Memo: Kaders voor nieuwe Edukoppeling Architectuur

Aan	Edustandaard werkgroep Edukoppeling
Van	Erwin Reinhoud
Datum	24-09-2024
Betreft	Kaders voor nieuwe architectuur (actiepunt #131)

1. Achtergrond

Deze memo is bedoeld om de discussie in de werkgroep te ondersteunen bij de te maken keuzes die aan de basis staan van de uitwerking van de nieuwe Edukoppeling afsprakenset. Daarnaast geeft het invulling aan actiepunt #131 om een overzicht te maken van initiatieven en de keuzes die daarin gemaakt zijn c.q. worden ten aanzien van OAuth.

We hebben het plan[1] om Q1 2025 een nieuwe Edukoppeling Architectuur op te leveren waarin het gedachtegoed van een API strategie[2], de betreffende architectuur[3] en een OAuth profiel[4] centraal staan. De documenten (zie voetnoten) waarbij we ons op baseren bieden voor concrete implementaties echter nog veel keuzes.
Daarnaast zijn er allerlei nationale en internationale initiatieven[5] die deels hier gebruik van maken, maar ook deels eigen keuzes maken. Deze zijn niet op elkaar zijn afgestemd. Het beeld wat bij ons ondertussen is ontstaan is dat het ook binnen het onderwijs lastig is om tot één eenduidige architectuur en OAuth-profiel te komen in combinatie met een eenduidige methode om toestemming te organiseren.

We zien een aantal aandachtsgebieden rond de structuur en inhoud van de nieuwe architectuur waarover we een standpunt moeten innemen, willen we gericht verder gaan met de uitwerking. We hebben daarvoor de volgende vragen opgesteld:

- Biedt het nieuwe informatie-uitwisselingsmodel de juiste aandachtsgebieden om op hoog niveau tot een structuur voor de architectuur te komen?
- Gaan we uit van een flexibele architectuur die meerdere communicatiekanalen ondersteunt, of een specifiek M2M kanaal waarin andere keuzes kunnen worden gemaakt[6] dan bij andere (bijvoorbeeld H2M) kanalen?

[1] Besluit #16
[2] In min of meerdere mate die van het Kennisplatform API's (werkversie https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Inleiding/)
[3] Werkversie https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Architectuur/
[4] Werkversie https://logius-standaarden.github.io/OAuth-NL-profiel/
[5] Zie **Fout! Verwijzingsbron niet gevonden.** bij hoofdstuk 3
[6] Denk hierbij aan de OAuth standaard die verschillende profielen ondersteunt waarbij een authorization server zowel tokens uitgeeft aan clients na client authenticatie (M2M) of in combinatie met toestemming van een resource owner (H2M, toestemming door persoon).

- Sturen we op één M2M profiel of zijn er verschillende (sub)profielen die toegepast moeten worden voor een bepaalde context[7]?
- We sluiten aan op de API strategie maar er zijn daarbinnen nog keuzes te maken en hiervoor kijken we naar initiatieven op nationaal en internationaal niveau. Willen we er een leidend laten zijn?

Aan de hand van een toelichting op de verschillende aspecten van het informatie-uitwisselingsmodel en de samenhang daartussen en het overzicht van de initiatieven, zoomen we verder in op deze vragen met als doel hier een gezamenlijk standpunt in te nemen.

Het is een eerste aanzet dus we moeten ons er van bewust zijn dat het nog niet sluitend en volledig is. Het doel is om na het overleg een aantal concrete uitgangspunten te hebben voor de nieuwe Edukoppeling architectuur.

[7] Denk hierbij bijvoorbeeld aan het REST profiel (mTLS/PKIo) wat we nu hebben een en een eventuele extra beveiligingsprofiel op basis van OAuth. Of een Oauth profiel met een bearer token of een profiel met een proof-of-possession-token.

