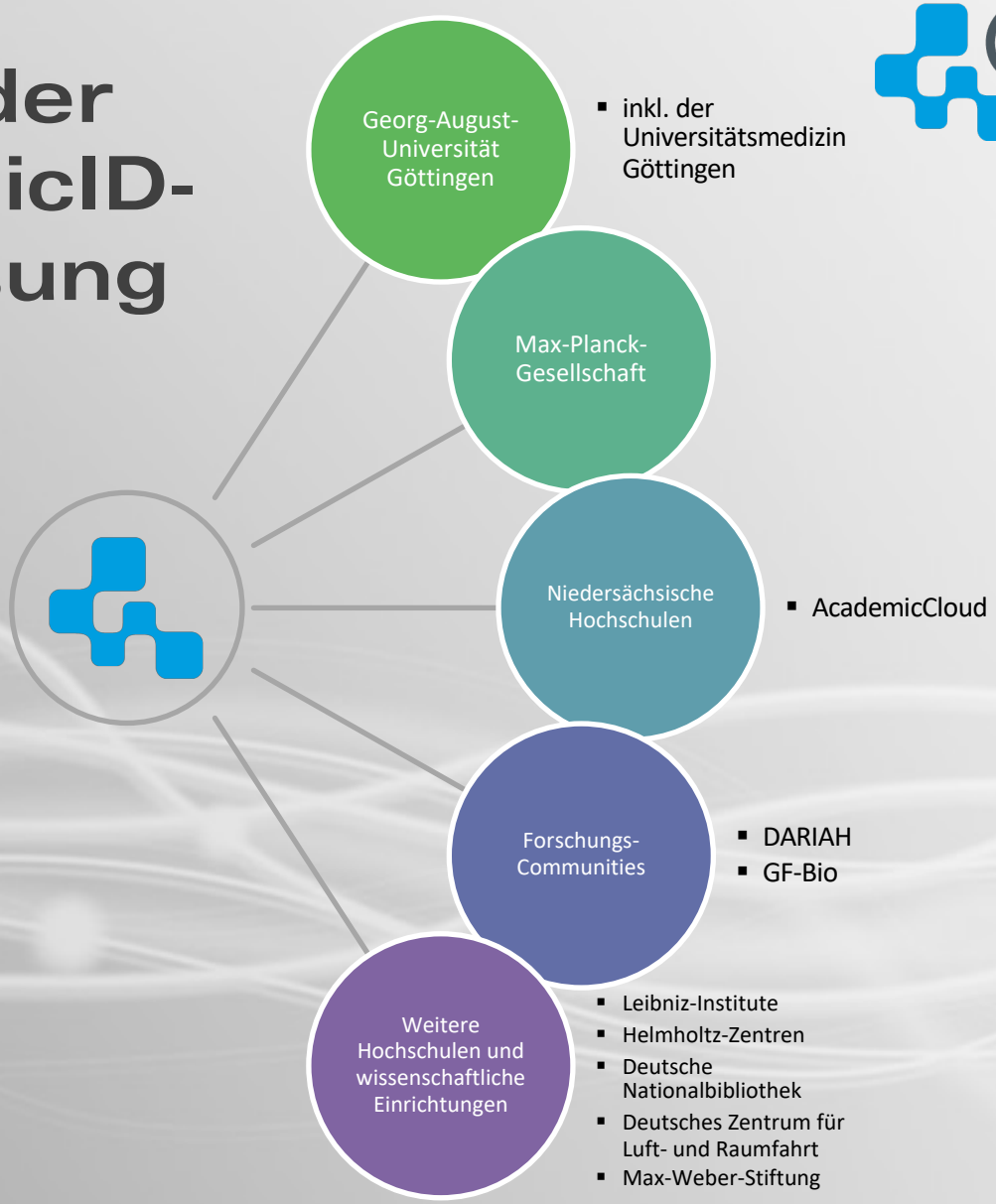
AcademicID Identity- und Access-Management

