Edukoppeling

M2M gegevensuitwisseling binnen het onderwijs

Edukoppeling OAuth Best Practices

(Gebaseerd op NL GOV Assurance profile for OAuth 2.0 v1.1)

Edustandaard

Datum: juni 2024

Versie: 0.1

edustandaard

Inhoudsopgave

Inhoud

edustandaard

1. Status van dit document

Dit document is een conceptversie van de Edukoppeling OAuth Best Practices en is gebaseerd op het NL GOV Assurance profile for OAuth 2.0[1] (hierna NL GOV OAuth profiel). Deze Edukoppeling OAuth Best Practices hebben ten aanzien van OAuth hetzelfde detailniveau als die van het NL GOV OAuth profiel. Er zijn geen aanvullingen op het niveau van alle OAuth gerelateerde zaken.

Met opmerkingen [ER1]: Link aanpassen zodra versie 1.1 is gepubliceerd

1.1. Documenthistorie

Versie	Status	Auteur	Datum	Opmerking
0.1	Concept	E. Reinhoud (BES)	21 mei 2024	Initiële versie gebaseerd op NL GOV OAuth versie 1.1

1.2. Overzicht actuele documentatie en compliance

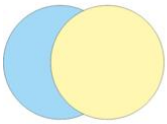
Naast deze best practices wordt er ook een “Overzicht actuele documentatie en compliance juni 2024” gepubliceerd welke een overzicht geeft van de verschillende normatieve en ondersteunende, informatieve Edukoppeling-documenten. Deze wordt gepubliceerd om ontwikkelingen in de tijd te plaatsen en ook de oplevering van de nieuwe set Edukoppeling afspraken richting Q1 2025 te duiden. E.e.a. wordt schematisch weergegeven in Figuur 2. Het overzicht geeft naast de nieuwe ontwikkelingen, zoals deze Oauth best practices, ook aan welke documenten we op termijn niet meer zullen ondersteunen.

Tot voor kort hebben we altijd Digikoppeling[2] als basis gebruikt voor Edukoppeling. Digikoppeling staat op de pas-toe-leg-uit-lijst van Forum Standaardisatie[3] en is onderdeel van de Generieke Digitale Infrastructuur (GDI[4]) van de overheid. We hebben echter al eerder onderkend bij de ontwikkeling van een REST-profiel dat Edukoppeling en Digikoppeling niet altijd in hetzelfde tempo worden doorontwikkeld zodat er verschillen kunnen zijn. Er wordt actief gestreefd om die verschillen klein en tijdelijk te houden. Zo ook met betrekking tot deze OAuth best practices. In dit OAuth best practices document kiezen we er echter voor om het NL GOV OAuth profiel als basis te nemen omdat er nog geen Digikoppeling OAuth profiel of best practices zijn. Het beeld is echter nu al dat als er een Digikoppeling OAuth profiel komt deze zeer waarschijnlijk een aantal andere keuzes zal maken dan in dit document staan.

1.3. Conformance

Het NL GOV OAuth profiel stelt dat implementaties fully conformant[5] zijn als deze alle voorschriften implementeren. In deze OAuth best practices worden niet alle voorschriften overgenomen. Daarnaast worden er een aantal bestaande voorschriften toegevoegd, bijvoorbeeld het toepassen van het UBV TLS basis profiel. Als gevolg van de inperkingen en aanvullingen zijn de implementaties die voldoen aan deze best practices niet fully conformant, maar consistent[6] aan het NL GOV OAuth profiel.

[1] https://logius-standaarden.github.io/OAuth-NL-profiel/ (werkversie)
[2] Logius | Digikoppeling
[3] Digikoppeling | Forum Standaardisatie
[4] Generieke Digitale Infrastructuur (GDI) Generieke Digitale Infrastructuur (GDI) - Digitale Overheid
[5] NL GOV Assurance profile for OAuth 2.0 versie 1.1: “*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*.”
[6] TOGAF Architecture Compliance The TOGAF Standard, Version 9.2 - Architecture Compliance (opengroup.org)



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.

