

Authenticatie en provisioning standaarden

De Gemeente maakt gebruik van moderne authenticatie op basis van Azure Federatie. Onderstaande tabel bevat de door Utrecht ondersteunde protocollen en toepassing daarvan. Er is een IAM loket beschikbaar welke de federatieve koppeling samen met de leverancier realiseert. (IAM@Utrecht.nl)

Authenticatie middelen (1,2)

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloud-applicaties
1	OpenID Connect Oauthv2	Voorkeur	Azure Federatie (3)	Ja	Ja
2	SAML v2.0	Alternatief	Azure Federatie	Ja	Ja
3	Kerberos	Alleen intern	Active Directory	Ja	Nee
4	LDAPS	Niet toegestaan		n.v.t.	n.v.t.

Identity Provisioning^s

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/ Cloudapplicaties
1	SCIMv2 (Omada Identity Cloud)	Voorkeur	SCIM endpoint	Ja	Ja
2	SCIMv2 (Entra ID)	Alternatief	SCIM endpoint	Ja	Ja
3	Maatwerk REST API	Alleen bij uitzondering		Ja	Ja
4	Maatwerk XML SOAP	Alleen bij uitzondering		Ja	Ja
5	Eigen implementatie	Alleen bij uitzondering		Ja	Ja
6	Handmatig	Afhankelijk van BIV classificatie toegestaan		Ja	Ja
7	Microsoft LDAPS	Niet toegestaan		n.v.t.	n.v.t.
8	Bestand: XML, JSON (beveiligd)	Niet toegestaan		n.v.t.	n.v.t.

Toelichting;

1. Nummering van protocollen staat in volgorde van voorkeur
2. De mate en inrichting van identity provisioning is mede afhankelijk BIV-classificatie en het gebruik van rollen.
3. Bij Container platform met Keycloak als broker
4. 5,6 – Alleen bij uitzondering; na afstemming met product owner en architectuur