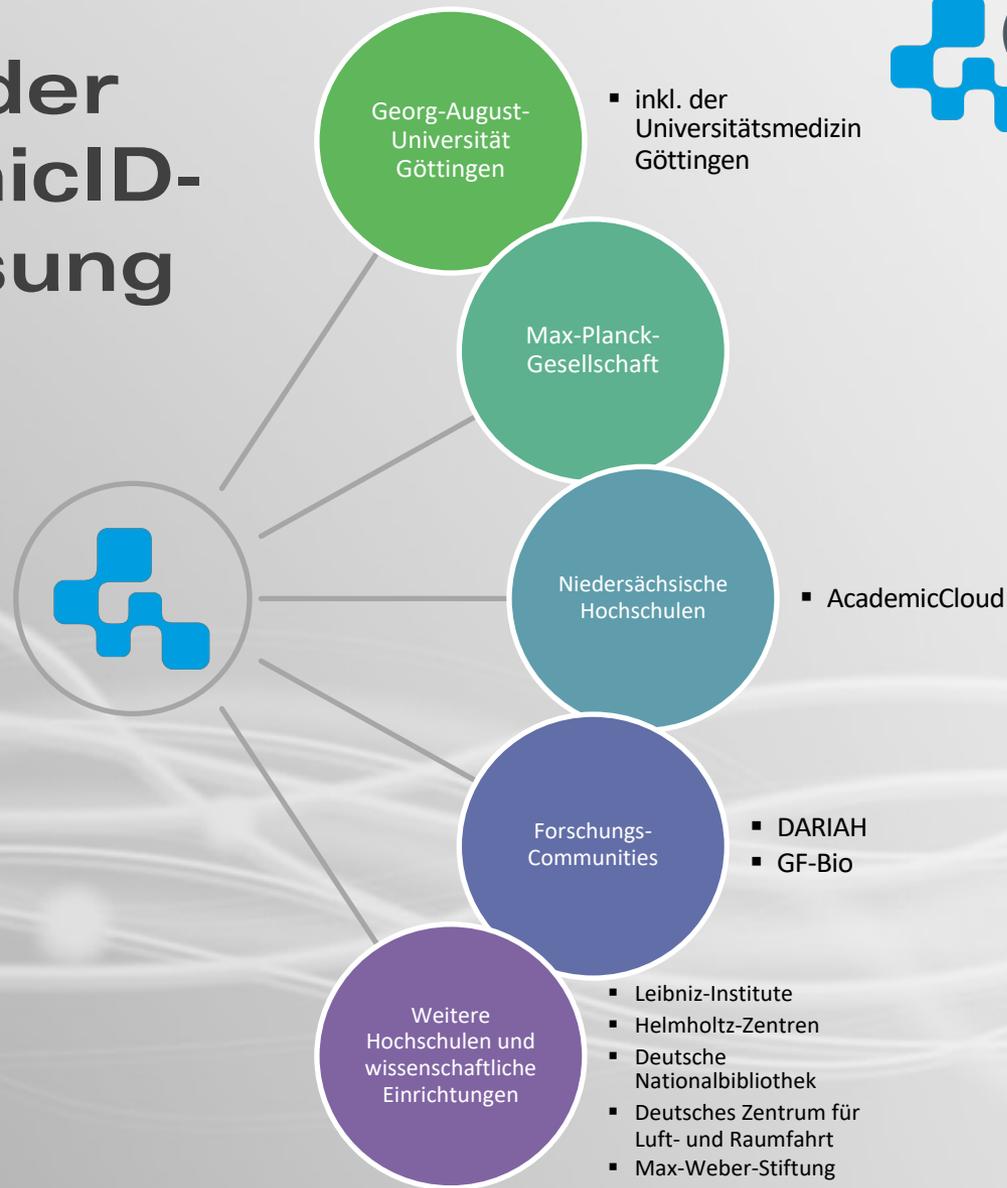


# **AcademicID Identity- und Access-Management**

NFDI-AAI-Kernteam, 17. März 2022

# Nutzer der AcademicID-IAM-Lösung

## Auswahl



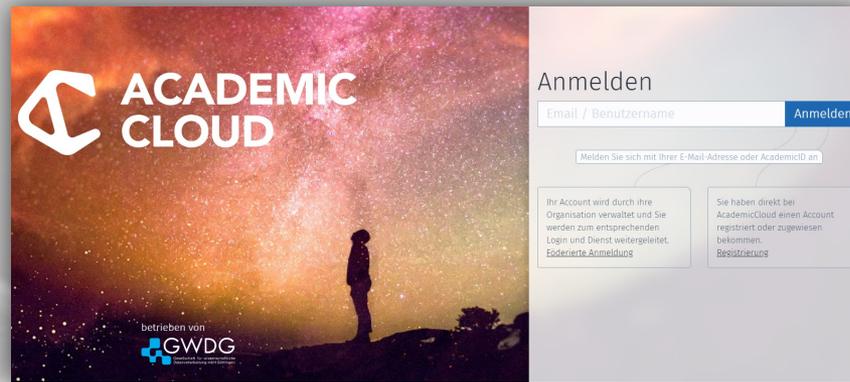
# Funktionsübersicht

- 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

An account is required to use or request for services.

Already have an account? [Find it here](#)

Email Address

We will send an e-mail to this address for verification. The account is available once the e-mail address has been confirmed.

First Name  Last Name

New Password

Confirm Password

Your password must at least contain:

- 10 or more characters
- Capital letter
- Small letter
- at least one number
- at least one special character

Mobile phone number (optional)

With a mobile phone number you can reset your password via mTAN. We will send a mTAN for verification. This number will not be used to contact you.

I confirm that I have read and understood the [Terms of Use](#)

[Create Account](#)

Security

Password

[Change Password ...](#)

**!** We recommend to change your password

Two-factor authentication

[Learn more](#)

On

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

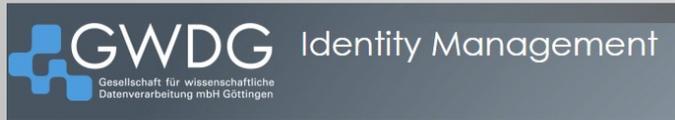


AcademicID

AcademicID IAM

# Das AcademicID-IAM

Gesamtarchitektur



IDM-Admin-Portal



KONTOVERWALTUNG

Account-Selfservice



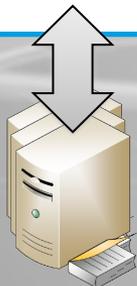
SSO-Proxy

**GWGD Next-Gen-IAM API**

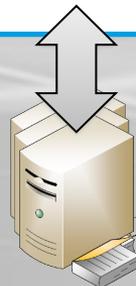
**midPoint**



ID-Vault



