



Home



Inhoudsopgave



Heiko Hudig

Martin van der Plas

Alexander Green

Stas Mironov

Frank Terpstra

Update Open Authentication (*OAuth/OIDC*)



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 Forum
Standaardisatie

Versie 1.2 zie Project board ;-)

Versie 2 ?



Hoe regelen we toegang tot API's ?

- > Standaarden
- > Stelsels (afspraken)
- > Voorzieningen
- > ...Techniek (Tokens)





Home



Inhoudsopgave

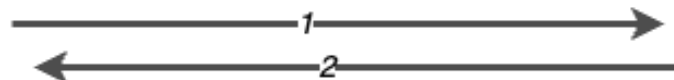


Regie op stelsels en
standaarden

Layer - onboarding



User /
business



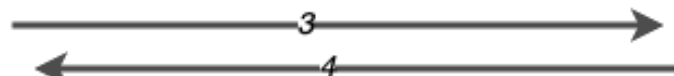
Identity Server



Layer - Client registration



Client



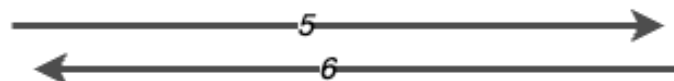
Authorization Server



Layer - Runtime Resource access



Client



Resource Server





Home

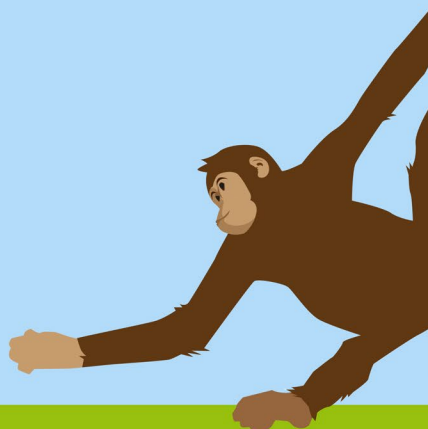
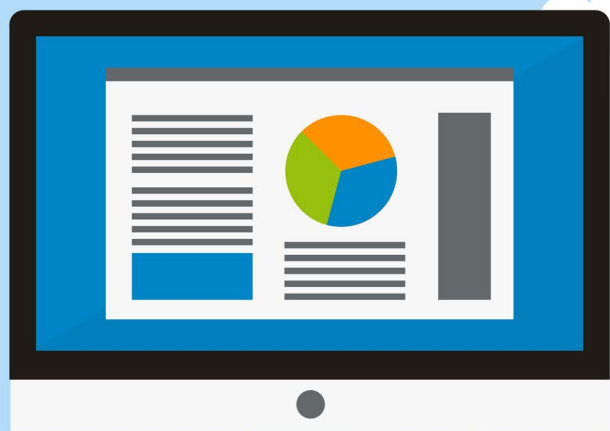


Inhoudsopgave



OpenID iGov OAuth profile update

Er komt een nieuwe versie aan, wat zit daar in...





inhoud

- Wat is iGov
- Nieuwe versie iGov
- Toevoegingen van NL-Gov assurance profile Oauth op versie 1.0
- Welke toevoegingen lijken overgenomen
- Andere significante wijzigingen?
- Hoe verder



Wat is iGov

- OpenID foundation maakt profielen op OpenIDConnect en OAuth
 - > FAPI (financieel)
 - > HEART (Zorg)
 - > iGov (overheid)
- iGov OAuth profiel 2.0 basis voor Nederlands profiel OAuth
 - > (ook de reden dat we meerdere NL-Gov standaarden hebben)



Nieuwe versie iGov profiel

- De werkgroep is OpenIDfoundation is actief issues en best practices bij blijven houden en heeft draft versie bijgewerkt
- Zit nu dicht bij uitbrengen nieuwe versie 2.1
 - > Interne review binnen de hele OpenIDfoundation
 - > Gevolgd door stemmingsronde voor leden OpenIDfoundation
 - > Kan binnen 2 maanden afgerond zijn



Aanvullingen in NL-Gov Oauth profiel

- TLS client auth mogelijk [RFC8705]
- PKCE verplicht wanneer client authorization server benaderd (inclusief extra maatregelen)
- Ondersteuning voor PS256 signing algorithm [RFC7518] for the signing of the private_key_jwt.
- Gebruik PKIOverheid en OIN
- Claims for Authorization Outside of Delegation Scenarios [RFC9068]
- Geen access tokens in query parameters
- Richtlijnen voor proof of possession implementatie



Aanvullingen in NL-Gov Oauth profiel

Wat lijkt er in iGov Oauth 2.1 te zitten?

- TLS client auth mogelijk (rfc8705)
- PKCE verplicht wanneer client authorization server benaderd (inclusief extra maatregelen)
- Ondersteuning voor PS256 signing algorithm [RFC7518] for the signing of the private_key_jwt.
- Gebruik PKIOverheid en OIN
- Claims for Authorization Outside of Delegation Scenarios [rfc9068]
- Geen access tokens in query parameters
- Richtlijnen voor proof of possession implementatie
- TLS volgens NCSC



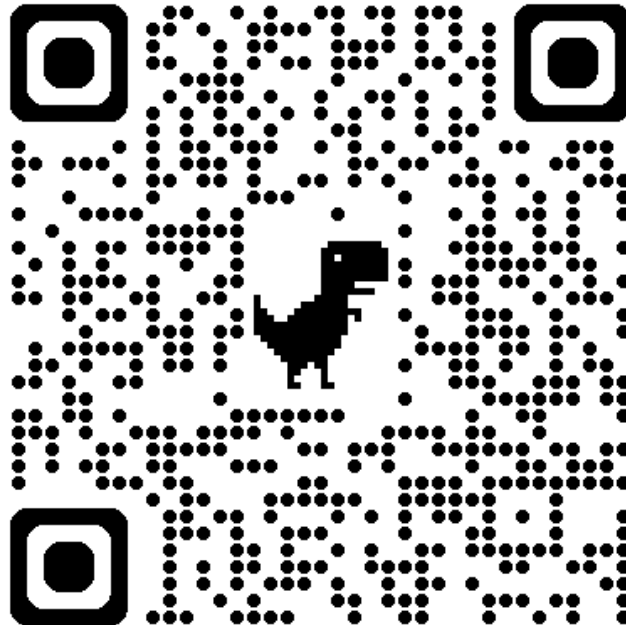
Andere opvallende zaken in 2.1

- Ondersteuning DPOP [RFC9449]
- Geen ondersteuning token exchange
- TLS Enhancements (veiliger aanbevolen cipher suites, TLS versies e.d.)