Figuur 1 – De Edukoppeling OAuth best practices zijn consistent aan het NL GOV OAuth profiel

2. Inleiding

2.1. Doel en doelgroep

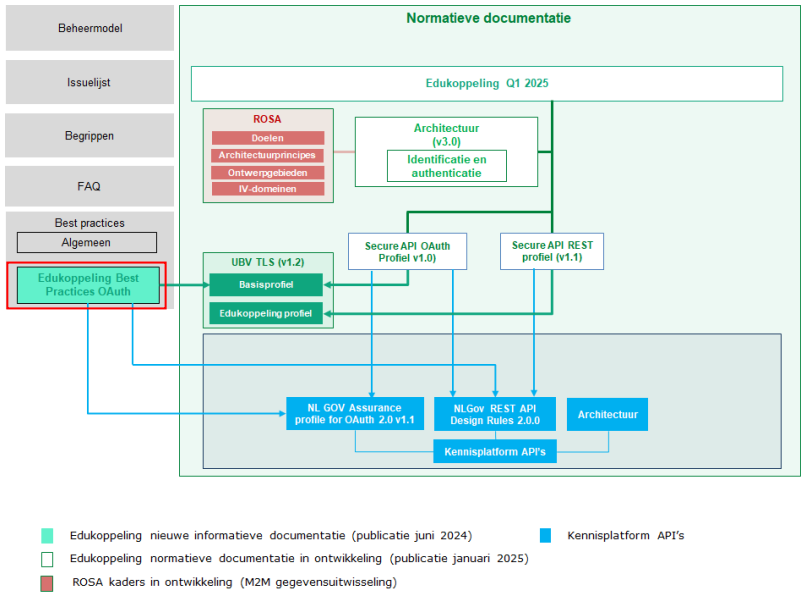
Het doel van deze OAuth best practices is om binnen het betreffende werkingsgebied en functioneel toepassingsgebied op een uniforme manier machine-naar-machine (M2M) vertrouwelijke gegevens te kunnen uitwisselen binnen de onderwijssector.

Dit document is bedoeld voor ICT-specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van een M2M koppelvlak. Het gaat hier om werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties, zowel in de publieke als private sector.

De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerorganisatie Edustandaard[7].

2.2. Positionering binnen Edukoppeling

Deze OAuth best practices staan op zichzelf en zijn nog geen onderdeel van een Edukoppeling release. Het is niet op Edukoppeling documenten gebaseerd en gebruikt enkel het NL GOV OAuth profiel en Edustandaard UBV TLS als basis. Deze best practices geven nadere invulling aan de inrichting van een M2M[8]-koppeling binnen het onderwijs op basis van een OAuth 2.0 client credentials grant. In Figuur 2 wordt wel alvast schematisch weergegeven uit welke onderdelen de nog te ontwikkelen release van Edukoppeling waarschijnlijk gaat bestaan.



Figuur 2 – Edukoppeling OAuth Best Practices i.r.t. overige (nog te ontwikkelen) producten

[7] https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/. Reageren kan via info@edustandaard.nl.

[8] Machine-naar-machine

2.3. Organisatorisch werkingsgebied

Het organisatorisch werkingsgebied van Edukoppeling is de geautomatiseerde gegevensuitwisseling in het onderwijs tussen informatiesystemen van onderwijsorganisaties[9] en ketenpartners (onderling, met bedrijven of met de overheid). Onderwijsorganisaties kunnen hierbij deze informatiesystemen lokaal hebben draaien of hebben uitbesteed in de cloud. Onderwijsorganisaties gebruiken deze informatiesystemen om de eigen processen te ondersteunen of om invulling te geven aan samenwerkingsrelaties met andere onderwijsorganisaties, met de overheid, met gemeenten én met private organisaties.

2.4. Functioneel toepassingsgebied[10]

Het functionele toepassingsgebied van deze OAuth best practices betreft M2M-gegevensuitwisseling via een point-to-point verbinding voor uitwisseling van vertrouwelijke gegevens (gesloten data) tussen een confidential client[11] en een gesloten API. Edukoppeling bevat kaders voor dit M2M koppelvlak[12]. Het koppelvlak bestaat in de basis uit een extern (G2G[13]) gerichte gesloten API voor gesloten data waar een client slechts toegang toe krijgt op basis van een valide (access) token. Het NL GOV OAuth profiel definieert voor de client credentials flow de volgende use case: "*The client credentials flow can be used in usecases where there is a Client to Resource server connection where no user information is needed by the resource server.*"

2.5. Notatiewijze voorschriften

Voor elk voorschrift wordt aangegeven in welke mate hier invulling aan moet worden gegeven. Hiermee kunnen we duidelijk aangeven wat de grenzen van dit profiel zijn ten opzichte van de mogelijke externe bron(nen) waar het voorschrift eventueel van wordt overgenomen. We gebruiken hiervoor de notatiewijze van RFC2119[14]. Deze gebruikt de volgende termen: "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL".

