



# Oauth profiel v 1.1

---

## Kennisplatform API's

---





Logius  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

# **UPDATE 2024-05-13**

## **- Oauth NL profiel**

Door:  
Martin van der Plas - Logius



Toegang



Interactie



Gegevensuitwisseling



Infrastructuur

Regie op stelsels  
en standaarden

# Gegevensuitwisseling

Uw gegevens kunt u veilig, betrouwbaar en gestandaardiseerd uitwisselen tussen overheden, burgers en bedrijven. Logius maakt dit mogelijk als ketenpartner voor de digitale overheid. Daarbij bieden we ook oplossingen om de gegevens in de basisregistraties op orde te houden en uit te wisselen.

## Stelsels

- > Standard Business Reporting
- > PEPPOL

## Standaarden

- > Digikoppeling
- > XBRL
- > API Standaarden
- > e-Procurement

## Voorzieningen

- > Digipoort
- > Stelseldiensten
- > Stelselcatalogus
- > Digikoppeling compliance voorziening
- > Platform Stelsel voor basisregistraties
- > RijkOverheidsAccessPoint op PEPPOL
- > DigiInkoop

## Aanvullende dienstverlening

- > Kenniscentrum XBRL
- > e-Procurement diensten
- > Oneigenlijk gebruik & misbruik detectie



# De formele tekst en uitleg

## Een kort overzicht

Via API's kunnen applicaties gegevens uitwisselen. Hoe, wanneer en onder welke voorwaarden je gegevens uitwisselt beschrijven we in architectuur en standaarden.

Hoe API's zich verhouden tot de enterprise,- en/of solution architectuur is beschreven in de Nederlandse API Strategie en de NORA.

## Logius beheert de volgende API-standaarden:

- [De REST-API Design Rules \(ADR\)](#)
- [Het NL GOV Assurance profile for OAuth 2.0 \(OAuth-NL\)](#)
- [NL GOV Assurance profile for OpenID Connect](#)

Meer detail over de beheerde standaarden?

> [logius.nl/diensten/api-standaarden](https://logius.nl/diensten/api-standaarden)

## Hoe werkt het?

De API Standaarden die Logius beheert zijn ontstaan vanuit de Nederlandse API Strategie van het Kennisplatform API's.

In de voorbereidingsfase kunnen organisaties kennis nemen van de API standaarden die publiek toegankelijk gepubliceerd zijn. Vragen kunnen worden gemaild aan [api@logius.nl](mailto:api@logius.nl)

In de ontwikkelfase kunnen engineers en developers de standaarden toepassen bij de ontwikkeling van een API. Ook kunnen de API Design Rules worden geverifieerd met unit tests zodat kan worden vastgesteld dat de API qua design en techniek voldoet aan de standaarden.

In de operationele fase kan de API worden gepubliceerd op [developer.overheid.nl](https://developer.overheid.nl). Gepubliceerde API's worden automatisch getest op basis van de testbare design rules uit de standaard. De Open API Specificatie en test score van je API zijn daarna publiek toegankelijk voor gebruik door developers die iets voor of met de overheid ontwikkelen.

Meer (technische) informatie over de standaarden?

> [logius.nl/diensten/api-standaarden/hoe-werkt-het](https://logius.nl/diensten/api-standaarden/hoe-werkt-het)



