Roadmap OAuth

Heiko Hudig

Martin van der Plas

Alexander Green

Mogelijke uitbreidingen met nieuwe RFC’s van de OpenID foundation (2018-2023)

Wat is het ?

Betreft:
NL GOV Assurance profile for OAuth 2.0
NL GOV Assurance profile for OpenID Connect 1.0

Gebaseerd op IGov profile

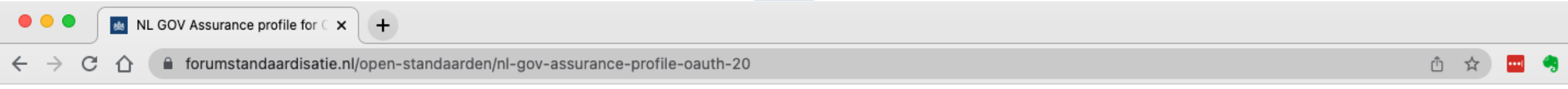
Versie 1 op de lijst verplichte standaarden

Versie 1.1 is in behandeling bij het MIDO en Forum Standaardisatie

Versie 1.2 zie Roadmap ;-)

Versie 2 ?

Inhoudsopgave



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

Logius Standard - Proposed version

TABLE OF CONTENTS

NL GOV Assurance profile for OAuth 2.0

Logius Standard
Proposed version July 10, 2024

This version:
https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.1.0-rc.2/

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)

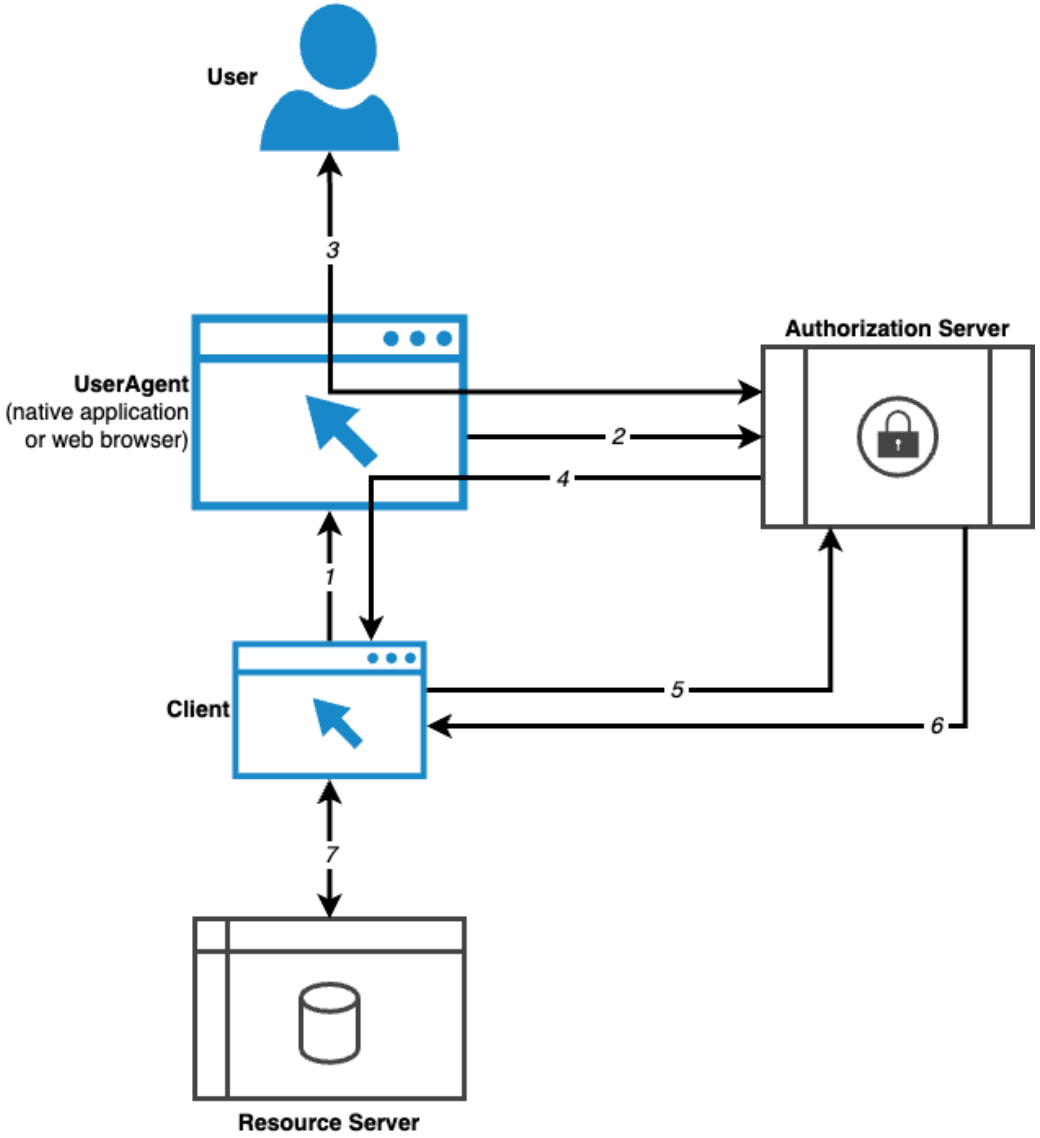
Authors:

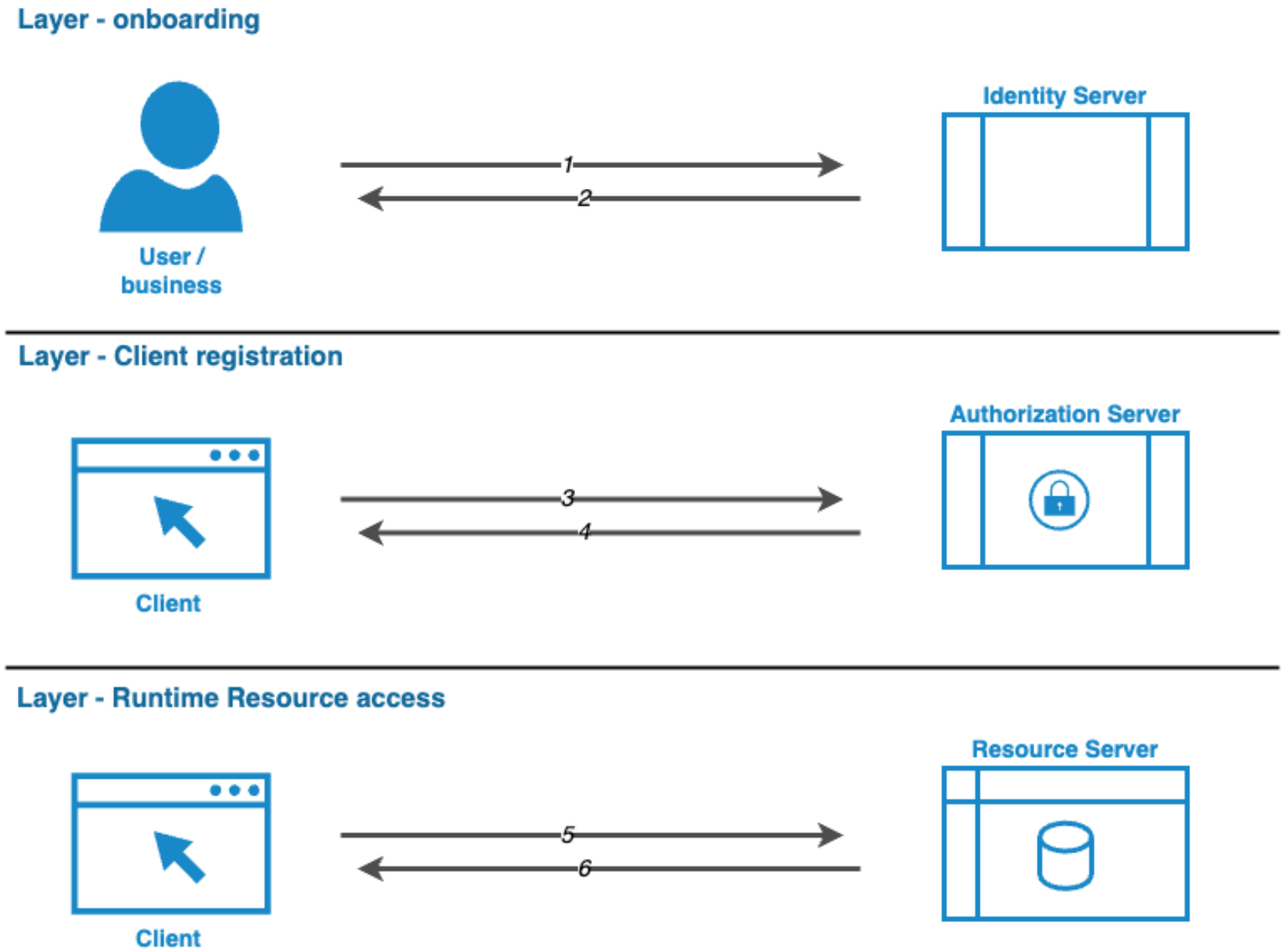
Jaron Azaria (Logius)
Martin Borgman (Kadaster)
Marc Fleischeuers (Kennisnet)
Peter Haasnoot (Logius)
Leon van der Ree (Logius)
Bob te Riele (RvIG)
Remco Schaar (Logius)
Frank Terpstra (Geonovum)
Jan Jaap Zoutendijk (Rijkswaterstaat)

Participate:

GitHub Logius-standaarden/OAuth-NL-profiel

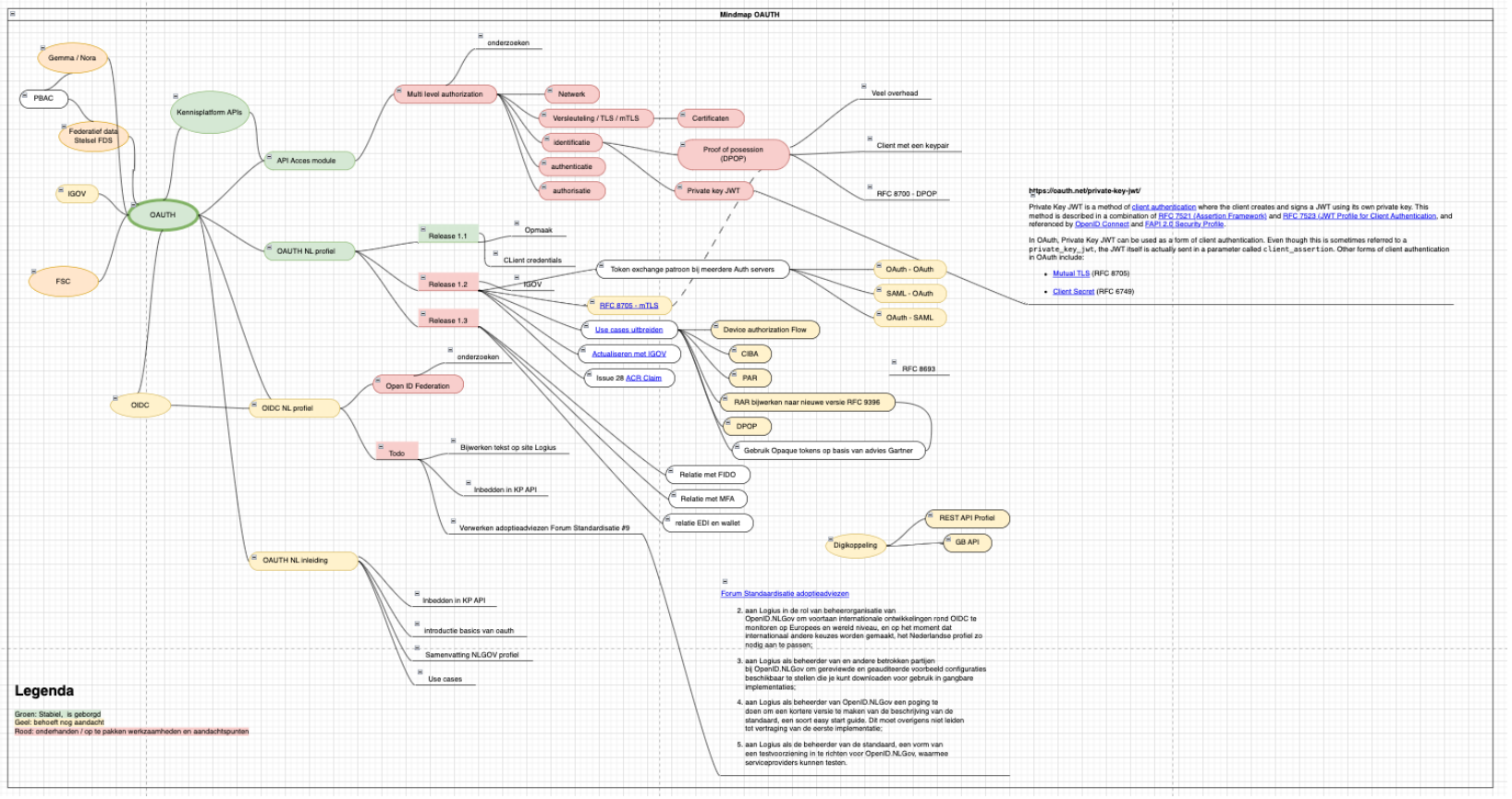
Authorization code flow




Layer - onboarding
Identity Server
1
2
User / business
Layer - Client registration
Authorization Server
3
4
Client
Layer - Runtime Resource access
Resource Server
5
6
Client