Hoe verder?

- Nauwkeurige verschillen analyse
- NL-Gov assurance profile for Oauth versie 1.3 baseren op iGov 2.1?





Inhoudsopgave

iGOV-ontwikkelingen

Roadmap

Terugblik

Features

Input/meewerken

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

Step 5. Access Token Request

Step 6. Access Token Response

Step 7. Resource interaction

1. Conformance

1.1 Requirements Notation and Conventions

1.2 Terminology

1.3 Conformance

2. Client Profiles

2.1 Client Types

2.1.1 Full Client with User Delegation

2.1.2 Native Client with User Delegation

NL GOV Assurance profile for OAuth 2.0 v1.1.0

Logius Standard

Definitive version December 03, 2024

This version:<https://gitdocumentatie.logius.nl/publicatie/api/oauth/v1.1.0/>**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](#)[File an issue](#)[Commit history](#)



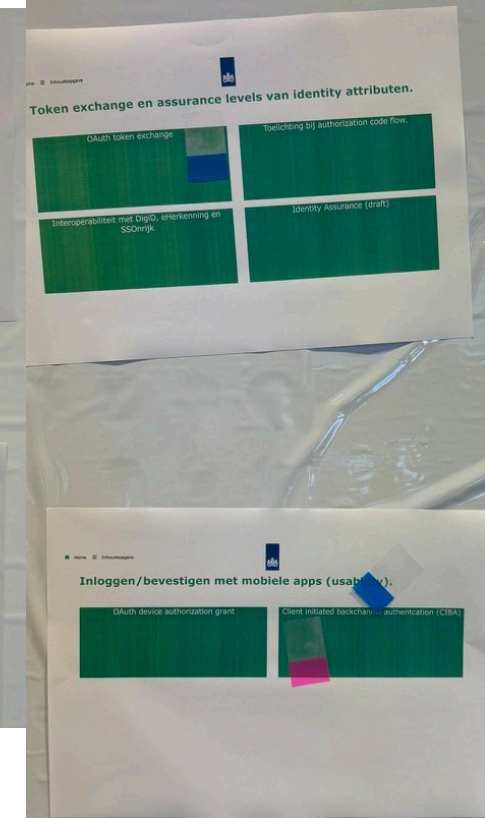
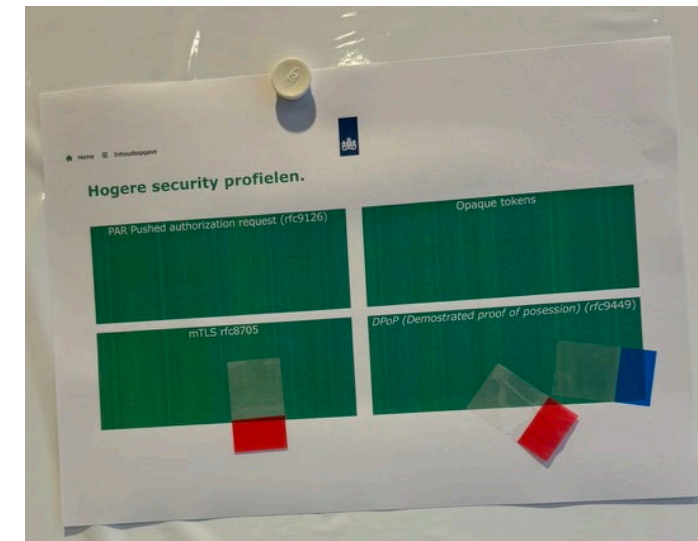
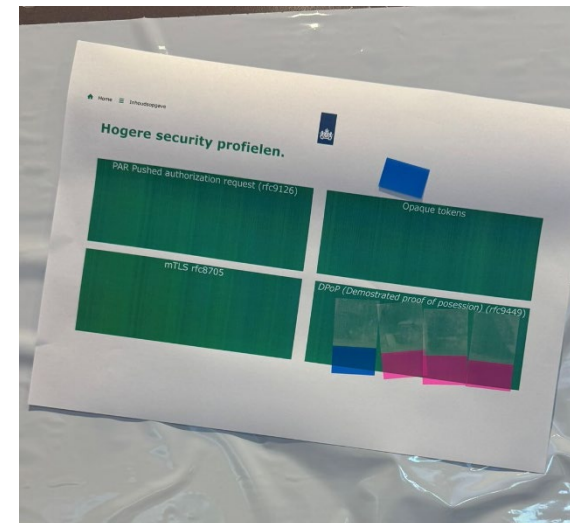
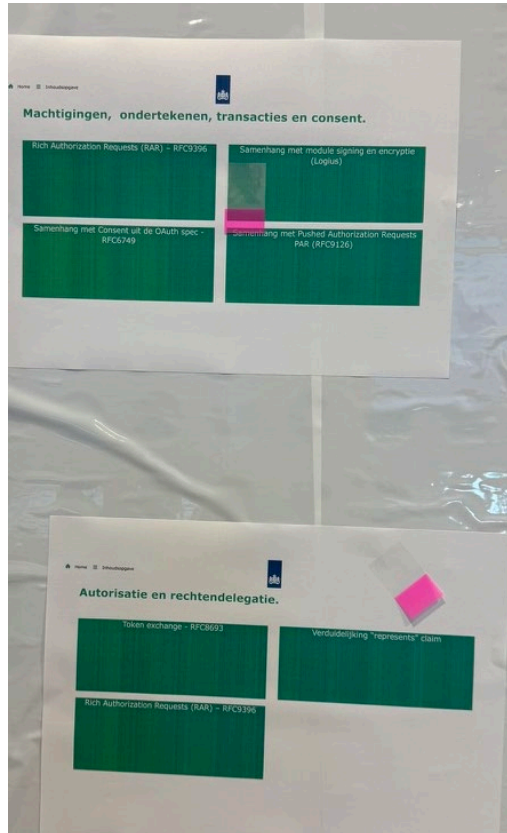
Home