Maarten van der Veen

Peter Haasnoot

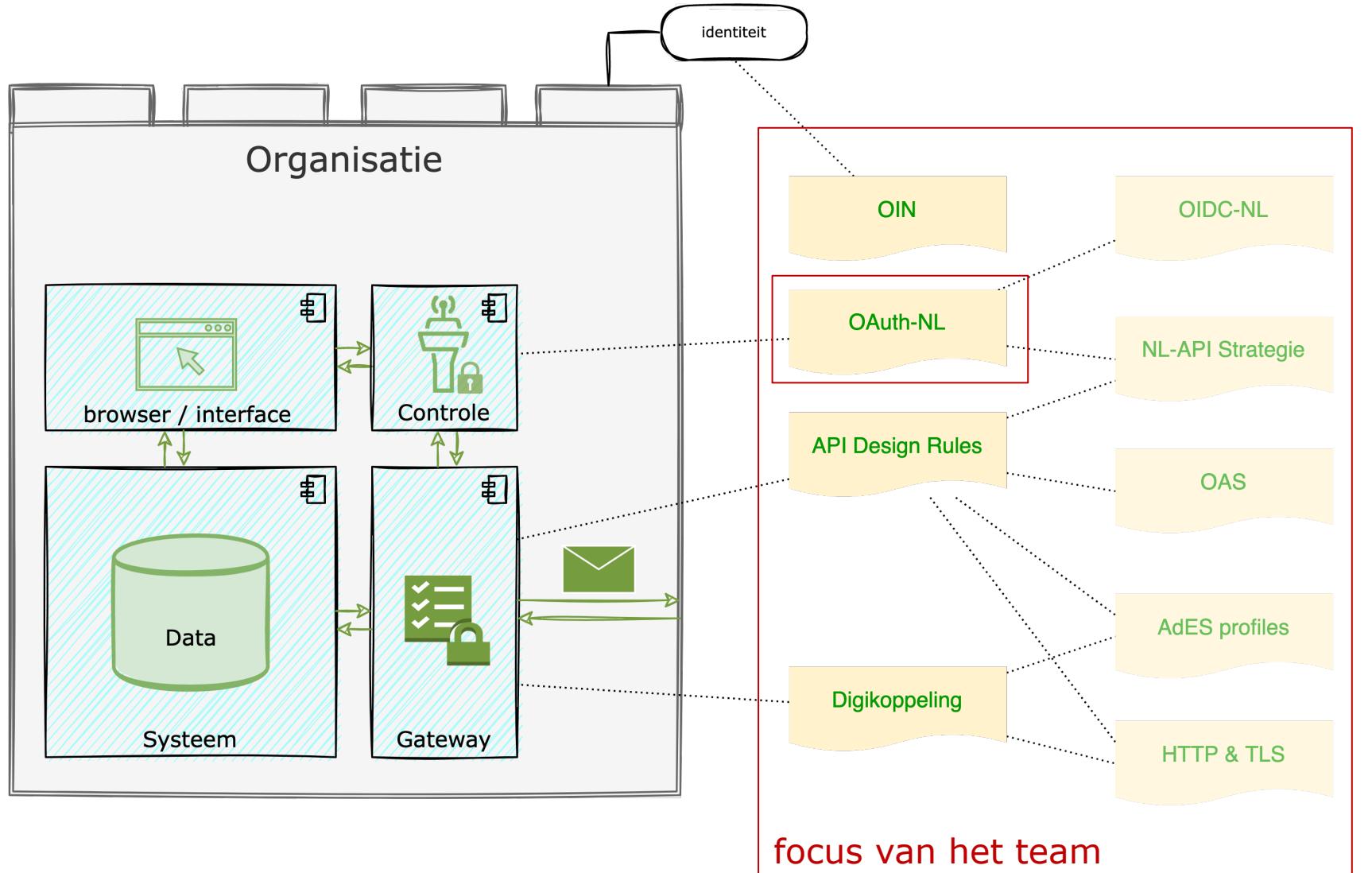
Edwin Wisse

Alexander Green

Martin van der Plas

# Ons Team

# Positionering standaarden



Internat en beweeglijk	
DKIM	Echtheidsmerk voor ontvangen mail
DMARC	Bijeld bij SPF- en DKIM ongeldige mail
DNSSEC	Controle van echtheid domeinnaam
HTPS en HTTPS	Versterking van webverkeer
IPV6 en IPv4	Internetadressering
ISO 27001	Managementsysteem informatiebeveiliging
ISO 27002	Richtlijnen en principes informatiebeveiliging
NL-GOV Assurance profile for OAuth 2.0	Automatie
RPKI	Veilige netwerk routing
SAML	Authenticatie
SPF	Machtiging om mail te verzenden
STARTTLS en DANE	Versleuteling van mailverkeer
STIX en TAXII	Uitwisseling van dreigingsinformatie
TLS	Extra versleuteling van webverkeer
WAPI en Enterprise	Toegang tot en WiFi-netwerk met account