NFDI-AAI-Kernteam, 17. März 2022

Nutzer der AcademicID-IAM-Lösung

Auswahl

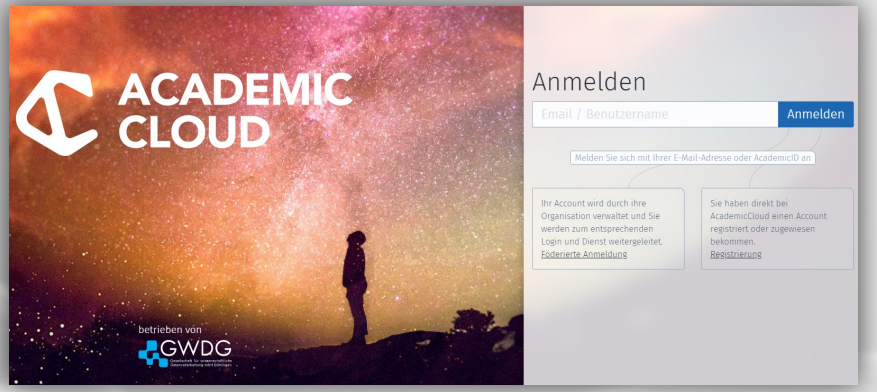


Funktionsübersicht

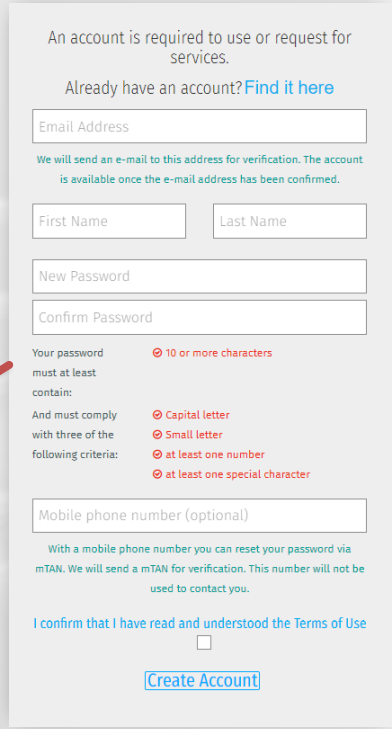
- Single-Sign-On (SSO) – primär SAML, ADFS und OIDC
- Accountverwaltung
  - Selfservice für Standard-Funktionen (Passwort ändern, MFA-Token registrieren, SSH-Key hinterlegen, X.509-Zertifikate, ...)
  - Admin- und Support-Portal
- Selbstregistrierung
  - Integration von „Homeless“-Nutzern
- AcademicID
  - Zentraler Identifier für angeschlossene Systeme
  - Account-Linking mit anderen IDs möglich (z.B. ORCID)
- Organisations-Management
  - Organisationen, Communities, Gruppen, Projekte, ...
  - Einladungsfunktion, Teilnahme-Codes
  - Verwaltung von Dienste-Zugriffen, Quota, ...

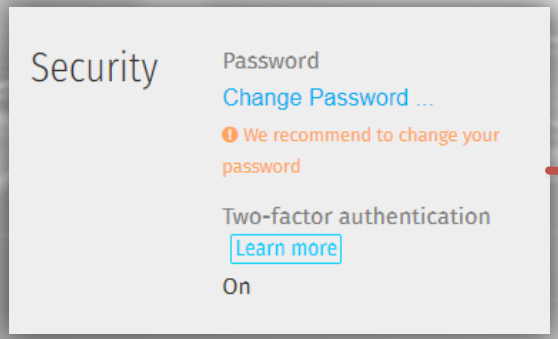
Customizing einer Community – Beispiel Academic Cloud

Zentraler Login
(z.B. sso.academiccloud.de)