Inhoudsopgave



Uitslag stemming





Project board

Open Authentication standaarden

Backlog Team capacity Current iteration Roadmap My items Table view + New view

Filter by keyword or by field

No Status 6 Estimate: 0	Intake 7/5 Estimate: 0	Backlog 13/10 Estimate: 0	To do 6/5 Estimate: 0	In progress 6 Estimate: 0	Review 4/3 Estimate: 0	Pull Requests 4 Estimate: 0	Done 21 Estimate: 0
<ul style="list-style-type: none">OAuth-NL-profiel #59 Use cases voor: Rich Authorization request (RAR, rfc9396) Medium MDraft AAS - OIDC testvoorzieningOAuth-Inleidend #1 Opaque token use case toevoegenOAuth-NL-profiel #63 Use case: Relatie met SAML en eHerkenning / SSOonRijkOIDC-NLGOV #9 Forum Standaardisatie adoptieadviezenOAuth-NL-profiel #93 foutje verwijzing BFS	<p>Will be fixed, needs refinement</p> <ul style="list-style-type: none">OAuth-NL-profiel #26 Inhoud access token in lijn brengen met RFC9068OAuth-Inleidend #2 Stroomlijnen structuur documentOIDC-NLGOV #10 Register new claims at IANAOAuth-NL-profiel #92 Aanpassen van revocation paragraaf OAuthOIDC-NLGOV #23 BeheerOIDC-NLGOV #21 Tussenvoegsels in OIDCOAuth-NL-profiel #35 RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens en PKI-Overheid certificaten	<p>This issue hasn't been started</p> <ul style="list-style-type: none">OAuth-Inleidend #3 Verschillende security niveau's beschrijven High XLOAuth-Inleidend #4 Lessons learned uit eDelivery REST API toepassen Lower LOAuth-NL-profiel #84 Specifieke aanvullingen voor gebruik OAuth iom eHerkenning en SSOonRijk Lower MDraft Epic: Release 2 afrondenOAuth-NL-profiel #64 Onderzoek Verifiable claims irt OAuth en OIDC XLOIDC-NLGOV #18 Connect Client-Initiated Backchannel Authentication Flow (CIBA) opnemenOIDC-NLGOV #16 AA4 - Korte versie OIDC profiel makenDraft Inleidend document API Access standaarden vaststellen (1.2.X release)OAuth-NL-profiel #75 RFC 8628 device authorization flowOAuth-Inleidend #5 Beschrijven van de use-case/flow bij het kadaster met toepassing van RAR(step up, eenvoudige transactie met consent) in het OAuth inleidend document	<p>Needs work for the next release</p> <ul style="list-style-type: none">OIDC-NLGOV #11 Repo op Gitlab archiverenOAuth-NL-profiel #90 Updaten van alle referenties naar hun laatste statusOIDC-NLGOV #20 Opschonen OIDC NL GOV profielOIDC-NLGOV #17 Her schrijven OIDC NLGOV profiel gelijk met OAuth NLGOVOAuth-NL-profiel #25 Aanbevelen of verplichten van response_mode=form_postOIDC-NLGOV #12 [bug] De betekenis van 'sub' is niet compatibel met de OAuth 2.0 standaard	<p>What we are working on at the moment</p> <ul style="list-style-type: none">OAuth-NL-profiel #60 Use case: Token exchange grant type (rfc8693) High MOIDC-NLGOV #15 AA2 - Internationale ontwikkelingen rond OIDC te monitoren Medium SDraft Epic: release 1.2 afronden en indienen bij MIDOOAuth-NL-profiel #86 Korte beschrijving RAR opnemen in het OAuth inleidend document.OIDC-NLGOV #26 Sync with iGovDraft Vorbereiden presentatie KPAPI 26 maart	<p>Still needs a review before done</p> <ul style="list-style-type: none">OAuth-NL-profiel #58 Use Case: PAR High SOAuth-NL-profiel #38 paragraaf 4.2 token introspection Medium XSOAuth-NL-profiel #61 Use case: Opaque tokensOIDC-NLGOV #19 Identity Assurance in OIDC op basis van eIDAS	<ul style="list-style-type: none">OIDC-NLGOV #24 Identity Assurance icm eIDASOAuth-NL-profiel #91 Toevoegen PAR beschrijvingOAuth-NL-profiel #85 Toevoegen RAR stukken aan OAuth NL GovOAuth-NL-profiel #88 Verduidelijking van het gebruik van Introspection #38	<p>This has been completed</p> <ul style="list-style-type: none">OAuth-NL-profiel #76 Wrong auto highlighting of HTTP High XSDraft OAuth v1.1 aanmelden bij MIDO High S IterationOAuth-NL-profiel #83 Aparte specificatie met de mapping tussen SAML en OpenID connect trust mechanismen. Medium MDraft Use Cases voor OAuth uitbreiden Medium M IterationOAuth-NL-profiel #62 Use case: Cross-device SSOOIDC-NLGOV #22 Link Logisch ontwerp BRPOAuth-NL-profiel #65 Use case: DPoP - Demonstrating Proof-of-Possession (RFC 9449)OAuth-NL-profiel #16 Claims for Authorization Outside of Delegation ScenariosOAuth-NL-profiel #28 RFC ACR claimOAuth-NL-profiel #36 Use case uitbreidingenOAuth-NL-profiel #71 Update Authorization Server Profile.md



Inhoudsopgave

Toelichting en nut bij iedere RFC

Token exchange tussen domeinen, (bijv. DigiD, EH en SSO Rijk)

Inloggen/bevestigen met mobiele apps (usability)

Machtigingen, ondertekenen transacties/consent

Delegatie & autorisatie

Hogere security profielen

- Token exchange SAML → OAuth/OIDC
- Identity Assurance en SAML → OAuth bridge
- Client initiated Backchannel Authentication (CIBA)
- OAuth device authorization grant (rfc8628)
- OpenID for Verifiable Creds (eIDAS ID-wallet)
- Rich Authorization Request (RAR) op de client
- Rich Authorization Request en rechtendelegatie
- Token exchange (back-end)
- OAuth 2.1,
- mTLS Client authentication (rfc8705),
- Demonstrating Proof-of-Possession (DPoP) (rfc9449),
- Pushed Authorization Requests (PAR) (rfc9126),
- Opaque tokens