Documenten en web applicaties	
ADFS Baseline Profiles	Digitaal ondertekenen van documenten
Digitegelsakket	Toegankelijkheid web content
ODF	Documenten voor bewerking
OWMS	Metadata overheidsinformatie
PDN (N-ISO)	Documenten voor afdrukken en/of archiveren
SKOS	Thesauri en begrippenoverboden
REST API's	
OpenAPI Specification	Beschrijven van REST API's
REST-API Design Rules	Structureren van REST API's
E-facturering en administratie	
NLICUS	Elektronische factureren

WDO Databank	Douane-informatie
XBRL	Bedrijfsrapportages
<b>Stelselstandaarden</b>	
Digikoppeling	Veilige berichtenuitwisselingen
Geo-standaarden	Geografische informatie
STUF	Uitwisseling administratieve overheidsgegevens

<b>Aquo-standaarden</b>	Waterbeheer
<b>GWSW</b>	Gegevenswoordenboek stedelijk waterbeheer
<b>SIV Basis</b>	Milieutechnische bodem/informatie

## SIKBo102 Archeologische bodeminformatie

NLCS	2D tekenstandaard
VISI	Bouwprocesinformatie

BWB	Wet- en regelgeving
ECLI	Rechterlijke uitspraken
JCDR	Decentrale regelgeving

Onderwijs en loopbaan	
E-Portfolio NL	Uitwisseling werkervaring en competenties
NL_LOM	Metadata onderwijscontent

## Overig

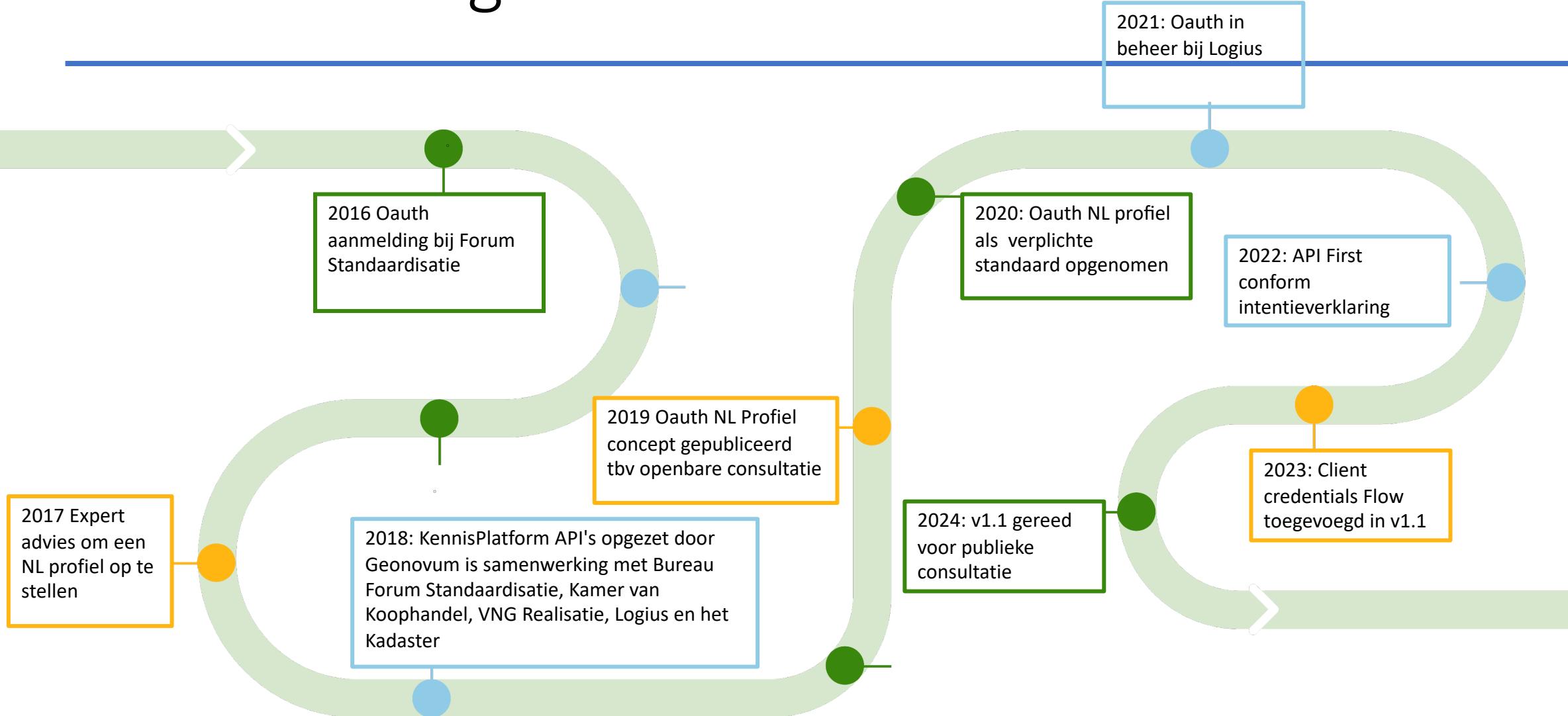
Een standaard is een afspraak over informatie of over een proces. Standaarden versoepelen de samenwerking tussen het bedrijfsleven, de burger en de overheid. Gebruik van open standaarden zorgt voor uitwisselbaarheid van digitale informatie, kostenbesparingen, innovatie en meer vrijheid bij het kiezen van leveranciers.

