TGV: Koppeldocument Applicatie

Date 05/15/2026
Version v.3

Booleans IAM

Honesty meets Excellence

Table of contents

Dit document beschrijft de vereisten en parameters voor het koppelen van externe applicaties met de centrale Identity Provider (IdP) van het Nederlands Instituut Publieke Veiligheid (NIPV).

Onze standaard voor moderne applicaties is **OpenID Connect (OIDC)**. Voor legacy applicaties of specifieke enterprise-pakketten ondersteunen wij tevens **SAML 2.0**.

1 OpenID Connect (OIDC) Koppeling

Indien uw applicatie een OAuth2 en/of OIDC intergratie heeft, geniet OIDC de absolute voorkeur. We maken daarbij een onderscheid in 2 type applicaties:

1.1 Applicatietypes

Bij de registratie moeten we vaststellen welk type applicatie u koppelt. Dit bepaalt de beveiligingsmethode:

- **Confidential Client:** Applicaties die in staat zijn om veilig een geheim (**Client Secret**) te bewaren op een server (bijv. traditionele webapps zoals Java, .NET, PHP of Node.js backend-apps).
- **Public Client:** Applicaties die **geen** geheim kunnen bewaren omdat de code direct toegankelijk is voor de eindgebruiker (bijv. Single Page Applications zoals React/Angular in de browser, of native mobiele iOS/Android apps).

1.2 Ondersteunde Grant Types

Wij ondersteunen uitsluitend veilige, moderne flows. De **Implicit Flow** en **Resource Owner Password Credentials Flow** zijn om security-redenen **niet** toegestaan.

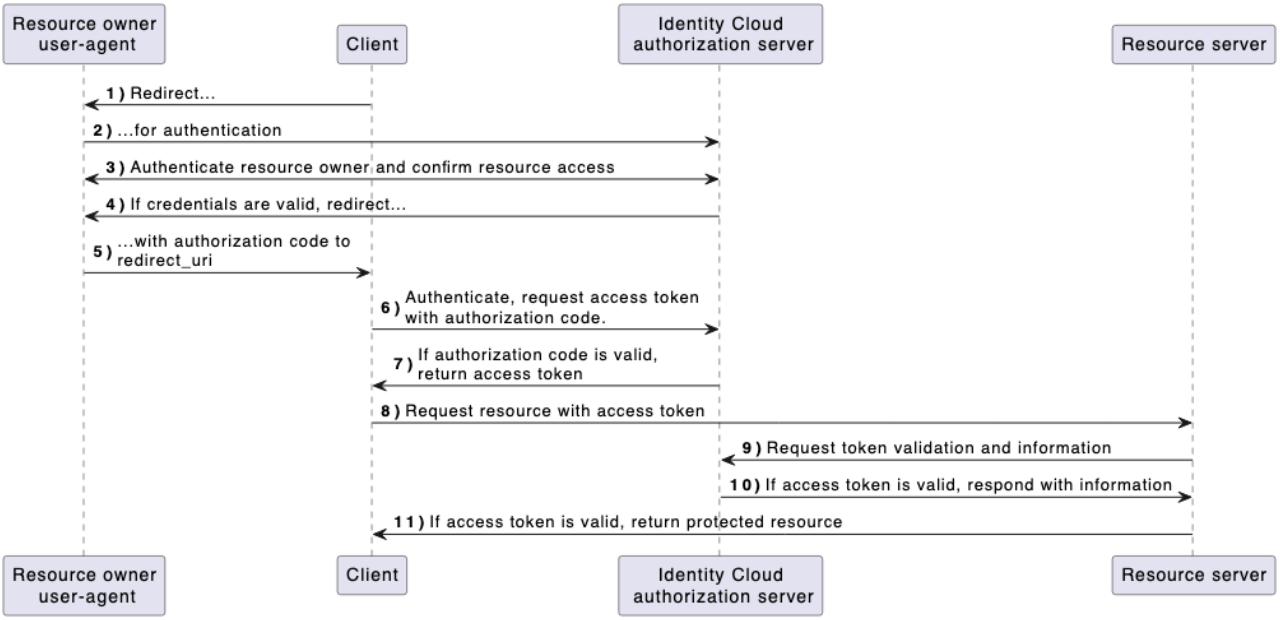
1. **Confidential Clients:** Maken gebruik van de **Authorization Code Grant Type**.
2. **Public Clients:** Maken verplicht gebruik van de **Authorization Code Grant Type + PKCE** (Proof Key for Code Exchange) om interceptie van de authorization code te voorkomen.