Inhoudsopgave

Mindmap


Mindmap OAUTH
Gemma / Nora
PBAC
Federatief data Stelsel FDS
IGOV
FSC
OAUTH
OIDC
Kennisplatform APIs
API Acces module
OAUTH NL profiel
OIDC NL profiel
OAUTH NL inleiding
Multi level authorization
onderzoeken
Netwerk
Versleuteling / TLS / mTLS
identificatie
authenticatie
authorisatie
Certificaten
Proof of posession (DPOP)
Private key JWT
Veel overhead
Client met een keypair
RFC 8700 - DPOP
Release 1.1
Opmaak
CLient credentials
Release 1.2
IGOV
Release 1.3
RFC 8705 - mTLS
Use cases uitbreiden
Actualiseren met IGOV
Issue 28 ACR Claim
Token exchange patroon bij meerdere Auth servers
OAuth - OAuth
SAML - OAuth
OAuth - SAML
Device authorization Flow
CIBA
PAR
RFC 8693
RAR bijwerken naar nieuwe versie RFC 9396
DPOP
Gebruik Opaque tokens op basis van advies Gartner
Open ID Federation
onderzoeken
Todo
Bijwerken tekst op site Logius
Inbedden in KP API
Verwerken adoptieadviezen Forum Standardisatie #9
Relatie met FIDO
Relatie met MFA
relatie EDI en wallet
Digkoppeling
REST API Profiel
GB API
Inbedden in KP API
Introductie basics van oauth
Samenvatting NLGOV profiel
Use cases
https://oauth.net/private-key-jwt/
Private Key JWT is a method of client authentication where the client creates and signs a JWT using its own private key. This method is described in a combination of RFC 7521 (Assertion Framework) and RFC 7523 (JWT Profile for Client Authentication, and referenced by OpenID Connect and FAPI 2.0 Security Profile.
In OAuth, Private Key JWT can be used as a form of client authentication. Even though this is sometimes referred to a private_key_jwt, the JWT itself is actually sent in a parameter called client_assertion. Other forms of client authentication in OAuth include:
Mutual TLS (RFC 8705)
Client Secret (RFC 6749)
Forum Standaardisatie adoptieadviezen
2. aan Logius in de rol van beheerorganisatie van OpenID.NLGov om voortaan internationale ontwikkelingen rond OIDC te monitoren op Europees en wereld niveau, en op het moment dat internationaal andere keuzes worden gemaakt, het Nederlandse profiel zo nodig aan te passen;
3. aan Logius als beheerder van en andere betrokken partijen bij OpenID.NLGov om gereviewde en geauditeerde voorbeeld configuraties beschikbaar te stellen die je kunt downloaden voor gebruik in gangbare implementaties;
4. aan Logius als beheerder van OpenID.NLGov een poging te doen om een kortere versie te maken van de beschrijving van de standaard, een soort easy start guide. Dit moet overigens niet leiden tot vertraging van de eerste implementatie;
5. aan Logius als de beheerder van de standaard, een vorm van een testvoorziening in te richten voor OpenID.NLGov, waarmee serviceproviders kunnen testen.
Legenda
Groen: Stabiel, is geborgd
Geel: behoeft nog aandacht
Rood: onderhanden / op te pakken werkzaamheden en aandachtspunten

Milestones

Labels | Milestones

New milestone

4 Open ✓ 0 Closed Sort

v1.1 - Client credentials Flow

Past due by 2 months Last updated 2 months ago

96% complete 1 open 28 closed

Edit Close Delete

minor release met

- een aanvulling voor de Client credentials Flow
- verschillende kleine correcties en verbeteringen

Inleidend document API Access Standaarden

Due by December 31, 2024 Last updated 2 months ago

0% complete 2 open 0 closed

Edit Close Delete

v1.2 - uitbreiding en actualisering

Due by July 01, 2025 Last updated 2 months ago

0% complete 9 open 0 closed

Edit Close Delete

Placeholder voor de volgende release

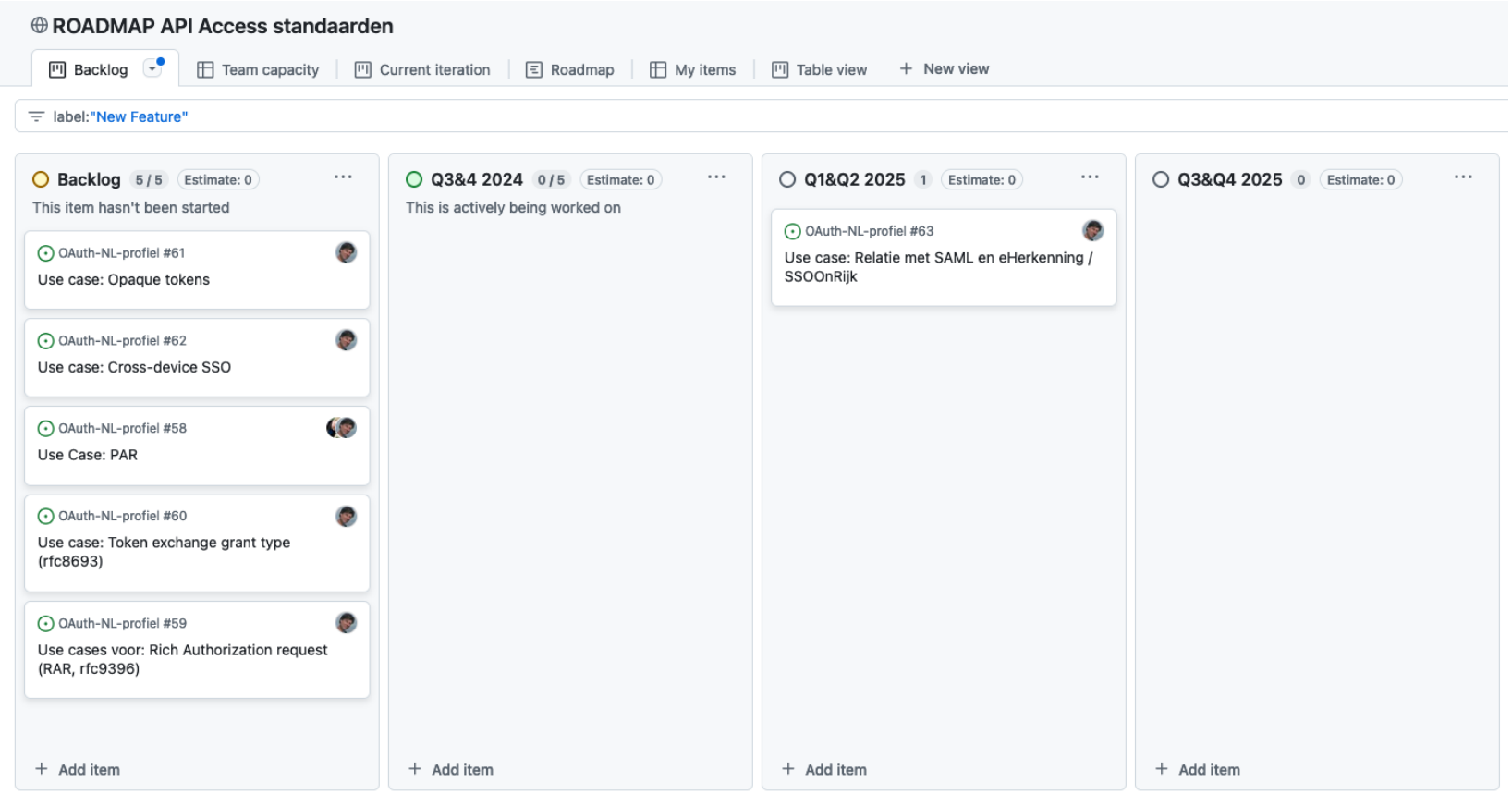
V2 tbd

Due by July 01, 2025 Last updated 2 months ago

0% complete 0 open 0 closed

Edit Close Delete

Roadmap - voorlopig



Link: https://github.com/orgs/Logius-standaarden/projects/2/views/1?filterQuery=label%3A%22New+Feature%22

Inhoudsopgave

Inhoudsopgave

Inhoudsopgave

Aanleiding

Mindmap

Toelichting en nut bij iedere RFC

Vragen

Aangeven prioriteit

(met geeltjes)

- 3? Post-it briefjes per persoon
- De volgende onderwerpen
- Je mag er iets bijschrijven, hoeft niet.

