatie functie is vergelijkbaar met de mandaten die binnen Edukoppeling onderkend worden. De technische inrichting is echter geheel anders en ook decentraal.

[35] Common Ground / Standards / FSC · GitLab
[36] FSC - Core (commonground.gitlab.io)
[37] FSC - Delegation (commonground.gitlab.io)
[38] FSC - Logging (commonground.gitlab.io)

5. Bijlage C: Compliance



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.