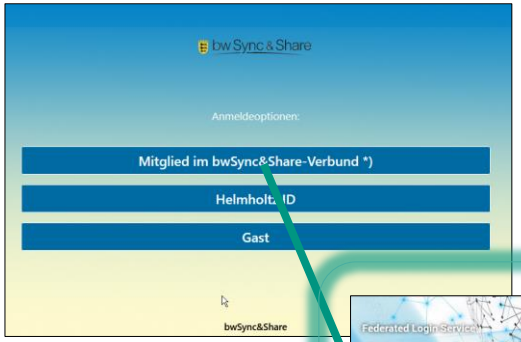
Karlsruher Institut für Technologie

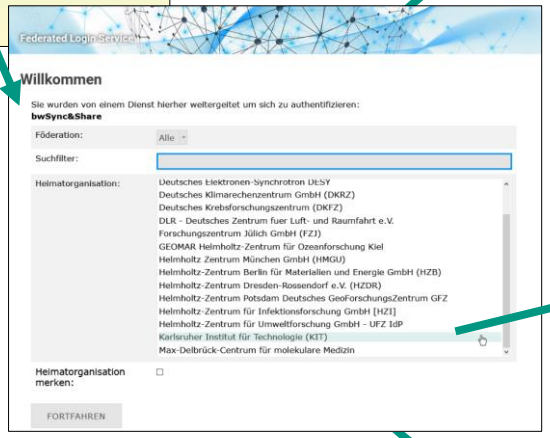
RegApp – Community AAI

Michael Simon, Ulrich Weiß
Karlsruher Institut für Technologie

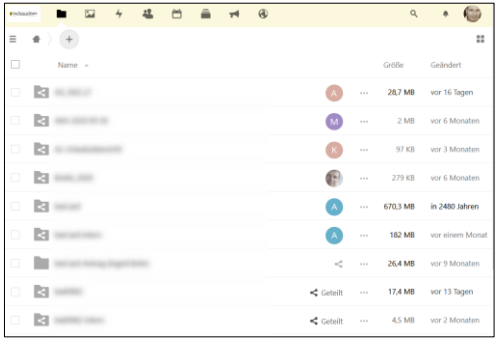
Dienst-Login mit Heimataccount



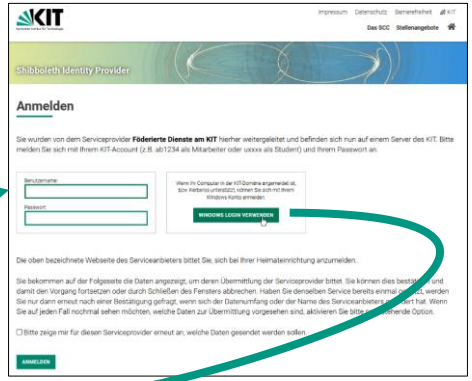
Service



RegApp AAI-SW

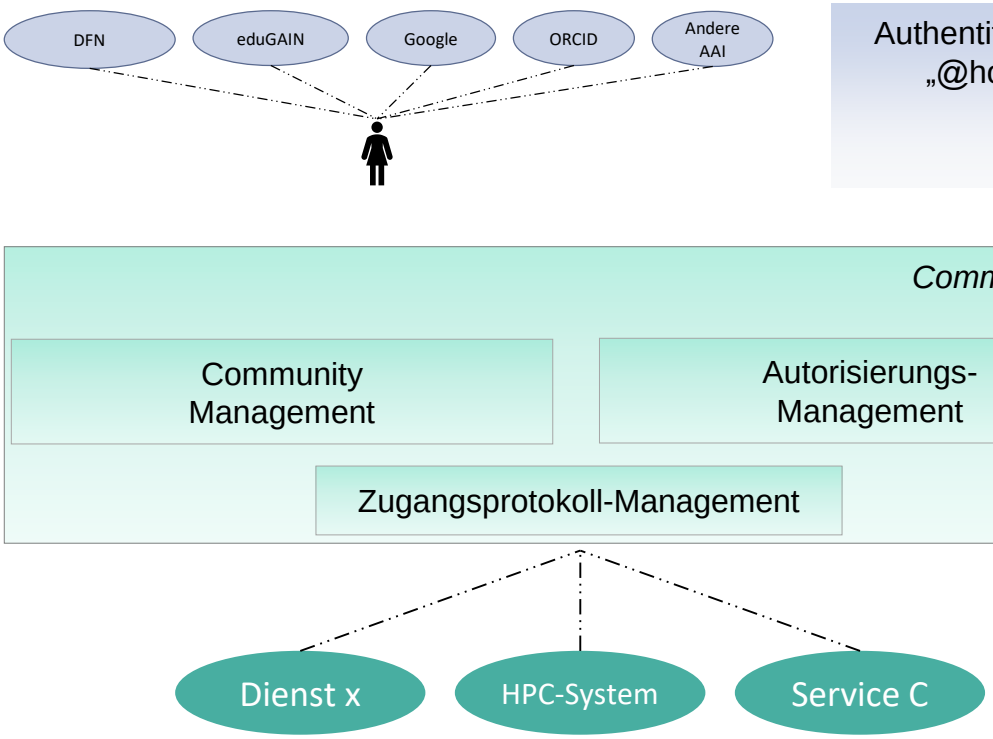


Service

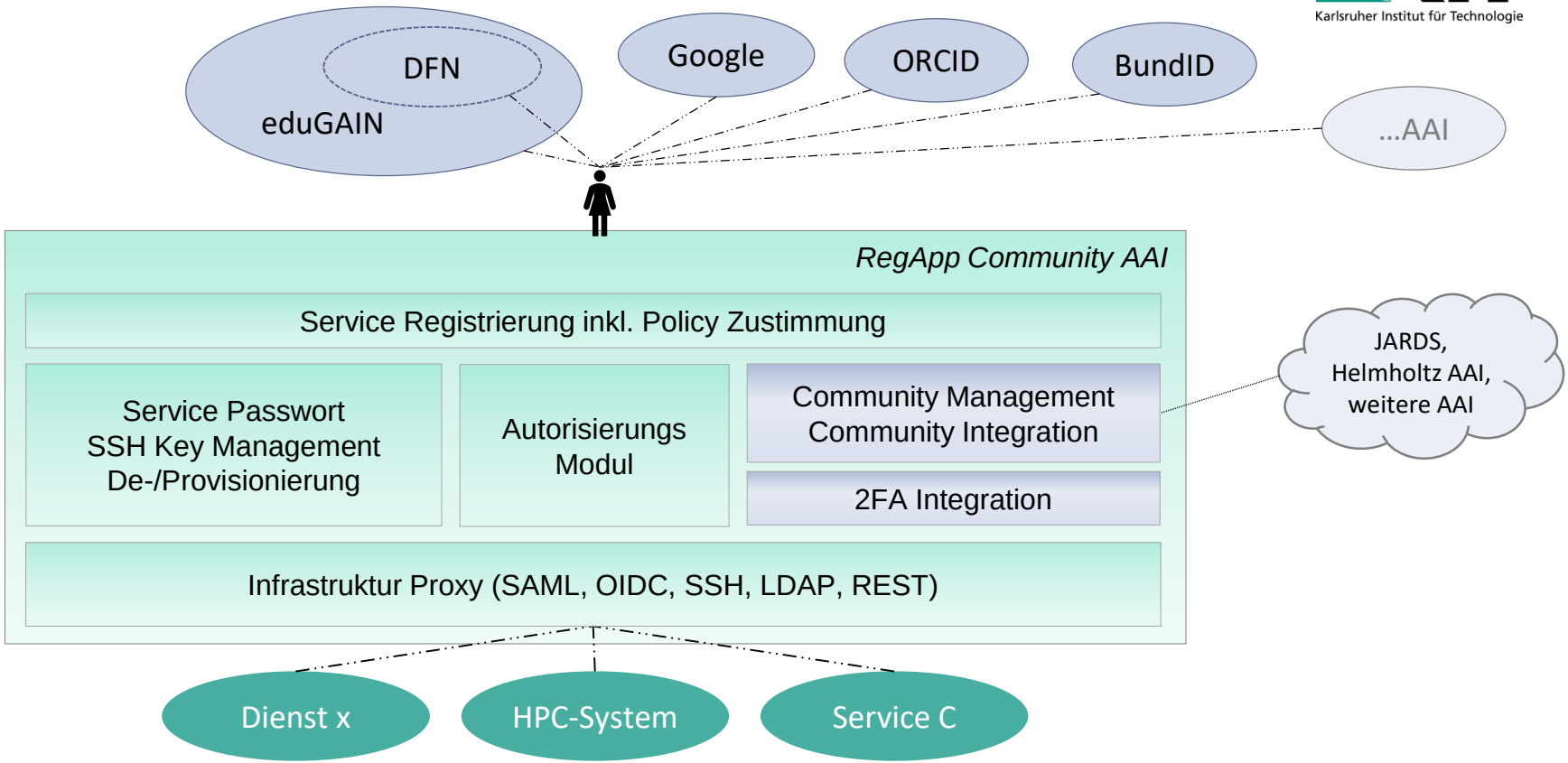


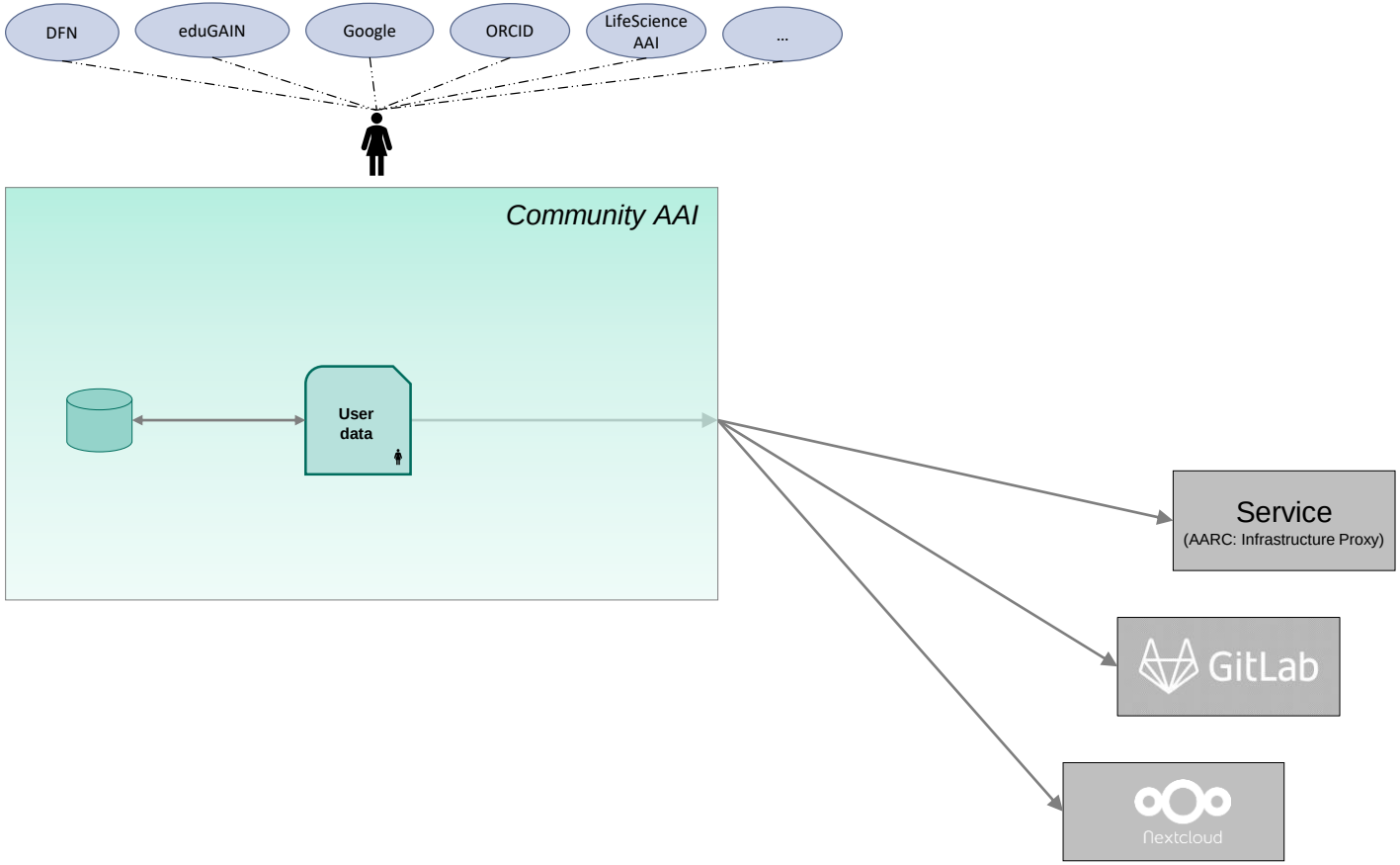
Heimat IdP

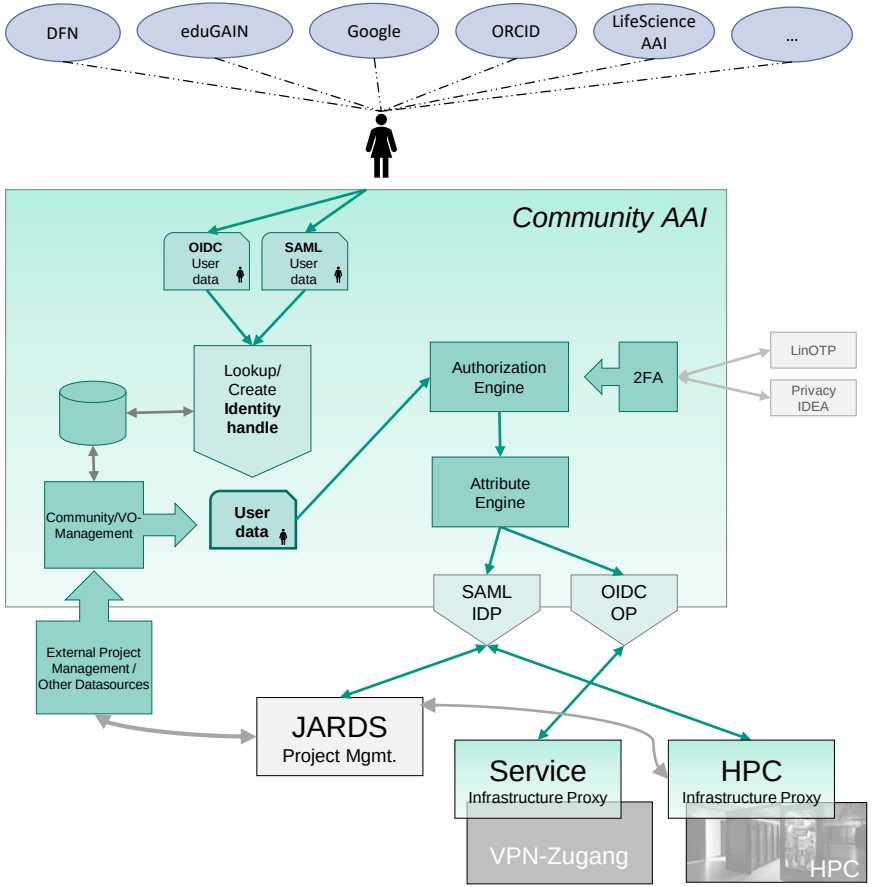
Community Authentifizierungs- und Autorisierungs-Infrastruktur (CAAI)

