



# Aansluitvoorwaarden applicaties op NWO platform

Den Haag, november 2024  
Nederlandse Organisatie voor Wetenschappelijk Onderzoek



## Document gegevens

Onderwerp	
<b>Auteur</b>	Zonneveld, H. van [Hans]
<b>Eigenaar</b>	Juffermans, B. [Bart]
<b>Versie status</b>	V1.1 <span>FINALE VERSIE</span>
<b>Bestandsnaam</b>	20241121 1D Aansluitvoorwaarden applicaties op NWO platform.docx
<b>Publicatie datum</b>	Bijgewerkt op: donderdag 21 november 2024

## Revisie geschiedenis

Auteur	Omschrijving	Datum	Versie
Hans van Zonneveld	Opzet	01-07-2024	0.1
Hans van Zonneveld	Concept, aangevuld en opmerkingen naar aanleiding van eerste opzet verwerkt	24-07-2024	0.9
Hans van Zonneveld	Wijzigingen na review I. Meinema en L. Marckx	31-07-2024	0.95
Hans van Zonneveld	Wijzigingen na review I. Meinema	14-08-2024	1.0
Hans van Zonneveld	Uitbreiding provisioning en MS Graph	21-11-2024	1.1

## Document goedkeuring

Naam	Rol	Datum	Versie	Actie	Actie
Bart Juffermans	PM	22-07-2024	0.1	Akkoord	NVT
Bart Juffermans	PM	25-07-2024	0.9	Akkoord	NVT
Bart Juffermans	PM	31-07-2024	0.95	Akkoord	NVT
Bart Juffermans	PM	14-08-2024	1.0	Akkoord	NVT
Bart Juffermans	PM	21-11-2024	1.1	Akkoord	NVT

# Introductie

Het IT-landschap van NWO is continu in beweging. Naast het uitfasen van verouderde IT onderdelen (zoals applicaties, netwerkcomponenten en storage) komen er ook nieuwe IT onderdelen bij die nodig zijn voor de ondersteuning van de bedrijfsprocessen.

Dit document beperkt zich tot applicaties. Een applicatie kent verschillende verschijningsvormen en primair zijn deze aansluitvoorwaarden van toepassing op de volgende applicatiesoorten:

- **Cloudapplicaties:**  
Specifiek een SaaS-applicatie die wordt aangeboden door een externe partij en via een webbrowser wordt benaderd;
- **Desktopapplicaties:**  
Specifiek een lokaal op de laptop geïnstalleerde applicatie van een leverancier waarmee een SaaS applicatie of externe data wordt benaderd;
- **Mobiele apps:**  
Specifiek een op een smartphone geïnstalleerde app van een leverancier waarmee een SaaS dienst wordt benaderd;
- **Embedded applicaties:**  
Specifiek een add-in of extension binnen een lokaal geïnstalleerde applicatie of cloudapplicatie die verbinding maakt met een externe SaaS dienst;
- **Toepassing:**  
Een eigenhandig geprogrammeerde interface gebaseerd op een formeel beschikbaar gestelde applicatie waarvan beheer en documentatie uiterst matig is ingeregeld;

Om te borgen dat deze applicaties passen binnen de IT-architectuur van NWO-D dienen deze applicaties op voorhand (en aldus voor livegang) te voldoen aan een aantal technische uitgangspunten.

## Wat dit document is

Dit document omvat de richtlijnen en aansluitvoorwaarden voor applicaties die door medewerkers van NWO benaderbaar zijn en gekoppeld worden met de Microsoft Entra ID tenant van NWO. Dit omvat zowel applicaties die door NWO zelf worden beheerd op een extern PaaS of IaaS platform en applicaties die als dienst worden afgenomen bij externe (SaaS) leveranciers. De koppelingsmogelijkheden omvatten federatieve SSO, provisioning via SCIM en toegang tot de Microsoft 365 tenant van NWO via de Microsoft Graph API.

## Wat dit document niet is

Dit document is geen handleiding welke stappen moeten worden uitgevoerd om een (federatieve) SSO-koppeling met een NWO-applicatie te realiseren. Ook zijn de richtlijnen en aansluitvoorwaarden niet van toepassing voor applicaties of gegevens die door NWO worden beheerd en worden aangeboden aan niet-NWO medewerkers (gastgebruikers).

Het uitgangspunt voor deze aansluitvoorwaarden is dat applicaties of diensten ondersteuning bieden voor een SSO koppeling met Entra ID. Dit document bevat geen richtlijnen voor applicaties:

- Die gebruik maken van andere (cloud) Identity Providers zoals Google, Facebook en DigiD
- Met een eigen Identity Store en zonder dat gebruik wordt gemaakt van federatieve SSO met de Entra ID tenant van NWO.
- Die zonder enige vorm van authenticatie gebruikt kunnen worden (bijvoorbeeld een publieke webapplicatie).

## Doelgroep

Dit document is technisch van aard en bedoeld voor intern gebruik binnen de NWO-D organisatie. Het is een onderdeel van het selectieproces voor de aansluiting van nieuwe applicaties zoals opgesomd in de introductie (onderhands of door middel van een aanbesteding).