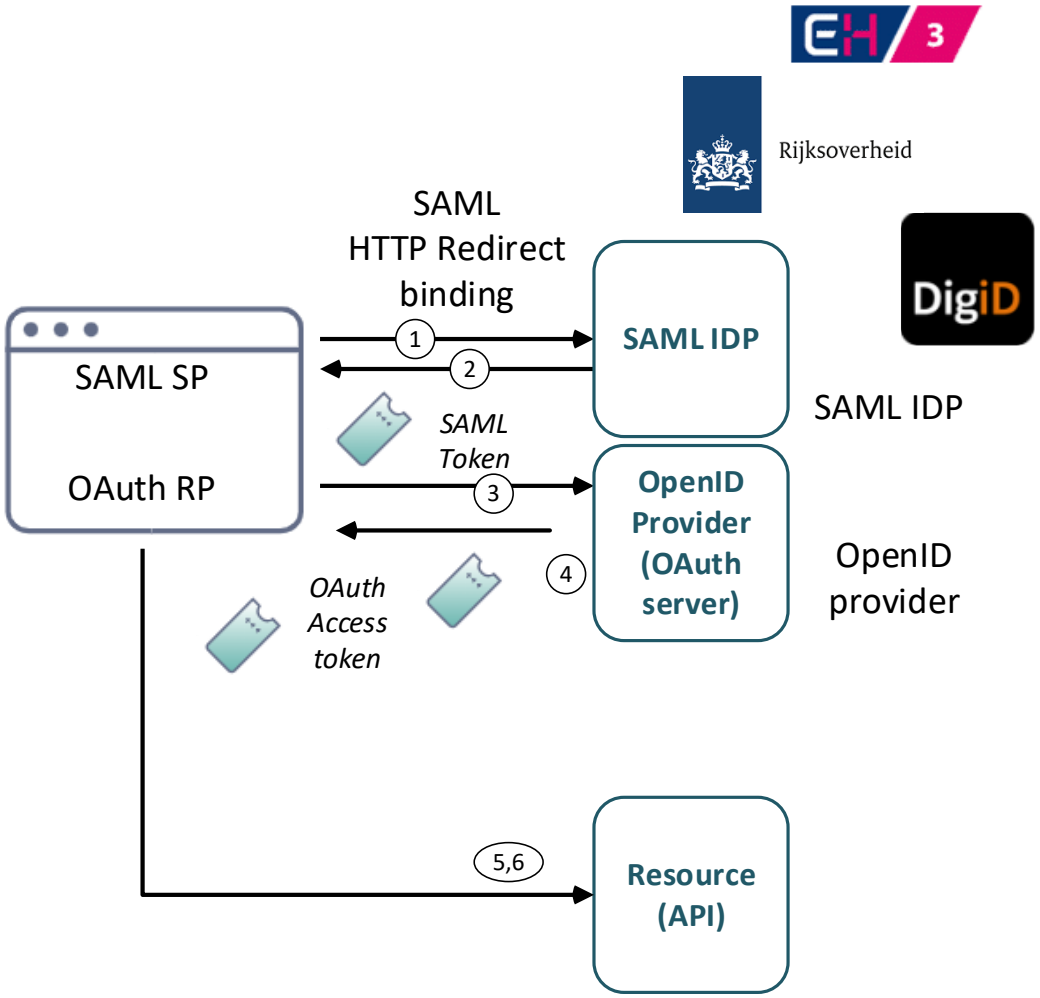
Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Token exchange en assurance levels van identity attributen.

OAuth token exchange
Interoperabiliteit met DigiD, eHerkenning en SSOnrijk
Toelichting bij authorization code flow.
Identity Assurance (draft)

OAuth token exchange (RFC8693)

→ Vanuit de client (Relying Party)



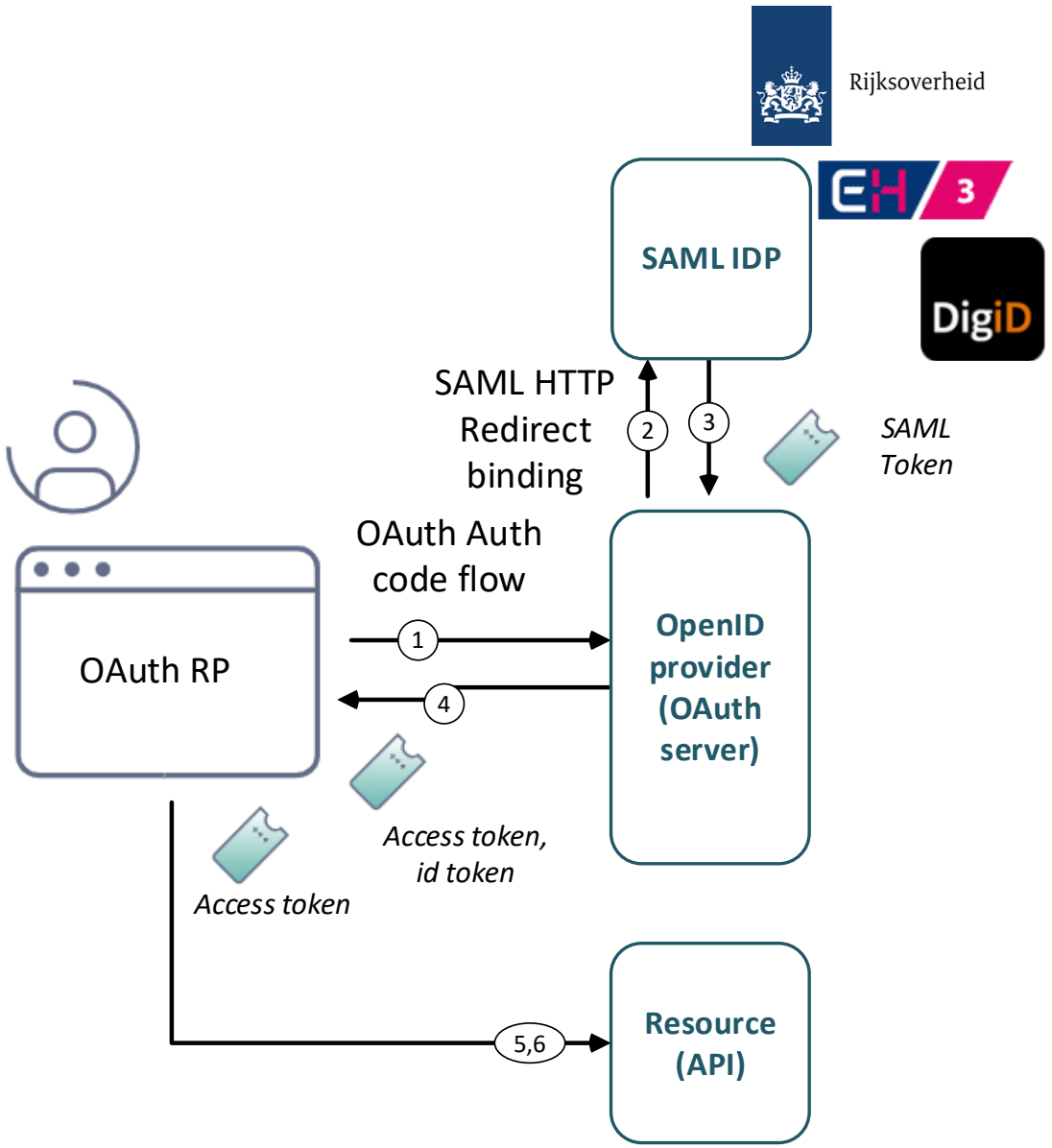
Token exchange: inwisselen van een token voor ander token (van een ander domein)

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

1. Inwisselen van een SAML token voor een OAuth token (bijvoorbeeld DigiD, eherkenning SSOnRijk)
2. Inwisselen tokens tussen oveheidsorganisaties.