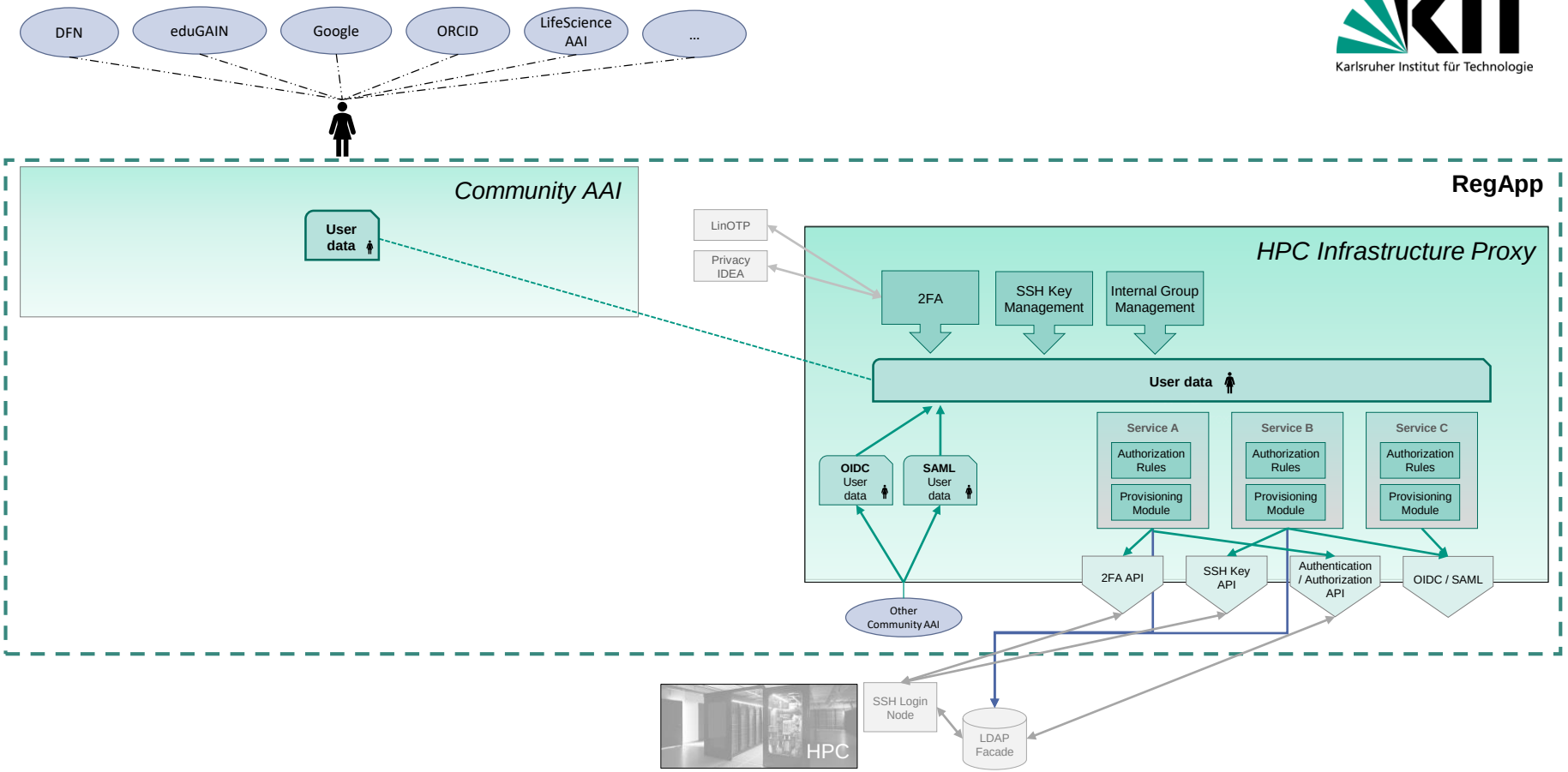


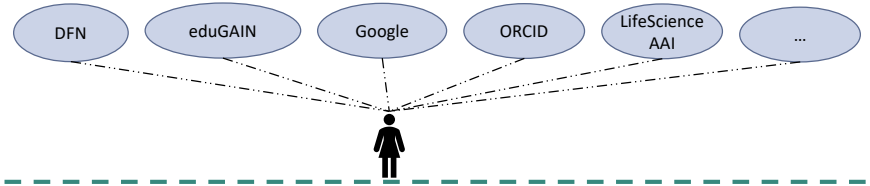
RegApp CAAI


DFN
eduGAIN
Google
ORCID
BundID
...AAI
RegApp Community AAI
Service Registrierung inkl. Policy Zustimmung
Service Passwort
SSH Key Management
De-/Provisionierung
Autorisierungs
Modul
Community Management
Community Integration
2FA Integration
Infrastruktur Proxy (SAML, OIDC, SSH, LDAP, REST)
JARDS,
Helmholtz AAI,
weitere AAI
Dienst x
HPC-System
Service C


DFN
eduGAIN
Google
ORCID
LifeScience AAI
...
Community AAI
User data
Service
(AARC: Infrastructure Proxy)
GitLab
Nextcloud