# Inhoud

<b>1</b>	<b>Inleiding</b>	<b>5</b>
<b>2</b>	<b>Richtlijnen</b>	<b>6</b>
2.1	Verschil tussen authenticatie en autorisatie	6
2.2	Richtlijn 1: SSO	6
2.3	Richtlijn 2: Federatie	7
2.4	Richtlijn 3: Niet federatieve SSO	7
2.5	Richtlijn 4: @nwo.nl	7
2.6	Richtlijn 6: Ondersteuning van RBAC	7
2.7	Richtlijn 8: Minimale uitwisseling	8
<b>3</b>	<b>Verantwoordelijkheden</b>	<b>9</b>
3.1	Authenticatie (SSO)	9
3.2	Provisioning	9
3.3	Microsoft Graph API koppeling	10
<b>4</b>	<b>Aansluitvoorwaarden SAML</b>	<b>11</b>
4.1	SAML eisen set 1: Identity Provider	11
4.2	SAML eisen set 2: Service Provider	11
<b>5</b>	<b>Aansluitvoorwaarden OAuth/OIDC</b>	<b>12</b>
5.1	OAuth/OIDC eisen set 1: Identity Provider	12
5.2	OAuth/OIDC eisen set 2: Service Provider	12
<b>6</b>	<b>Aansluitvoorwaarden user provisioning</b>	<b>13</b>
<b>7</b>	<b>Aansluitvoorwaarden Microsoft Graph API</b>	<b>14</b>
<b>8</b>	<b>Bronvermelding</b>	<b>16</b>
8.1	Documenten	16
8.2	Externe bronnen	16
<b>Bijlage 1: SSO processen</b>		<b>17</b>
	OIDC (Open ID Connect)	17
	OAuth 2.0	17
	SAML (Security Assertion Markup Language)	18

# 1 Inleiding

Het IT-landschap van NWO is continu in beweging. Naast het uitfaseren van verouderde applicaties komen er ook nieuwe applicaties bij die nodig zijn voor de ondersteuning van de bedrijfsprocessen. Vanuit het oogpunt van informatiebeveiliging en beheersbaarheid van applicaties, zijn er een aantal randvoorwaarden waaraan een applicatie minimaal moet voldoen voor een veilige toegang en een beheersbare authenticatievoorziening.

In dit document zijn de richtlijnen opgenomen ten aanzien van de gebruikte authenticatiemechanismen waaraan een applicatie moet voldoen om opgenomen en beheerd te kunnen worden binnen het IT landschap van NWO. Hierbij wordt ook benoemd welke verantwoordelijkheden er horen bij de ICT afdeling van NWO (als Identity Provider) en welke verantwoordelijkheden horen bij de leverancier van de applicatie (als Service Provider).

Naast aansluitvoorwaarden ten aanzien van authenticatie is ook opgenomen waaraan applicaties moeten voldoen die extra persoonsgegevens vereisen. Dit omvat applicaties die door middel van federatieve SSO zijn gekoppeld en ook een profiel binnen de applicatie vereisen. Voorbeelden van applicaties die extra gegevens vereisen zijn TOPdesk, Joost en Ubeeo.

Tot slot zijn er applicaties die voor toegang tot gegevens binnen de Microsoft 365 omgeving van NWO gebruik maken van de Microsoft Graph API. De voorwaarden aan applicaties om via deze API te koppelen zijn ook in de aansluitvoorwaarden opgenomen.

Deze aansluitvoorwaarden op Entra ID zijn een onderdeel van alle aansluitvoorwaarden. De verhouding van dit aansluitdocument ten opzichte van alle aansluitdocumenten is dat in dit document de technische voorwaarden zijn opgenomen die aan een applicatie worden gesteld. In de overige aansluitdocumenten wordt ingegaan op andere aspecten zoals beveiliging, architectuur en functionaliteit.

## 2 Richtlijnen

Wanneer een nieuwe applicatie voor medewerkers van NWO wordt geselecteerd, zijn niet alleen de functionele eisen van belang maar dient ook rekening gehouden te worden met technische eisen. Er zijn veel verschillende technische eisen, waaronder de technische eisen aan de authenticatie. Deze technische authenticatie-eisen zijn belangrijk om te kunnen borgen dat:

- De toegang tot de applicatie voor medewerkers zo laagdrempelig mogelijk is;
- Authenticatie en autorisatie op een centrale plaats geborgd kan worden;
- De toegang tot een applicatie op een veilige manier kan plaatsvinden;
- Er een aansluiting mogelijk is met het Identity & Access Management platform van NWO.

Voor alle applicaties die aan medewerkers aangeboden worden gelden de volgende uitgangspunten:

- Applicaties worden alleen aangesloten op de ICT omgeving van NWO als deze de mogelijkheid bieden om gekoppeld te worden op basis van Entra ID;
- Applicaties die een federatieve SSO mogelijkheid hebben met Entra ID worden altijd op basis van deze aansluitvoorwaarden aangesloten;
- Applicaties met een eigen Identity Store worden niet aangesloten op de ICT omgeving van NWO maar kunnen wel beschikbaar worden gesteld aan medewerkers.

### 2.1 Verschil tussen authenticatie en autorisatie

Dit document gaat over de authenticatie voor applicaties die aangesloten worden op de IT omgeving van NWO. Het verschil tussen authenticatie en autorisatie is belangrijk in de context van beveiliging en toegang tot systemen.

