



Den Haag

Aansluitvoorwaarden Azure AD

Federatieve Authenticatie

Versie: 1.0
Status: Definitief

Colofon

Titel	Aansluitvoorwaarden Federatieve Koppelingen Azure AD
Ondertitel	Federatieve Authenticatie
Versie	1.0
Status	Definitief
Datum laatst bijgewerkt	17 mei 2022
Samengesteld door	Tofail Wagid Hosain & Erik Paulsen
Opdrachtgever	Robert Garskamp
Projectleider	-
Laatste versie bewerkt door	Tofail Wagid Hosain
Bestandsnaam	Federatieve Authenticatie - Aansluitvoorwaarden Federatieve Koppelingen Azure AD 1.0

© 2022 Gemeente Den Haag

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande toestemming van Gemeente Den Haag.

No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by Gemeente Den Haag.

Inhoudsopgave

1.....	Inleiding	5
1.1.....	Doel van dit document	5
1.2.....	Doelgroep	5
1.3.....	Afbakening & beperkingen	5
1.4.....	Referenties	5
1.5.....	Afkorting en begrippen	6
1.6.....	Leeswijzer	6
2.....	Context Diagram	7
3.....	Aansluitvoorwaarden	8
3.1.....	Persoonsgegevensverwerking	8
3.2.....	Beveiliging	8
3.3.....	Meldplicht	8
3.4.....	Exclusiviteit	8
3.5.....	Geheimhouding	8
3.6.....	Informatie en documentatie	8
3.7.....	Financiële verplichtingen	8
3.8.....	Auditing	8
3.9.....	Duur en beëindiging	9
3.10.....	OTAP	9
3.11.....	Beveiliging en/of privacy incidenten	9
3.12.....	Onderhoud	9
3.13.....	Verstoringen	9
3.14.....	Troubleshooting	9
3.15.....	Accordatie aansluitvoorwaarden	9
4.....	Benodigde Gegevens	10

4.1.1.	Algemene Informatie.....	10
4.1.2.	OAuth 2.0 / OpenID Connect Federatie.....	10
4.1.3.	SAML Federatie	10
5.	Privacy & Beveiliging	11
5.1.....	<i>Gebruikers Authenticatie</i>	11
5.1.1.	Gebruikersnaam, Wachtwoord en Multi-Factor Authenticatie	11
5.2.....	<i>Gebruikersgegevens</i>	11
5.2.1.	SAML Assertions.....	11
5.2.2.	OAuth 2.0 Gegevens Authorisatie & Permissies (Graph API).....	12
5.2.3.	OAuth 2.0 Consent Framework.....	12
5.3.....	<i>Applicatie Authenticatie</i>	12
5.4.....	<i>Best Practices</i>	13
6.	Bijlagen	14
6.1.....	<i>Formulier aanvraag OAuth 2.0 / OpenID Connect Federatie</i>	14
6.2.....	<i>Formulier aanvraag SAML Federatie</i>	14
6.3.....	<i>Optionele SAML Claims</i>	14

1. Inleiding

1.1. Doel van dit document

De aansluitvoorwaarden van Gemeente Den Haag zijn de voorwaarden waaronder Gemeente Den Haag haar diensten op gebied van federatieve authenticatie verleent aan afnemers. Ze benoemen rechten en verplichtingen voor zowel Gemeente Den Haag als afnemers bij aansluiting op en gebruikmaking van de federatieve koppeling van Gemeente Den Haag.

1.2. Doelgroep

Onder de doelgroep (afnemers) verstaan we functioneel beheerders en externe partijen die gebruik willen maken van de federatieve authenticatie dienst om medewerkers van de Gemeente Den Haag toegang te geven (op basis van hun persoonlijk GDH inlogaccount) tot digitale informatiebronnen om zo externe samenwerking met (keten)partners te faciliteren.