DFN
eduGAIN
Google
ORCID
LifeScience AAI
...
Community AAI
OIDC User data
SAML User data
Lookup/ Create Identity handle
Authorization Engine
2FA
LinOTP
Privacy IDEA
Attribute Engine
Community/VO-Management
User data
SAML IDP
OIDC OP
External Project Management / Other Datasources
JARDS
Project Mgmt.
Service
Infrastructure Proxy
HPC
Infrastructure Proxy
VPN-Zugang
HPC


DFN
eduGAIN
Google
ORCID
LifeScience AAI
...
Community AAI
User data
RegApp
LinOTP
Privacy IDEA
HPC Infrastructure Proxy
2FA
SSH Key Management
Internal Group Management
User data
Service A
Authorization Rules
Provisioning Module
Service B
Authorization Rules
Provisioning Module
Service C
Authorization Rules
Provisioning Module
OIDC User data
SAML User data
2FA API
SSH Key API
Authentication / Authorization API
OIDC / SAML
Other Community AAI
HPC
SSH Login Node
LDAP Facade



RegApp

Community AAI

Multi-Protokoll Proxy

IdP

OP

SAML

OIDC

Service

Client

Service Registrierung inkl. Policy Zustimmung

Service Passwort SSH Key Management De-/Provi-sionierung

Autori-sierungs Modul

Community Management Community Integration

2FA Integration

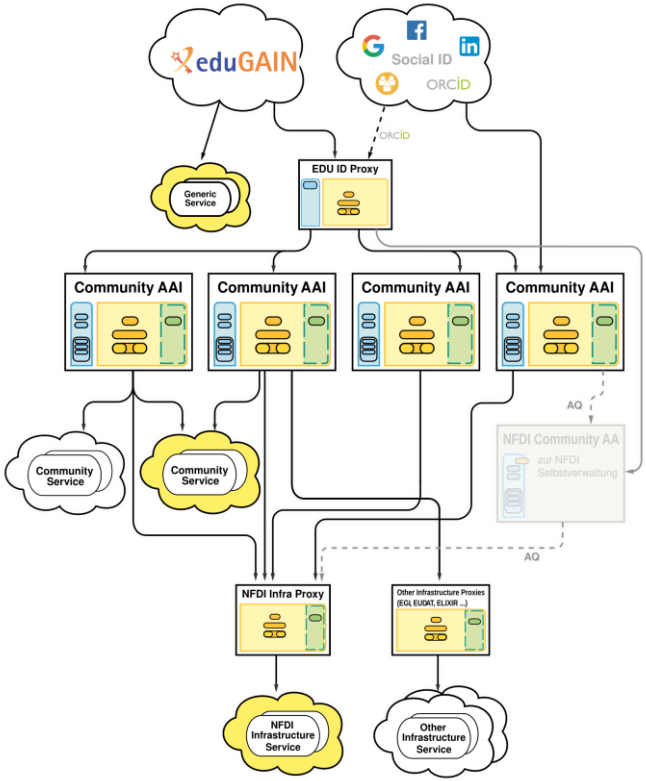
Infrastructure Proxy

Umfassende Benutzer-Provisionierung und Deprovisionierung:

Aktuelle Module

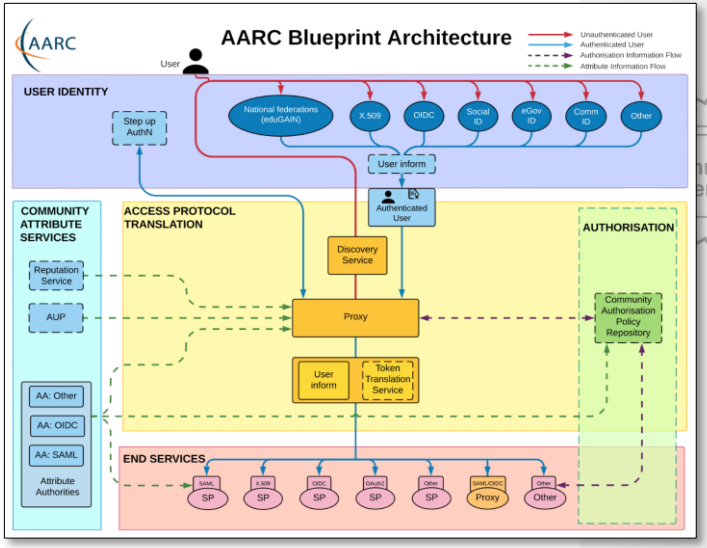
- LDAP (Attribute mit Vorlagen oder skriptgesteuert)
- Samba
- OpenStack
- NextCloud
- Powerfolder
- Gitlab
- REST

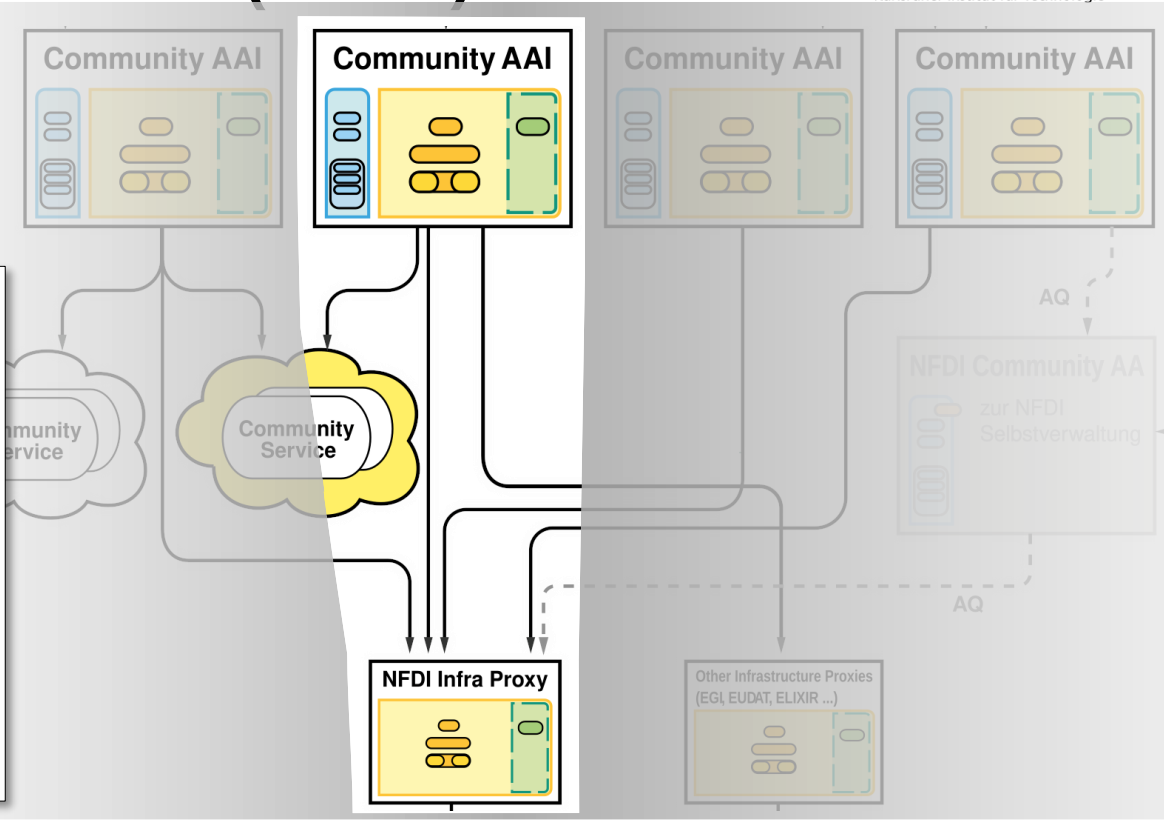
AARC Blueprint Architecture



Authentication and Authorisation for Research and Collaboration
https://aarc-project.eu/

AARC Blueprint Architecture (4NFDI)