Overheden en organisaties in de publieke sector zijn verplicht de relevante open standaarden uit deze lijst te kiezen bij aanschaf van ICT-producten en -diensten vanaf €50.000,- Afwijken van deze

terug te vinden is in het jaarverslag.  
Heeft u hulp nodig om te beslissen welke standaarden u moet uitvragen? Gebruik de Beslisboom op onze website.  
Klik op [www.forumstandaardisatie.nl](http://www.forumstandaardisatie.nl) voor de meest actuele versie.

M: [info@forumstandaardisatie.nl](mailto:info@forumstandaardisatie.nl)  
T: 070 888 77 76

# Ontwikkeling OAuth





NL GOV Assurance profile for C X +

forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20

Home Menu

Voer uw zoekterm in Zoeken

[Forum Standaardisatie](#) > [Lijst open standaarden](#) > **NL GOV Assurance profile for OAuth 2.0**

## NL GOV Assurance profile for OAuth 2.0

OAuth 2.0 is een afspraak over de beveiliging van applicaties die gegevens uitwisselen met behulp van REST APIs. NL GOV Assurance is een Nederlandse versie van deze afspraak. Dankzij de beveiliging kunnen gebruikers een website of app autoriseren om hun gegevens via een REST API op te halen bij een ander systeem.

### Inhoudsopgave

Status Nut en werking Toepassing Toetsingsinformatie Detailinformatie

### Status



NL GOV Assurance profile for OAuth 2.0

https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.1.0-rc.1/

## TABLE OF CONTENTS

**Abstract**

**Status of This Document**

**Dutch government Assurance profile for OAuth 2.0**

Usecases

Introduction

Resource Server

Authorization Server

Client

Use case: Client credentials flow

Step 1. Client Authentication

Step 2. Access Token Response

Step 3. Resource interaction

Use case: Authorization code flow

Step 1. Authorization initiation

Step 2. Authorization Request

Step 3. User Authorization and consent

Step 4. Authorization Grant

# NL GOV Assurance profile for OAuth 2.0

**Logius Standard**

**Proposed version May 13, 2024**

**This version:**

<https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.1.0-rc.1/>

**Latest published version:**

<https://gitdocumentatie.logius.nl/publicatie/api/oauth/>

**Latest editor's draft:**

<https://logius-standaarden.github.io/OAuth-NL-profiel/>

**Previous version:**

<https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.0/>

**Editors:**

Frank Terpstra ([Geonovum](#))

Jan van Gelder ([Geonovum](#))

Alexander Green ([Logius](#))

Martin van der Plas ([Logius](#))