1.3. Afbakening & beperkingen

- Alle applicatie federaties dienen middels een TOPdesk verzoek aangevraagd te worden door de interne applicatie eigenaar/beheerder van Gemeente Den Haag.
- De identity store van de gemeente is Microsoft Azure Active Directory. Hierin bevinden zich alle identiteiten van de medewerkers van Gemeente Den Haag. De bron van deze identiteiten wordt beheerd door het IAM team van Gemeente Den Haag.
- Het toekennen van applicatirollen en/of rechten wordt zo veel mogelijk gedaan door het IAM proces of door functioneel beheer van de Gemeente Den Haag.
- Voor zowel interne als externe toegang tot applicaties maken medewerkers gebruik van een persoonlijk toegewezen Gemeente Den Haag gebruikersaccount. Hiermee tonen ze aan wie ze zijn d.m.v. een accountnaam + wachtwoord en een MFA token (authenticatie).
- Applicaties die een eigen userstore nodig hebben voor het toekennen van rechten moeten deze koppelen aan de federatieve Den Haag identiteiten op basis van een unieke identifier (bijvoorbeeld UPN, e-mailadres).
- De federatieve platformen DigiD (burgers) en E-Herkenning (medewerkers namens bedrijven) zijn buiten scope van dit document.

1.4. Referenties

Federatieve koppelingen zijn een onderdeel van het Identity & Access Managementproces (IAM) van Gemeente Den Haag.

#	Referentie	Document
1	Architectuurprincipes Gemeente Den Haag	Architectuurprincipes van Gemeente Den Haag
2	IAM Doelarchitectuur	
3	Memo Privacy advies t.b.v. IAM	Privacy advies ten behoeve van IAM (Gemeente Den Haag)
4	Microsoft best-practices	Microsoft best-practices
5	Microsoft Identity Platform documentatie	Microsoft identity platform documentation Microsoft Docs
6	Industriestandaarden federatie	SAML OAuth2 en Open ID Connect.
7	Ontwerp Azure AD Platform	

8	Procesinrichting Federaties Gemeente Den Haag	
---	--	--

1.5. Afkortingen en begrippen

Aangezien dit document voor diverse doelgroepen bedoeld is, is het in algemene zin belangrijk dat de voornaamste begrippen en afkortingen op een eenduidige manier geïnterpreteerd worden. Hieronder zijn deze nader verklaard.