Randvoorwaarden/beperkingen

- Client moet zowel SAML als OAuth implementeren



OAuth en inloggen op een SAML IDP (zonder token exchange).

Inloggen met OAuth client

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

- Een OAuth client appicatie wil gebiuik maken van een SAML IDP zoals DigiD, eHerkenning of SSOnRijk

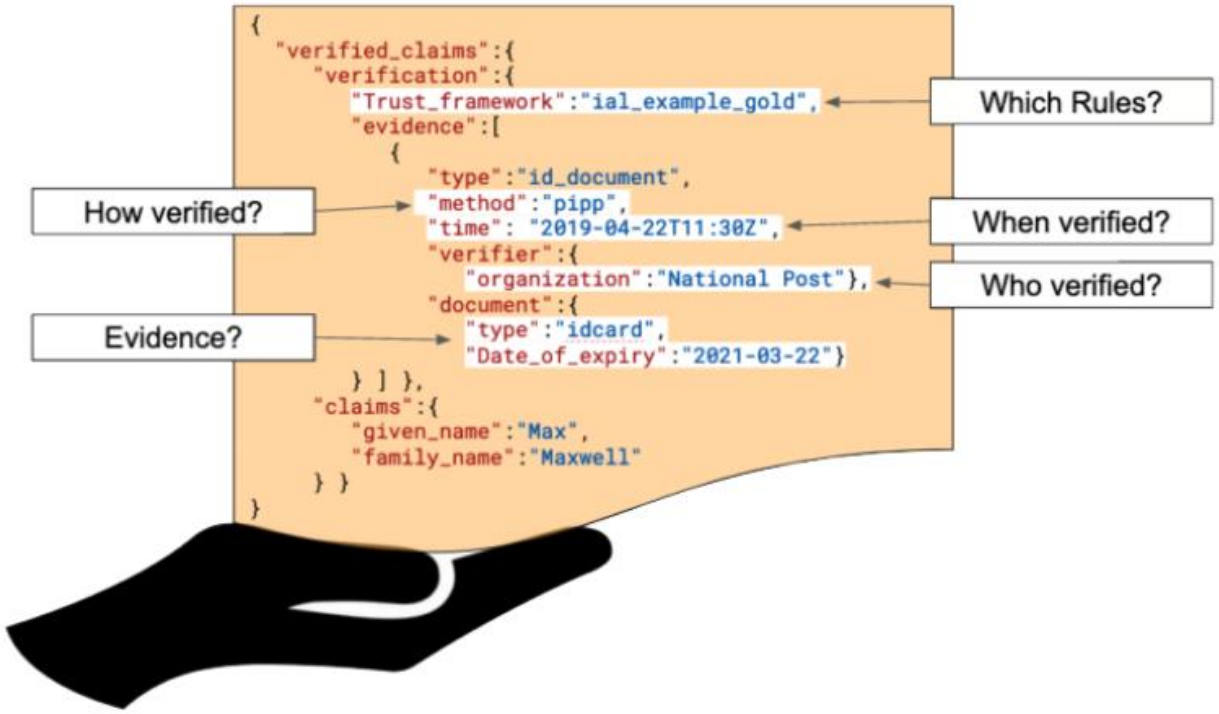
Randvoorwaarden/beperkingen

- OpenID provider vertaalt tussen OAuth en SAML

Aandachtgebieden

- Assurance levels bij de identiteisvastelling (WID-controle) (zie volgende slide)
- Inlogniveau. Dit is reeds beschreven in de NL GOV Assurance profile for OpenID Connect 1.0, en bevat voorbeelden voor de invulling van acr_value claims met het eIDAS stelsel.
- Aandachtpunten bij de technische vertaling tussen SAML en OAuth.

OpenID for identity assurance



Identiteitsvaststelling bij de WID-controle

- Beschrijft het zekerheidsniveau van de identiteitsattributen bij de WID controle. (en andere kenmerken in dat proces)
- Heeft betrekking op de userInfo en id_token specificaties
- Toe te passen bij eHerkenning, eIDAS, of de identiteitsvaststelling bij (semi)oveheden en bedrijven.

Randvoorwaarden/beperkingen

- Is een raamwerk, bevat dus geen direct bruikbare specificaties/voorbeelden.
- Voor eIDAS zijn er voorbeelden opgenomen.
- Toepassing in bijvoorbeeld SSOnRijk, of specificaties op organisatieniveau zal opgepakt moeten worden met andere werkgroepen.
- De specificatie is in draft, dus kan nog wijzigen.

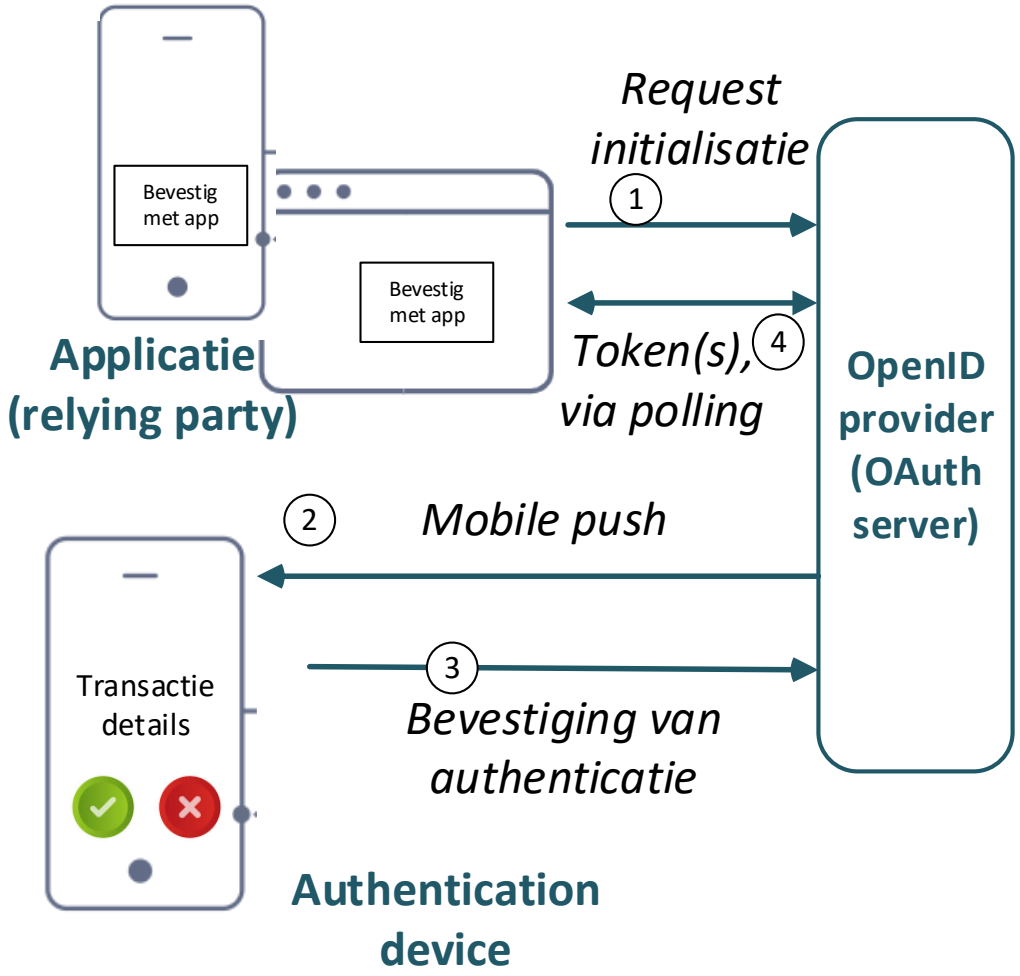
Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inloggen of bevestigen met een mobiele app