Selbstregistrierung



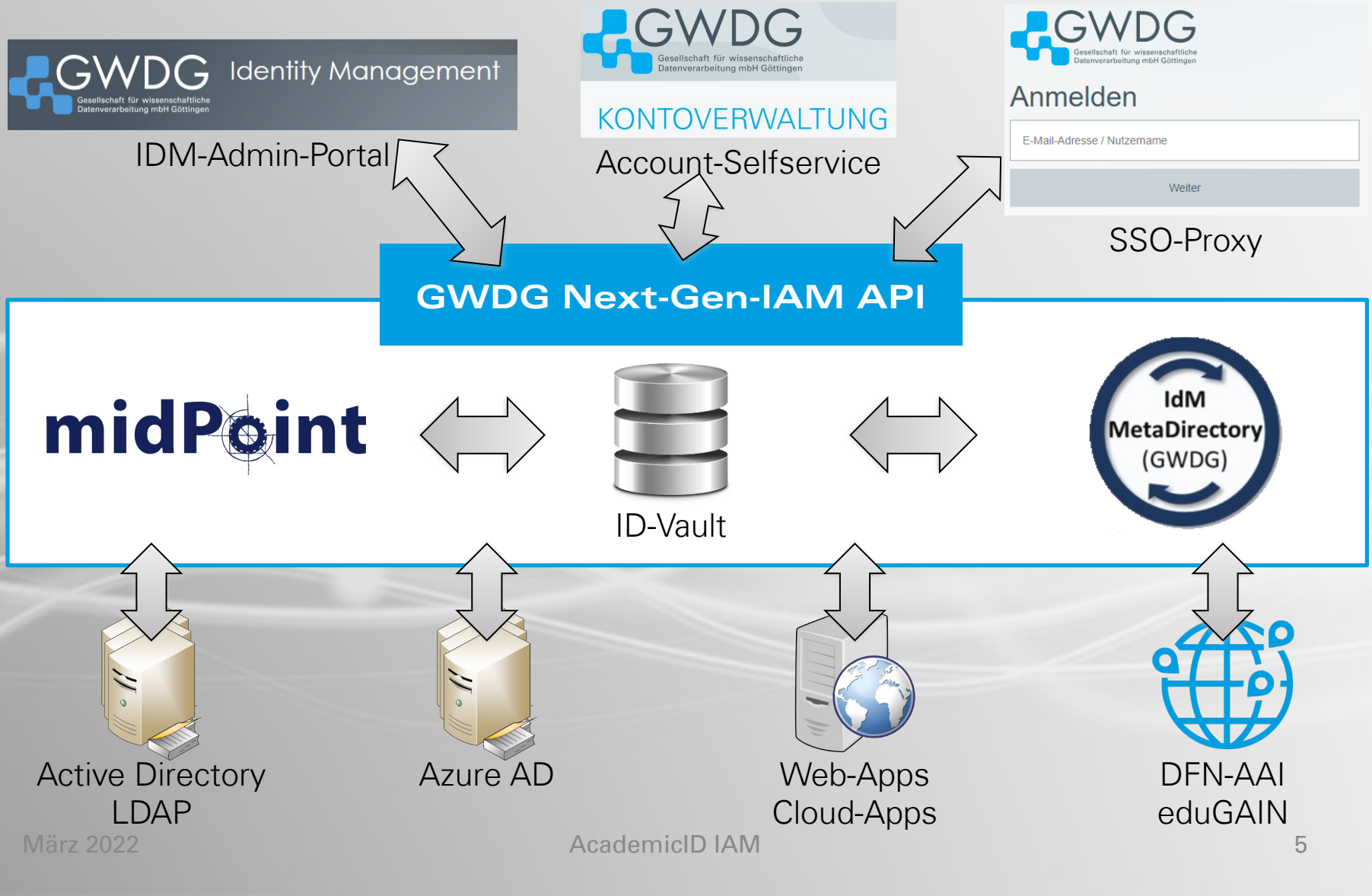


Accountverwaltung
(z.B. accounts.academiccloud.de)