Inhoudsopgave

iGOV-ontwikkelingen

Roadmap

Terugblik

Features

Input/meewerken



Inhoudsopgave

GOV-ontwikkelingen

Roadmap

Terugblik

Features

Input/meewerken



- Demonstrating Proof-of-Possesion (DPoP)
- Rich /Pushed Authorization Rrequests (RAR/PAR)
- Token Exchange
- OIDC Verifiable Credentials



Hogere security profielen

OAuth 2.1

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

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

Sender contained access token (zie volgende slides)

PAR Pushed authorization request (rfc9126) (zie volgende slides)

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

Opaque tokens

- Opaque tokens in de client toestaan



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Demonstrating Proof-of-Possesion

Opgenomen in FAPI 2.0



Proof of possession (sender constrained access token)

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

Essentie token alleen bruikbaar vanuit de applicatie waar deze is aangemaakt ("sender constrained")

Voordelen

- Verhoogde onweerlegbaarheid t.o.v. het gewone OAuth profiel
- Kan gemakkelijk toegevoegd worden aan bestaande client.
- Bij ieder inlogmechanisme (grant type) te gebruiken.

Randvoorwaarden / beperkingen / kenmerken

- Dit voegt complexiteit toe, dus alleen toepassen bij bijzonder hoge eisen voor onweerlegbaarheid.
- Beide zijn alleen toe te passen in een client met een private key. Dus (ten minste ten dele) een confidentiële client.
- Onderdeel van het FAPI 2.0 profiel.

Twee varianten:

1. Met mTLS (detail volgende slide)

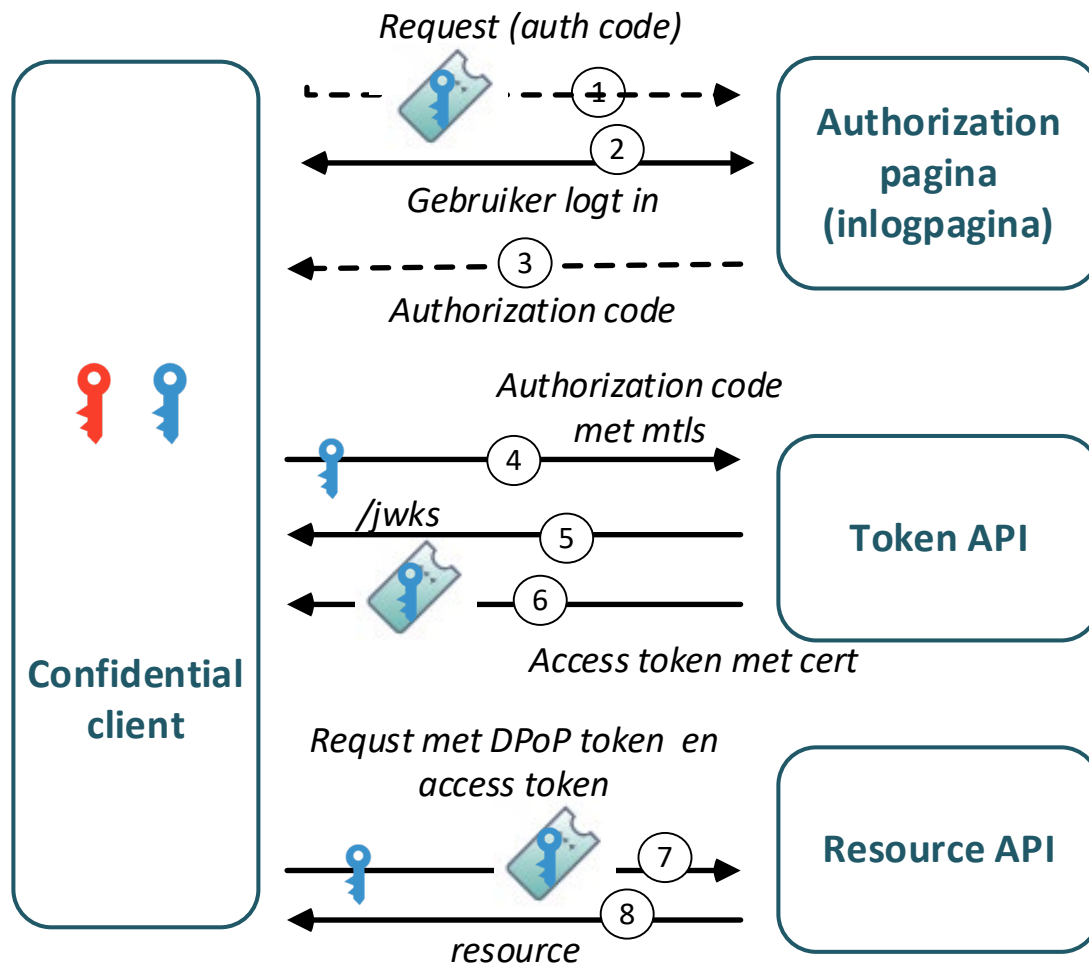
- Aanroep van resources met een mtls verbinding.
- Reeds aanwezig op het iGOV OAuth profiel, in paragraaf advanced security options.
- Confidential client vereist

2. DPoP (*Demonstrated proof of possession*) (rfc9449)

- Kan in een public client gebruikt worden. Dus ondersteunt aanroepen van API's vanuit een browser (SPA)
- Vereist een secure deel in de client voor het aanmaken van de DPoP headers.
- Werkt onafhankelijk van TLS. Werk daardoor in omgevingen met TLS proxies.



