

Bijlage F – Aansluitvoorwaarden en eisen Architectuur/Security v. 6-8-2025

Aansluitvoorwaarden – Richtlijnen voor zover van toepassing

- Het systeem biedt ondersteuning voor Single Sign-On (SSO) en sluit daarbij aan op Entra ID;
- Alle federatieve SSO-protocollen voor NWO-applicaties worden ondersteund:
 - SAML 2.0 – gebruikt voor authenticatie en autorisatie;
 - OAuth 2.0 – wordt gebruikt voor autorisatie;
 - OIDC (OpenID Connect) – wordt gebruikt voor authenticatie.
- Niet-federatieve SSO wordt zoveel als mogelijk vermeden, waarbij Integrated Windows Authenticatie of Header Based SSO niet worden ondersteund;
- 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.

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-mailadres voor toegang tot de applicatie bij de SaaS leverancier niet mogelijk is;
- 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 accountinformatie wordt gebruik gemaakt van SCIM 2.0 of een standaard koppeling die binnen het IAM-platform van NWO beschikbaar is;
- Ondersteuning van Role Based Access (RBAC) wordt ondersteund via
 - 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.

Aansluitvoorwaarden – richtlijnen Microsoft Graph API voor zover van toepassing

Voor toegang tot gegevens in de Microsoft 365 tenant geldt:

- Delegated en application permissions zijn mogelijk waarbij delegated permissions de voorkeur hebben;
- Toegang is alleen mogelijk voor gebruikeraccounts uit de Entra ID directory van NWO.

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.

Aansluitvoorwaarden – algemene richtlijn minimale uitwisseling voor zover van toepassing

De uitwisseling van gegevens tussen de Identity Provider en de Service Provider voor SSO, provisioning en toegang via de Graph API worden geminimaliseerd en beperkt tot de vereiste gegevens voor een correcte werking van de applicatie.

Bij het uitwisselen van gegevens anders dan basisgegevens (zoals een e-mailadres of naam) vindt de beoordeling en - het geven van toestemming tot het uitwisselen van deze persoonsgegevens – plaats door de privacy officer van NWO.

Eisen

- Het CMS wordt als SaaS-dienst aangeboden;
- De SaaS-dienst moet geïmplementeerd zijn op een (server)infrastructuur welke zich bevindt op Europees grondgebied en valt onder Europese wetgeving (GDPR in geval van persoonsgegevens);
- De (server)infrastructuur van de Opdrachtnemer en/of eventuele derde partij waarop de SaaS-dienst is geïmplementeerd moet gehuisvest zijn in een fysieke omgeving (computerruimte) die aantoonbaar adequaat, in lijn met de NEN-ISO-27001-code of equivalent, is ingericht en beveiligd;
- De Opdrachtnemer en/of eventuele derde partij die de SaaS-dienst levert voldoet in de gehele keten aan de NEN-ISO-27001- code voor Informatiebeveiliging of equivalent;
- De Opdrachtnemer stelt NWO, zonder voorbehoud, in staat te voldoen aan alle van toepassing zijnde Nederlandse wet- en regelgeving. Hierbij staat de Opdrachtnemer garant voor alle derde partijen die door de Opdrachtnemer zijn gecontracteerd voor het uitvoeren van werkzaamheden ten behoeve van NWO;
- De SaaS-dienst wordt minimaal 1 keer per jaar onderworpen aan een uitgebreide beveiligingstest die wordt uitgevoerd door een externe partij. De resultaten van de beveiligingstests zijn door NWO in te zien;
- NWO heeft een auditrecht bij de Opdrachtnemer;
- Opdrachtnemer verschaft inzicht aan Opdrachtgever in de aard en omvang van de uitgevoerde beveiligingstest(en) alsmede de resultaten ervan;
- Opdrachtnemer hanteert strikte procedures die ondervangen zijn conform NEN ISO 27001 of equivalent en werkinstructies voor beheer, onderhoud en ontwikkeling;
- Opdrachtnemer geeft aan welke andere integratiemogelijkheden er zijn met Microsoft'365, anders dan eerdergenoemde;
- Single Sign On (SSO) moet binnen het NWO-kantoor via laptops van Opdrachtgever mogelijk zijn;
- De SaaS-dienst dient gebruik te maken van minimaal versies van TLS die industry standard zijn, wat op dit moment betekent versie 1.2 en bij voorkeur TLS versie 1.3;
- De applicatie bevindt zich achter een firewall in een eigen segment voor NWO;
- De infrastructuur dient gebruik te maken van een Intrusion Detection- (IDS) en/of een Intrusion Prevention-systeem (IPS);
- De infrastructuur dient gebruik te maken van programmatuur die controleert of voldaan wordt aan een overeengekomen baseline t.a.v. softwareversies, instellingen, actieve services etc., of de gebruikte softwareversies nog actueel zijn en of de juiste en actuele beveiligingspatches actief zijn;
- Op alle servers binnen de dienstverlening is antivirussoftware actief;
- De SaaS-dienst dient minimaal de laatste en voorlaatste versie van de Microsoft Edge browser, Chrome, Firefox en Safari te ondersteunen;
- Adaptief onderhoud wordt uitgevoerd om te blijven voldoen aan geldende wet- en regelgeving.