2. Informatie-uitwisselingsmodel

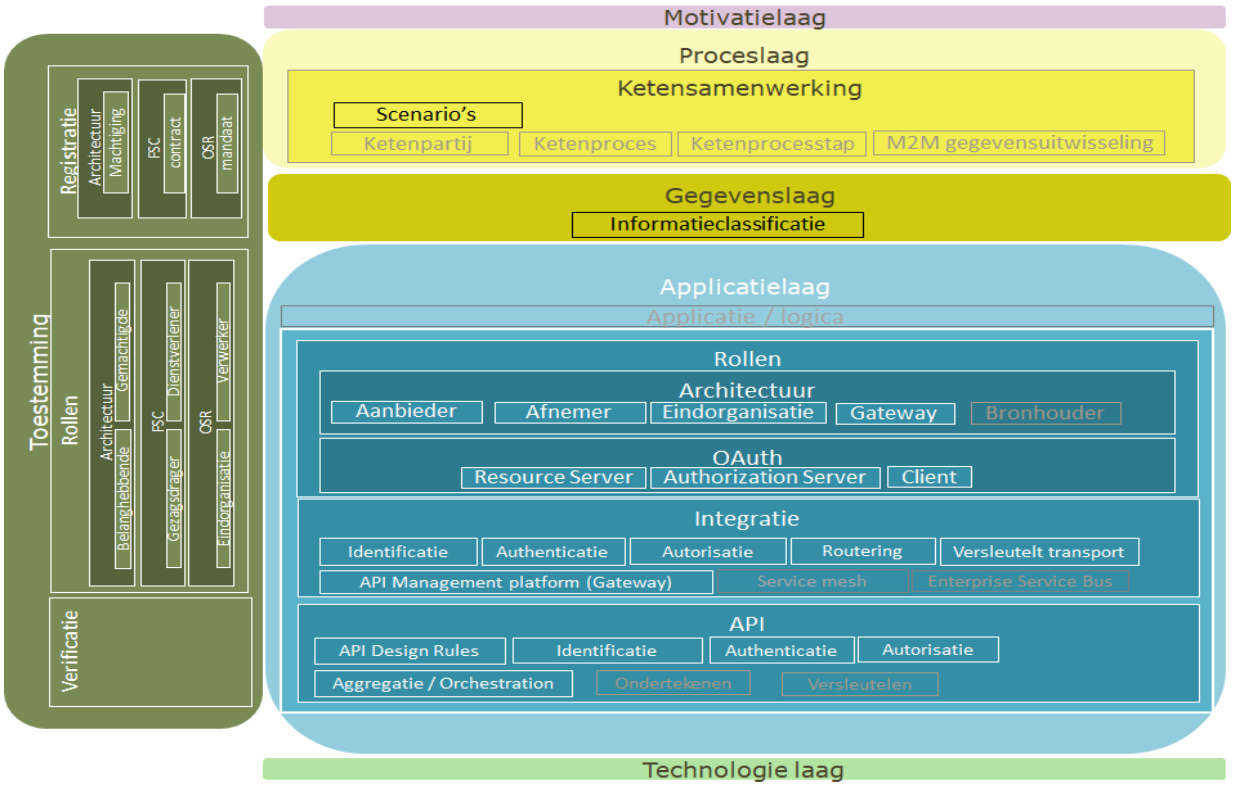
Om onderdelen van de architectuur te kunnen structureren is het voorstel om een nieuw informatie-uitwisselingsmodel te gebruiken waarin naast meer aandacht voor API's is ook toestemming is opgenomen.

De architectuur onderkent een abstractie voor rollen en functies. Zo zijn de toegepaste begrippen ontkoppelt van een bepaalde standaard en hoeven we bij doorontwikkeling van de architectuur de abstracte laag alleen op functioneel niveau aan te passen en kunnen de onderliggende concrete standaarden die hier invulling aan gegeven vervangen worden. Zo gebruiken we in de toestemmingslaag in de basis de rollen gemachtigde en belanghebbende en in de applicatielaag aanbieder en afnemer.

In het nieuwe model onderkennen we de volgende lagen:

- proceslaag (relevant welke informatiestromen binnen een ketensamenwerking plaatsvinden);
- informatie-/gegevenslaag (relevant voor de informatieclassificatie);
- toestemmingslaag*;
- applicatielaag*;

* Edukoppeling heeft met name betrekking op deze lagen.