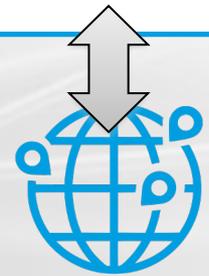
Active Directory  
LDAP



Azure AD



Web-Apps  
Cloud-Apps



DFN-AAI  
eduGAIN

# Single-Sign-On (SSO) – Beispiele Customizing



**ACADEMIC CLOUD**

betrieben von **GWGD**

## Anmelden

Email / Benutzername  **Anmelden**

Melden Sie sich mit Ihrer E-Mail-Adresse oder AcademicID an

Ihr Account wird durch ihre Organisation verwaltet und Sie werden zum entsprechenden Login und Dienst weitergeleitet.  
**Föderierte Anmeldung**

Sie haben direkt bei AcademicCloud einen Account registriert oder zugewiesen bekommen.  
**Registrierung**

**MAX-PLANCK-GESELLSCHAFT**

## Anmeldung

Wählen Sie Ihre Einrichtung aus

**Weiter**

Deutsch ▾

Der persönliche Login auf MAX/CHB/MySite/Teamräume ist erforderlich, damit die personalisierten und Standortbezogenen Inhalte genau für Sie ausgegeben werden können. So können Sie direkt auf Ihre individuellen Lesazeichen, Teamräume und sozialen Funktionen zugreifen. Der Single-Sign-On-Prozess muss nur einmal pro Tag durchgeführt werden und speichert danach automatisch Ihre Anmeldeinformationen für den nächsten Besuch der oben erwähnten Seiten.

**DARIAH AAI** AUTHENTICATION AUTHORITY INFRASTRUCTURE

## Organisation auswählen

**DARIAH >**

Um auf den Dienst DARIAH AAI zuzugreifen, wählen oder suchen Sie bitte die Organisation, der Sie angehören.

**Organisation**

Geben Sie den Namen der Organisation ein, der Sie angehören...

Auswahl für die laufende Webbrowser Sitzung speichern.

Auswahl permanent speichern und diesen Schritt von jetzt an überspringen.

