edustandaard

Agenda Edustandaard werkgroep Edukoppeling

Leden:	Edwin Verwoerd (Iddink/VDOD), Gerald Groot Roessink (DUO), Robert Kars (DUO), Maarten Kok (SBB), Erik Borgers (Kennisnet, OSR), Koen Voermans (Edu-v), Patrick van der Veer (SURF), Brian Dommisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES)
Gastleden	Bart Geesink (SURF), Edwin Kense (Basispoort)
Agendalid:	Ernst-Jan van Heuseveldt (Rovict/VDOD)

Datum en locatie
22 april 2024, 09:00-11:00 uur
Locatie: Online / TEAMS

1. Opening, mededelingen en vaststellen agenda
2. Voorstel publicatie conceptversie met compliance document (uitfasering WUS profiel)
3. Bespreking Edukoppeling Secure API OAuth profiel
4. Rondvraag / Sluiting

Ad 2 Voorstel publicatie conceptversie met compliance document
We hebben eerder afgesproken dat we in een nieuwe versie van het *Overzicht actuele documentatie en compliance* willen gaan aangeven tot welke datum (naar verwachting) een (normatief) document in beheer blijft.
Bij alle normatieve onderdelen zijn nu voorstellen opgenomen voor “Einde ondersteuning”, alleen bij het WUS-profiel nog niet. In het bijzonder willen we aangeven dat we naar REST standaarden bewegen en WUS (SOAP/WSDL) feitelijk niet meer actief gaan beheren. Ketenpartners kunnen in het kader van ketensamenwerkingen deze natuurlijk nog blijven gebruiken, maar we zullen het profiel niet meer aanpassen op een datum die later valt dan bij “Einde ondersteuning” is aangegeven. Ketens die WUS nog blijven toepassen gebruiken zo mogelijk een profiel wat niet meer wordt ondersteund en waarover Edustandaard het advies geeft deze ook niet meer te gebruiken en aanraadt migratieplannen voor aansluiting op een ander profiel van Edukoppeling te starten.

Gevraagd besluit:
Aan de werkgroep wordt gevraagd of we de datum “Einde ondersteuning” voor WUS-profiel willen gaan koppelen aan het publiceren van een nieuwe release van Edukoppeling (naar verwachting begin 2025) of dat we besluiten om een eerdere datum voor “Einde ondersteuning” te kiezen om alvast een duidelijk signaal af te geven.

We zullen zoals gezegd bij volgende releases van Edukoppeling (Architectuur versie 3.0) geen WUS-profiel meer opnemen. Ons voorstel is om een nieuwe conceptversie van Edukoppeling te publiceren waarin we de huidige ontwikkelingen beschrijven, maar waarin nog geen normatieve documenten zijn opgenomen. De nieuwe versie van het *Overzicht actuele documentatie en compliance* zal hierin wel opgenomen worden om de ontwikkelingen te kunnen duiden en een indicatie te geven van nieuwe versies van o.a. de Edukoppeling Architectuur. Het document is op Teams te vinden bij de andere stukken die 22 april besproken worden.

Ad 3 Bespreking Edukoppeling Secure API OAuth profiel
Tijdens het afgelopen overleg is er geen besluit genomen in hoeverre een Edukoppeling Secure API OAuth profiel (initieel) compliant moet zijn aan het NL GOV OAuth profiel. Dit is een belangrijk vertrekpunt voor de verdere discussie over het profiel en de Edukoppeling Architectuur versie 3.0. Er is afgesproken dat de leden de achterban consulteren of en welke

inperkingen nu noodzakelijk worden geacht. We gaan de reeds geleverde input (zie bijlage A) bespreken. Leden die niets hebben aangeleverd worden tijdens het overleg nog in de gelegenheid gesteld om een toelichting te geven en/of op de reeds ingebrachte input te reageren.

We streven ernaar om duidelijk te krijgen of een Edukoppeling Secure API OAuth profiel op korte termijn noodzakelijk is of dat er (voorlopig) naar NL GOV OAuth profiel[1] verwezen kan worden. Het beperken (uitsluiten van verplichte onderdelen) binnen onderwijs betekent dat we de standaard niet volledig volgen:

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.*

Daarnaast kan het zijn dat er een NL GOV OAuth compliancevoorziening komt. Deze zal dan binnen het onderwijs zeer waarschijnlijk niet te gebruiken zijn.