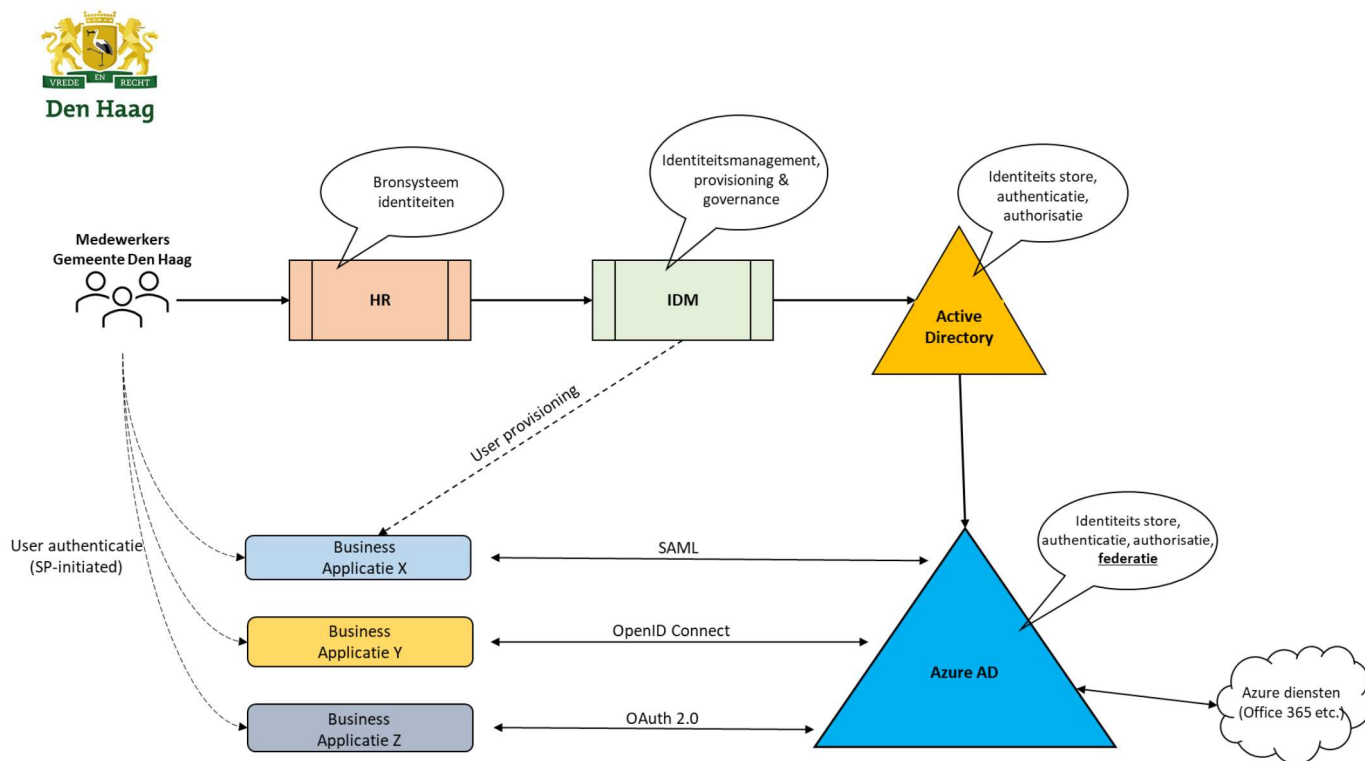
Afktorting	Toelichting
Identity Provider (IDP)	De Identity Provider (IdP) is de partij die de identiteiten van de gebruikers bevat
SAML	SAMLv 2.0 standaard, ook SAML2.0 genoemd. SAML staat voor Security Assertion Markup Language.
Service Provider (SP)	De Nederlandse vertaling van de SAML-term Service Provider is dienstaanbieder en is de informatiebron waarop de gebruiker inlogt.
SSO	Dit staat voor Single Sign On en dit maakt het mogelijk om van meerdere gerelateerde diensten gebruik te maken zonder dat een medewerker hiervoor opnieuw moet inloggen.
IAM	Identity & Access management; Proces waarmee gebruikersaccounts en rechten gekoppeld worden aan natuurlijke personen.
MFA	Multi-Factor Authenticatie (MFA) voegt een extra veiligheidslaag toe bovenop de gebruikersnaam en het wachtwoord
SaaS	Software as a Service, applicatie die in een extern datacenter wordt gehost. De applicatie wordt als een dienst aangeboden.
OAuth 2.0	OAuth 2.0 is een autorisatiestandaard voor met web gebaseerde applicaties die gegevens uitwisselen met behulp van API's. OAuth 2.0 maakt gebruik van 'tokens' waardoor vertrouwelijke gegevens als een gebruikersnaam of wachtwoord niet afgegeven hoeven te worden.
OpenID Connect	OpenID Connect (OIDC) is een verificatieprotocol dat is gebouwd op OAuth 2.0 dat u kunt gebruiken om een gebruiker veilig aan te melden bij een toepassing.
RBAC	Role Based Access Control; op basis van rol of functie worden autorisaties automatisch toegekend
Azure AD	Azure Active Directory is de cloud-gebaseerde identiteits- en toegangsbeheerdienst van Microsoft.

1.6. Leeswijzer

- [Hoofdstuk 1](#) beschrijft de inleiding van dit document.
- [Hoofdstuk 2](#) geeft een visuele context van de federatie oplossing zoals geboden door Gemeente Den Haag.
- [Hoofdstuk 3](#) beschrijft de aansluitvoorwaarden waar de afnemer en/of leverancier aan dient te voldoen.
- [Hoofdstuk 4](#) beschrijft de benodigde gegevens van de afnemer en/of leverancier t.b.v. het aanmaken van een federatieve koppeling.
- [Hoofdstuk 5](#) beschrijft de privacy en security aspecten waar de aangesloten applicatie aan dient te voldoen.
- [Hoofdstuk 6](#) biedt meerdere bijlagen waar naar gerefereerd wordt in dit document.

2. Context Diagram

De onderstaande afbeelding geeft een sterk versimpelde weergave van de Azure AD federatie context binnen Gemeente Den Haag.



3. Aansluitvoorwaarden

De aansluitvoorwaarden beschrijven de condities waarop Gemeente Den Haag (GDH) haar diensten aanbiedt aan een afnemer en/of leverancier op gebied van applicatie federatie.