Figuur 1- Edukoppeling informatie-uitwisselingsmodel

Ketensamenwerking (proceslaag)

De proceslaag is niet direct relevant voor Edukoppeling. Edukoppeling is een generieke oplossing voor M2M gegevensuitwisselingen die toegepast moeten kunnen worden bij meerdere ketensamenwerkingen[8] en de ketenprocessen en ketenprocesstappen die hieronder vallen. De proceslaag stelt echter wel kaders voor de toestemmingslaag en applicatielaag. Zo kunnen er verschillende proceskarakteristieken verschillende eisen stellen aan de M2M gegevensuitwisseling. Binnen de proceslaag wordt duidelijk wat de reikwijdte voor toestemming moet zijn. De keuze hierin heeft vervolgens weer een relatie met de reikwijdte van een autorisatie op de applicatielaag. De toestemmingsreikwijdte kan de ketensamenwerking als geheel zijn, een proces of een processtap en de API('s) die dit ondersteunen. De Edukoppeling-architectuur moet op dit punt flexibel zijn en verschillende scenario's kunnen ondersteunen met één of meer profielen.

Informatieclassificatie (gegevenslaag)

Ook de gegevenslaag is niet direct relevant voor Edukoppeling, een principe dat we al langer binnen onze architectuur hanteren is '*geen boodschap aan de boodschap*'[9], maar stelt wel kaders voor de architectuur. Vooraf aan de daadwerkgelijke uitwisseling moet er zijn vastgesteld welke gegevens partijen binnen een bepaalde ketenprocesstap met elkaar uitwisselen. We onderkennen hiervoor op hoog niveau de volgende indeling[10]:

- Open (publieke) data
- Gesloten data
    - Bedrijfskritische gegevens
    - Persoonsgegevens

Ook op dit punt moet de Edukoppeling architectuur flexibel zijn en verschillende informatieclassificaties kunnen ondersteunen met één of meer profielen.

Toestemmingslaag

Met de toestemmingslaag willen we de rechtmatigheid van een M2M gegevensuitwisseling kunnen borgen. De toestemmingslaag geeft invulling aan de eis dat een belanghebbende aan één of meerdere gemachtigden toestemming (machtiging)[11] moet kunnen geven voor M2M gegevensuitwisselingen binnen een bepaalde ketensamenwerking (doelbinding).

In het informatie-uitwisselingsmodel is de toestemmingslaag loodrecht op de overige lagen geplaatst omdat we hiermee willen benadrukken dat we dit als een aparte laag moeten zien en ook betrekking heeft op meer dan alleen de applicatielaag. Zo nemen we aan dat de

[8] Ketensamenwerkingen - ROSA Wiki (wikixl.nl)
[9] Principes en andere kaders zullen expliciet terecht gaan komen in de ROSA architectuurkaders.
[10] Binnen het onderwijs zijn er verschillende (BIV) toetsingskaders voor informatieclassificaties en maatregelen die bij transport hiervan van belang zijn. Deze toetsingskaders en maatregelen zijn niet uniform. Bij de ontwikkeling van de Edukoppeling architectuur is het streven dat transportbeveiliging zo is ingericht dat het voldoet aan de verschillende toetsingskaders.
[11] Een herroepbare bevoegdheid die aan een entiteit (vertegenwoordiger) is verleend betreffende een andere entiteit (belanghebbende).

registratie van de toestemming voor een uitwisseling de proceslaag raakt. De belanghebbende en gemachtigde moeten zichzelf elektronisch kunnen identificeren en authentiseren. Er zijn rond toestemming dus waarschijnlijk ook kaders[12] in de proceslaag en gegevenslaag[13] nodig.

De toestemmingslaag raakt ook de applicatielaag. Hierin moet een verificatie kunnen worden uitgevoerd. De applicatielaag moet kunnen vaststellen welke API's binnen de scope (ketensamenwerking, proces of processtap) van de machtiging vallen waar een bepaalde client een token voor aanvraagt.

Applicatielaag

De applicatielaag vormt de kern van de Edukoppeling afspraak. We definiëren hierbinnen rollen, de integratielaag en een API-laag.

Rollen
Met het omarmen van het gedachtegoed van de API strategie van het Kennisplatform[14] maken we hiermee ook de keuze om uit te gaan van API's. Voor het definiëren van de rollen op architectuurniveau kijken we deels naar de GDI domeinarchitectuur gegevensuitwisseling. Voor de beveiliging van API's maken we gebruik van de OAuth 2.0 standaard. Hiermee wordt ook meer concreet invulling geven aan de rollen in de applicatielaag.