**AUSWÄHLEN**

**MÄRBACH WEIMAR WOLFENBÜTTEL FORSCHUNGS VERBUND**

## Anmelden

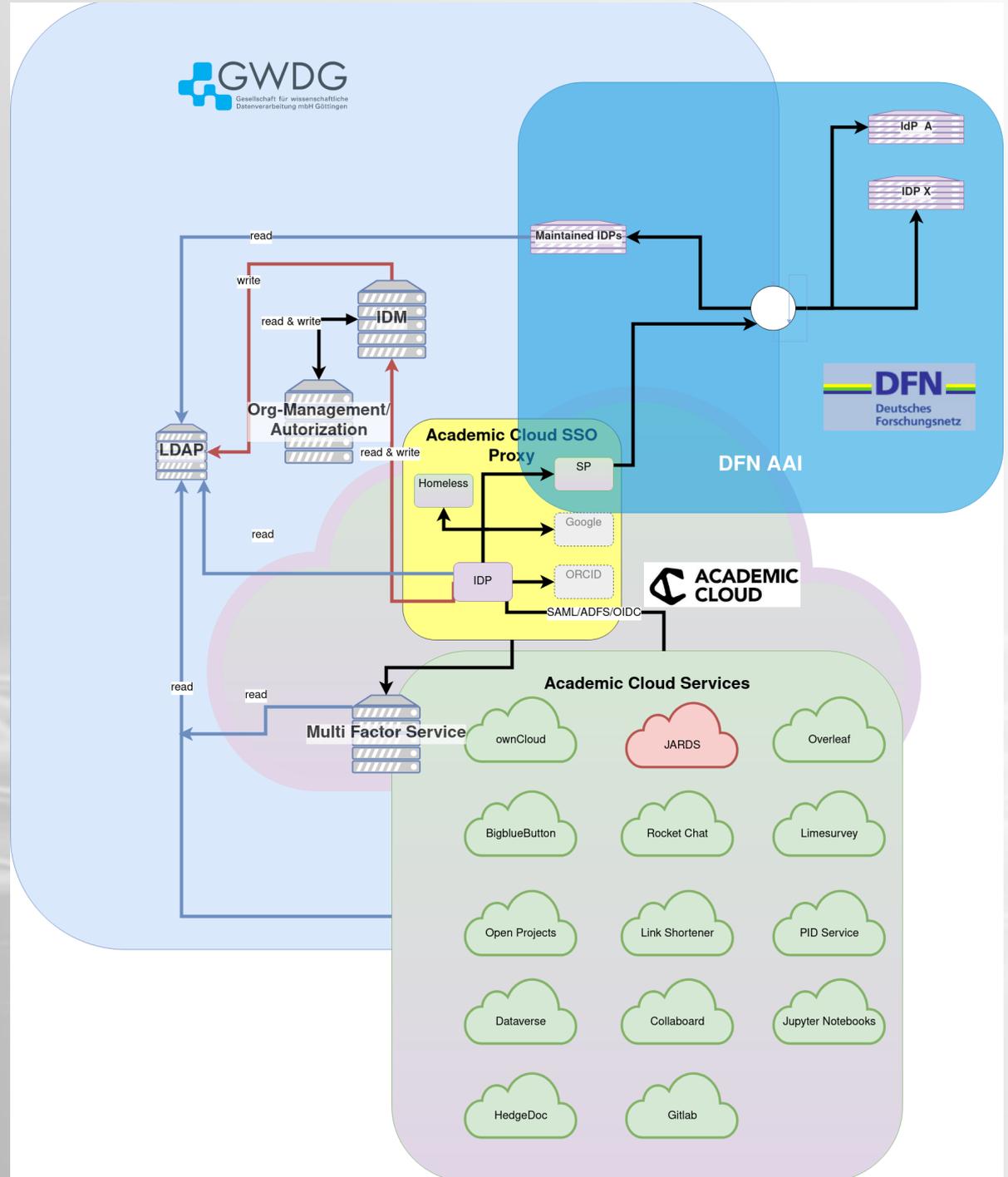
Email / Benutzername  **Anmelden**

Melden Sie sich mit Ihrer E-Mail-Adresse oder AcademicID an

Ihr Account wird durch ihre Organisation verwaltet und Sie werden zum entsprechenden Login und Dienst weitergeleitet.  
**Föderierte Anmeldung**

Sie haben direkt bei MWW-VFR einen Account registriert oder zugewiesen bekommen.  
**Registrierung**

# IAM- Architektur



# 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



März 2022