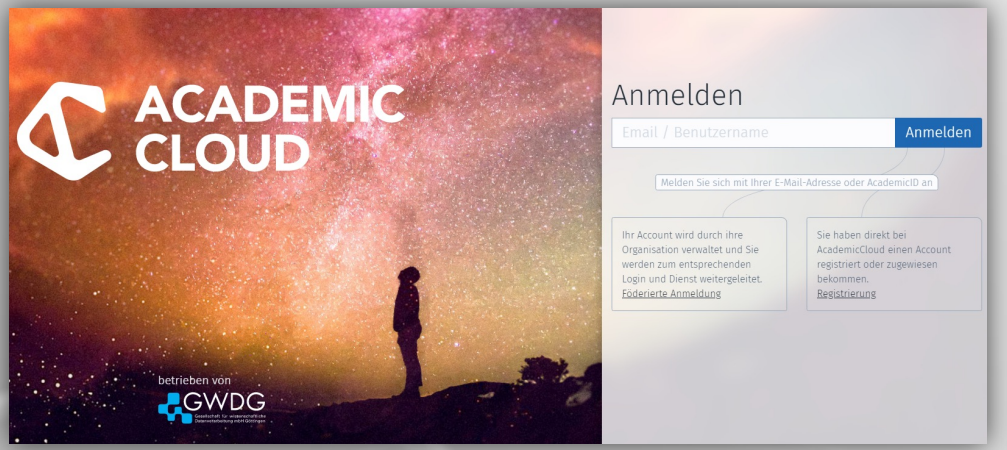
AcademicID

Das AcademicID-IAM

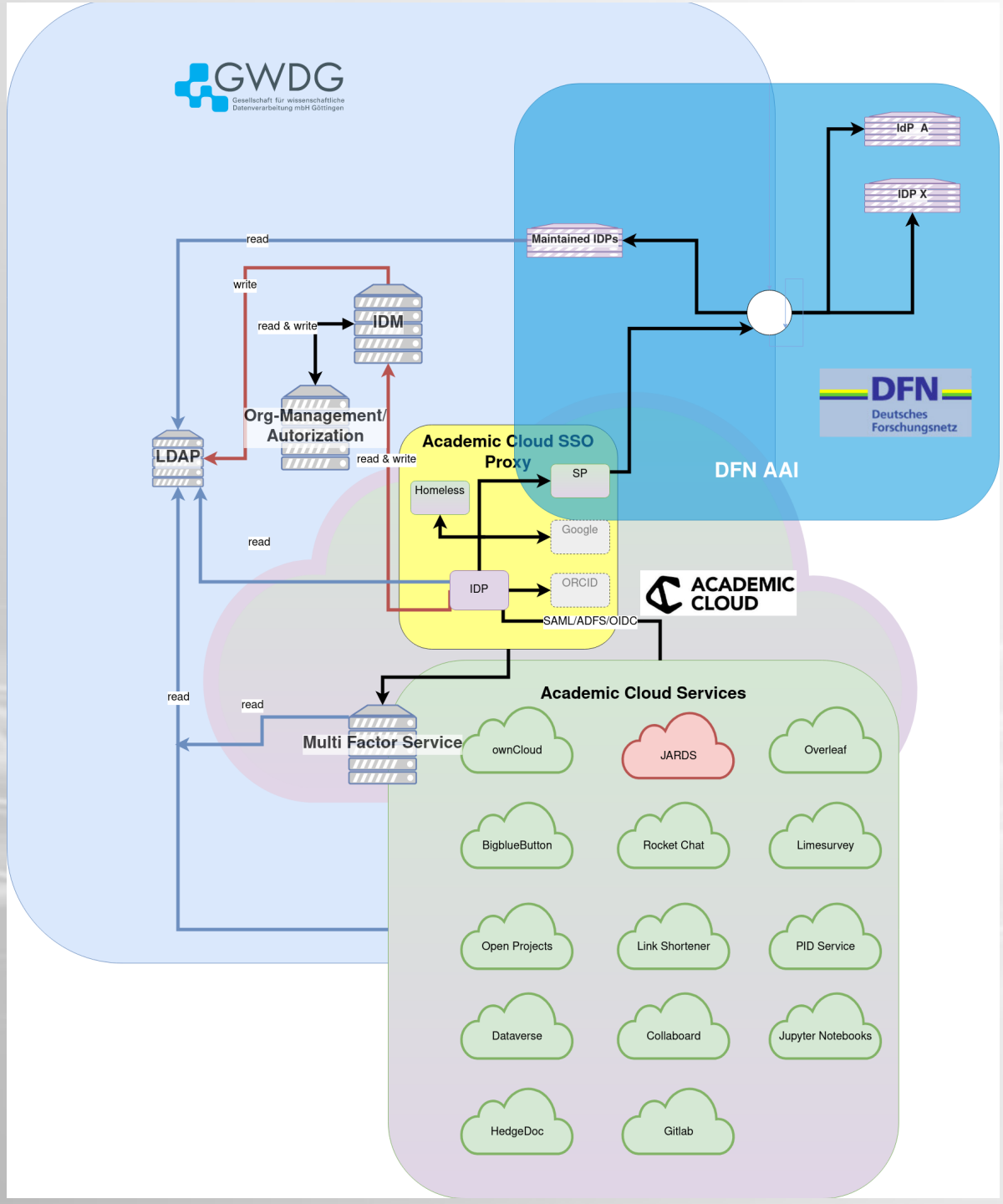
Gesamtarchitektur



Single-Sign-On (SSO) – Beispiele Customizing



IAM-Architektur



März 2022

Verwendete Produkte

- Kommerziell:
  - IDM: NetIQ Identity Manager
  - ADFS: Microsoft ADFS
- Open Source
  - IDM: midPoint
  - SAML IdP/SP: SimpleSAMLphp
  - OIDC: Keycloak
  - SAML-/OIDC-/ADFS-Proxy: SimpleSAMLphp
  - MFA: privacyIDEA

Referenzen

- Academic Cloud: (https://academiccloud.de/)
- IdM der Max-Planck-Gesellschaft (MPG)
- DFG Projekt GFBio (https://www.gfbio.org/)
- DARIAH-DE (https://de.dariah.eu/)
- MWW Virtueller Forschungsraum (https://vfr.mww-forschung.de/)
- PIM-Projekt
- EU Projekt Up to University

MAX-PLANCK-GESELLSCHAFT

DARIAH AAI AUTHENTICATION AUTHORISATION INFRASTRUCTURE

gfbio GERMAN FEDERATION FOR BIOLOGICAL DATA