2.6. Leeswijzer

[todo]

[9] Onderwijsorganisatie wordt als volgt gedefinieerd: https://rosa.wikixl.nl/index.php/A0a55699-3c0b-4dce-bbb0-3c55fbf4760c

[10] Het functioneel toepassingsgebied wijkt af van dat van het NL GOV OAuth profiel bij Forumstandaardisatie omdat deze (d.d. 22052024) nog gericht is op de authorization code grant en niet is toegespitst op de client credentials grant waar deze best practices op zijn gebaseerd.

[11] https://datatracker.ietf.org/doc/html/rfc6749#section-2.1

[12] Koppelvlak - NORA Online

[13] Government 2 Government / Overheid naar Overheid

[14] https://tools.ietf.org/html/rfc2119

3. Best practices

3.1. Inperkingen van het NL GOV OAuth profiel

De best practices hieronder vereisen kennis van het NL GOV OAuth profiel. Alle voorschriften in het NL GOV OAuth profiel zijn van toepassing tenzij hieronder een uitzondering is aangegeven.

In het NL GOV OAuth profiel staan soms doorgehaalde teksten. Als de best practice in dit document afwijken van niet doorgehaalde tekst in het NL GOV OAuth profiel dan is deze tekst doorgehaald en rood gemaakt. Als de best practice in dit document afwijken van een doorgehaalde tekst in het NL GOV OAuth profiel dan is deze tekst rood gemaakt. Hiermee is het verschil met de in het NL GOV OAuth profiel teksten hopelijk duidelijk.

3.1.1. MUST: Client credentials flow

Deze best practice vereist de toepassing van de client credentials flow[15].

NL GOV OAuth use cases[16]:

- ~~There are two use cases: The client credentials flow and the authorization code flow.~~

3.1.2. MUST: Direct Access Client

Deze best practice vereist de toepassing van direct access clients.

NL GOV OAuth client types - Direct Access Client[17]:

- *This profile applies to clients that connect directly to protected resources and do not act on behalf of a particular resource owner, such as those clients that facilitate bulk transfers.*
- ~~*One of the client authentication methods private_key_jwt or tls_client_auth [rfc8705] MUST be used*~~.

3.1.3. May: Dynamic client registration

Conform NL GOV OAuth mag dynamic registration toegepast worden. We gaan er over het algemeen vanuit dat de direct access clients out-of-band worden geregistreerd via een registratieproces dat buiten deze best practice valt.

NL GOV OAuth Client Registration[18]:

- *Client registration MAY be completed by either static configuration (out-of-band, through an administrator, etc...) or dynamically.*

NL GOV OAuth Authorization Server Profile - Dynamic Registration[19]

- *Clients MUST NOT dynamically register for the client credentials grant type. Authorization servers MAY limit the scopes available to dynamically registered clients.*

[15] https://logius-standaarden.github.io/OAuth-NL-profiel/#use-case-client-credentials-flow
[16] https://logius-standaarden.github.io/OAuth-NL-profiel/#usecases
[17] https://logius-standaarden.github.io/OAuth-NL-profiel/#direct-access-client
[18] https://logius-standaarden.github.io/OAuth-NL-profiel/#client-registration
[19] https://logius-standaarden.github.io/OAuth-NL-profiel/#dynamic-registration

3.1.4. MUST: Client Authenticatie conform OIDC private_key_jwt methode

Deze best practice vereist dat client authenticatie bij het request naar het Token Endpoint van de Authorization Server is gebaseerd op een JWT conform RFC7523[20] en de OpenID Connect Core (OIDC[21]) private_key_jwt methode.

In de “iGov-NL : Additional content” wordt aangegeven dat de grant_type de waarde “authorization_code” moet bevatten en dat er code en redirect_uri opgenomen moet zijn. Deze best practice vereist confrom RFC6749 dat bij een request naar token endpoint door confidential clients (die zich moeten authenticeren) en toepassing van de client credentials grant het grant_type de waarde “client_credentials” moet hebben en dat de “code” en de “redirect_uri” niet opgenomen mogen worden.

NL GOV OAuth Requests to the Token Endpoint[22]:

- *Full clients, native clients with dynamically registered keys, and direct access clients as defined above MUST authenticate to the authorization server's token endpoint using a JWT assertion as defined by the [JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants][rfc7523] using only the private_key_jwt method defined in [OpenID Connect Core] [OpenID.Core].*