**Authors:**

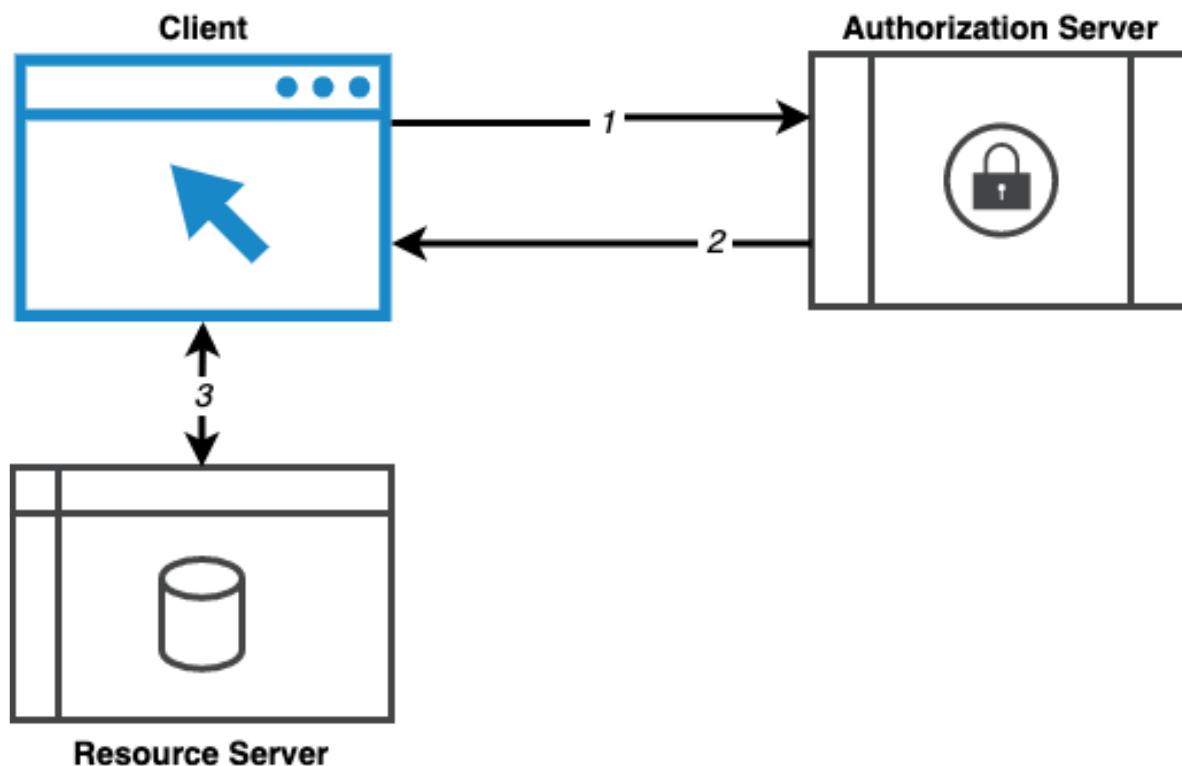
Jaron Azaria ([Logius](#))