Proof of possession (met mTLS)



Authorization pagina (stap 1-3) zoals gebruikelijk

Werking token API

Stap 4: Token aanvraag met één van deze 2 client authentication methods

- mTLS conform rfc8706
- Private_key_jwt

Stap 5: callback jwks uri (aanbevolen) en validatie certs

Stap 6: Uitgeven token met "cnf"

Resource API's

Stap 7: Aanroep met token en mTLS

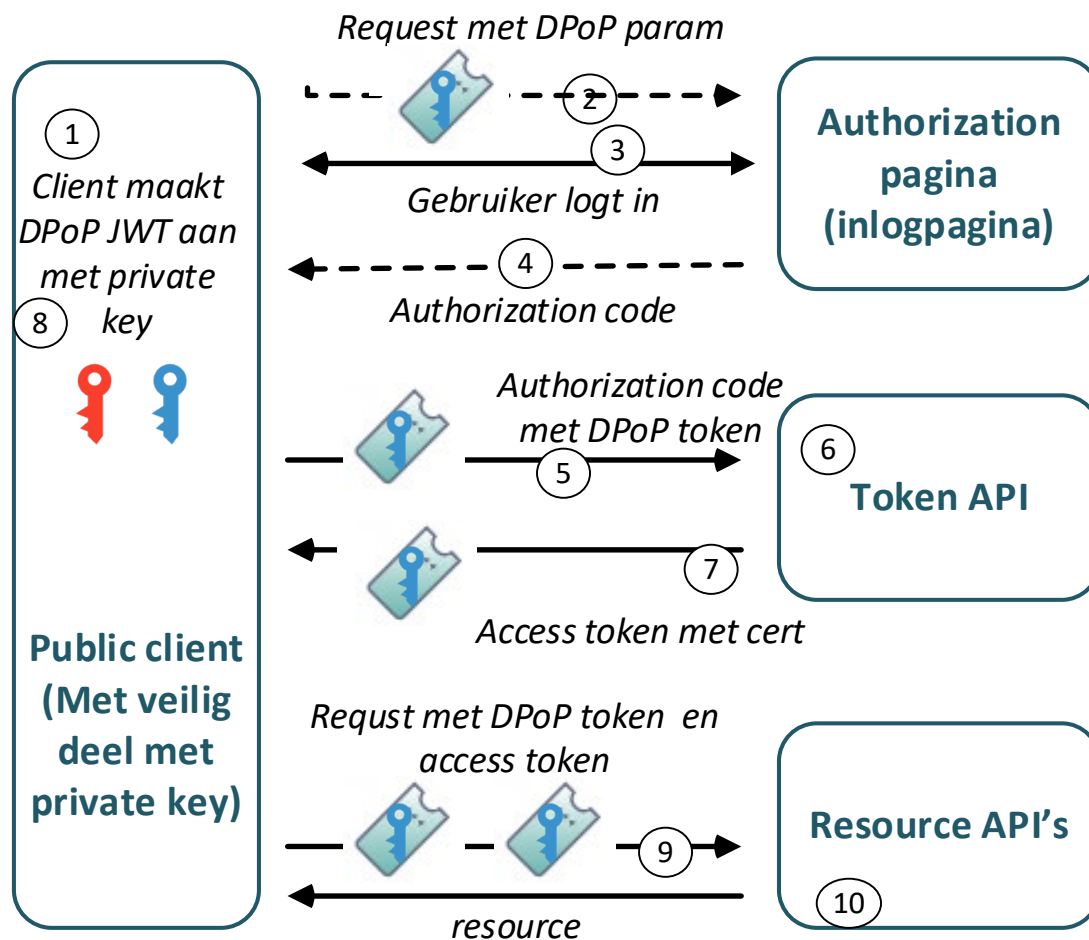
Stap 8: Controle cnf claim (met thumbprint van het certificaat) tegen mTLS cert

Beperkingen

- Geen API aanroepen vanuit browser
- Niet te gebruiken indien TLS proxies



Demonstrated proof of Possession DPOP



Client: Stap 1: Aanmaken DPoP tokens voor auth pagina en token API

Authorization pagina (stap 2-4) zoals gebruikelijk, maar met DPoP parameter.

Token API

Stap 5: Token aanvraag met DPoP token meegestuurd.

Stap 6: validatie: Client obv DPoP token en clientID.

Stap 7: Uitgeven en retourneren access token met "cnf" met thumbprint (type DPoP)

Client: Stap 8: Aanmaken DPoP token voor resource request.

Resource API's

Stap 9: Aanroep met token en mtlS

Stap 10: Controle cnf claim (met thumbprint van het certificaat) tegen DPoP token. Validatie DPoP token



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

RAR & PAR



Rich Authorization Requests (RAR) RFC9396

In de client applicatie (relying party)

Wanneer is deze specificatie te gebruiken?

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

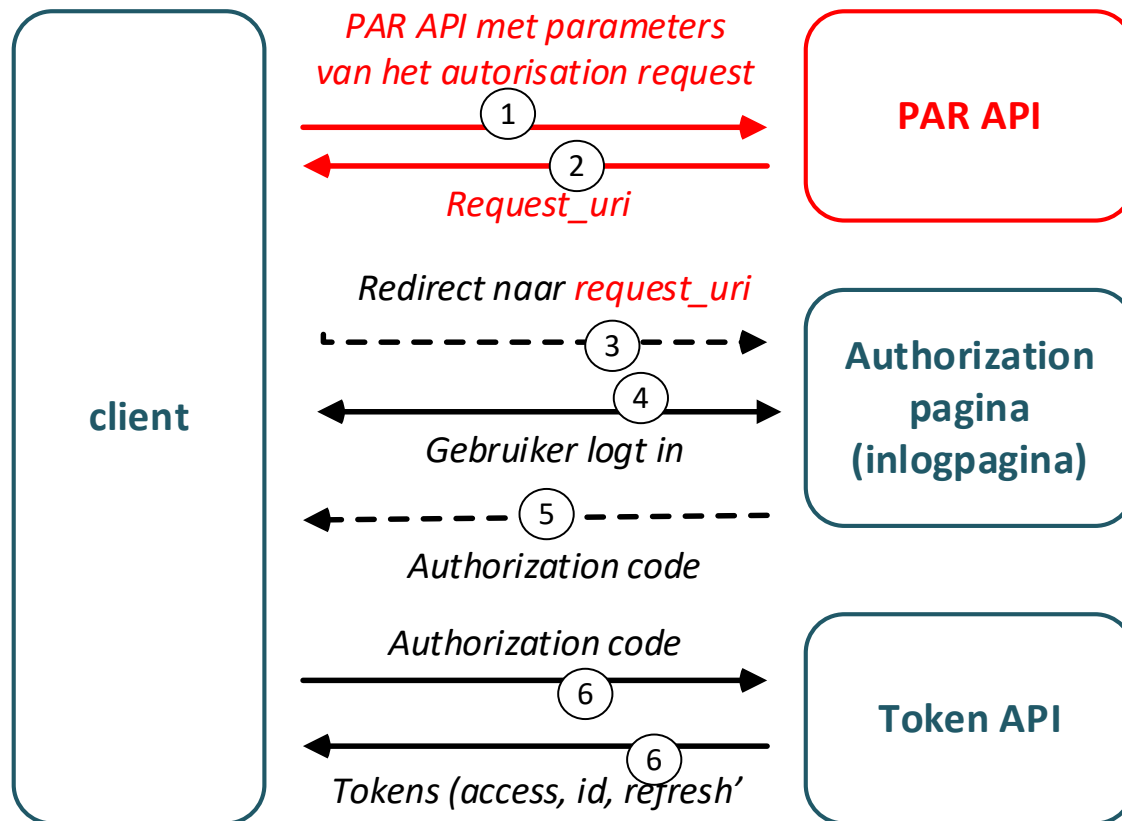
- Goedkeuren / bevestigen van een document / transactie / verzoek
- Ondertekenen van een aangifte, acte of document.
- Vaak in combinatie met opnieuw inloggen.