#### 2.1.1 Authenticatie

Authenticatie is het proces waarbij wordt gecontroleerd of iemand is wie hij of zij beweert te zijn. Dit gebeurt meestal door middel van:

- **Wachtwoorden:** Een gebruiker voert een wachtwoord in dat overeenkomt met een opgeslagen wachtwoord.
- **Biometrische gegevens:** Zoals vingerafdrukken of gezichtsherkenning.
- **Twee-factor authenticatie (2FA):** Een extra beveiligingslaag waarbij naast een wachtwoord ook een tweede factor, zoals een SMS-code, wordt gebruikt.

#### 2.1.2 Autorisatie

Autorisatie is het proces waarbij wordt bepaald welke middelen of gegevens een geauthentiseerde gebruiker mag openen of gebruiken. Dit gebeurt meestal door:

- **Toegangsrechten:** Gebruikers krijgen specifieke rechten of rollen toegewezen die bepalen wat ze kunnen doen binnen een systeem.
- **Beleidsregels:** Regels die bepalen welke acties een gebruiker mag uitvoeren, gebaseerd op hun rol of andere criteria.

Nb. In deze aansluitvoorwaarden zijn de technische voorwaarden opgenomen om het autorisatiebeleid centraal te kunnen beheren. Het beleid hoe omgegaan wordt met autorisatie binnen NWO is vastgelegd in het autorisatiebeleid wat gepubliceerd is op JOOST en is buiten scope van deze aansluitvoorwaarden.

### 2.2 Richtlijn 1: SSO

Een uitgangspunt is dat een applicatie moet voldoen aan de technische architectuurprincipes van NWO en zijn vastgelegd in het HLD IT Architectuur. In het kader van aansluitvoorwaarden voor applicaties is architectuurprincipe TA06 het meest belangrijk:

**Het systeem biedt ondersteuning voor SSO (Single Sign-On) en sluit daarbij aan op Entra ID.**

## 2.3 Richtlijn 2: Federatie

Een SSO koppeling tussen een applicatie en Entra ID kan op verschillende manieren plaatsvinden. Om een applicatiekeuze zo min mogelijk te beperken door technische eisen is het uitgangspunt dat **alle federatieve koppelingsmogelijkheden met Entra ID worden ondersteund** mits deze ook volledig door Microsoft worden ondersteund. Dit houdt in dat onderstaande federatieve SSO protocollen voor NWO applicaties worden ondersteund:

- SAML 2.0 (Security Assertion Markup Language), zie ook hoofdstuk 4.  
[Wordt gebruikt voor authenticatie en autorisatie.](#)
- OAuth 2.0, zie ook hoofdstuk 5.  
[Wordt gebruikt voor autorisatie.](#)
- OIDC (OpenID Connect), zie ook hoofdstuk 5.  
[Wordt gebruikt voor authenticatie.](#)

OIDC maakt gebruik van het OAuth 2.0 framework en wordt daarom als één koppelingsmogelijkheid beschouwd in dit document. In bijlage 1 is schematisch de werking van bovenstaande protocollen opgenomen.

## 2.4 Richtlijn 3: Niet federatieve SSO

Het gebruik van niet-federatieve SSO zoals Password SSO en Linked SSO dient zoveel mogelijk te worden vermeden en wordt standaard niet ondersteund door NWO. Gebruik van Integrated Windows Authenticatie (IWA) of Header Based SSO wordt per definitie **niet** door NWO ondersteund voor een applicatie.

## 2.5 Richtlijn 4: @nwo.nl

Is er een SSO koppeling gerealiseerd tussen NWO en de Service Provider, dan moet door de SaaS leverancier worden geborgd dat het aanmaken en gebruik van inlogaccounts op basis van een @nwo.nl, @regieorgaan-sia.nl en/of @nwo-i.nl e-mail adres voor toegang tot de applicatie bij de SaaS leverancier niet mogelijk is.

Authenticatie en autorisatie met een @nwo.nl, @regieorgaan-sia.nl en/of @nwo-i.nl e-mailadres mag alleen via de SSO koppeling en Entra ID plaatsvinden.

## Richtlijn 5: Provisioning

Provisioning van persoonsgegevens in een gekoppelde applicatie is alleen toegestaan indien deze applicatie via federatieve SSO is gekoppeld met de Entra ID tenant van NWO. Voor provisioning van account informatie wordt gebruik gemaakt van SCIM 2.0 of een standaard koppeling die binnen het IAM platform van NWO beschikbaar is.

## 2.6 Richtlijn 6: Ondersteuning van RBAC

Indien er binnen een applicatie verschillende rollen aan accounts toegewezen kunnen worden, dan is de doelstelling om het specifieke autorisatieniveau binnen de applicatie per medewerker op basis van het lidmaatschap van een Entra ID applicatiegroep toe te kennen.