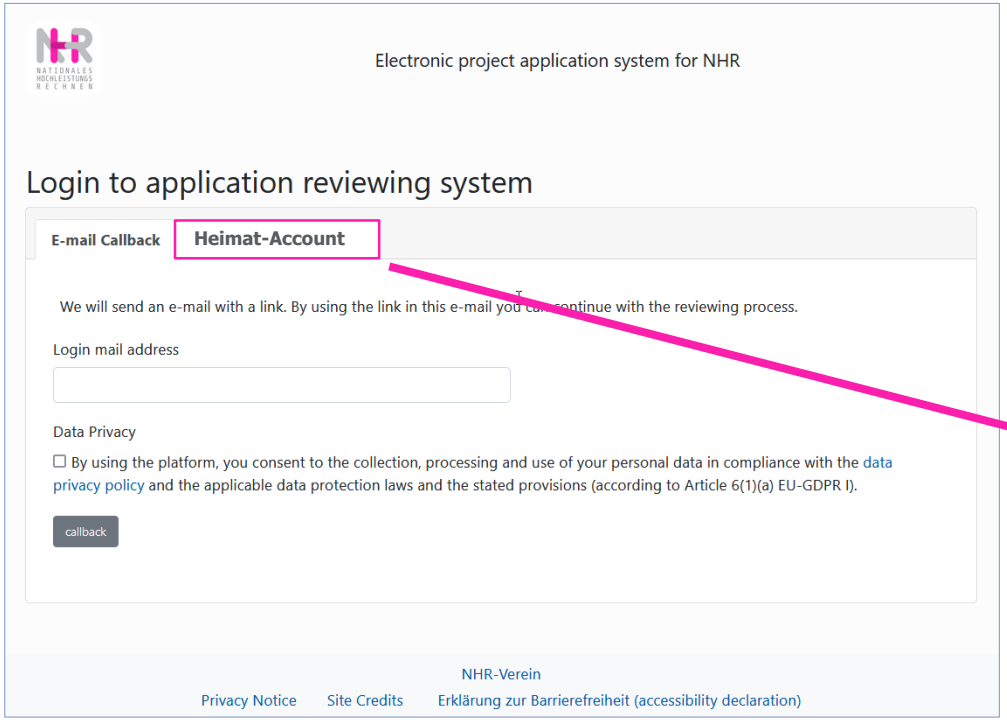


RegApp Funktionalitäten

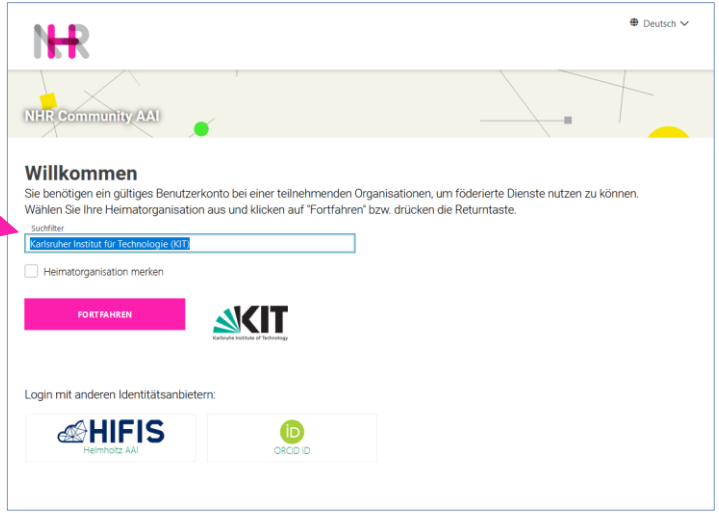
CAAI für Single Sign-On Umgebungen

- Transparente Anbindung von SAML-Föderationen
- SSO Protokoll-Proxy OIDC ↔ SAML
- Provisionierung und Deprovisionierung von Benutzeridentitäten
- Endnutzerportal zur Dienstregistrierung
- Hinterlegen/Verwalten/Provisionierung von SSH-Schlüsseln
- Infrastruktur-Proxy für LDAP-Dienste
- Multifaktor-Authentifizierung für Web- und Non-Web-Dienste
- Frei programmierbare Autorisierungsregeln und Attribut Handling/Freigabe
- **Delegierbares Community-/Projektmanagement**
- **Account-Linking**

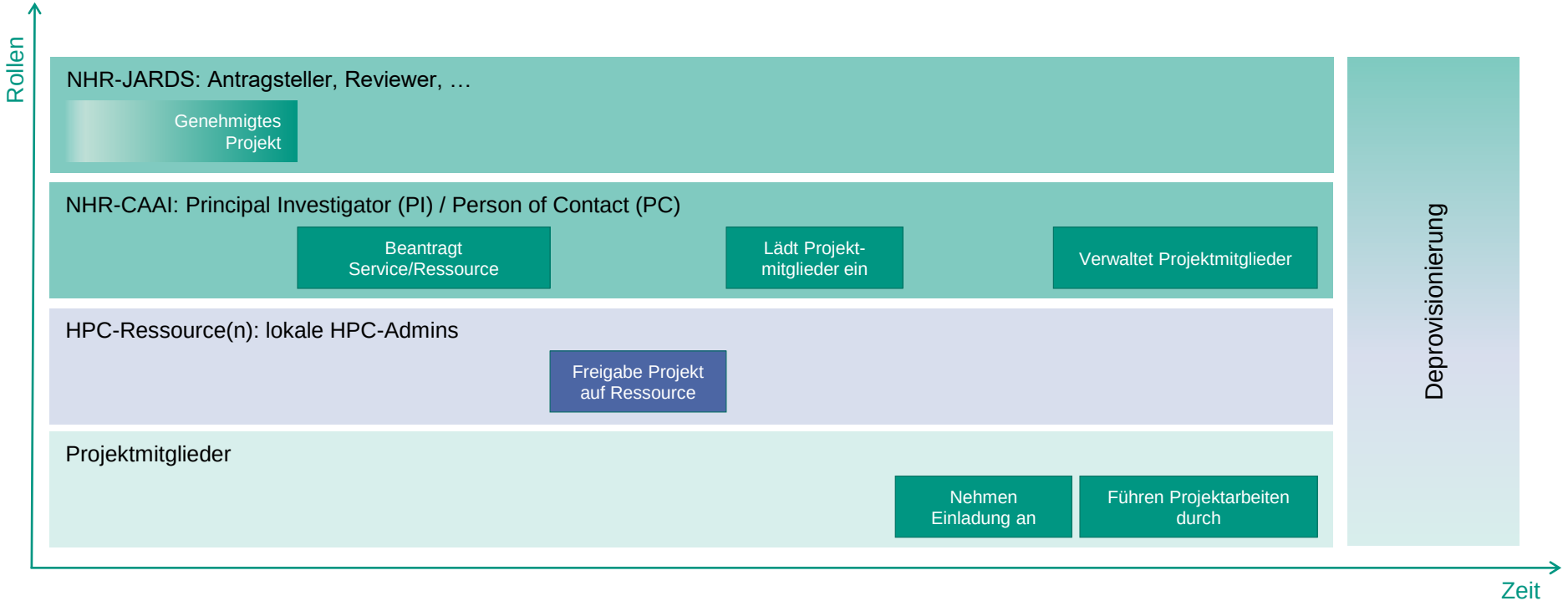
Einsatz Community Management (NHR)



Projektmanagment-/Lifecycling-Tool
Für Antragstellende, Reviewer, Projektverwaltende



Autorisierung via Community Management



Community Management: Projekte

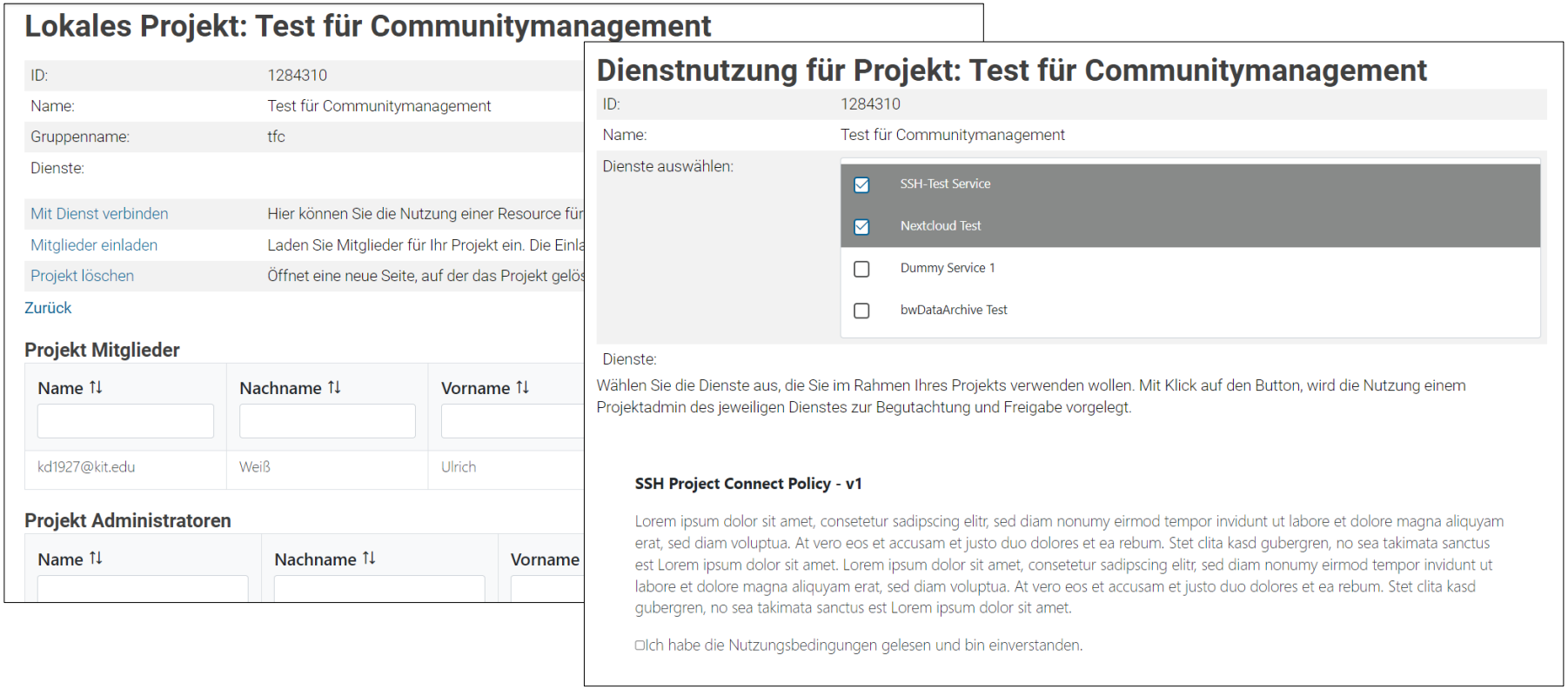
Neues Projekt anlegen

Legen Sie hier ein neues Projekt an. Im folgenden können Sie Mitglieder zum Projekt einladen und die Nutzung innerhalb von Diensten beantragen.
Name: Der volle Name des Projekts (z.B. Forschungs-Projekt Alpha)
Kurzname: Das Akronym/Kürzel des Projekts (z.B. fpa)
Gruppenname: Vorschlag für einen Gruppennamen bei den genutzten Diensten. Dieser Wert kann von dem Dienst überschrieben werden. Z.B. fpa