## Verwerkt in versie 1.1

---



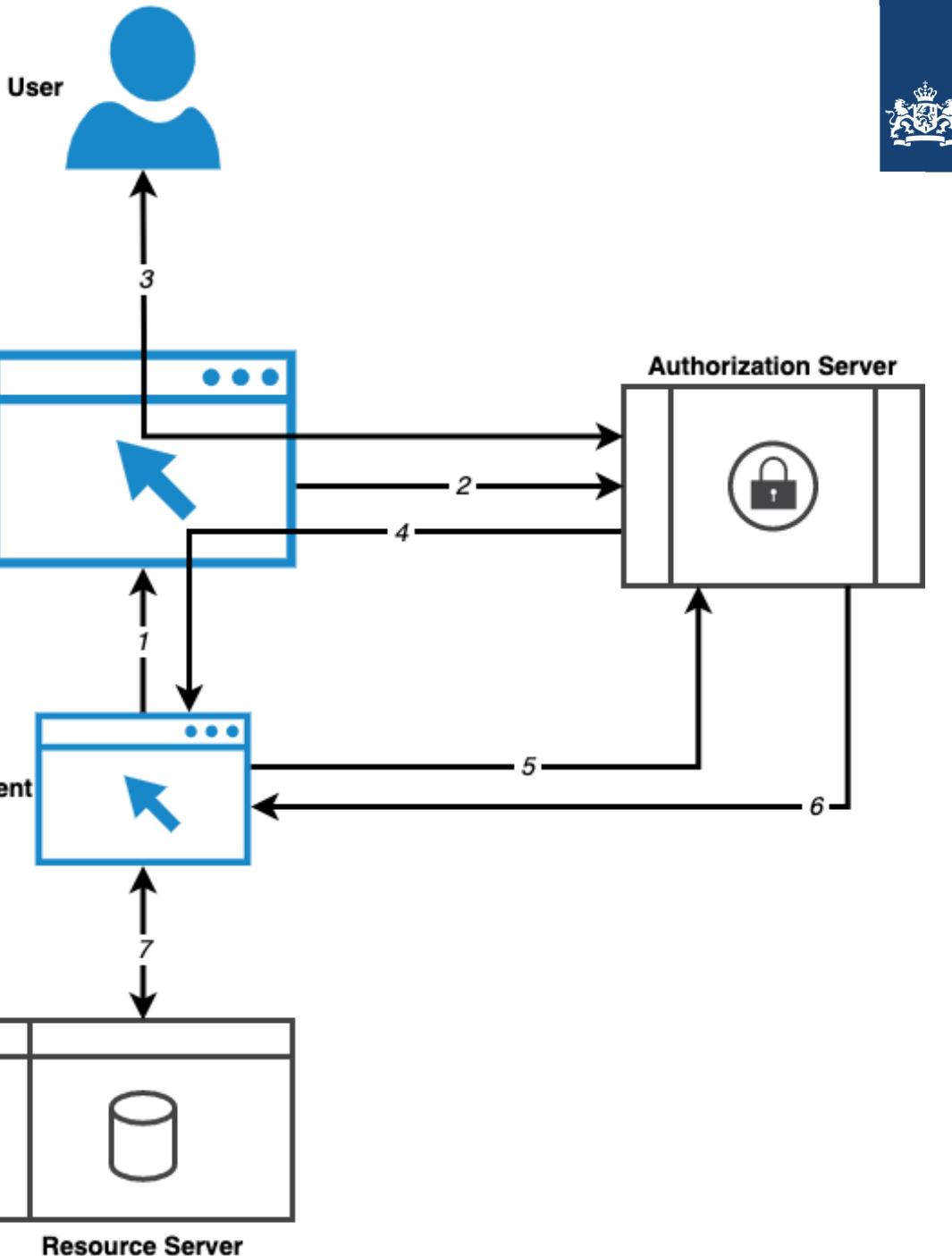
- Client credentials Flow
- Aangepaste opmaak



## Wat is het ?

---

“NL GOV Assurance profile for OAuth 2.0”



## Toelichting stappen

---

1. Authorization initiation
2. Authorization Request
3. User Authorization and consent
4. Authorization Grant
5. Access Token Request
6. Access Token Response
7. Resource interaction