OAuth device authorization grant
Client initiated backchannel authentcation (CIBA)

bevestigen met mobiele apps (usability)

Client initiated backchannel authentication (CIBA)



Essentie: bevestigen van een transactie / step-up via een push bericht naar een mobiele app.

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

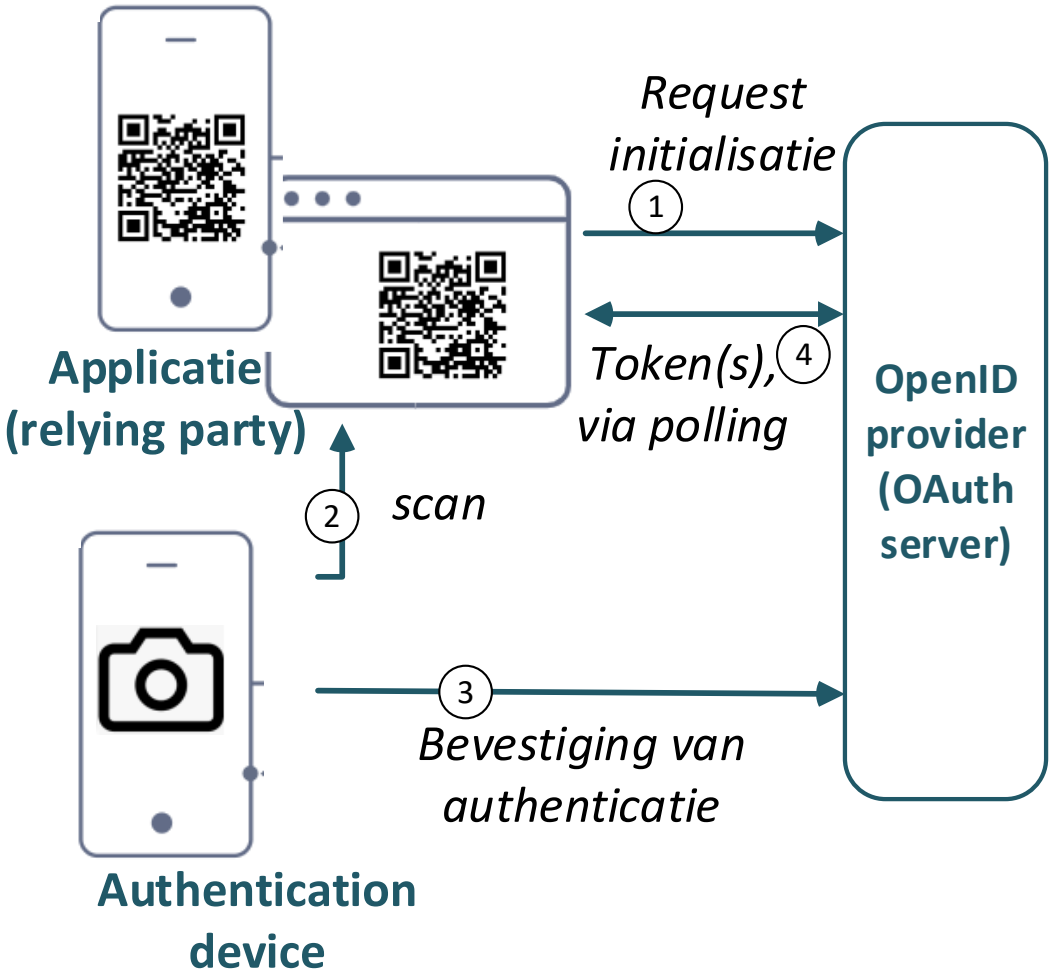
- Inloggen via pushbericht
- Goedkeuren/bevestigen van een transactie (step-up)
- Goedkeurig door een tweede persoon: bijvoorbeeld een burger of een medewerker met bepaalde bevoegdheden.

Randvoorwaarden/beperkingen

- Vereist een push mechansime naar de app zoals GCM/Firebase
- Vereist wel een "authentication device": een app met bijvoorbeeld biometrie of passcode (bijvoorbeeld o.b.v. FIDO2 en een bevestigingsmechanisme dan aansluit op CIBA.
- Alleen toe te passen in een confidential client (dus een client met een private key of secret)

Inloggen/bevestigen met mobiele apps (usability)

OAuth Device Authorization grant (RFC8628)



Essentie: Inloggen op een applicatie of bevestigen van een transactie via een QR code scan, bluetooth of NFC.

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

- Inloggen op een multi-user applicatie. Bijvoorbeeld een webapplicatie, tablet of een applicatie in een gedeelde ruimte.
- Goedkeuren/bevestigen van een transactie (step-up) of toegang tot een fysieke ruimte. (kan eventueel i.c.m. RAR, rfc9396)
- Registeren van een nieuwe app of (IoT) apparaat (is dan herleidbaar naar persoon, zie o.a. de IoT richtlijnen van de VNG)