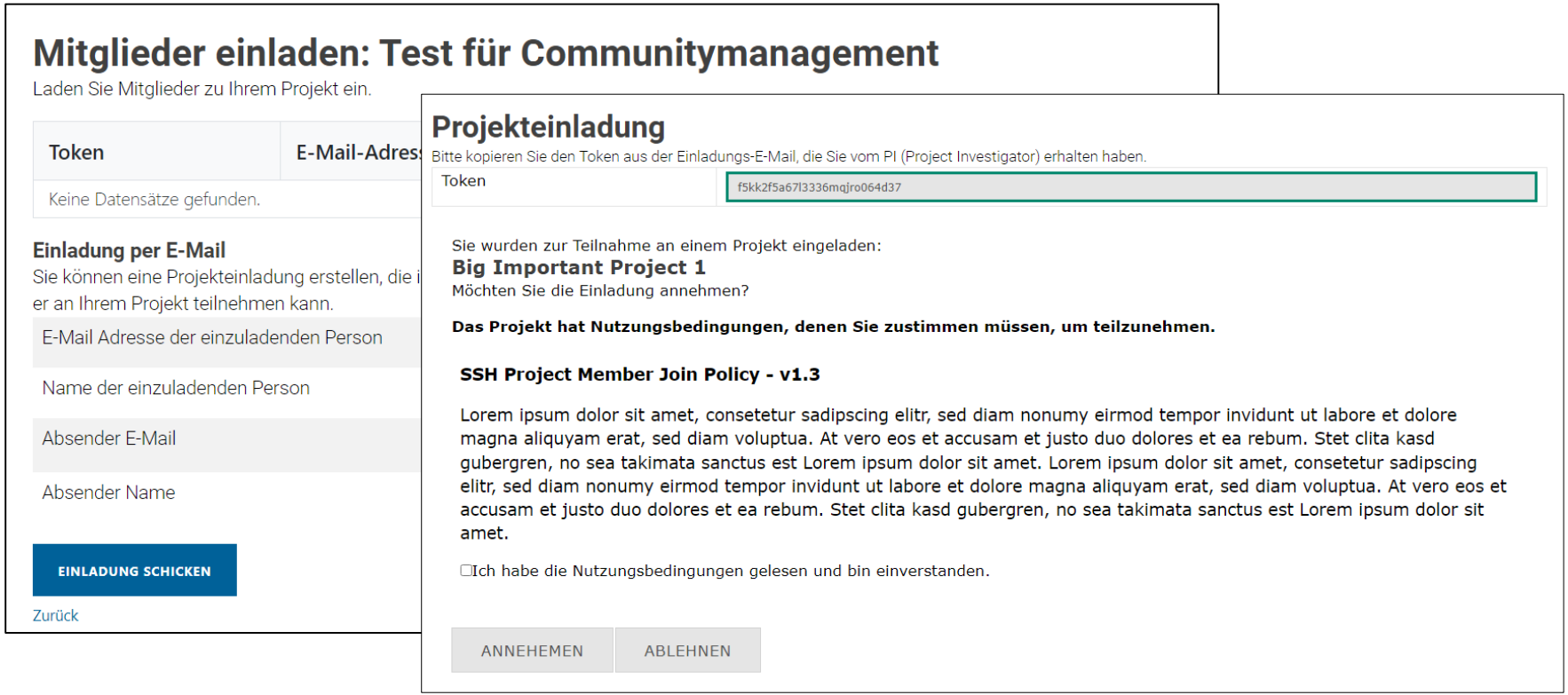
Name *	Test für Communitymanagement
Kurzname *	tfc
Gruppenname *	tfc
Kurze Beschreibung	RegApp-Communitymanagement
Beschreibung des Projekts	Verschachtelte Communities mit delegierten Verantwortlichen als Basis für Dienstzugänge.
Selbst Mitglied werden	on

ABBRECHEN SPEICHERN

Community Management: Service Registration



Community Management: User Management

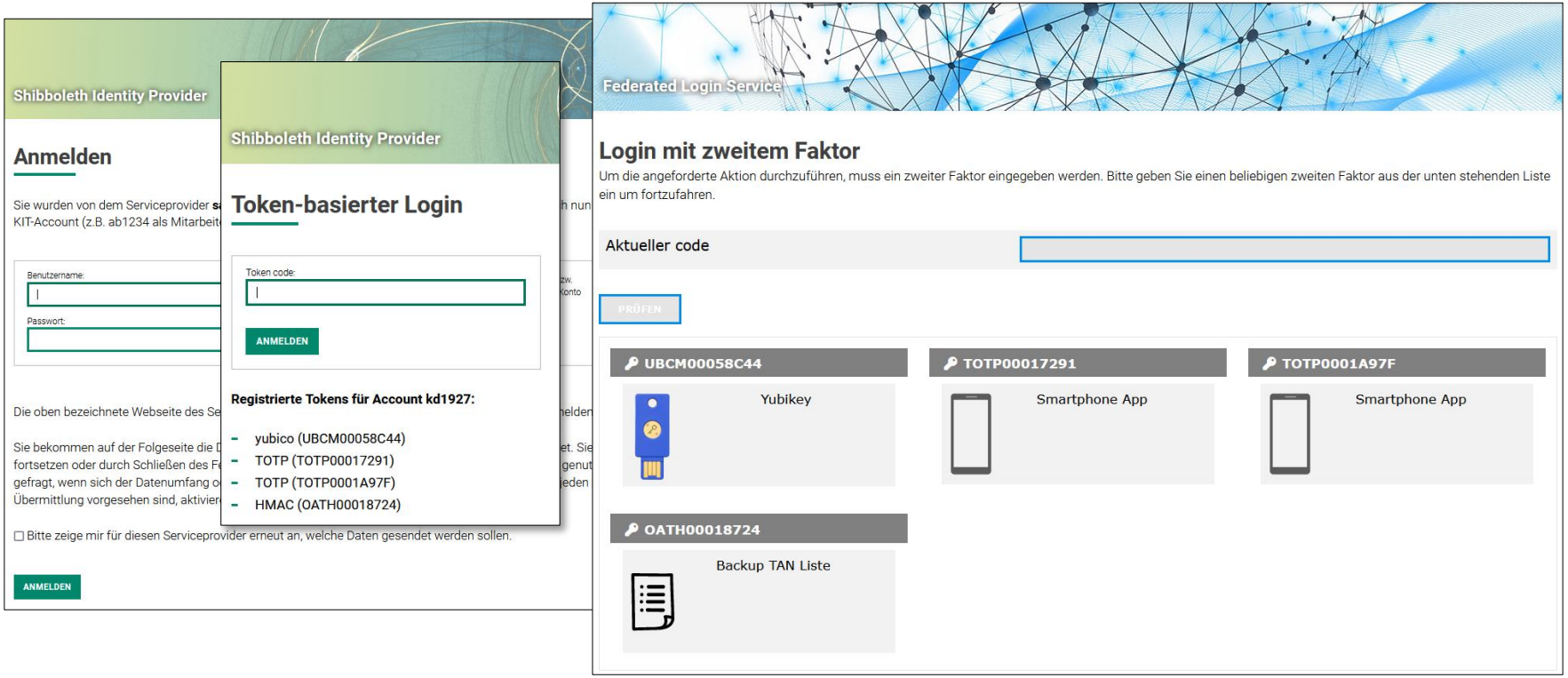


Community Management

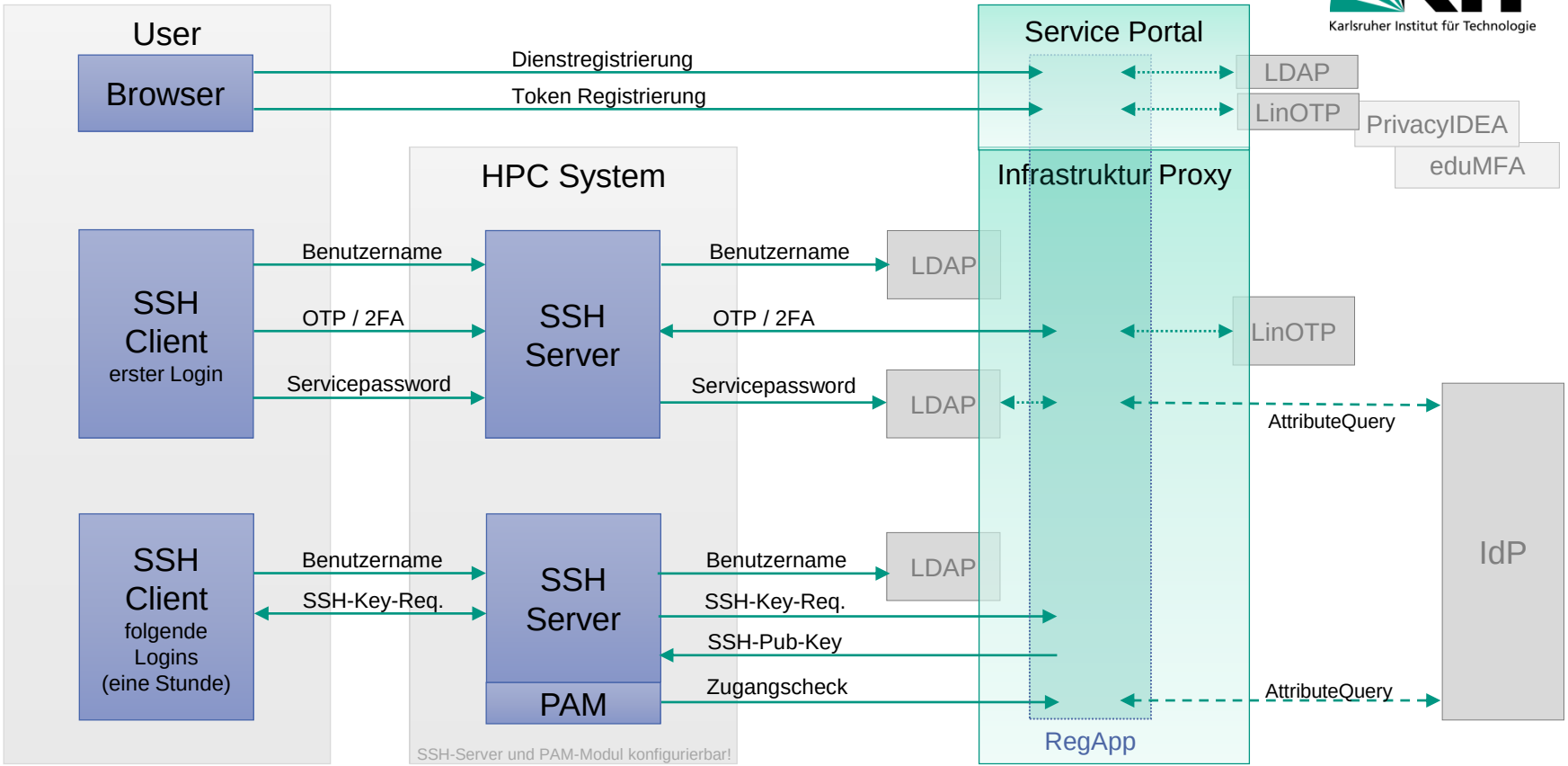
- Delegation an ein/mehrere PIs
- Schachtelung von Communities möglich

- Beispiele
  - HPC – Lokal am KIT und in einigen NHR-Zentren
  - Gitlab – Projektverwaltung
  - Geplant – Zugang zum Landesverwaltungsnetz via VPN