## Client profiel

---

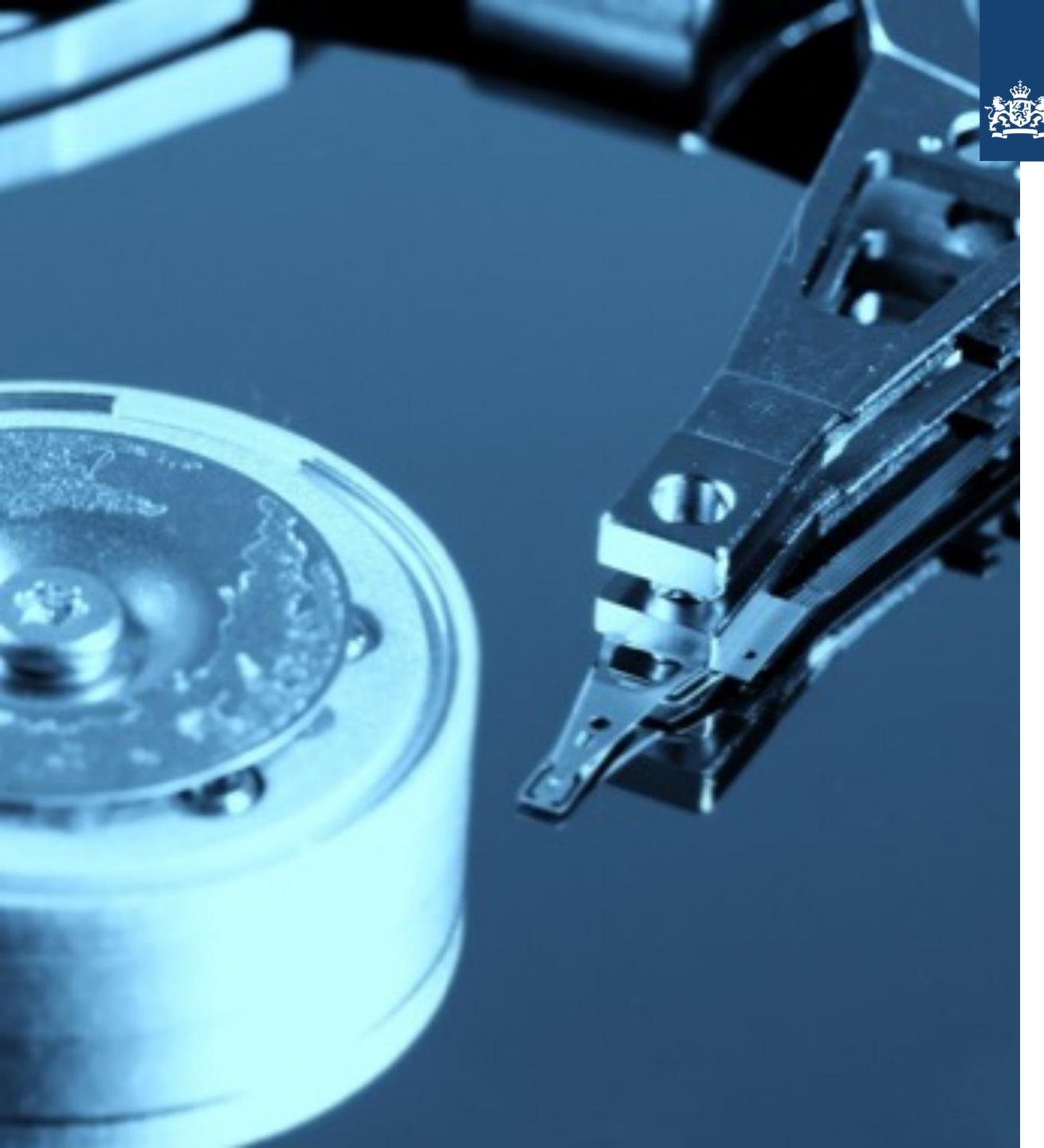
- Clients zijn Full clients, ofwel web applicaties die centraal draaien, of Native clients, instanties van software die draaien op het device van de user, de zogenaamde apps. Beide client types hebben verschillende vereisten.
- Clients moeten vooraf zijn geregistreerd bij de Authorization Server.
- Clients mogen geen gebruik maken van een redirect naar de localhost en mogen ook geen waardes doorsturen naar andere URI's.
- Clients moeten een willekeurige status parameter genereren en koppelen aan de client sessie om deze vervolgens mee te sturen naar de Authorization server en te verifiëren of deze ook correct in de response wordt meegegeven.
- Clients moeten de volledige redirect URI meesturen in het verzoek aan de Authorization server.
- De Authorization Server moet de redirect URI controleren ten opzichte van de URI die vooraf is geregistreerd door de Client.
- Native Clients moeten PCKE toepassen.
- Wanneer de API, Client en Authorisation Server niet onder verantwoordelijkheid vallen van één organisatie moeten PKIOverheid certificaten worden gebruikt (met OIN).
- Clients moeten autorisatie requests over TLS sturen en moeten het certificaat van de API verifiëren.



## Authorization Server profiel

---

- De Authorization Server moet alle communicatie versleutelen met TLS en voldoen aan alle security eisen.
- De Authorization Server moet dynamic client registration toestaan. De autorisatie server mag de Scopes beperken van dynamisch geregistreerde clients.
- De Authorization Server moet de user laten weten welke Client is geregistreerd en welke access die Client vraagt.
- De Authorization Server moet OpenID.Discovery aanbieden.
- De Authorization Server moet op verzoek van de Client tokens intrekken.
- De Authorization Server moet JWT tokens verstrekken die de API kan verifiëren.
- De Authorization Server moet authenticatie vereisen voor de revocation en introspection endpoints.
- Alle uitgegeven tokens mogen worden ingetrokken.
- Access tokens hebben verschillende lifetimes.
- De Authorization Server zou Scopes moeten definiëren en documenteren.