Standaard koppelingsmogelijkheden die door NWO worden ondersteund voor RBAC binnen applicaties met een SSO koppeling zijn:

- Ondersteuning van Groups binnen Entra ID
- Ondersteuning van App Roles in een applicatie die binnen Entra ID gekoppeld wordt
- SCIM (System for Cross-domain Identity Management)



- API koppeling

## Richtlijn 7: Toegang via de Microsoft Graph API

Voor toegang tot gegevens in de Microsoft 365 tenant van NWO geldt:

- **Delegated en application permissions zijn mogelijk.** Toegang op basis van delegated permissions (scopes) zorgt er voor dat een applicatie namens een geauthentiseerde gebruiker toegang heeft en bij gebruik van application permissions (app roles) heeft de applicatie zelf toegang. Het gebruik van delegated permissions heeft de voorkeur boven het gebruik van application permissions omdat de scope van delegated permissions beperkt is tot alleen gegevens waarop de geauthentiseerde gebruiker daadwerkelijk rechten heeft. Bij gebruik van application permissions heeft de applicatie in principe toegang tot gegevens van alle gebruikers binnen de Microsoft 365 tenant.
- **Toegang is alleen mogelijk voor gebruikersaccounts die zich bevinden in de Entra ID directory van NWO.** Het gebruik van persoonlijke Microsoft accounts is niet toegestaan. Dit houdt in dat alleen de “signInAudience” van het type “AzureADMyOrg” wordt toegestaan voor zowel delegated als application permissions.
- **Het aanmaken, muteren of verwijderen van gegevens binnen de Microsoft 365 tenant via de Microsoft Graph API is niet toegestaan.** De Microsoft Graph API mag alleen worden gebruikt voor het lezen van gegevens; schrijfrechten worden niet toegekend.

## 2.7 Richtlijn 8: Minimale uitwisseling

Het uitwisselen van gegevens tussen de Identity Provider en de Service Provider (voor zowel SSO, provisioning en toegang via de Graph API) wordt geminimaliseerd en is beperkt tot de gegevens die vereist zijn voor een correcte werking van de applicatie. Bij het uitwisselen van gegevens anders dan basisgegevens (zoals een e-mail adres of naam) vindt de beoordeling en - het geven van toestemming tot het uitwisselen van deze persoonsgegevens – plaats door de privacy officer van NWO.

## 3 Verantwoordelijkheden

Bij het realiseren en onderhouden van:

- Een federatieve SSO koppeling met het Entra ID platform van NWO en een applicatie.
- Een koppeling voor provisioning van gebruikersgegevens naar een externe applicatie.
- Het gebruik van de Microsoft Graph API om applicatietoegang te krijgen tot informatie in de Microsoft 365 tenant van NWO.

Zijn er voor zowel NWO als de aanbieder van de applicatie er over-en-weer verantwoordelijkheden. Deze zijn in dit hoofdstuk op hoofdlijnen beschreven.

### 3.1 Authenticatie (SSO)

Bij het realiseren en onderhouden van een federatieve koppeling zijn er verantwoordelijkheden voor zowel NWO als de serviceprovider.

#### 3.1.1 Verantwoordelijkheden NWO

De verantwoordelijkheden voor NWO (in de rol van Identity Provider) omvatten:

- Het maken en onderhouden van de app-registratie binnen het Entra ID platform;
- Aanleveren van de metadata URL van de app registratie aan de service provider;
- Borgen dat de benodigde attributen op de juiste wijze zijn gevuld voor gebruikersaccounts in Entra ID;
- Koppelen van autorisaties aan gebruikersaccounts op basis van groepslidmaatschappen;
- Monitoring van de beschikbaarheid en werking van de identity store;
- Troubleshooting bij authenticatie- of autorisatieproblemen;
- Periodiek vernieuwen van encryptie keys voor de federatieve koppeling;
- Beheer van MFA instellingen voor een federatief gekoppelde applicatie;
- Beoordeling of de door de Service Provider gewenste attributen gedeeld mogen worden.

#### 3.1.2 Verantwoordelijkheden Service Provider

De verantwoordelijkheden voor de (externe) leverancier van de SaaS dienst (in de rol van Service Provider) omvatten:

- Beschikbaar hebben van een beschrijving van een standaard federatieve koppeling voor de SaaS applicatie;
- Beschikbaar hebben van een beschrijving van rollen binnen de SaaS applicatie;
- Aangeven van de noodzakelijke attributen die van de Identity Provider worden verlangd en waarom deze nodig zijn zodat deze door NWO beoordeeld kunnen worden;
- Aanleveren van de metadata;
- Monitoren van de beschikbaarheid van de eigen dienst;
- Tijdig vernieuwen van de keys voor de federatieve koppeling;
- Borgen dat NWO medewerkers alleen via de federatieve SSO koppeling kunnen inloggen met een @nwo.nl e-mail adres en NIET via een achterdeur-zonder-SSO.

## 3.2 Provisioning

Wordt een applicatie gekoppeld voor provisioning van persoonsgegevens aan het IAM platform van NWO dan hebben zowel NWO als de applicatieleverancier hierin verantwoordelijkheden.

#### 3.2.1 Verantwoordelijkheden NWO

De verantwoordelijkheden voor NWO (in de rol van Identity Provider) omvatten:

- Het maken en onderhouden van de koppeling op basis van SCIM of custom API met het doelsysteem;
- Het aanleveren van een uniek “externalId” aan de service provider die voor de SCIM koppeling wordt gebruikt;
- Borgen dat de benodigde attributen op de juiste wijze worden aangeboden aan het doelsysteem;
- Monitoring van de beschikbaarheid en werking van het IAM platform;
- Troubleshooting bij authenticatie- of connectiviteitsproblemen met het doelsysteem;
- Periodiek vernieuwen van encryptie keys voor de koppeling;
- Beoordeling of de door de Service Provider gewenste attributen gedeeld mogen worden.