3.1. Persoonsgegevensverwerking

De afnemer en/of leverancier dient de verkregen attributen (claims, assertions) op gebied van persoonsgegevens uitsluitend te gebruiken binnen de aangesloten applicatie. Op verzoek van de desbetreffende medewerker of Gemeente Den Haag als organisatie dienen de gebruikersgegevens aantoonbaar verwijderd te kunnen worden.

3.2. Beveiliging

De federatief aangesloten applicatie dient te voldoen aan de minimaal gangbare beveiligingseisen zoals encryptie van data, toegangsbeveiliging, functiescheiding (RBAC) etc. Eventuele additionele eisen kunnen door de IT security / privacy afdeling van Gemeente Den Haag worden vereist.

3.3. Meldplicht

De afnemer en/of leverancier dient (de vertegenwoordiger van) Gemeente Den Haag te informeren indien er wordt afgeweken van de afgesproken configuratie m.b.t. authenticatie en gegevensgebruik.

3.4. Exclusiviteit

De federatieve authenticatiegegevens dienen exclusief gebruikt te worden voor de daarvoor bedoelde applicatie. Uitwisseling van deze gegevens met andere applicaties (of instanties van deze applicaties) dient d.m.v. een nieuw verzoek aangemeld te worden bij Gemeente Den Haag. Uitzonderingen hierop dienen door de IT security afdeling van GDH goedgekeurd te worden.

3.5. Geheimhouding

Het delen van (persoons-)informatie met derden, verkregen via een federatieve koppeling is niet toegestaan.

3.6. Informatie en documentatie

De afnemer en/of leverancier dient informatie en/of documentatie op te leveren over de aan te sluiten federatieve applicatie in de vorm van een ontwerp of product documentatie.

3.7. Financiële verplichtingen

Indien er financiële verplichtingen bestaan bij het gebruik van de gefedereerde applicatie (per gebruiker, per dienst, per resource etc.), dan dient de afnemer en/of leverancier hier formeel goedkeuring voor te krijgen van de desbetreffende kostenplaatsverantwoordelijke(n).

3.8. Auditing

De afnemer en/of leverancier gaat akkoord met periodieke toetsing van de naleving van aansluitvoorwaarden door de gebruikersorganisatie en door een Gemeentelijke accountantsdienst.

3.9. Duur en beëindiging

Een federatieve koppeling is te allen tijde voor bepaalde tijd en wordt periodiek herzien (afhankelijk van het classificatie niveau van de applicatie). Zowel de Gemeente Den Haag als afnemer en/of leverancier dienen hier vóór verstrijken van deze periode op te acteren zodat er geen productie verstoringen plaats vinden.

3.10. OTAP

De Gemeente Den Haag biedt uitsluitend federatieve koppelingen in de fases Acceptatie en Productie. Ontwikkeling en Testen van applicaties dienen in de bij Microsoft (gratis te verkrijgen) development Azure AD tenants plaats te vinden. Hiermee worden fouten en verstoringen in het productielandschap tot een minimum beperkt.

3.11. Beveiliging en/of privacy incidenten

Indien er beveiligings en/of privacy incidenten plaats vinden op de desbetreffende aangesloten federatieve applicatie, dient de afnemer en/of leverancier zo snel mogelijk contact op te nemen met (de vertegenwoordiger van) Gemeente Den Haag. Hierbij is het verplicht om de privacy en security afdelingen van Gemeente Den Haag op de hoogte te stellen van de bevindingen. De Gemeente Den Haag behoudt zich het voorrecht om federatieve koppelingen per direct inactief te stellen o.b.v. het (security) incident proces.

3.12. Onderhoud

Indien er gepland onderhoud plaats vindt op een aangesloten federatieve applicatie dient dit ruim voortijdig gemeld te worden bij de verantwoordelijke(n) van Gemeente Den Haag zodat de Gemeente de gebruikersorganisatie tijdig hierop kan voorbereiden o.b.v. het change of release proces. Wijzigingen dienen geregistreerd te worden in de [wijzigingskalender](#).

3.13. Verstoringen

Indien er verstoringen plaats vinden op de aangesloten federatieve applicatie dient zo snel mogelijk gemeld te worden bij de verantwoordelijke(n) van Gemeente Den Haag zodat de Gemeente de gebruikersorganisatie tijdig hierop kan voorbereiden o.b.v. het incident management proces

n.b. de Gemeente Den Haag is afhankelijk van Microsoft voor de technische werking van Azure AD en kan geen invloed uitoefenen op eventuele (technische) verstoringen op het SaaS platform.