Voordelen.

- Standaard OAuth voor step-up (inlog of bevestiging) 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 autorisatie, etc.
- Attributen kunnen back-channel worden uitgewisseld, bijvoorbeeld persoonsgegevens, activatiecodes. Of het gehele access token op de client is een opaque token.
- Minimale effort/verantwoordelijkheid voor de developer van de client applicatie



Pushed Authorization Requests (PAR) RFC9126



Voordelen.

- Voorkomt man-in-the-middle attack.
- Daarbij wijzigt de hacker url parameters in de browser redirect naar de authorization page,
- Parametrs zoals prompt, acr_value, scope, en authorization_detail szijn zeer gevoelig

Werking

- **Toevoegingen** op de reguliere authorization code flow **in het rood**
- In PAR worden de parameters in het authorization request met een API opgestuurd
- Via de redirect wordt alleen een referentie gestuurd naar de parameters.
- Alternatief is JAR/JARM (FAPI 1.0)



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

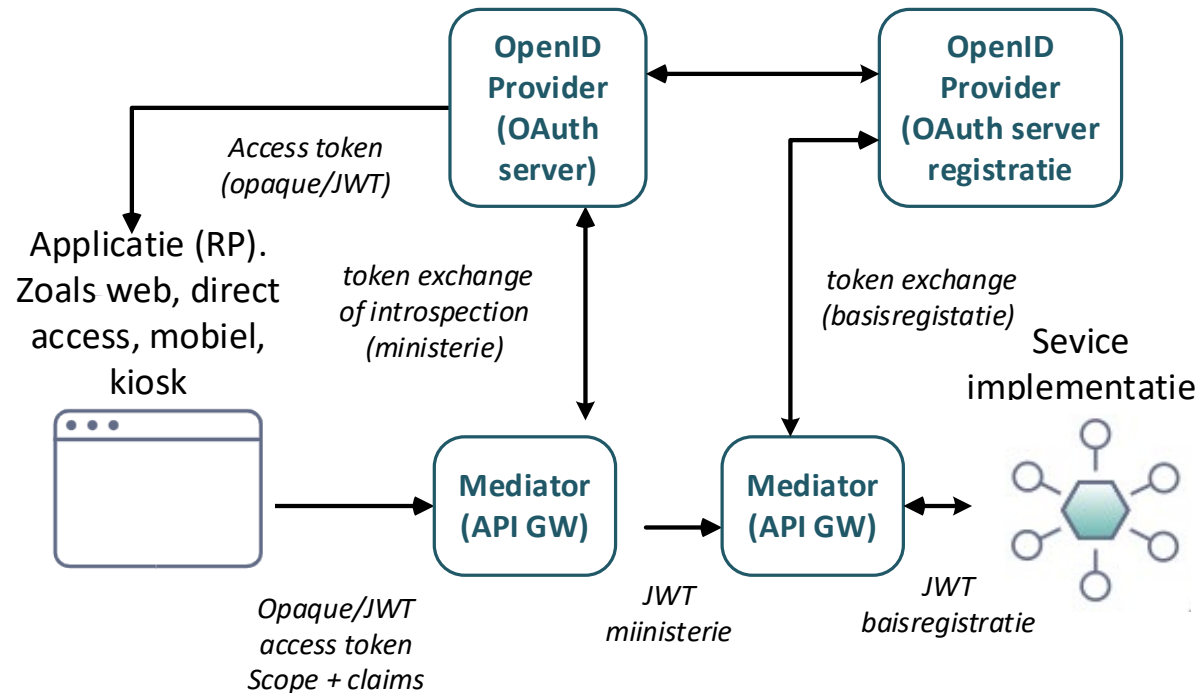
Token exchange en assurance levels van identity attributen.

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



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.



OAuth token exchange (RFC8693)

→ Vanuit de client (Relying Party)