Integratielaag
We maken hierbinnen afspraken hoe identificatie en authenticatie en autorisatie moet worden ingericht bij M2M een gegevensuitwisseling. De API-Management tooling speelt een belangrijke rol in de integratielaag. Hierin worden de verschillende API's vanuit de API-laag gepubliceerd. De gateway heeft mogelijk verschillende functies, zoals het afhandelen van transportbeveiliging, routeren, het registreren van client en verlenen van tokens (als AS) en op een hoog niveau verifiëren van tokens.

API-laag
Binnen de applicatielaag moeten de verschillende rollen zich kunnen identificeren en authentiseren. Dit geldt met name voor de client dat die geautoriseerd moet zijn voor toegang tot de resource server. Het verifiëren van een machtiging (toestemmingslaag) kan onderdeel zijn van de autorisatiebeslissing.

[12] We gaan er vanuit dat er een kader komt dat dergelijke registraties worden uitgevoerd door een natuurlijk persoon die namens een onderwijsorganisatie handelt. We nemen hiermee dus aan dat we binnen het onderwijs de onderwijsorganisatie en de betreffende bevoegde personen via een H2M kanaal gegevens laten registreren. Private partijen kunnen zich wel digitaal identificeren en authentiseren via certificaten. Voor onderwijsorganisaties willen we geen certificaten gebruiken.
[13] Onder andere voor het specificeren van een machtiging.
[14] Werkversie https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Inleiding/

3. Nationale en internationale initiatieven

We zijn niet de enige die een architectuur rond API's willen opstellen. Er zijn verschillende nationale en internationale initiatieven die hetzelfde doel hebben. Deze zijn zeker nog niet allemaal volwassen en sommige zijn niet verder gekomen dan een conceptversie. Om inzicht te krijgen in keuzes die elders gemaakt zijn is er gekeken naar de volgende initiatieven:

1. NL GOV[1]
2. Digikoppeling Koppelvlakstandaard REST-API v1.1.1[2]
3. Digikoppeling Koppelvlakstandaard REST-API i.c.m. FSC (in ontwikkeling)[3]
4. Edukoppeling OAuth BP 1.0[4]
5. Edukoppeling REST 1.0[5]
6. iGOV (Draft 03 -20218)[6]
7. FAPI 2.0[7]
8. 1EdTech (v1.1)[8]

[1] Proposed version https://logius-standaarden.github.io/OAuth-NL-profiel/ (client credentials profiel)
[2] https://gitdocumentatie.logius.nl/publicatie/dk/restapi/
[3] Nieuwe REST versie is nog in ontwikkeling, vulling gebaseerd op aanname rond huidige keuzes bij NL GOV OAuth en FSC
[4] Edukoppeling - Edukoppeling - juni 2024 - Edustandaard
[5] https://www.edustandaard.nl/app/uploads/2021/02/2021-02-10-Edukoppeling-REST_SaaS-profiel-versie-1.0-definitief-1.pdf
[6] International Government Assurance Profile (iGov) for OAuth 2.0 - draft 04 (openid.net)
[7] FAPI 2.0 (oauth.net) (client credentials profiel)
[8] 1EdTech Security Framework v1.1 | IMS Global Learning Consortium (client credentials profiel)

De verschillende (functionele) aspecten die we willen uitlichten zijn:

1. transportbeveiliging (TLS of mTLS);
2. vertrouwensanker (self signed certificaat / PKIo certificaat);
3. registratie (dynamisch / out-of-band);
4. OAuth flow (authorization code grant (acg) en/of client credentials grant(ccg);
5. OAuth client authenticatie (mTLS of private_key_jwt);
6. OAuth access token (bearer of sender constrained/proof-of-possession (PoP));
7. toestemming (OAuth acg, FSC contract of OSR mandaat).