Digikoppeling is een OAuth-werkgroep gestart. Deze werkgroep gaat met name over de formele vaststelling van NL GOV OAuth releases. Naar verwachting wordt er ergens komende maanden de 1.1 versie inclusief het client credentials profiel en 2 opties voor client authenticatie gepubliceerd. We hoeven dan ook niet meer naar de werkversie te verwijzen die altijd in beweging zal blijven. De beveiligingswerkgroep van het Kennisplatform API's blijft het NL GOV OAuth profiel inhoudelijk ontwikkelen.

Digikoppeling wordt ook doorontwikkeld en een nieuwe versie van de Digikoppeling Koppelvlakstandaard REST-API[2] vereist mogelijk de toepassing van Federatieve Service Connectiviteit welke op zijn beurt weer de toepassing van het NL GOV OAuth client credentials profiel zal vereisen. Of dit allemaal daadwerkelijk ook realiteit gaat worden is nu onduidelijk.

Verder is het NL GOV OAuth profiel gebaseerd op het iGOV profiel. Ook dit onderliggende profiel is in beweging[3] en vanuit de Kennisplatform API's beveiligingswerkgroep en Digikoppeling OAuth werkgroep worden deze ontwikkelingen gevolgd. Een nieuwe versie van het iGOV profiel zal zo waarschijnlijk weer de basis gaan vormen voor een nieuwe versie van het NL GOV OAuth profiel (v1.2).

[1] Het gaat dan om de werkversie die nog in beweging is. Naar verwachting komt er voor de zomer nog een versie 1.1 van het NL GOV OAuth profiel waarin ook client credentials is opgenomen.
[2] Overleg/OAuth/2024-04-11 at main · Logius-standaarden/Overleg (github.com) en 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)
[3] Zie o.a. openid / igov / issues / #45 - Clarify requirements for client authentication — Bitbucket

edustandaard

Bijlage A: Input leden en achterban rond NL GOV OAuth profiel

De onderstaande tabel geeft een overzicht van de voorkeur van de leden rond het wel of niet beperken van het NL GOV OAuth profiel[4]. Er is ook een kolom van DK REST (Digikoppeling REST) opgenomen met hierin de waarschijnlijke keuzes rond een nieuwe versie van het DK REST profiel.

Onderdeel	DUO	Edu-V	SBB	Kennisnet	SURF	MBO Digitaal	DK REST
OAuth flows	-	Enkel CC toestaan	-	0	-	-	Enkel CC toestaan(?)
Client authenticatie	pkjwt	pkjwt	-	0	-	-	mTLS
PKI	PKIo	PKIo	-	0	-	-	PKIo
Dynamic registration	NVT	NVT	-	NVT	-	-	NVT
TTL Access Token	15min	1 uur	-	-	-	-	-

pkjwt = private-key-jwt
PKIo = PKIoverheid
= niets aangegeven
0 = geen inperkingen/voorkeur
CC = client credentials
DK REST = Voorspelling o.b.v. huidige info. Er is nog geen nieuwe versie van DK REST

Bij instemming van beperkingen is ons vertrekpunt een eigen versie van een Edukoppeling Secure API OAuth profiel. Deze zal dan afwijken van NL GOV OAuth en zeer waarschijnlijk ook van een nieuwe versie van het DK REST profiel. We nemen hier dus al initieel een andere keuze dan (op termijn) overheidsbreed genomen kan gaan worden.
Daarnaast is bij de openbare consultatie van het vorige Edukoppeling OAuth profiel o.a. aangegeven dat voor het profiel de architectuur en overige context ontbreekt. Voor het opstellen van een Edukoppeling Secure API OAuth profiel zal hetzelfde kunnen gaan gelden. Ook deze keer wordt wellicht een specifiek profiel opgesteld zonder een onderliggende eigen architectuur. We gaan ervanuit dat de API Strategie en de betreffende architectuur[5] voldoende context geeft ondanks dat we dus NL GOV Oauth mogelijk gaan beperken. We sluiten echter niet uit dat een beperking op NL GOV OAuth mogelijk impact op de Edukoppeling architectuur en ROSA kaders gaat hebben. Deze zullen we de komende periode gaan opstellen.