NL GOV OAuth Requests to the Token Endpoint *iGov-NL : Additional content*

- ~~*Direct access clients that are using the client credentials grant type and are not using 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].*~~
- ~~*In addition to private_key_jwt, the client authentication method tls_client_auth [rfc8705] MAY also be used.*~~
- *In addition to above signing methods, the Authorization server SHOULD support PS256 signing algorithm [RFC7518] for the signing of the private_key_jwt. Effectively, the Token Request has the following content:*
    - ~~*grant_type - Mandatory. MUST contain the value authorization_code*~~
    - ~~*code - Mandatory. MUST be the value obtained from the Authorization Response.*~~
    - ~~*redirect_uri - Mandatory. MUST be an absolute HTTPS URL, pre-registered with the Authorization Server.*~~
    - *client_id - Mandatory. MUST have the value as obtained during registration.*
    - *client_assertion_type - Mandatory. MUST have the value urn:ietf:params:oauth:client-assertion-type:jwt-bearer, properly encoded.*
    - *client_assertion - Mandatory. MUST have the above specified signed JWT as contents.*

3.1.5. MUST: Client Key en toepassing van PKIo certificaat

Het NL GOV OAuth profiel vereist dat PKIoverheid certificaten worden gebruikt als niet alle componenten onder de controle van één partij vallen. Deze best practices gaan uit van een ketensamenwerking waarbij per definitie sprake is dat de client beheerd wordt door een andere partij dan de beheerder van de resource server en authorization server. Deze best practices vereisen dan ook de toepassing van PKIoverheid certificaten. Gezien de toepassing van PKIoverheid wordt er een publiek en privaat sleutelpaar toegepast en wordt de ketenpartner geïdentificeerd op basis van een OIN.

[20] https://www.rfc-editor.org/rfc/rfc7523
[21] https://openid.net/specs/openid-connect-core-1_0.html
[22] https://logius-standaarden.github.io/OAuth-NL-profiel/#requests-to-the-token-endpoint

NL GOV OAuth Client keys[23]

- *Clients using the authorization code grant type or direct access clients using the client credentials grant type MUST have a public and private key pair for use in authentication to the token endpoint. These clients MUST register their public keys in their client registration metadata by either sending the public key directly in the jwks field or by registering a jwks_uri that MUST be reachable by the authorization server. It is RECOMMENDED that clients use a jwks_uri if possible as this allows for key rotation more easily. This applies to both dynamic and static (out-of-band) client registration.*
- *iGov-NL : Additional content*
  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. The PKIoverheid certificate MUST be included either as a x5c or as x5u parameter, as per [rfc7517] §4.6 and 4.7. Parties SHOULD at least support the inclusion of the certificate as x5c parameter, for maximum interoperability. Parties MAY agree to use x5u, for instance for communication within specific environments.

3.1.6. MUST: Access Token sub claim identificeert de client

Deze best practice vereist dat de sub claim in het access token gevuld is met de client_id.

NL GOV OAuth Connections with protected resources - JWT Bearer Tokens[24]

- Sub: ~~The identifier of the end-user that authorized this client, or~~ the client id of a client acting on its own behalf (such as a bulk transfer). ~~Since this information could potentially leak private user information, it should be used only when needed. End-user identifiers SHOULD be pairwise anonymous identifiers unless the audiance requires otherwise~~.
- iGov-NL : Additional content : ~~The identifier of the end-user that authorized this client. In iGov-NL the sub claim MUST be present as is evident from the use case in scope of this profile. Since this information could potentially leak private user information, end-user identifiers SHOULD be pairwise pseudonymious identifiers, unless another identifier is explicit needed and agreed upon for the context of the application.~~

3.1.7. MUST: Access token levensduur niet groter dan 1 uur

Deze best practice vereist dat de levensduur van een access token niet groter is dan 1 uur.

NL GOV OAuth Token lifetime[25]":

- ~~For clients using the client credentials grant type, access tokens SHOULD have a valid lifetime no greater than six hours.~~

3.2. Aanvullende voorschriften

3.2.1. MUST: Transportbeveiliging op basis van UBV TLS basisprofiel

Deze best practice vereist dat voor TLS de voorschriften van het Edustandaard Uniforme Beveiligingsvoorschriften (UBV TLS[26]) basisprofiel worden toegepast.

[23] https://logius-standaarden.github.io/OAuth-NL-profiel/#client-keys
[24] https://logius-standaarden.github.io/OAuth-NL-profiel/#jwt-bearer-tokens
[25] https://logius-standaarden.github.io/OAuth-NL-profiel/#token-lifetimes
[26] Meer informatie via Werkgroep Uniforme Beveiligingsvoorschriften:
https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/

3.2.2. MUST: API design conform Kennisplatform API Design Rules

Deze best practice vereist dat voor API design de API Design Rules van het Kennisplatform API's[27] worden toegepast.

[27] Meest recente versie NLGov REST API Design Rules (logius-standaarden.github.io), vastgestelde versie REST-API Design Rules (Nederlandse API Strategie IIa) 1.0 (logius.nl)