Belangrijk: Client Authenticatie Methode (`client_secret_post`)

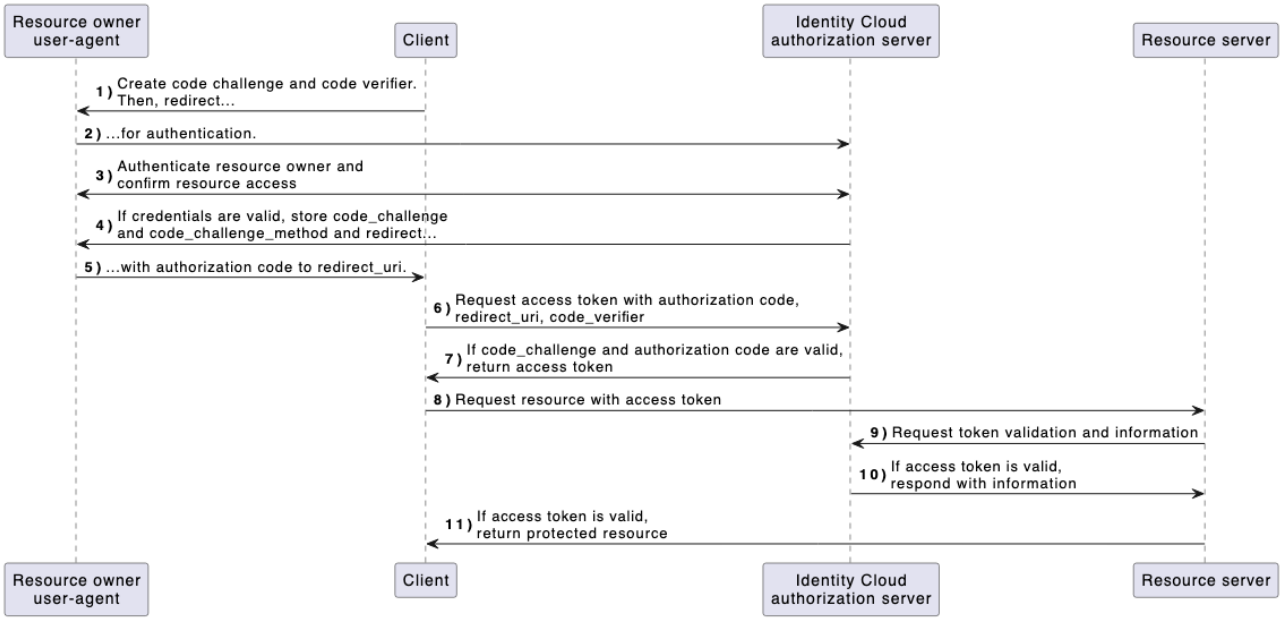
Voor Confidential Clients hanteren wij strikt de `client_secret_post` methode voor authenticatie bij het `/token` endpoint.

- **Wat dit betekent:** Uw applicatie moet de `client_id` en `client_secret` meesturen in de **POST-body** (`application/x-www-form-urlencoded`) van het verzoek.

Authorization Code Grant Type



Authorization Code Grant Type with PKCE



1.3 Tokens & Scopes

- **Access Token:** Dit token wordt **puur gebruikt voor toegang**, niet om te bepalen wie de gebruiker is. Wij geven **Opaque Access Tokens** uit (een onleesbare string). Uw applicatie kan dit token **niet** lokaal parsen. U kunt dit token verder gebruiken om op te valideren of het token nog geldig is en welke gebruiker bij dit token hoort via:
  - De `/userinfo` endpoint (om aanvullende gebruikersprofieldata op te halen).
  - De `/introspect` endpoint (om de geldigheid en scopes van het token te controleren).
- **ID Token:** U ontvangt een getekend JWT (JSON Web Token) met de identiteitsgegevens van de gebruiker.
  - **Belangrijk (`sub` claim):** De `sub` (subject) claim bevat bij ons altijd het e-mailadres van de unieke gebruiker (bijvoorbeeld: `"sub": "testuser@example.com"`). Dit is de unieke sleutel waarmee u de gebruiker binnen uw applicatie identificeert.
- **Ondersteunde Scopes:**
  - `openid` (Geeft aan dat het een OIDC-verzoek is en een ID Token naast het Access Token wordt verstrekt)
  - `profile` (Naam, voornaam, voorkeursnaam)
  - `email` (E-mailadres en verificatiestatus)
  - `roles` (Toegewezen Applicatie Rollen. Nu alleen gebruikt binnen de IDP, kan in de toekomst worden gebruikt voor applicatie doeleinde)
  - `offline_access` (indien nodig/gewenst)

1.4 Wat wij van u nodig hebben (OIDC)

- **Application Type:** Confidential of Public.
- **Redirect URI(s):** De exacte URL('s) waar de gebruiker naartoe wordt gestuurd na succesvol inloggen (moet HTTPS zijn).
- **Post-Logout Redirect URI(s):** De URL waar de gebruiker landt na uitloggen.