1.1. Input Edu-V[6]

We zien mogelijkheden om expliciete keuzes en implicaties helder te maken in het NL GOV profiel:

1.1.1. Ondersteuning verschillende OAuth flows

In het NL GOV profiel is het Client Credentials profiel nog niet volledig uitgewerkt. Vooral het voorbeeld van de grant_type is niet conform client_credentials en ook

[4] Het gaat hierbij nog steeds om de werkversie (https://logius-standaarden.github.io/OAuth-NL-profiel/) van het NL GOV Oauth profiel welke nog in ontwikkeling is. De verwachting is dat er voor de zomer een nieuwe vastgestelde versie beschikbaar komt met hierin een client credentials grant flow. Daarna zal deze nog doorontwikkeld worden omdat de werkgroep nu al onderkend dat er bepaalde wijzigingen na publicatie besproken moeten worden.
[5] Zie ook genomen besluiten vorig overleg
[6] Zie voor de volledige input de Teams-omgeving van de werkgroepbijeenkomst

iedere autorisatieserver moet authorization_code ondersteunen. Dat is niet strikt noodzakelijk bij een autorisatieserver die alleen operationeel is voor Direct Access Clients.

1.1.2. Client authenticatie o.b.v. mTLS of private-key-jwt

Het NL GOV development profiel heeft alleen de Private Key JWT variant uitgewerkt. mTLS wordt niet genoemd. Wat ons betreft is mTLS dan ook niet meer nodig. Topicus heeft hier nog naar gekeken en geeft het volgende mee:

a. Voorkeur te hebben voor de Private Key JWT.
b. mTLS zit nog niet in het profiel en heeft niet de voorkeur omdat de gegevens over de client dan uit het client certificaat gehaald moeten worden. Met Private Key JWT houd je dit netjes gescheiden.
c. Het is mogelijk om beiden te ondersteunen als Client. Als autorisatieserver is dit niet wenselijk omdat dit kan leiden tot conflicten in de operatie. Bijvoorbeeld toepassing van beiden. Via het discovery endpoint kan een Client opvragen wat een autorisatieserver ondersteunt.

1.1.3. PKIo / X.509 certificaat

Het profiel geeft aan dat het PKI-certificaat verplicht is in een situatie waarbij de Client en de Resourceserver van een andere organisatie zijn. Dat is altijd het geval bij een ketensamenwerking. Dus dit betekent dat PKI ook verplicht wordt.

1.1.4. Dynamic registration

Dynamic registration wordt genoemd als optie. We stellen voor om dit niet toe te passen.

1.1.5. TTL Access Token

De levensduur van een token is maximaal 6 uur. We denken dat dit te lang is en stellen voor om dit verder in te perken naar 1 uur.

1.2. DUO[7]

1.2.1. mTLS of private-key-jwt

De keuze tussen deze twee is relevant op twee plekken:

1. Van client naar RS
   In NL-GOV staat dat proof-of-possession (POP) als geavanceerde security wordt ingezet om te voorkomen dat iemand een token steelt en gebruikt voor illegale dingen. Daarbij genoemd staan mTLS en private-key-jwt als opties. De rechtmatigheid kun je controleren. In het ene geval door de request (met token) te beveiligen met mTLS en in het andere geval doordat de requester het token met PKI (mede?) ondertekend.

   DUO: laat proof-of-possession maar even zitten tot het moment dat NL-GOV een conclusie trekt. De kans op een gestolen token achten we in de tussentijd klein als de geldigheidsduur wordt beperkt tot een kwartier.

2. Van client naar AS
   In paragraaf 2.3.3. van NL-GOV, werkversie en standaardversie, staat dat private_key_jwt verplicht is, MUST, ook voor direct access clients relevant in

[7] Zie volledige input van DUO de Teams-omgeving van de werkgroepbijeenkomst.

Edukoppeling. Dit kan nog veranderen ten gunste van mTLS of iets anders, maar hoe en wanneer weten we niet.
DUO: Wij zien geen nadelen van private-key-jwt die het interessant maken om iets anders te introduceren. Daarom is het voorstel om de huidige tekst te volgen en niet zelf iets anders te verzinnen.

Anders gezegd, wij kunnen langere tijd uit te voeten met de huidige teksten in NL-GOV en wat DUO betreft verandert er op dit punt niks in de concept werkversie.

1.3. Reactie Kennisnet/OSR

Het is nog niet met al onze voorzieningen afgestemd, maar voor nu achten we het raadzaam om NL GOV te volgen en compliant te zijn aan alles wat zij stellen. NL GOV heeft ook een mooie compacte lijst/publicatie waar zij aangeven waar zij afwijken van de hogere standaard (OAuth-NL-profiel/Additional specification and constraints of iGov-NL to the iGov profile.md at develop · Logius-standaarden/OAuth-NL-profiel · GitHub). Dat scheelt het standaardisatieproces bij Edustandaard een hoop werk en maakt meteen duidelijk wat de echte keuzes/afwijkingen zijn. We pleiten ervoor dat wij dat ook doen, dus alleen de afwijkingen beschrijven.