Standard	Transport beveiliging	Certificaat	Registratie	OAuth flow	OAuth client authentication (ccg)	OAuth AT(ccg)	Toestemming
NL GOV	TLS of mTLS	public and private key pair of PKIo[1]	Dynamisch of out-of-band	OAuth 2.0 acg en ccg	mTLS (RFC8705) of OIDC private_key_jwt	Bearer	acg
DK REST-API	mTLS	PKIo	out-of-band	-	-	-	-
DK REST-API i.c.m. FSC	mTLS	PKIo	out-of-band	OAuth 2.0 ccg	mTLS (RFC8705?)	(RFC8705?)	Contract
EK BP 1.0	TLS	PKIo (en public and private key pair voor AS?)	out-of-band	OAuth 2.0 ccg	OIDC private_key_jwt	Bearer	-
EK REST 1.0	mTLS	PKIo	out-of-band	-	-	-	Mandaat
iGOV	TLS	public and private key pair	Dynamisch of out-of-band	OAuth 2.0 acg en ccg	OIDC private_key_jwt	Bearer	acg
FAPI 2.0	TLS of mTLS	public and private key pair		OAuth 2.0 acg (en ccg)	mTLS (RFC8705[2]) of OIDC private_key_jwt	Bearer of PoP (RFC8705) of DPoP (RFC9449[3])	acg
1EdTech	TLS	public and private key pair	Dynamisch en/of out-of-band	OAuth 2.0 acg en ccg	client_secret_basic: key and secret with the HTTP Basic Authentication method (as described in [RFC2617])	Bearer JSON object of JWT	acg

[1] Is afhankelijk of rollen onder controle van dezelfde partij staan. Indien dit niet zo is dan is PKIo verplicht. Onduidelijk is of in combinatie met client authenticatie op basis van private_key_jwt de AS en/of RS een PKIo moeten toepassen voor TLS verbinding.
[2] https://datatracker.ietf.org/doc/html/rfc8705
[3] https://datatracker.ietf.org/doc/html/rfc9449

Tabel 1 - Overzicht van verschillende standaarden[15]

[15] Dit overzicht is een conceptversie en is een wat versimpelde weergave van de aspecten die in de verschillende afspraken beschreven worden. De invulling in grijs is nog niet geverifieerd of standaard is nog in ontwikkeling.

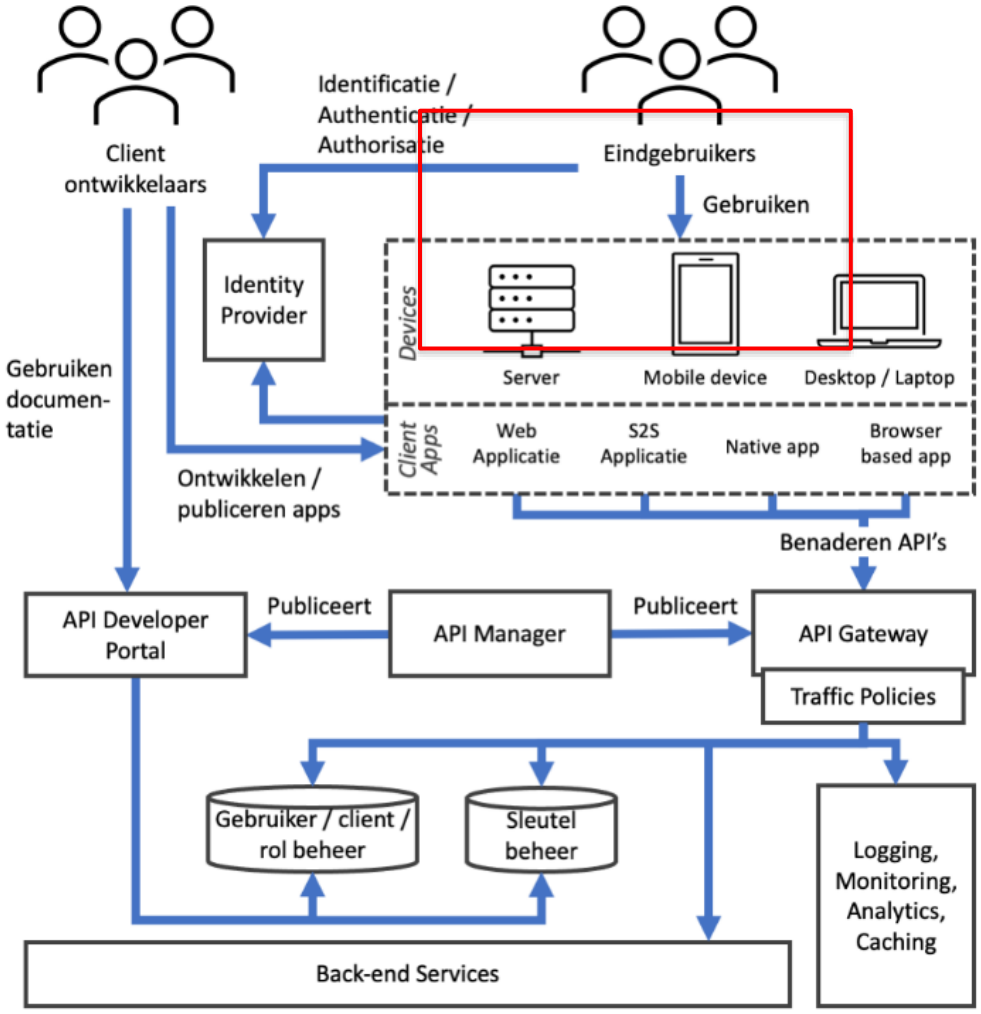
4. Flexibele architectuur of specifiek M2M kanaal