### 3.2.2 Verantwoordelijkheden service provider

De verantwoordelijkheden voor de (externe) leverancier van de applicatie (in de rol van Service Provider) omvatten:

- Beschikbaar hebben van een beschrijving van de gebruikte API voor provisioning;
- Aangeven van de noodzakelijke attributen die worden verlangd en waarom deze nodig zijn zodat deze door NWO beoordeeld kunnen worden;
- Het aanleveren van een uniek ID voor de SCIM koppeling;
- Aanleveren van de metadata;
- Monitoren van de beschikbaarheid van de eigen dienst;
- Tijdig vernieuwen van de keys voor de koppeling;

## 3.3 Microsoft Graph API koppeling

Krijgt een applicatie toegang tot gegevens binnen de Microsoft 365 tenant van NWO dan hebben zowel NWO als de applicatieleverancier hierin verantwoordelijkheden.

### 3.3.1 Verantwoordelijkheden NWO

De verantwoordelijkheden voor NWO (in de rol van Identity Provider) omvatten:

- Het maken en onderhouden van de app-registratie binnen het Entra ID platform;
- Aanleveren van de app registratie ID's aan de service provider;
- Monitoring van de beschikbaarheid en werking van de Microsoft 365 tenant;
- Troubleshooting bij authenticatie- of autorisatieproblemen via toegang tot de Graph API;
- Periodiek vernieuwen van encryptie keys voor de API koppeling;
- Beoordeling of de door de Service Provider gewenste Microsoft 365 toegangsrechten via de MS Graph API toegekend mogen worden.

### 3.3.2 Verantwoordelijkheden service provider

De verantwoordelijkheden voor de (externe) leverancier van de applicatie (in de rol van Service Provider) omvatten:

- Beschikbaar hebben van een beschrijving van de MS Graph API toegangsrechten voor de SaaS applicatie en waar deze rechten binnen de applicatie voor worden gebruikt;
- Monitoren van de beschikbaarheid van de eigen dienst;
- Tijdig vernieuwen van de keys voor de koppeling.

## 4 Aansluitvoorwaarden SAML

Om een federatieve koppeling te realiseren op basis van SAML moet voldaan worden aan een aantal eisen en zijn metagegevens nodig. In dit hoofdstuk is beschreven welke gegevens door NWO worden aangeleverd aan de Service Provider en welke gegevens NWO verwacht.

### 4.1 SAML eisen set 1: Identity Provider

NWO maakt gebruik van Microsoft Entra ID als Identity Provider (IdP). Voor het aansluiten van de SP op de IdP via SAML geldt onderstaande:

- Alleen SAML 2.0 of hoger wordt ondersteund;
- Er wordt gebruik gemaakt van een URL voor de SP om IdP metadata aan te leveren in XML formaat;
- In verzoeken naar de IdP moet encryptie van NameID toegepast worden;
- SAML assertions moeten encrypted en ondertekend zijn.

### 4.2 SAML eisen set 2: Service Provider

De metadata van de Service Provider kan op twee verschillende manieren worden aangeleverd.

- Via een Microsoft Gallery registratie (voorkeur)
- Via een publiek beschikbare URL
- Via een XML-geformatteerd bestand

De volgende gegevens dienen minimaal in de metadata te zijn beschreven:

Element	Type	Waarden
<b>entityID</b>	EntityDescriptor	Uniform Resource Identifier
<b>protocolSupportEnumeration</b>	SPSSODescriptor	urn:oasis:names:tc:SAML:2.0:protocol
<b>AuthnRequestsSigned</b>	SPSSODescriptor	TRUE
<b>WantAssertionsSigned</b>	SPSSODescriptor	TRUE
<b>use</b>	KeyDescriptor	signing
<b>certificate</b>	KeyDescriptor, KeyInfo, X509Data, X509Certificate	Base64 encoded
<b>use</b>	KeyDescriptor	Encryption
<b>certificate</b>	KeyDescriptor, KeyInfo, X509Data, X509Certificate	Base64 encoded
<b>Binding</b>	SingleLogoutService	POST, Redirect
<b>Location</b>	SingleLogoutService	URL
	NameIDFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
<b>Binding</b>	AssertionConsumerService	POST, Redirect
<b>Location</b>	AssertionConsumerService	URL

## 5 Aansluitvoorwaarden OAuth/OIDC

Indien OAuth in combinatie met OIDC wordt gebruikt voor een SSO-koppeling tussen de Service Provider en Identity Provider moet voldaan worden aan een aantal eisen en zijn specifieke gegevens nodig voor beide partijen.

### 5.1 OAuth/OIDC eisen set 1: Identity Provider

NWO maakt gebruik van Microsoft Entra ID als Identity Provider (IdP). Voor het aansluiten van de SP op de IdP via OAuth 2.0/OIDC geldt onderstaande:

- Ondersteunde applicatieplatformen zijn web en native;
- Zowel een OIDC koppeling op basis van authenticatie als toestemming (consent) wordt ondersteund;
- NWO levert aan de SP de volgende gegevens aan:
  - Client ID (Application ID)
  - Client Secret Value
  - Directory ID (Tenant ID)
- Bearer tokens zijn geformatteerd als JSON Web Tokens (JWT).