1.5 Wat u van ons krijgt (OIDC)

- **Issuer URL / Discovery Endpoint:** `https://tgv.nipv.nl/.well-known/openid-configuration` (Hier vindt u automatisch alle endpoints zoals `/authorize`, `/token`, en `/userinfo`).
- **Client ID:** Een unieke identificatie voor uw applicatie.
- **Client Secret:** (Alleen bij Confidential Clients) Een veilig geheim dat u geheim moet houden.

  Zie formulier onderaan.

2 SAML 2.0 Koppeling (Legacy / Enterprise)

Voor applicaties die geen OAuth2 en/of OIDC ondersteunen, bieden we SAML 2.0 aan. Omdat SAML complexer is qua security, hanteren wij strikte eisen om de integriteit van de authenticatie te waarborgen.

2.1 Onze Security Eisen voor SAML2

Als IdP eisen wij de volgende configuratie van uw applicatie (Service Provider / SP):

- **Signed Assertions & Responses:** Wij ondertekenen standaard de SAML Assertion (en optioneel de Response). Wij verwachten dat uw applicatie de handtekening valideert met ons IdP-certificaat.
- **Signed AuthnRequests (Aanbevolen):** Wij eisen bij voorkeur dat de AuthnRequests die vanuit uw applicatie komen digitaal ondertekend zijn door uw SP-certificaat om **spoofing** te voorkomen.
- **Encrypted Assertions (Optioneel/Strikt):** Indien de applicatie privacygevoelige data ontvangt, kunnen wij de SAML Assertion versleutelen (encryptie) met de public key van uw applicatie.
- **Binding Types:** * **HTTP-Redirect** voor het AuthnRequest (van SP naar IdP).
  - **HTTP-POST** voor de SAML Response (van IdP naar SP). Artifact binding wordt op dit moment niet ondersteund maar kan als het nodig is.
- **NameID Format:** Wij hanteren strikt het e-mailformaat als unieke identifier: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` Zorg ervoor dat uw applicatie (SP) dit formaat verwacht en correct configureert in het AuthnRequest.
- **SHA-256:** Alle handtekeningen en algoritmes moeten minimaal SHA-256 gebruiken. SHA-1 is uitgesloten.

2.2 Wat wij van u nodig hebben (SAML2)

- **SP Metadata XML:** De meest foutloze manier om te koppelen. Als alternatief ontvangen we graag handmatig:
  - **Entity ID / Audience:** De unieke identifier van uw applicatie.
  - **Assertion Consumer Service (ACS) URL:** De URL waar wij de SAML POST-request naartoe moeten sturen.
  - **Single Logout (SLO) URL:** (Optioneel) Voor centraal uitloggen.
- **SP Signing/Encryption Certificaat:** Het publieke x.509 certificaat van uw applicatie (om handtekeningen te verifiëren of data te versleutelen).

2.3 Wat u van ons krijgt (SAML2)

- **IdP Metadata URL / XML:** Bevat ons Entity ID, de Single Sign-On URL en ons publieke IdP-certificaat waarmee u onze handtekeningen kunt controleren.

3 Invulformulier voor de Aanvrager

Vraag de organisatie om de volgende tabel in te vullen bij de aanvraag:

Gegeven	Keuze / Waarde
Gekozen Protocol	[ ] OIDC / [ ] SAML2
Naam Applicatie	**[Naam]**
Omgeving	[ ] Test / [ ] Acceptatie / [ ] Productie
Indien OIDC: Client Type	[ ] Confidential / [ ] Public (SPA/Mobiel)
Indien OIDC: Redirect URI's	**https://...**
Indien SAML2: Entity ID	**[Entity ID]**
Indien SAML2: ACS URL	**https://.../saml/acs**
Indien SAML2: Metadata	**[Link naar XML of XML in bijlage]**

4 IdP Omgevingen NIPV

Gebruik voor de configuratie van uw applicatie de endpoints van de desbetreffende omgeving:

Omgeving	OIDC Well-Known Discovery Endpoint	SAML 2.0 IdP Metadata XML URL
Test	`https://tgv-test.nipv.nl/.well-known/openid-configuration`	`https://tgv-test.nipv.nl/auth/realms/{COT_NAAM}/saml/metadata`
Acceptatie	`https://tgv-acceptatie.nipv.nl/.well-known/openid-configuration`	`https://tgv-acceptatie.nipv.nl/auth/realms/{COT_NAAM}/saml/metadata`
Productie	`https://tgv.nipv.nl/.well-known/openid-configuration`	`https://tgv.nipv.nl/auth/realms/{COT_NAAM}/saml/metadata`