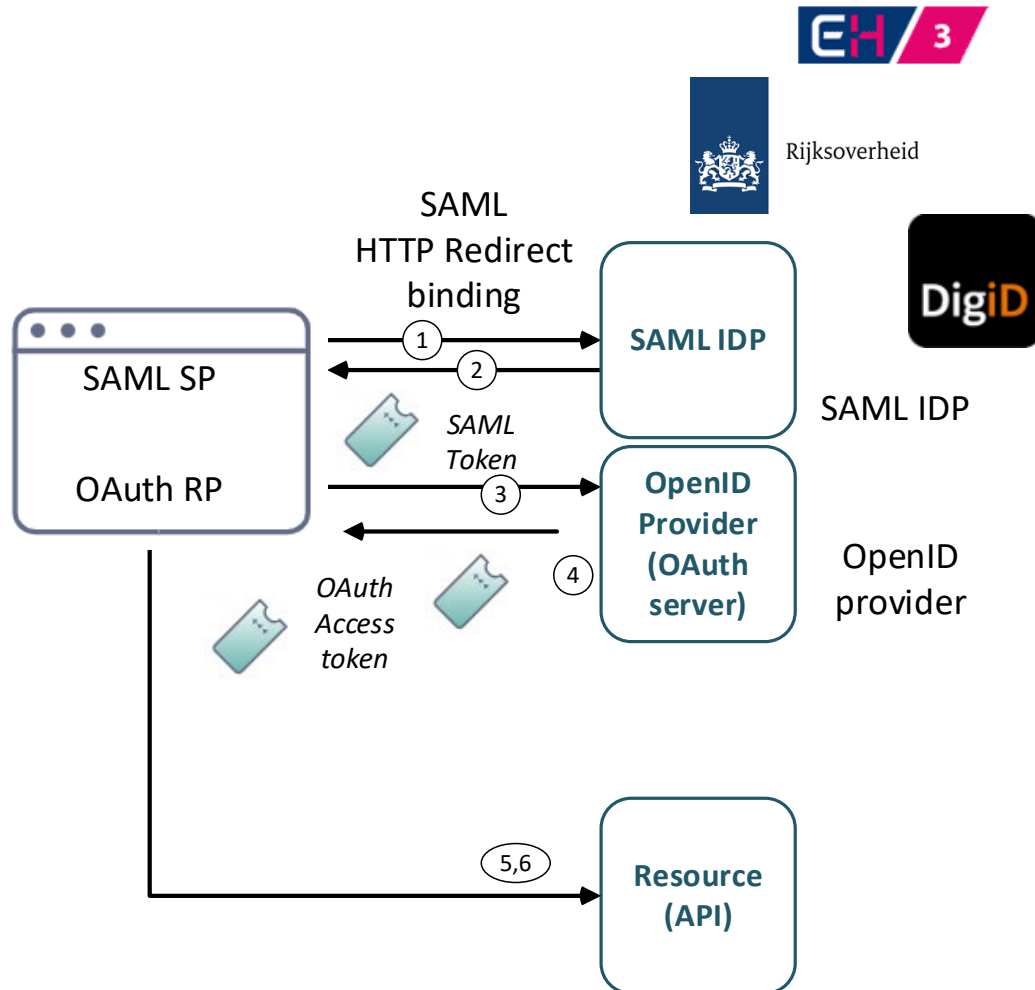
Token exchange: inwisselen van een token voor ander token (van een ander domein)

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 overheidsorganisaties.

Randvoorwaarden/beperkingen

- Client moet zowel SAML als OAuth implementeren





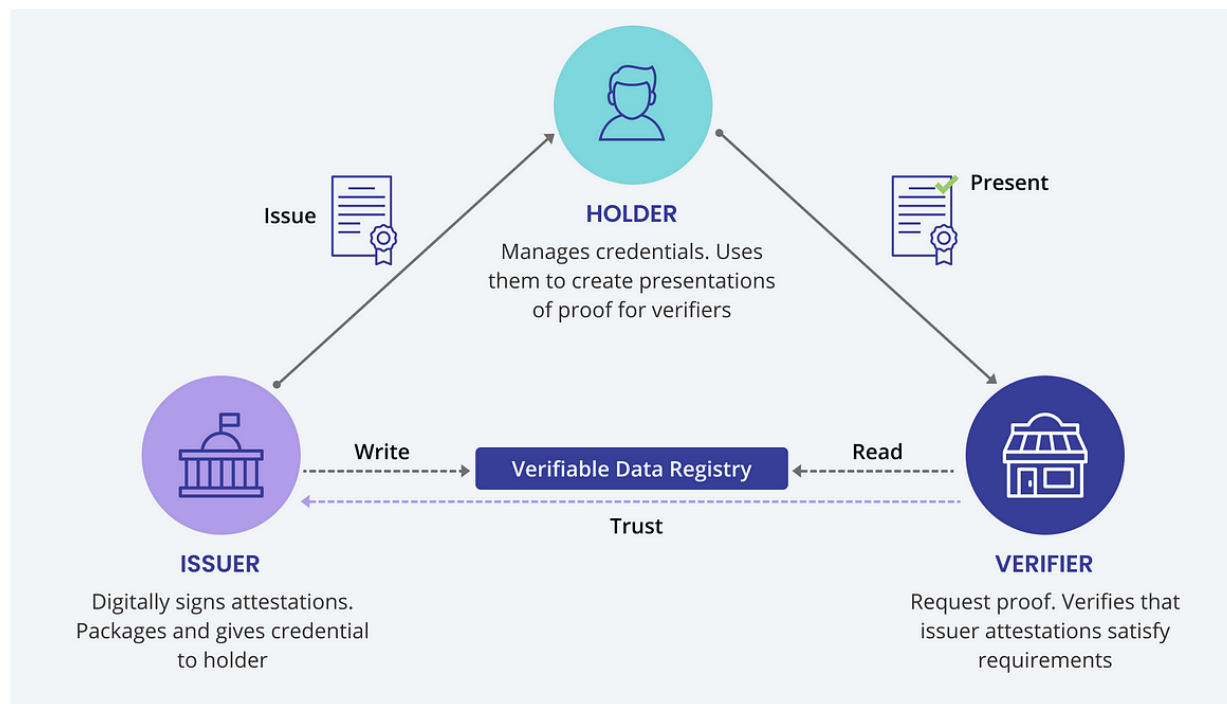
Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

OPENID 4 VC



OpenID for Verifiable 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.