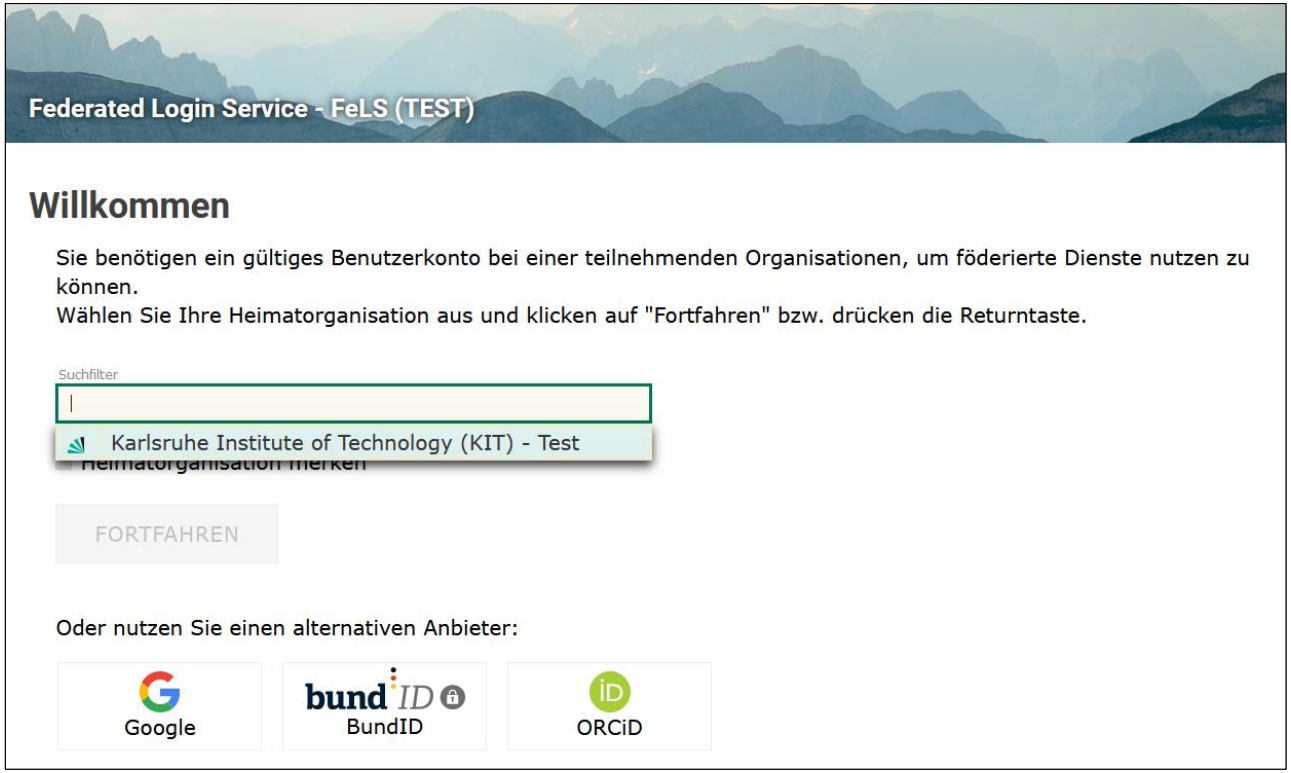
Zwei Faktor-Authentifizierung (2FA TOTP)



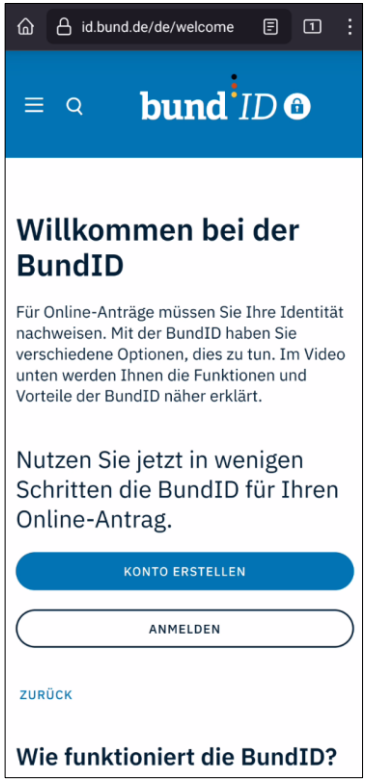
SSH-Zugang für HPC: 2FA ohne SSH-Keys im Filesystem

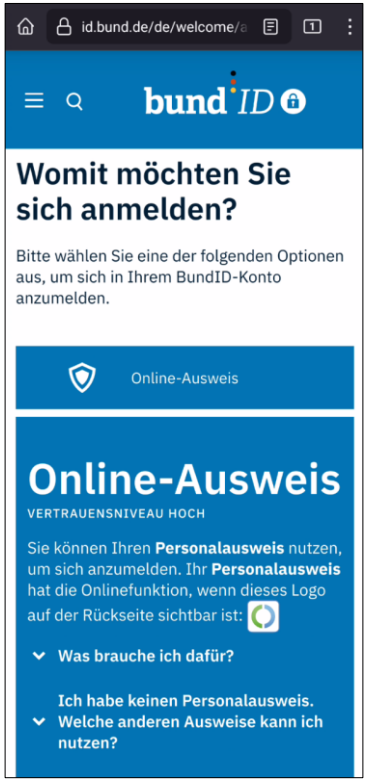


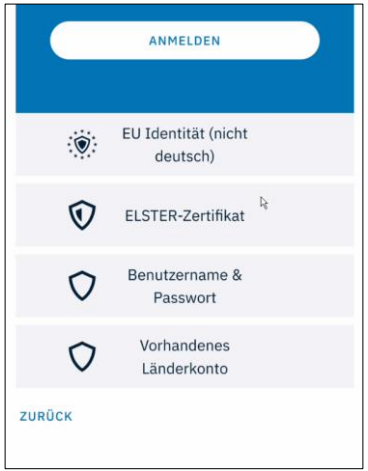
Erweiterung der föderierten Login-Dienste