3.14. Troubleshooting

Zowel de afnemer en/of leverancier als de Gemeente Den Haag hebben een afhankelijkheid en daarbij verantwoordelijkheid jegens elkaar op gebied van het troubleshooten van de desbetreffende federatieve aansluiting. Beide partijen dienen elkaar waar mogelijk te ondersteunen om de dienstverlening richting de medewerkers van Gemeente Den Haag te herstellen.

3.15. Accordatie aansluitvoorwaarden

Afnemer en/of leverancier dienen kennis te hebben genomen en akkoord te gaan met de in dit document beschreven aansluitvoorwaarden.

4. Benodigde Gegevens

4.1.1. Algemene Informatie

De volgende algemene informatie is benodigd voor het aanvragen van een federatieve aansluiting en de afnemer en/of leverancier zal dit aanleveren

- TOPdesk wijzigingsnummer
- Datum aanvraag
- Omschrijving
- Applicatiennaam
- Applicatie instantie (indien van toepassing)
- Logo (indien van toepassing)
- Naam contactpersoon GDH
- E-mail adres contactpersoon GDH
- Telefoonnummer contactpersoon GDH
- Dienst / afdeling contactpersoon GDH
- Naam contactpersoon leverancier
- E-mail adres contactpersoon leverancier
- Telefoonnummer contactpersoon leverancier
- PO en/of verklaring kostenplaatsverantwoordelijke
- Applicatie ontwerp en/of leveranciersdocumentatie
- Omschrijving m.b.t. het gebruik van persoonsgegevens en de doeleinden hiervan
- Omschrijving m.b.t. de inrichting van applicatiebeveiliging
- Akkoord met aansluitvoorwaarden

4.1.2. OAuth 2.0 / OpenID Connect Federatie

Zie [bijlage 6.1 Formulier aanvraag Azure AD OAuth 2.0 / OpenID Connect Federatie](#)

4.1.3. SAML Federatie

Zie [bijlage 6.2 - Formulier aanvraag Azure AD SAML Federatie](#)

5. Privacy & Beveiliging

5.1. Gebruikers Authenticatie

5.1.1. Gebruikersnaam, Wachtwoord en Multi-Factor Authenticatie

Alle medewerkers van Gemeente Den Haag authenticeren met een door Gemeente Den Haag verstrekte gebruikersnaam en wachtwoord tegen Azure AD met de diverse gefedereerde applicaties. Dit gebeurt afhankelijk van de locatie en het type apparaat op basis van Single Sign On (SSO). Toegang tot applicaties is uitsluitend toegestaan met een persoonlijk toegekend GDH account. Test en/of service accounts zijn niet toegestaan.

Het bronsysteem van alle medewerkers identiteiten is het P&O systeem. Het IDM platform zorgt voor user provisioning richting de applicaties, beheer van de accounts en de governance (indien mogelijk). Active Directory en Azure Active Directory fungeren als account stores en worden gebruikt t.b.v. authenticatie en autorisatie.

Azure AD gast accounts (B2B) worden d.m.v. IDM provisioning toegevoegd aan Azure AD. Multi-factor authenticatie voor deze accounts is verplicht.

Azure Multi-factor authenticatie is te alle tijden verplicht m.u.v. vanaf de interne (bekabelde) Gemeente Den Haag locaties. Op GDH Wifi netwerken is multi-factor authenticatie verplicht.

De mogelijkheid bestaat om ook voor interne verbindingen Multi-factor authenticatie te vereisen indien gewenst. Dit kan per gefedereerde applicatie aangevraagd worden.

5.2. Gebruikersgegevens

5.2.1. SAML Assertions

Door middel van SAML Assertions (claims) kunnen additionele attributen worden meegestuurd naar de gefedereerde applicatie.

Hieronder een overzicht van de standaard SAML claims en waarden zoals deze beschikbaar zijn binnen Azure AD:

Beschikbare assertions:

- Authentication assertions met daarin NameID en Authentication Context
- Attribute assertion met diverse attributen (zie tabel)
- Entitlement assertion met rechten (zelden gebruikt)

Claim	Attribuut	Toegestaan?
Nameidentifier (Name ID)	User.userprincipalname	Ja
Emailaddress	User.mail	Ja
Givenname	User.givenname	Ja
Name	User.userprincipalname	Ja
Surname	User.surname	Ja

Additioneel kunnen custom attributen meegestuurd worden als optionele claims. Een overzicht hiervan is te vinden in bijlage 6.3 [Optionele SAML Claims](#).