### 5.2 OAuth/OIDC eisen set 2: Service Provider

Voor het registreren van de Service Provider als client application zijn de volgende gegevens benodigd:

Parameter	Vereist/ Optioneel	Beschrijving	Waarden
<b>Client name</b>	Vereist	Naam van de Service Provider	
<b>Redirect URIs</b>	Vereist	Redirect URI waarden	
<b>Application type</b>	Optioneel	Web/native	
<b>Grants required</b>	Vereist	Gewenste grants	
<b>Token types</b>	Vereist	Gewenste token types	

## 6 Aansluitvoorwaarden user provisioning

Er zijn applicaties met een SSO koppeling waarbij gebruikersinformatie wordt opgeslagen en binnen deze applicatie wordt gebruikt en verrijkt; bijvoorbeeld voor het tonen van aanvullende persoonsinformatie die niet binnen Entra ID aanwezig is. Ook kan een applicatie gebruik maken van specifieke autorisatieniveaus die zijn gebaseerd op groepen die binnen een applicatie worden onderhouden.

Het uitgangspunt is dat provisioning van gebruikersinformatie (en indien relevant ook groepen en groepslidmaatschap) binnen een applicatie centraal plaatsvindt via het IAM platform van NWO. Bij voorkeur door gebruik te maken van de aanwezige standaardkoppelingen in het IAM platform. Is er geen standaardkoppeling aanwezig voor een applicatie, dan wordt gebruik gemaakt SCIM (System for Cross-domain Identity Management). Dit is de marktstandaard op dit gebied.

Ondersteunt een applicatie geen SCIM en maakt deze gebruik van een eigen API of synchronisatietool (via bijvoorbeeld de Microsoft Graph API), dan wordt specifiek beoordeeld of een koppeling met de identity store van NWO mogelijk is.

### Provisioning eisen set 1: Identity Provider

Wordt gebruik gemaakt van SCIM om een koppeling te realiseren voor provisioning van gebruikersinformatie of groepen naar een applicatie, dan dient het SCIM endpoint de volgende eigenschappen te ondersteunen:

- Er is een federatieve SSO koppeling tussen de Entra ID tenant van NWO met de te provisionen applicatie;
- Er wordt gebruik gemaakt van SCIM 2.0;
- Authenticatie vindt plaats op basis van OAuth 2.0 of bearer token (token secret);
- Communicatie vindt plaats via HTTPS;

### Provisioning eisen set 2: Service Provider

Voor het koppelen van SCIM 2.0 zijn de volgende gegevens van de Service Provider benodigd:

Parameter	Vereist/ Optioneel	Beschrijving	Waarden
<b>BaseURL</b>	Vereist	URL om de SCIM 2.0 API te benaderen	https://<FQDN>/scim/v2
<b>Unique ID</b>	Vereist	Unieke waarde voor de SCIM resource	GUID
<b>Token Secret</b>	Vereist		

Daarnaast gelden de volgende eisen:

- De waarde van het sub attribuut "type" van multivalued attributen moet uniek zijn. Voorbeeld: Het gebruik van twee verschillende e-mail adressen met als subtype "work" is niet toegestaan.
- De header voor alle antwoorden (responses) moet als content-Type "application/scim+json" bevatten

## 7 Aansluitvoorwaarden Microsoft Graph API

Sommige applicaties vereisen voor een juiste werking toegang tot informatie binnen de Microsoft 365 tenant die door NWO wordt gebruikt. Het kan bijvoorbeeld gaan om persoonsinformatie uit de Entra ID directory, een overzicht van groepen en groepslidmaatschappen, een lijst van alle SharePoint Online sites, Microsoft Teams die in gebruik zijn of bestanden die zijn opgeslagen op OneDrive. Deze toegang kan onder bepaalde voorwaarden op basis van de Microsoft Graph API worden verleend.

Toegang tot gegevens via de Microsoft Graph API vindt plaats op basis van OAuth access tokens zodat geverifieerd kan worden welke specifieke toegangsrechten voor een applicatie van toepassing zijn. Het is van belang dat een applicatie waarvoor toegang is vereist via de Microsoft Graph API via federatieve SSO gekoppeld is met Entra ID.

### Gegevenstoegang

Via de Microsoft Graph API is een grote hoeveelheid data binnen de Microsoft 365 tenant te raadplegen en kan ook data worden aangemaakt, gemuteerd of verwijderd. Sommige gegevens zijn vrij algemeen en vormen geen groot risico als deze worden gelezen voor het gebruik binnen een gekoppelde applicatie. Denk hierbij aan algemene account of profielinformatie van medewerkers. Er zijn ook gegevens die bij voorkeur niet beschikbaar gesteld worden aan applicaties omdat deze onder andere inzicht geven in de (security)configuratie van de tenant of alle bestanden kunnen lezen die binnen de Microsoft 365 omgeving zijn opgeslagen.

Het recht om gegevens aan te maken, te muteren of te verwijderen binnen de Microsoft 365 tenant via de Microsoft Graph API wordt niet toegekend omdat dit kan leiden tot grote beveiligingsrisico's.