De architectuur van de API strategie[16] gaat uit van een aantal standaardcomponenten. De API Gateway is over het algemeen de toegangspoort tot het achterliggende API landschap. De API Gateway heeft ook een centrale rol bij de beveiliging van API's. Het gaat dan vaak over grofmazige autorisaties zoals eventueel afhandeling van mTLS en het basaal verifiëren van OAuth access tokens. Dit component heeft ook een rol in het beheer en verifiëren van traffic policies. De API Gateway kan een verbinding met de Identity Provider hebben voor het geval door de Identity Provider afgegeven tokens onvoldoende informatie bevatten om autorisaties toe te passen.

De gateway kan als centraal component dus verschillende kanalen ondersteunen, die zowel H2M als M2M gebaseerd kunnen zijn. Dit sluit ook goed aan op de onderliggende standaarden zoals OAuth 2.0. Deze standaard (en ook het NL GOV OAuth profiel) ondersteunt verschillende profielen die goed aansluiten op de verschillende communicatiekanalen.

Voor de ontwikkeling van de nieuwe Edukoppeling architectuur willen we vroegtijdig inzicht hebben of we bij deze architectuur ook van deze flexibiliteit uit moeten gaan. Sturen we op zoveel mogelijk aansluiting op nationale (of internationale) open standaarden waarin meerdere keuzes mogelijk zijn die uiteindelijk vrijwel allemaal bij implementatie gemaakt worden. En gaan we er hierbij vanuit dat er altijd sprake is van een flexibele architectuur die voor elke variant beperkte implementatie-effort vereist. Of willen we juist specifieke keuzes maken voor het M2M kanaal en bepaalde zaken toevoegen of uitsluiten?

[16] Werkversie https://geonovum.github.io/KP-APIs/API-strategie-algemeen/Architectuur/



Figuur 1 - API Strategie Architectuur (informatief) – Via gateway kunnen verschillende kanalen de API's benaderen

5. Eén M2M profiel of meerdere profielen

Vanuit standaardisatie is het wenselijk om tot één profiel te komen. In theorie is dit goed mogelijk. De praktijk is echter dat zowel sectoren als ketenpartners in ketensamenwerkingen verschillende keuzes maken. We constateren ook dat het uniformeren door dezelfde standaarden te kiezen niet tot de gewenste uniformiteit leidt. Binnen een standaard zijn er nog keuzes te maken en hier lijkt men verschillend invulling aan te willen geven. Daarnaast speelt ook het in- en uitfaseren van standaarden een rol. Het is tenslotte zo dat als er nu voor bepaalde functionaliteit een standaard bestaat deze op termijn wordt vervangen door een nieuwe versie of een nieuwe standaard.

Moeten we in de nieuwe architectuur rekening houden met het bestaan van meerdere profielen? Het is echter wel wenselijk dat we goede bovenliggende kaders (ROSA ontwerpgebieden etc.) gebruiken om vast te stellen of het ook vanuit functioneel oogpunt wenselijk is dat meerdere profielen moeten onderkennen. We hebben nu nog een Edukoppeling WUS en REST profiel welke in combinatie met OSR gebruikt kunnen worden om ook toestemming vooraf aan de gegevensuitwisseling te kunnen vaststellen. De Edukoppeling OAuth Best Practices ondersteunen niet de verificatie van toestemming, maar wel toegang tot een API op basis van een OAuth access token. Moet het gebruik van toestemming en een OAuth access token optionele onderdelen zijn die afhankelijk van de context toegepast kunnen worden, of zetten we in op een profiel wat alle functies omvat en voor alle scenario's toepasbaar is?