Voordelen

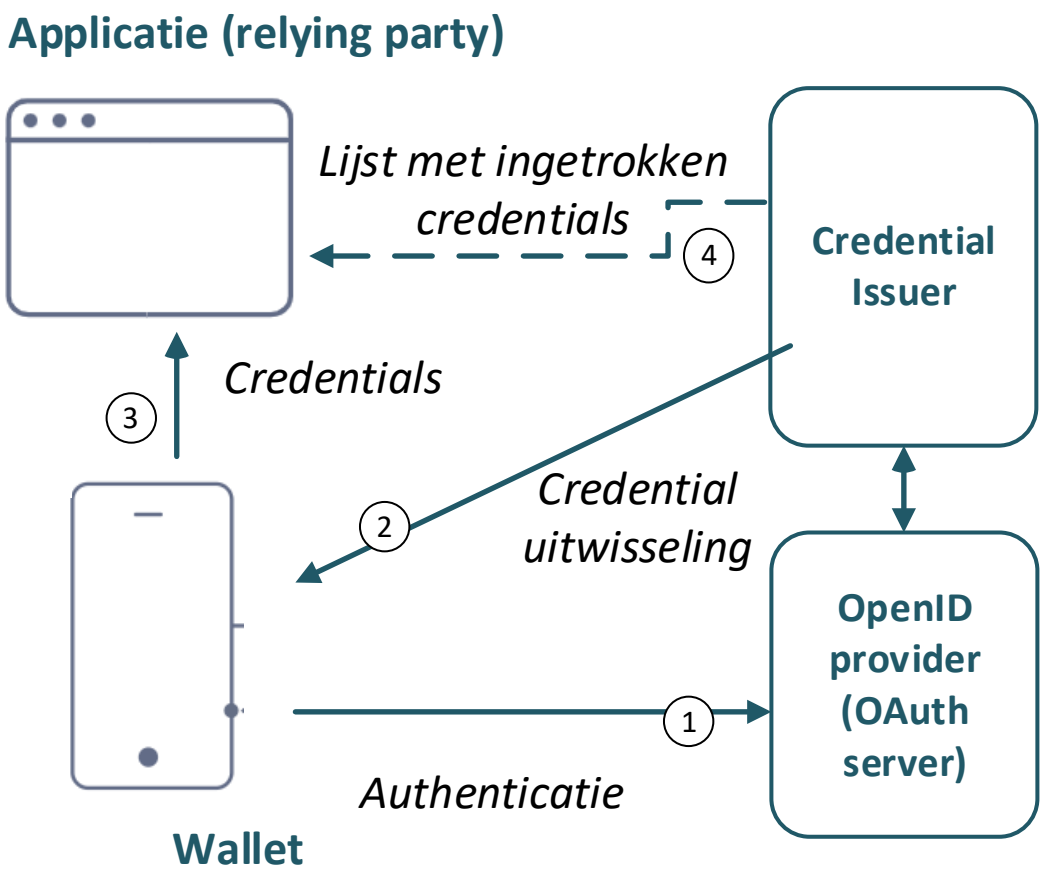
- Eenvoudig te implementeren. (Veel eenvoudiger dan alternatieven zoals de OIDC4VC of custom mechanismen zoals IRMA.)
- Kan worden aangevuld met extra security maatregelen via rfc's zoals (D)PoP, RAR, of message signing en encryptie.

Randvoorwaarden/beperkingen

- Vereist wel een "authentication device": een app met bijvoorbeeld biometrie of passcode (bijvoorbeeld o.b.v. FIDO2)

OpenID for Verilable Credentials

OPENID4VC



Essentie: bewaren en gebruiken van credentials in een wallet

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

- Mogelijkheid om persoonsgegevens gegevens in een wallet te bewaren en door te geven aan een applicatie (Relying Party) zonder dat de uitgevende overheidsinstantie (Issuer) dit te weten kan komen.
- Specificatie ligt aan de basis van de EU ID-wallet.

Randvoorwaarden/beperkingen

- Maakt gebruik van verschillende andere, in deze presentatie genoemde, RFCs
- Bevat verschillende opties

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Machtigingen, ondertekenen, transacties en consent

Rich Authorization Requests (RAR) – RFC9396
Samenhang met Consent uit de OAuth spec - RFC6749
Samenhang met module signing en encryptie (Logius)
Samenhang met Pushed Authorization Requests - PAR (RFC9126)

Rich Authorization Requests (RAR) RFC9396

In de client applicatie (relying party)

Wanneer is deze specificatie te gebruiken?

In alle situaties waar een specifieker access token gewenst is (specifieker dan een generieke scope aanduiding zoals een ketenproces)

- Goedkeuren / bevestigen van een document / transactie / verzoek
- Ondertekenen van een aangifte, acte of document.
- Vaak in combinatie met opnieuw inloggen.

Voordelen.

- Standaard OAuth voor step-up (inlog of bevesting) en consent.
- Verantwoordelijkheid van consent bij de authorization server.
- Werkt zoals ieder OAuth access token met alle mogelijkheden van dien. Dus extra security maatregelen zoals PAR, (D)PoP, toe te voegen
- Toe te passen in verschillende grant types waaronder de authorization code grant type, CIBA, Device authorization, etc.
- Attributen kunnen back-channel worden uitgewisseld, bijvoorbeeld persoongegevens, activatiecodes. Of het gehele access token op de client is een opaque token.
- Minimale effort/verantwoordelijkheid voor de developer van de client applicatie

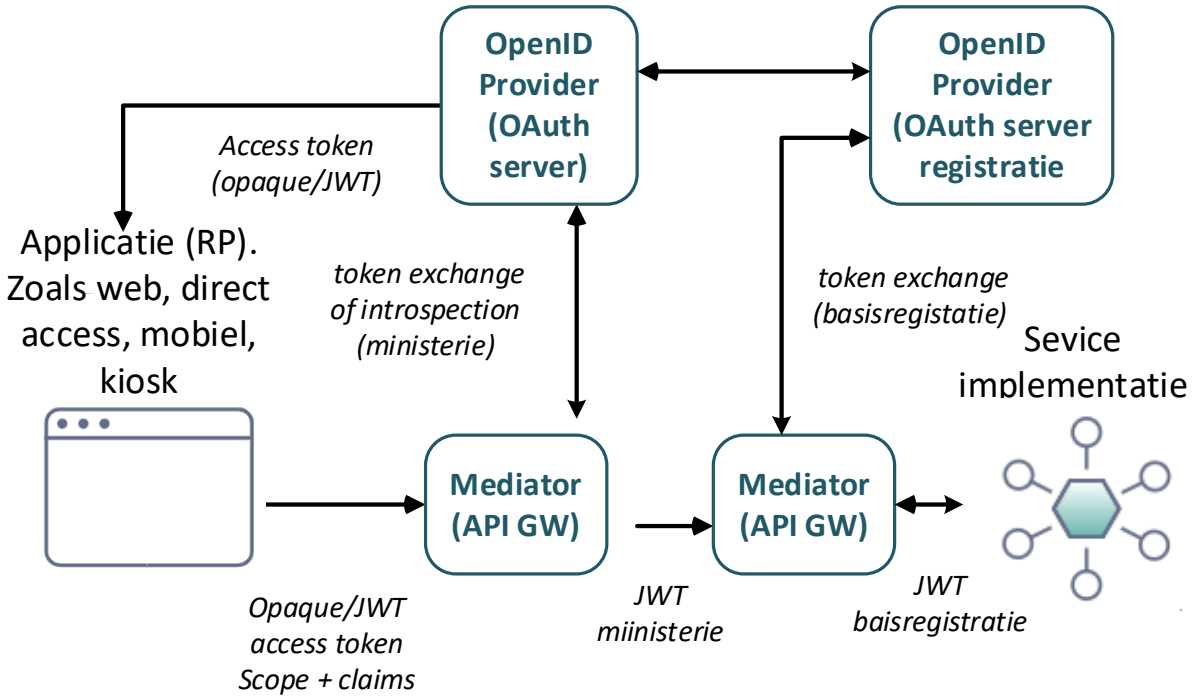
Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Autorisatie en rechtendelegatie

Token exchange - RFC8693
Rich Authorization Requests (RAR) – RFC9396
Verduidelijking “represents” claim

OAuth token exchange (RFC8693)

→ Vanuit de Edge of resource (API)



Essentie: inwisselen van een token voor een token van een ander domein

Wanneer is dit inlogmechanisme (grant type) te gebruiken?