Het verlenen van toegangsrechten tot gegevens die via de Graph API beschikbaar gesteld worden vindt plaats op relatief grofmazige wijze. Een voorbeeld is de toegang tot de persoonsinformatie die voor een gebruikersaccount is opgeslagen. Het verlenen van rechten op "User.Read.All" heeft tot gevolg dat alle attributen van een gebruikersprofiel gelezen kunnen worden. Dit zijn bijvoorbeeld niet alleen de weergavenaam, voornaam, achternaam, foto en e-mailadres maar ook attributen als een geboortedatum, datum in dienst en de password policy die van toepassing is. Het is niet mogelijk om via de Microsoft Graph API toegang te verlenen of te blokkeren tot specifieke attributen van een object. Hoewel het toekennen van rechten op grofmazige wijze plaatsvindt, zijn er nog een grote hoeveelheid rechten toe te kennen. Er zijn (tijdens het opstellen van deze aansluitvoorwaarden) 494 verschillende application permissions en 546 delegated permissions toe te kennen.

De gegevens die via de Microsoft Graph API geraadpleegd kunnen worden zijn op hoofdlijnen geclassificeerd om aan te geven:

- **Wat is toegestaan.** Het raadplegen van deze gegevens is voor alle gekoppelde applicaties toegestaan.
- **Wat door de CISO beoordeeld dient te worden.** Het raadplegen van deze gegevens is alleen toegestaan na expliciete goedkeuring door de CISO.
- **Niet is toegestaan.** Het raadplegen van deze gegevens wordt niet toegestaan.

Hierbij is onderscheid gemaakt tussen het verlenen van delegated permissions en application permissions.

#### Application permissions

Het toekennen van rechten op applicatieniveau dient altijd door de CISO beoordeeld te worden. In principe worden geen rechten op applicatieniveau toegekend die kunnen leiden tot het doorvoeren van mutaties in de cloud applicaties of diensten die via de Microsoft Graph API benaderbaar zijn, tenzij er een zwaarwegend belang is om hierop een uitzondering te maken.

### Delegated permissions

Voor gedelegeerde rechten geldt dat hier in principe ook geen schrijfrechten toegekend kunnen worden, tenzij er een zwaarwegend belang is om hierop een uitzondering te maken.

### Toe te kennen toegangsrechten

Leesrechten worden in principe toegestaan, mits:

- **De informatie niet security gerelateerd is.** Voorbeelden van rechten om security gerelateerde informatie te lezen zijn "AttackSimulation.Read.All", "AuditLog.Read.All" en "SecurityAlert.Read.All".
- **De informatie geen configuratiegegevens van de tenant bevat.** Voorbeelden van rechten waarmee configuratiegegevens gelezen kunnen worden zijn "Policy.Read.All", "AppCertTrustConfiguration.Read.All", "ManagedTenants.Read.All" en "PublicKeyInfrastructure.Read.All".

Het toekennen van delegated permissions voor andere informatie dan basis profielinformatie dient altijd door de CISO beoordeeld te worden.

### Toegang ten behoeve van user provisioning

Sommige applicaties maken gebruik van een eigen (decentraal) provisioning proces waarbij toegang via de Microsoft Graph API noodzakelijk is om persoonsgegevens en groepslidmaatschappen te lezen. Op basis van deze gegevens wordt binnen de bijvoorbeeld een lokaal gebruikersaccount aangemaakt of een medewerkersprofiel. Het uitgangspunt is dat provisioning van gebruikersaccounts in applicaties altijd via het IAM platform van NWO verloopt. Toegang tot de MS Graph API met als doel user provisioning binnen een applicatie wordt niet toegestaan.

## MS Graph API eisen set 1: Identity Provider

Voor het verlenen van toegang tot de MS Graph API geldt onderstaande:

- NWO levert aan de SP de volgende gegevens aan:
  - Client ID (Application ID)
  - Client Secret Value (voor web apps)
  - Directory ID (Tenant ID)
- Het ondersteunde account type is "Accounts in this organizational directory only" (single tenant)

## MS Graph API eisen set 2: Service Provider

Voor het registreren een applicatie voor toegang via de MS Graph API zijn de volgende gegevens benodigd:

Parameter	Vereist/ Optioneel	Beschrijving	Waarden
<b>Client name</b>	Vereist	Naam van de Service Provider	
<b>Redirect URI</b>	Vereist	Redirect URI waarde	
<b>Scope</b>	Vereist	Gewenste toegangsrechten	
<b>Token types</b>	Vereist	Gewenste token types	