Let op: Niet alle attributen bevatten per definitie een waarde!

In uitzonderlijke gevallen is het mogelijk om niet standaard claims als assertion mee te sturen. Dit zal per aanvraag beoordeeld moeten worden indien van toepassing.

5.2.2. OAuth 2.0 Gegevens Authorisatie & Permissies (Graph API)

Toegang tot gebruikersgegevens vindt plaats d.m.v. zogenaamde API permissies (scopes).

De volgende OAuth 2.0 permissies (scopes) mogen worden beschouwd als laag risico:

Permissie	Omschrijving	Toegestaan?
User.Read	sign in and read user profile	Ja
offline_access	maintain access to data that users have given it access to	Ja
openid	sign users in	Ja
profile	view user's basic profile	Ja
email	view user's email address	Ja

Toegang tot alle overige OAuth 2.0 permissies dienen per verzoek beoordeeld te worden op validiteit, privacy en beveiliging door de desbetreffende resource eigenaren.

Een overzicht van de beschikbare permissies o.b.v. de Microsoft Graph API is hier te vinden:

[Microsoft Graph permissions reference - Microsoft Graph | Microsoft Docs](#)

5.2.3. OAuth 2.0 Consent Framework

Alle Azure AD applicaties zijn afhankelijk van het Azure AD Consent Framework waarbij toestemming wordt gegeven om gebruik te mogen maken van specifieke gegevens of data (middels API's). Dit wordt bij Gemeente Den Haag gedaan door de tenant beheerder(s). User consent staat dus uitgeschakeld. Op deze manier worden alle API permissie verzoeken beoordeeld op validiteit, security en privacy aspecten.

Azure AD ondersteund twee type permissies namelijk:

- **Delegated permissions** worden gebruikt door apps met een aangemelde gebruiker. Voor deze apps geeft de beheerder toestemming voor de machtigingen die de app aanvraagt. De app wordt gedelegeerd met de machtigingen als de aangemelde gebruiker wanneer deze de resource (API) aanroept.
- **Application permissions** worden gebruikt door apps die worden uitgevoerd zonder een aangemelde gebruiker die aanwezig is, bijvoorbeeld apps die worden uitgevoerd als achtergrondservices of daemons.

De Gemeente Den Haag hanteert een “**Delegated permissions-tenzij**” beleid zodat het principe van least-privilege toegepast kan worden. In uitzonderlijke gevallen kunnen application permissions worden toegekend na beoordeling en goedkeuring van het IT Security team.

5.3. Applicatie Authenticatie

Applicaties gebruiken de verschillende authenticatie flows om gebruikers aan te melden en tokens te krijgen om beveiligde Azure AD API's aan te roepen.

Authentication Flow	Toegestaan?
OpenID Connect	Toegestaan
Implicit grant	Niet toegestaan
Authorization code	Toegestaan
On-Behalf-Of	Toegestaan
Client Credentials	Toegestaan
Device Code	Toegestaan
Resource Owner Password Credential (ROPC)	Niet toegestaan
SAML Bearer Assertion	Toegestaan

** Als alternatief voor de "Implicit Grant Flow" kan er gebruik gemaakt worden van de "Authorization Code Flow" i.c.m. PKCE. Meer informatie: <https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-third-party-cookies-spas>

*** In geval van het gebruik van de "Client Credentials Grant Flow" dient er te allen tijde gebruik gemaakt te worden van certificaten t.b.v. authenticatie.

5.4. Best Practices

Branding:

- Geef een betekenisvolle naam en logo op voor de toepassing. Deze informatie wordt weergegeven op de consentprompt van de toepassing. Zorg ervoor dat uw naam en logo representatief zijn voor uw bedrijf/product, zodat gebruikers weloverwogen beslissingen kunnen nemen. Zorg ervoor dat u geen handelsmerken schendt.