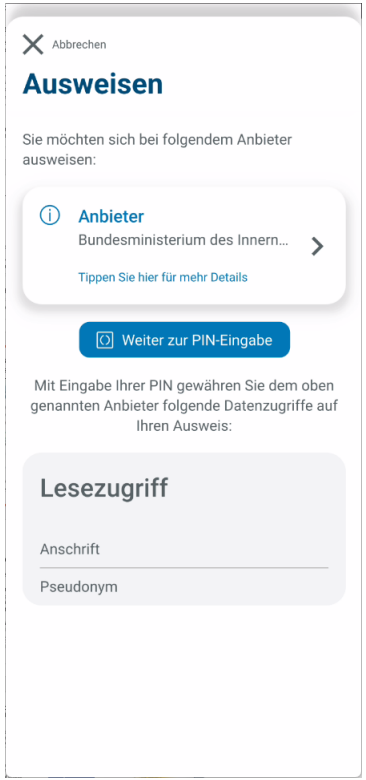
Nutzende – Login mit BundID

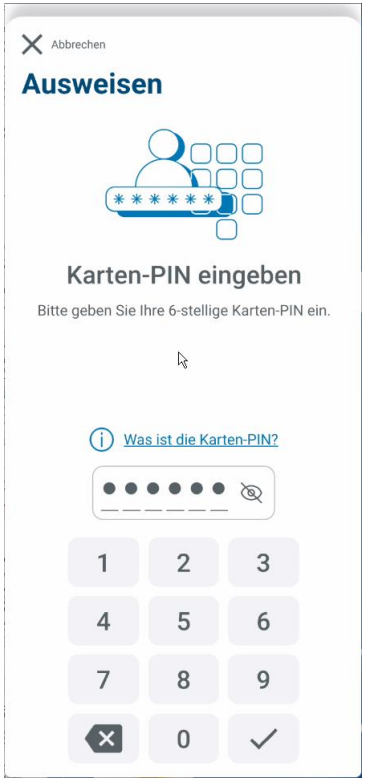


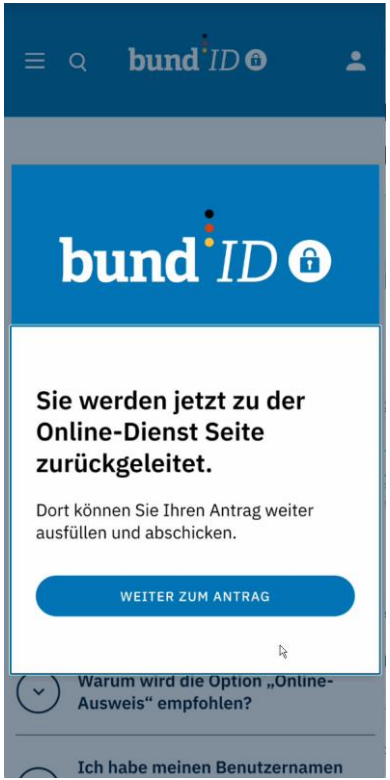




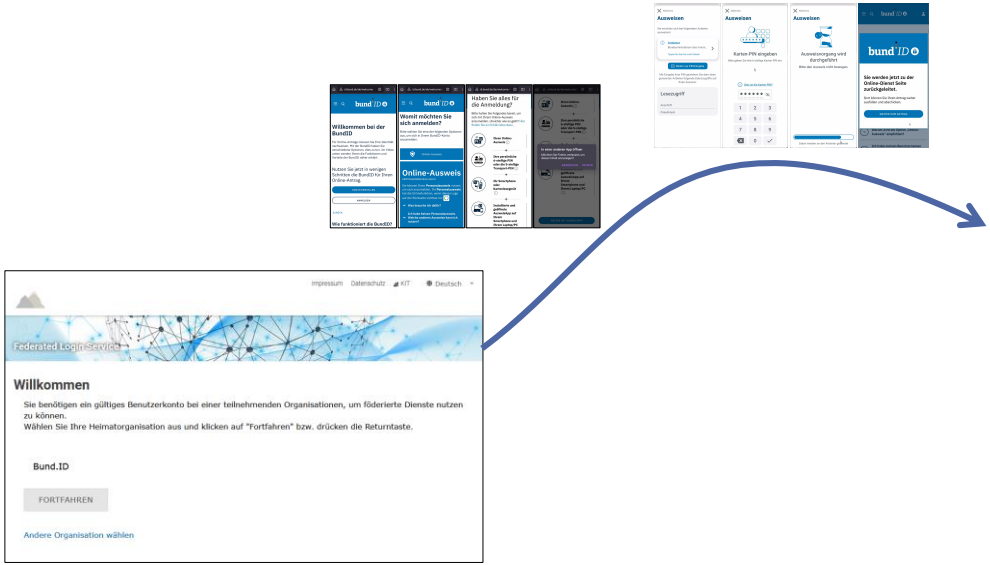
Nutzende – Ausweis-App





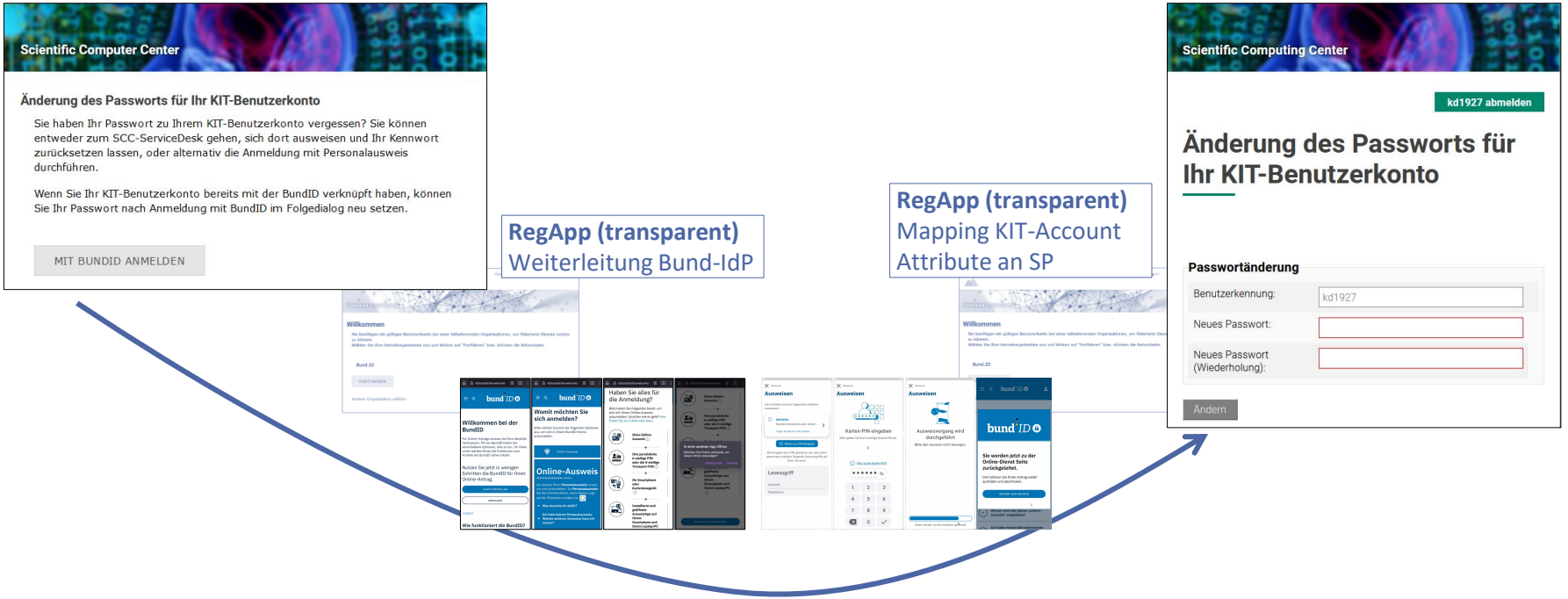


Service Provider – angebundener Dienst



Gelieferte Attribute & *Werte* des Personalausweis	
Name	**Wert**
Unbekanntes Attribut	Vl…NA
Vertrauensniveau	STORK-QAA-Level-4
Strasse	FIKTIVE STR. …
PLZ	76133
Postkorb ID	fac0…03b6
Geburtsdatum	19…-06-10
Email	uli.weiss@kit.edu
Geburtsort	IRGENDWOIMNORDEN
Vorname	ULRICH
Nationalität	DE
Bereichsspezifisches Personenkennzeichen	kHz…Yx8
Ausweisart	eID
Gültigkeit	2021.7.1
Anrede	1
Wohnort	KARLSRUHE
Nachname	WEIß

Dienstanbindung aus Nutzendensicht

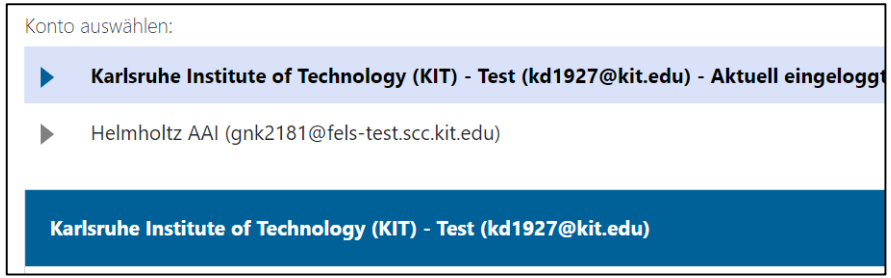


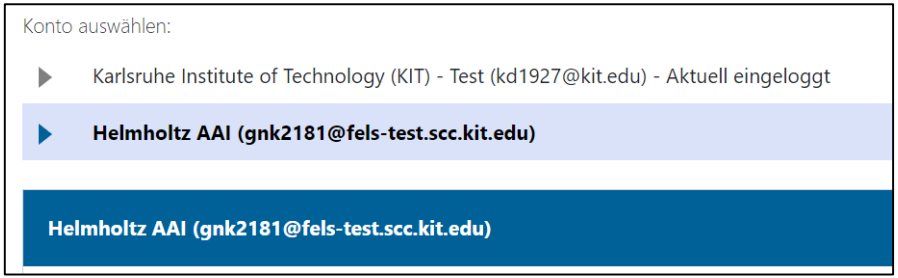
Erweiterung der föderierten Login-Dienste

Schwierigkeit:
Anmeldung BundID mit PA/eAT erfordert Lesegerät oder Smartphone mit Ausweis-APP.

→ Ausführung auf Smartphone erforderlich

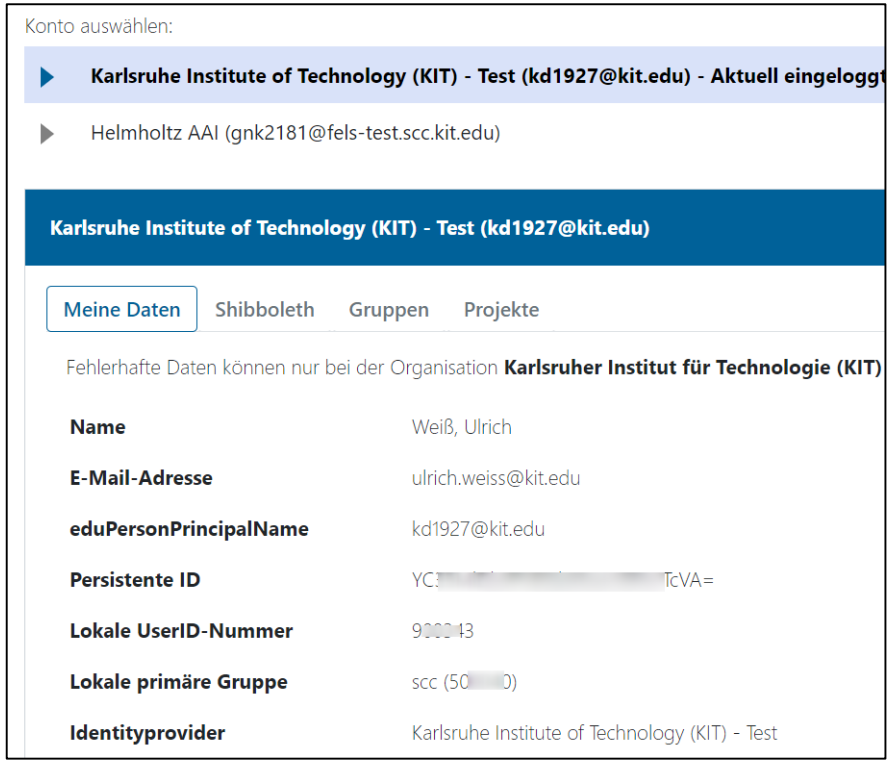
Account-Linking

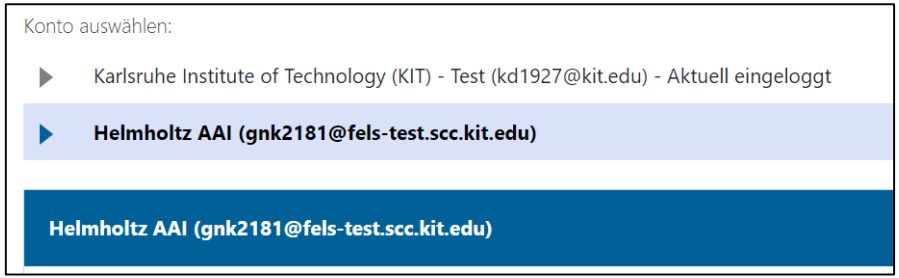




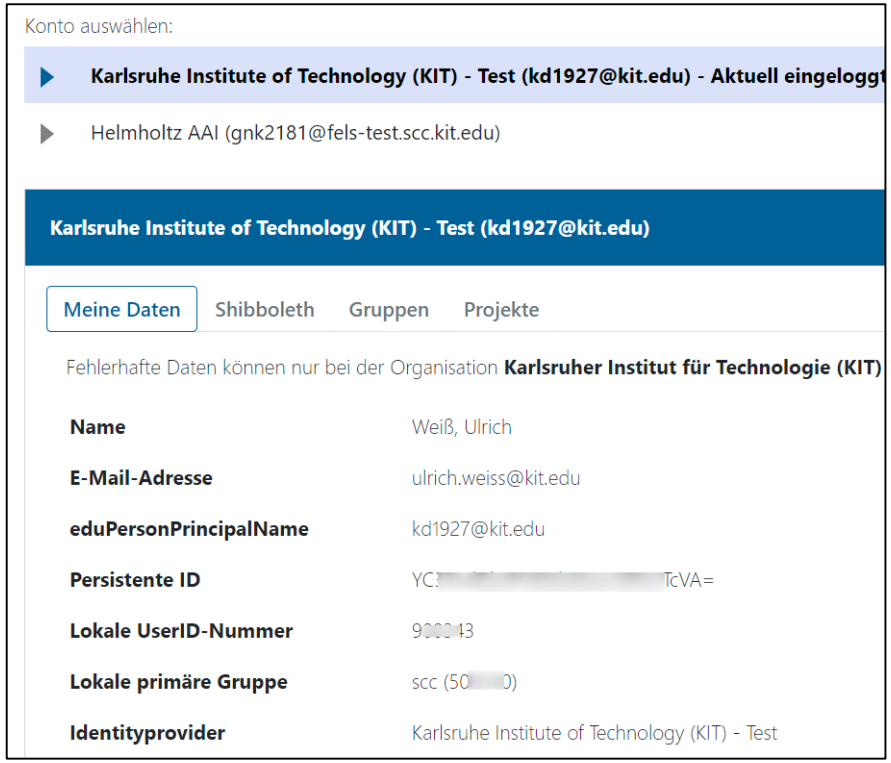
Konfigurierbare Heuristik zur Erkennung von potenziell zu verknüpfenden Accounts