Inwisselen van een OAuth token voor een (OAuth/Saml) token van een ander domein. bijvoorbeeld

- Aanroepen van API's in andere domeinen, zoals een (andere) basisregistratie of ministerie.
- Samenstellen van een token met specifieke autorisatie claims voor een bepaalde API (Daarbij kan optioneel gebruik worden gemaakt van maken van rfc9396 (RAR) en/of SCIM groepen)
- Delegation. Combineren van twee tokens tot een enkel token om een machtigings/delegatie relatie te propageren. Voor machtigen tussen rechtspersonen gebruiken we het "*represents*" claim (Zie NLGOV OIDC) op een soortgelijke wijze (omgekeerde relatieweergave).

Randvoorwaarden/beperkingen

- Flexibel mechanisme, dus nadere afspraken zijn noodzakelijk.
- Voor- en nadelen van het patroon diene goed afgewogen te worden.

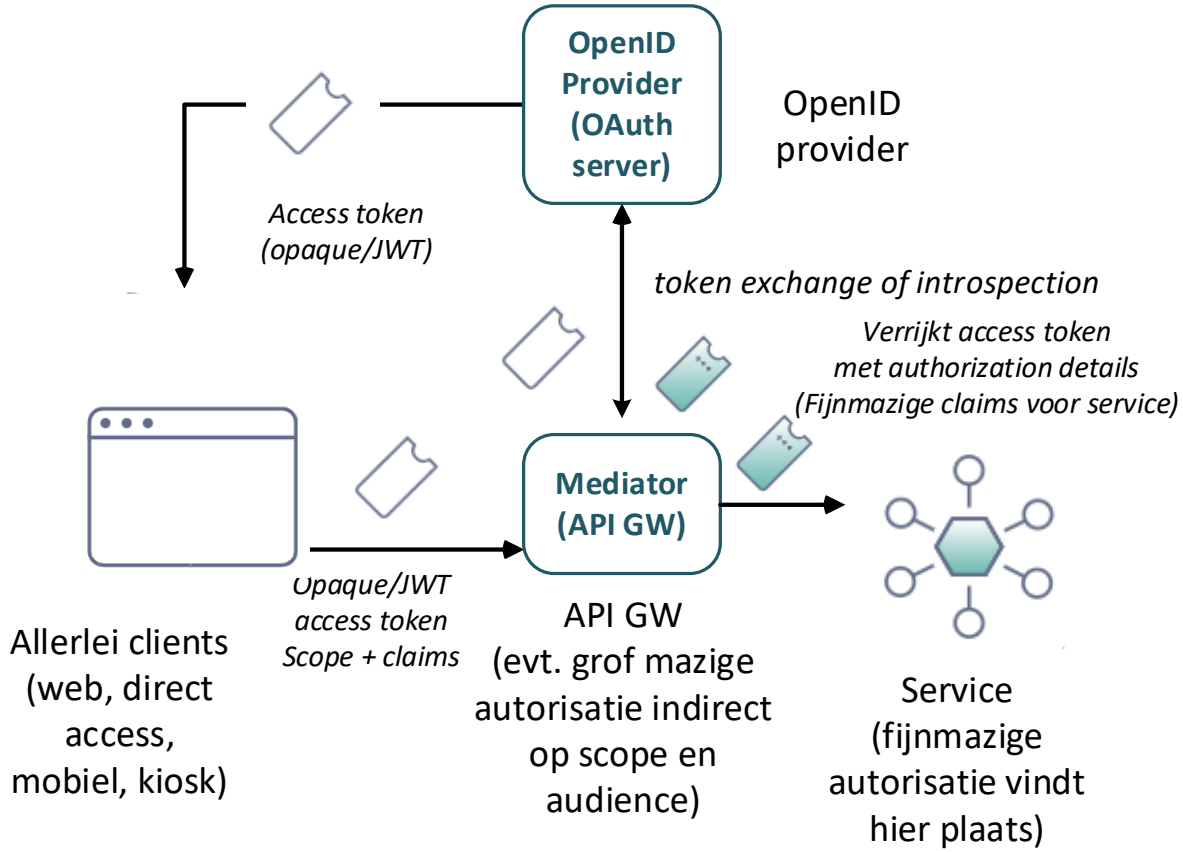
Rich Authorization Requests RFC9396

In een back-end

(Edge GW/mediator of API implementatie)

Wanneer is deze specificatie te gebruiken?

- toevoegen van (gevoelige) autorisatie claims, die op de client niet nodig zijn, maar voor een (bepaald) back-end systeem wel.
- Toevoegen van claim zoals rechtendelegatie tussen partijen zoals leveranciers en overheden, burgers, specifieke autorisatieclaims etc.
- Logische combinatie met token introspection (rfc7662) of token exchange (rfc8693)



Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Hogere security profielen

OAuth 2.1
PAR Pushed authorization request (rfc9126)
Opaque tokens
mTLS rfc8705
*DPoP (Demostrated proof of posession) (rfc*9449)

Hogere security profielen

<u>Optioneel</u> in de standaard. Toe te passen rfc's waar een hoger niveau van beveiliging nodig wordt geacht.

OAuth 2.1

- Verplicht maken PKCE voor het authorization code grant type
- Reeds verwerkt in het profiel.

PAR Pushed authorization request (rfc9126)

- Voor het authorization code grant type
- Uitwissen van het authorirization request via back-channel. Reeds verwerkt in NGOV OIDC profiel

Opaque tokens

- Opaque tokens in de client toestaan

Proof of posession

mTLS rfc8705

- Token aanvraag met een mtls verbinding. Optioneel mechanisme, naast private_key_jwt
- Reeds verwerkt in het profiel.

***DPoP (Demostrated proof of posession) (rfc*9449)**

- Maakt het Access token alleen bruikbaar vanuit de applicatie waar deze is aangemaakt.
- Is een alternatief voor het aanroepen van resources met mtls en een token met een cnf claim erin (zie paragraaf Advanced Security in het NLGOV OAuth profiel).
- Alleen toe te passen in een client met een private key. (dus tenminste ten dele een full client)
- Beter schaalbaal dan mtls (rfc8705)

Meewerken?

Token exchange en assurance levels van identity attributen.

OAuth token exchange

1

Toelichting bij authorization code flow.

Interoperabiliteit met DigiD, eHerkenning en SSOnrijk

1

Identity Assurance (draft)

1

Inloggen/bevestigen met mobiele apps (usability).

OAuth device authorization grant

Client initiated backchannel authentcation (CIBA)

2

OpenID for Verifiable credentials (OPENID4VC)

5

5

Machtigingen, ondertekenen, transacties en consent.

Rich Authorization Requests (RAR) – RFC9396

Samenhang met module signing en encryptie (Logius)

2

Samenhang met Consent uit de OAuth spec - RFC6749

1

Samenhang met Pushed Authorization Requests PAR (RFC9126)

1

1

5

Autorisatie en rechtendelegatie.

Token exchange - RFC8693

Verduidelijking “represents” claim

Rich Authorization Requests (RAR) – RFC9396

2

3

Hogere security profielen.

1

PAR Pushed authorization request (rfc9126)

Opaque tokens

mTLS rfc8705

1

*DPoP (Demostrated proof of posession) (rfc*9449)

6

Uitslag stemming