## Protected Resource (API) profiel

---

- De API geeft de Client toegang wanneer deze een geldig access token en de correcte Scope heeft. De API vertrouwd erop dat de Authorization Server de security en access control borgt.
- De API (met vertrouwelijke data) die een hoger vertrouwensniveau vereist van de eindgebruiker moet de data alleen beschikbaar stellen binnen een unieke Scope.
- De Client die vertrouwelijke data wil opvragen bij de API moet een hoger vertrouwensniveau Scope meegeven in het verzoek aan de Authorization Server.
- De Authorization Server moet de authenticatie van de eindgebruiker op het juiste vertrouwensniveau vaststellen.
- Een API moet Bearer tokens accepteren in de authorization header en mag deze ook accepteren als form parameter.
- Een API mag geen access tokens accepteren als query parameter.
- Een API moet documenteren welke scopes vereist zijn voor toegang tot vertrouwelijke data.
- Een API moet een access token verifiëren.
- Een API moet limiteren welke Authorization Servers het vertrouwt.



## PUBLICATIE

---

- Github
  - <https://github.com/Logius-standaarden>
- Latest version
  - <https://gitdocumentatie.logius.nl/publicatie/api/oauth/>
- Direct link
  - <https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.1.0-rc.1/>
- Forum Standaardisatie
  - <https://forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>
- Repository
  - <https://github.com/Logius-standaarden/OAuth-NL-profiel>



## OIDC

The screenshot shows the header of the website with the Dutch Royal Coat of Arms. Below it is a navigation bar with 'Home' and '☰ Menu'. A search bar contains 'Voer uw zoekterm in' and a 'Zoeken' button. The main content area shows the breadcrumb 'Forum Standaardisatie > Lijst open standaarden > OIDC'.

### OIDC

#### Inhoudsopgave

Status Nut en werking Detailinformatie Toepassing Toetsingsinformatie

#### Status

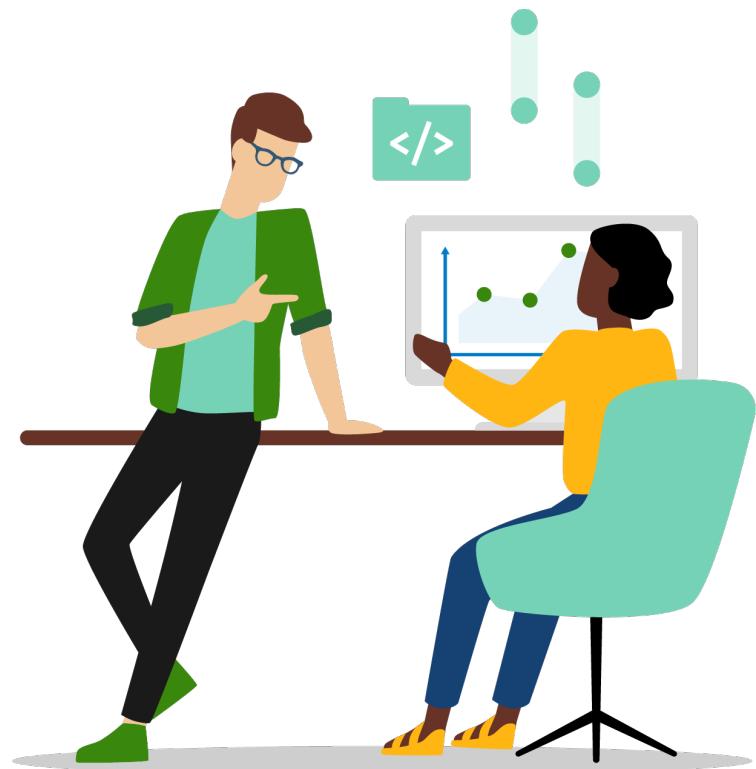
Lijst status ⓘ	Aanbevolen
Functioneel toepassingsgebied ⓘ	OpenID Connect kan toegepast worden bij het beschikbaar stellen van federatieve authenticatiediensten.
Organisatorisch werkingsgebied ⓘ	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
Europese status ⓘ	Nee

- <https://www.forumstandaardisatie.nl/open-standaarden/oidc>

- Opgenomen op de ‘Pas toe of leg uit’ lijst.



# Vragen



> Mail naar [API@Logius.nl](mailto:API@Logius.nl)