Privacy:

- Geef links naar de servicevoorwaarden en privacyverklaring van uw app

OAuth 2.0 authenticatie:

- Gebruik de OAuth2 Implicit grant toekenningsstroom niet in, tenzij dit expliciet vereist is.
- Gebruik geen resource owner password credential flow (ROPC), die de wachtwoorden van gebruikers rechtstreeks gebruikt.
- Gebruik bij voorkeur certificaten (geen client secrets).
- Programmeer niet rechtstreeks tegen protocollen zoals OAuth 2.0 en Open ID. Maak in plaats daarvan gebruik van de Microsoft Authentication Library (MSAL). De MSAL-bibliotheken verpakken beveiligingsprotocollen veilig in een gebruiksvriendelijke bibliotheek en u krijgt ingebouwde ondersteuning voor scenario's voor voorwaardelijke toegang, apparaatbrede eenmalige aanmelding (SSO) en ingebouwde ondersteuning voor token caching. Zie de lijst met door Microsoft ondersteunde [clientbibliotheken](#) voor meer informatie.

Redirect URIs:

- Behoud het eigendom van alle redirect-URI's en houd de DNS-records up-to-date.
- Gebruik geen wildcards (*) in uw URI's.
- Zorg er voor web-apps dat alle URI's veilig en encrypted zijn (HTTPS)
- Gebruik voor openbare clients platformspecifieke redirect-URI's, indien van toepassing (voornamelijk voor iOS en Android).
- Als uw app wordt gebruikt vanaf een geïsoleerde webagent, kan er gebruik gemaakt worden van <https://login.microsoftonline.com/common/oauth2/nativeclient>.

API Permissies

- Als de gegevens die uw app nodig heeft beschikbaar zijn via Microsoft Graph, vraag dan permissies voor deze gegevens aan met behulp van Microsoft Graph in plaats van de afzonderlijke API.
- Vraag alleen de minimale set API permissies aan die een eindgebruiker van een applicatie, service of systeem nodig heeft om de vereiste taken uit te voeren.
- Begrijp volledig welke permissies vereist zijn voor de API calls die de applicatie moet doen.
- Verwijder eventuele dubbele machtigingensets in gevallen waarin de app API calls doet met overlappende machtigingen.
- Audit de permissies die worden toegekend aan gebruikers of applicaties.
- Voer regelmatig een beoordeling uit om ervoor te zorgen dat alle geautoriseerde machtigingen nog steeds relevant zijn.

6. Bijlagen

6.1. Formulier aanvraag OAuth 2.0 / OpenID Connect Federatie



IAM Federatieve
Authenticatie - Aanvraag

6.2. Formulier aanvraag SAML Federatie



IAM Federatieve
Authenticatie - Aanvraag

6.3. Optionele SAML Claims

Attribuut	Toegestaan?
User.assignedroles	Ja
User.city	Ja
User.companyname	Ja
User.country	Ja
User.department	Ja
User.displayname	Ja
User.dnsdomainname	Ja
User.employeeid	Ja
User.extensionattribute1	Nee
User.extensionattribute2	Nee
User.extensionattribute3	Nee
User.extensionattribute4	Nee
User.extensionattribute5	Nee
User.extensionattribute6	Nee
User.extensionattribute7	Nee
User.extensionattribute8	Nee
User.extensionattribute9	Nee
User.extensionattribute10	Nee

User.extensionattribute11	Nee
User.extensionattribute12	Nee
User.extensionattribute13	Nee
User.extensionattribute14	Nee
User.extensionattribute15	Nee
User.facsimiletelephonenumber	Ja
User.givenname	Ja
User.jobtitle	Ja
User.localuserprincipalname	Ja
User.mail	Ja
User.mailnickname	Ja
User.netbiosname	Ja
User.objectid	Ja
User.onpremisesdistinguishedname	Ja
User.onpremisessecurityidentifier	Ja
User.onpremisesaccountname	Ja
User.onpremisesuserprincipalname	Ja
User.othermail	Ja
User.physicaldeliveryofficename	Ja
User.postalcode	Ja
User.preferredlanguage	Ja
User.primaryauthoritativeemail	Ja
User.secondaryauthoritativeemail	Ja
User.state	Ja
User.streetaddress	Ja
User.surname	Ja
User.telephonenumber	Ja
User.userprincipalname	Ja
User.approles	Ja