## 8 Bronvermelding

### 8.1 Documenten

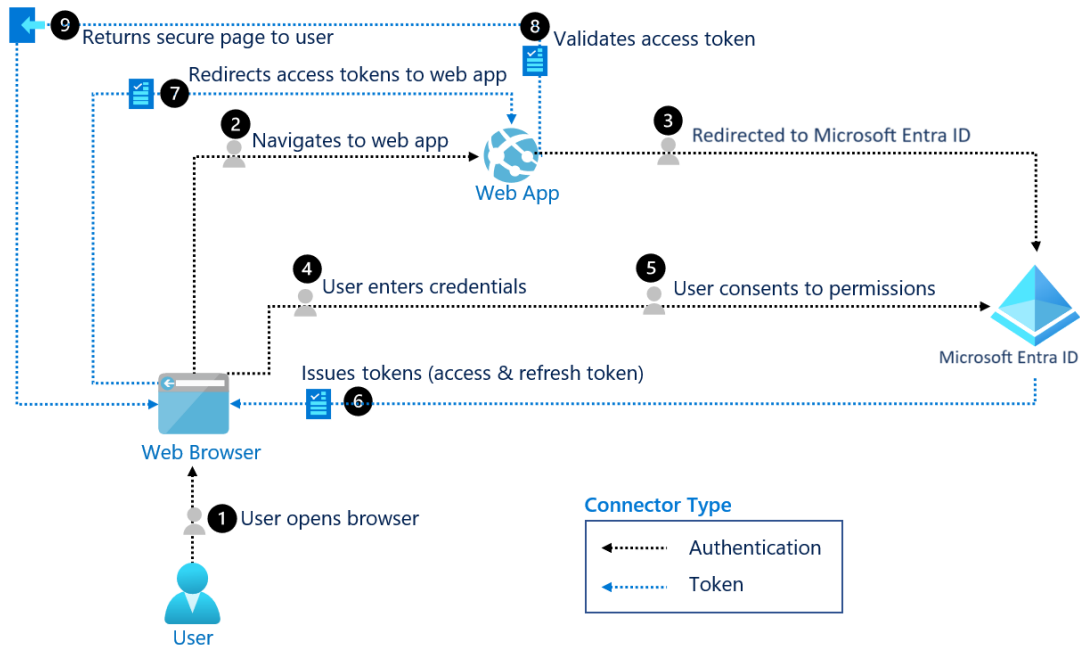
Document	Auteur	Versie/ Link
20240305 EA HLD IT Architectuur	Martijn ten Hacken	1.0
Autorisatiebeleid NWO	Irma Meinema	1.0
Informatiebeveiligingsbeleid NWO D	Irma Meinema	0.95
Security Referentie Architectuur NWO (SRAN)	Architecture Board	

### 8.2 Externe bronnen

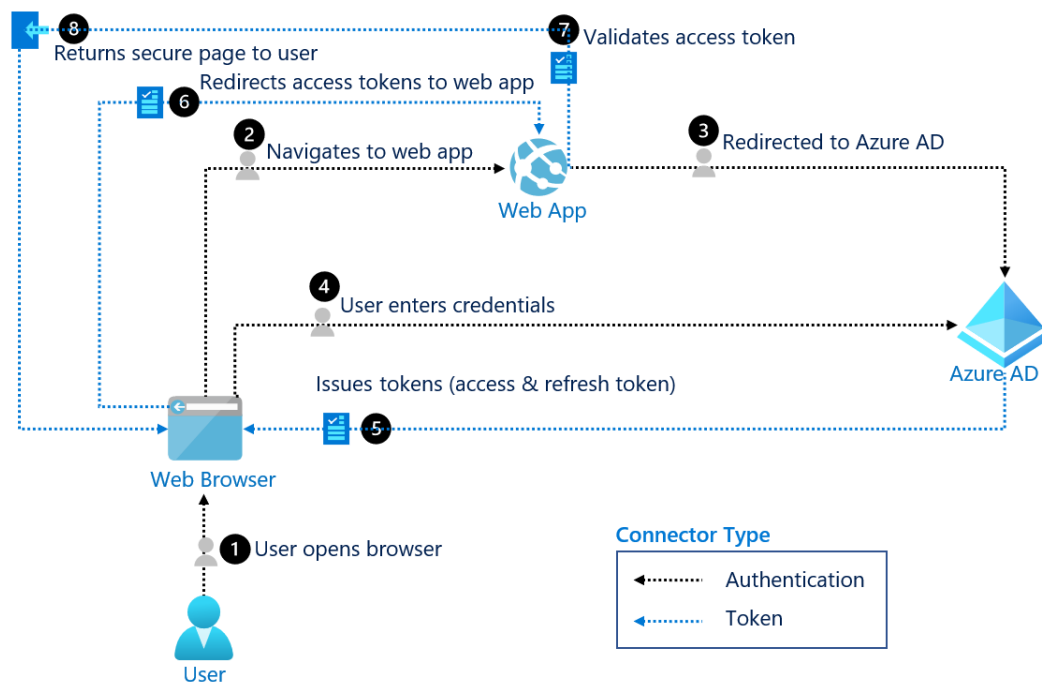
Titel	URL
<b>Website OpenID</b>	<a href="https://openid.net/">https://openid.net/</a>
<b>Plan SSO deployment</b>	<a href="https://learn.microsoft.com/en-in/entra/identity/enterprise-apps/plan-sso-deployment">https://learn.microsoft.com/en-in/entra/identity/enterprise-apps/plan-sso-deployment</a>
<b>App roles in apps</b>	<a href="https://learn.microsoft.com/en-us/entra/identity-platform/howto-add-app-roles-in-apps">https://learn.microsoft.com/en-us/entra/identity-platform/howto-add-app-roles-in-apps</a>
<b>SCIM - RFC 7643</b>	<a href="https://datatracker.ietf.org/doc/html/rfc7643">https://datatracker.ietf.org/doc/html/rfc7643</a>
<b>Microsoft Graph permissions reference</b>	<a href="https://learn.microsoft.com/en-us/graph/permissions-reference">https://learn.microsoft.com/en-us/graph/permissions-reference</a>

# Bijlage 1: SSO processen

## OIDC (Open ID Connect)



## OAuth 2.0



# SAML (Security Assertion Markup Language)