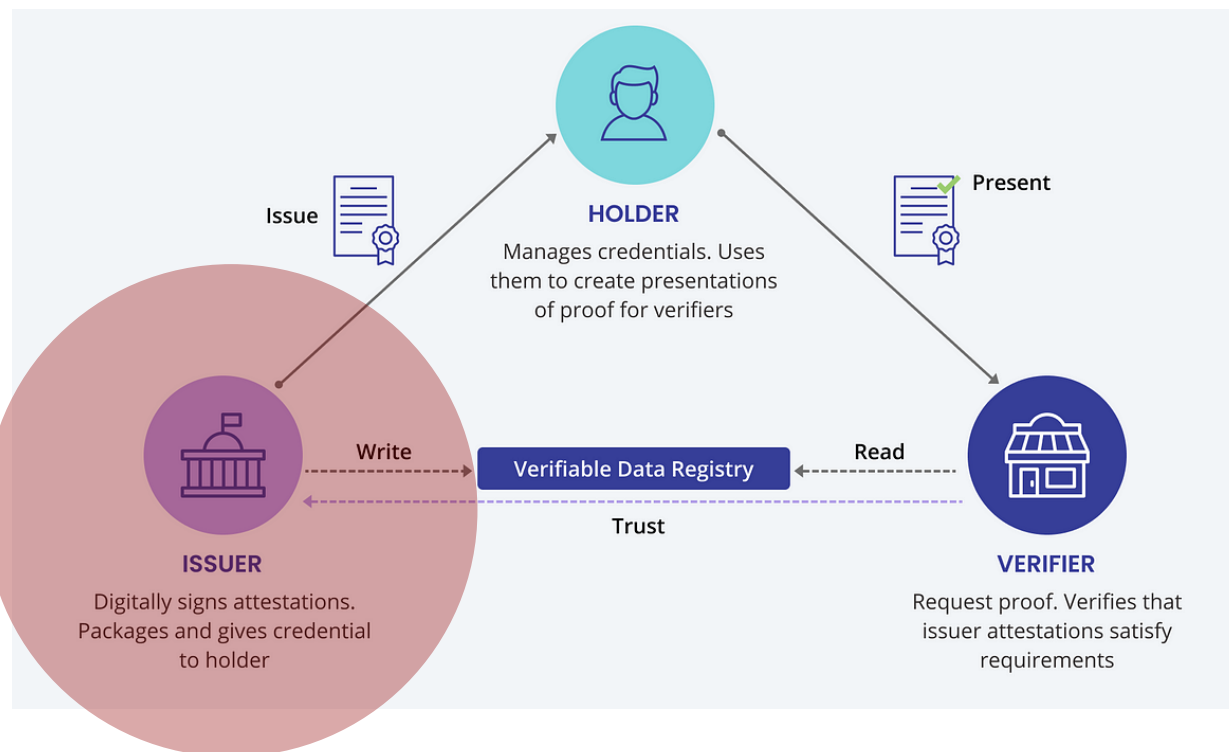
Randvoorwaarden/beperkingen

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



OpenID for Verifiable 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

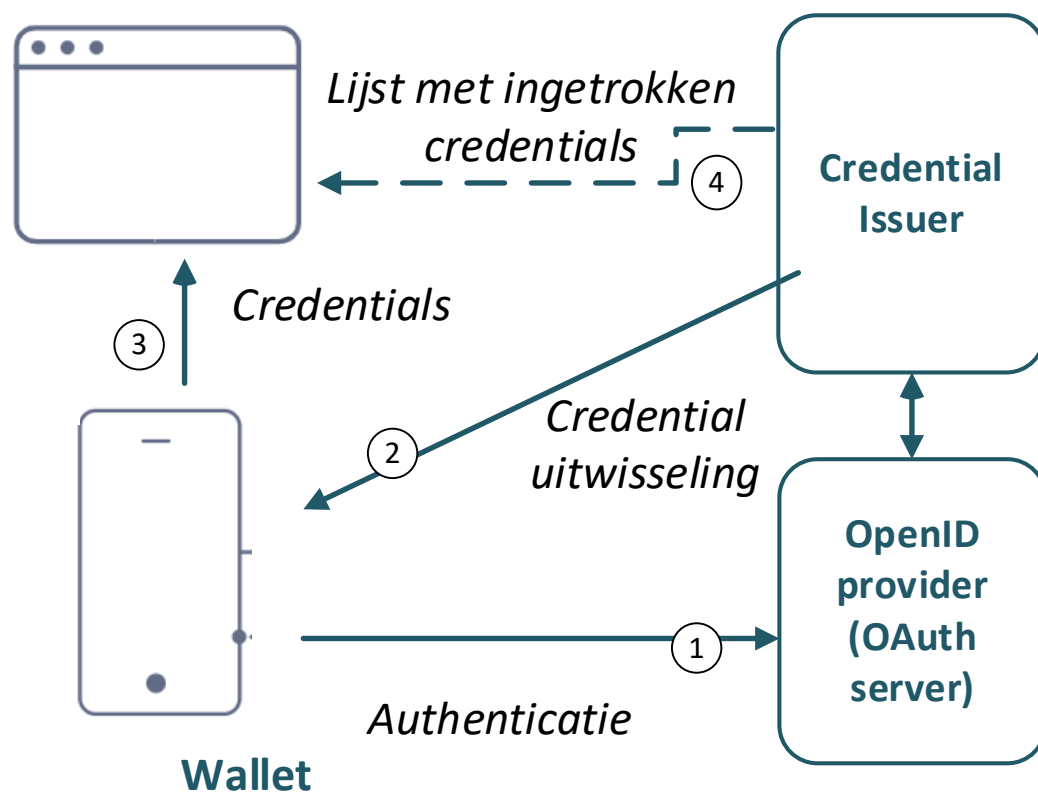
- Maakt gebruik van verschillende andere, in deze presentatie genoemde, RFCs
- Bevat verschillende opties



OpenID for Verifiable Credentials

OPENID4VC

Applicatie (relying party)



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

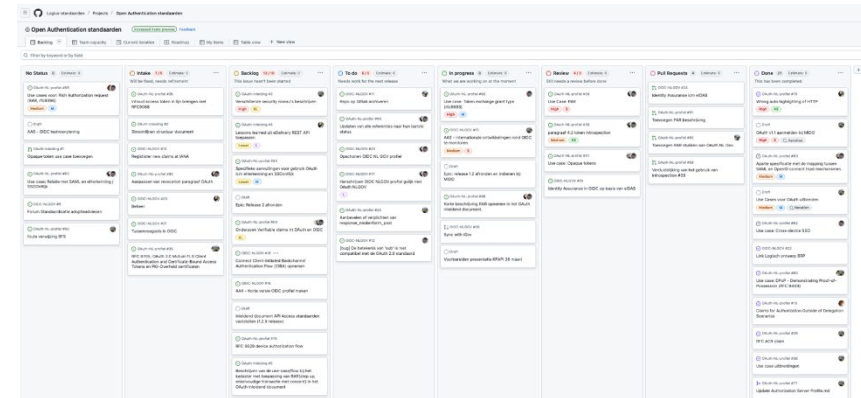


Werkgroep beveiliging

- Georganiseerd door **KP APIs**
- Frank Terpstra = **trekker**

Technisch Overleg

- Beheerd door **Logius** (Alexander Green, Stas Mironov, Heiko Hudig)
- Doel: transparante besluitvorming (*MIDO/PGDI*)
- Elk kwartaal een **TO** (*next 10-04-2025*)
- Openbaar:



- <https://github.com/orgs/Logius-standaarden/projects/2/views/1>
- Aanmelden kan via api@logius.nl



Home



Inhoudsopgave



Meewerken?