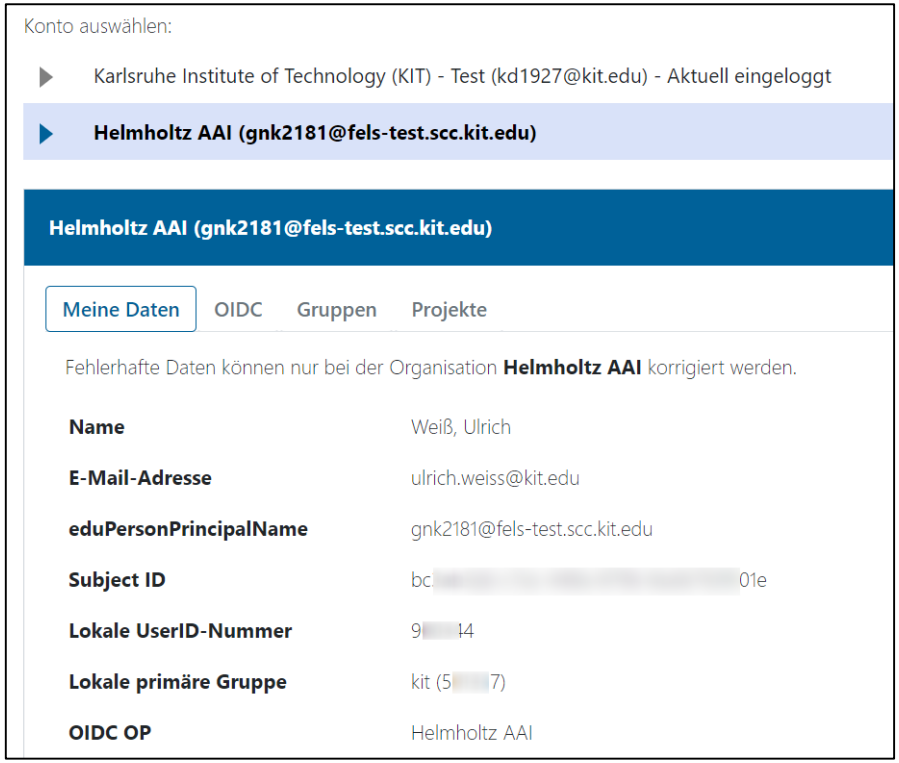
Account-Linking





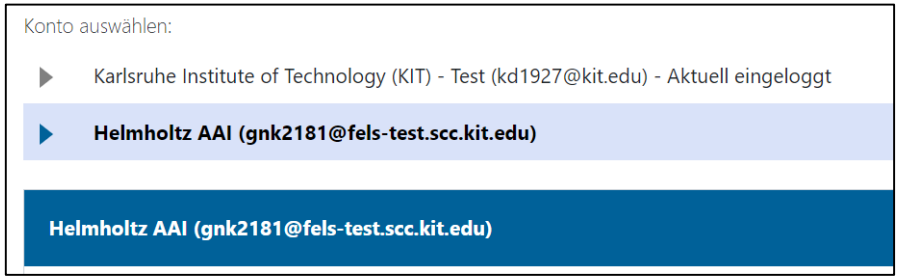
Account-Linking





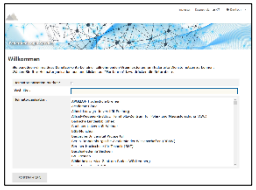
Account-Linking

- Kompliziert
- Benutzerführung
- Autorisierungen in Abhängigkeit der Dienstanforderungen

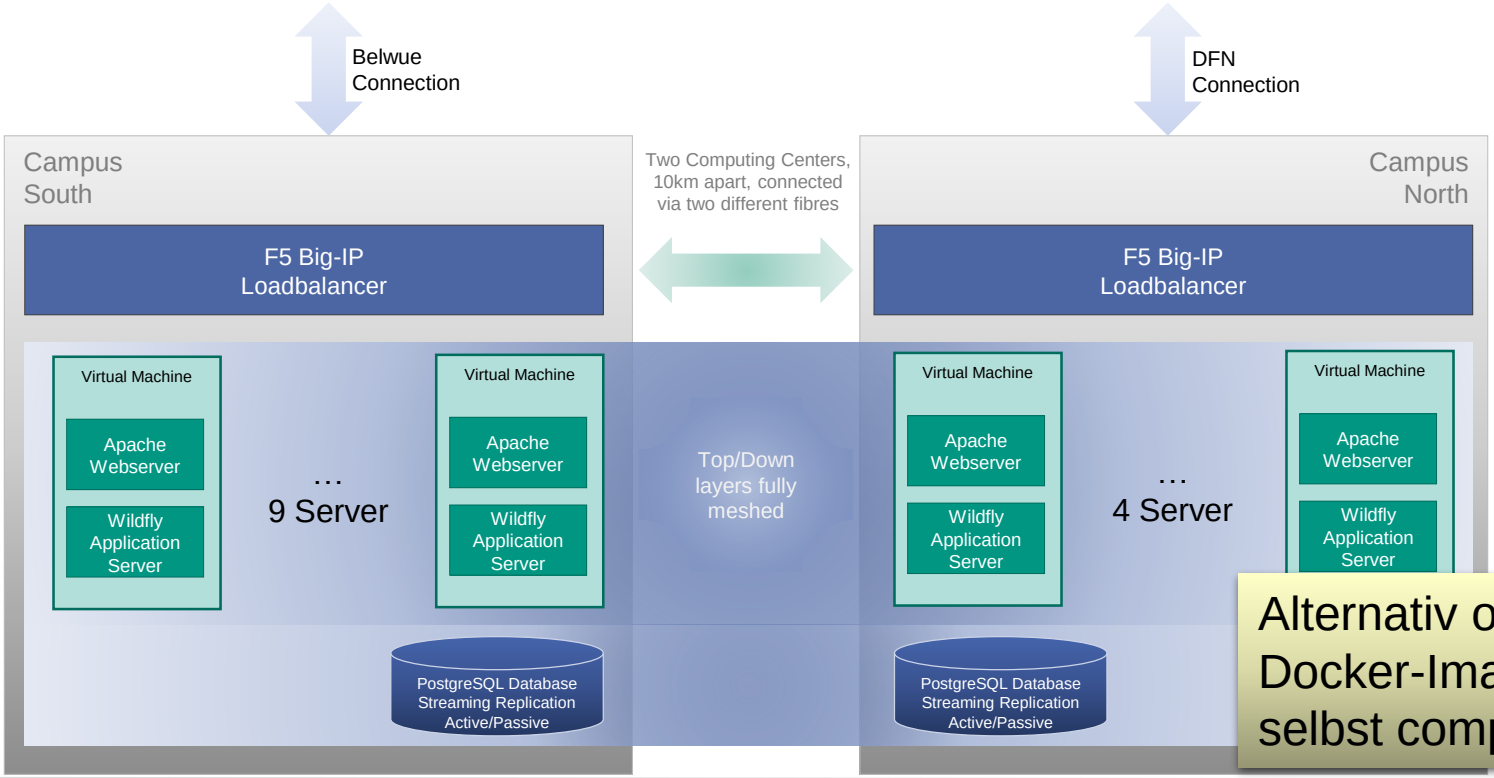


- Zugänge via Social-IdP (ORCID, Google, etc.) ermöglichen lebenslange Identität (nur Authentifizierung)
- Hinzufügen von E-Mail nach Dienstanforderung
- Attribute von den verschiedenen Quellen harmonisieren

RegApp – im Einsatz (2011 bis heute)



Mandantenfähiger Betrieb am KIT (2023)



Alternativ on-premise: Docker-Image oder selbst compiliert.

(Weiter-) Entwicklungen

- Verbesserung der Community-Funktionalität
  - Verwaltung von Projekten und virtuellen Organisationen
  - Bereitstellung aktiver Gruppenmitgliedschaften
- Account-Linking
  - Verbesserung der Benutzererfahrung bei der Verknüpfung von Konten
  - Attribute von den verschiedenen Quellen harmonisieren
- Unterstützung von modernen Authentifizierungsmethoden (geplant)
  - FIDO2-Schlüssel für SSH-Anmeldung
  - Webauthn/Passkeys für benutzer-/passwortlose Webanmeldung
- Verbesserungen in der Weiterverarbeitung der Attribute
  - REFEDS Assurance besser berücksichtigen
  - Den Benutzer stärker involvieren
- Anbindung edu-ID-Proxy
- Internes Redesign/Modularisierung

Fragen & Anmerkungen

Weitere Informationen

- **Web**
  - Deutsch: www.scc.kit.edu/dienste/regapp
  - Englisch: www.scc.kit.edu/en/services/regapp
- **Verfügbarkeit**
  - Gitlab: https://git.scc.kit.edu/reg-app/reg-app
  - Docker https://git.scc.kit.edu/reg-app/regapp-docker
- **Referenzen**
  - Föderiertes IDM der BaWü-Hochschulen bwIDM: login.bwidm.de
  - Helmholtz-AAI: fels.scc.kit.edu
  - Nationales Hochleistungsrechnen NHR: login.nhr-verein.de
  - Nationale Forschungsdateninfrastruktur NFDI: regapp.nfdi-aai.de
- **Kontakt**
  - uli.weiss@kit.edu und michael.simon@kit.edu