

RegApp – Community AAI

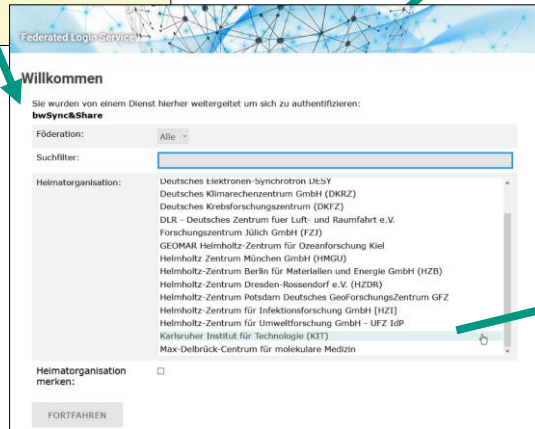
Michael Simon, Ulrich Weiß
Karlsruher Institut für Technologie



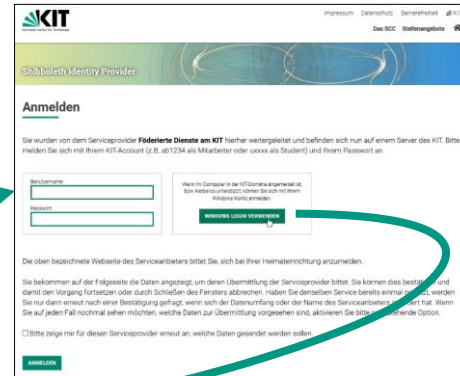
Dienst-Login mit Heimataccount



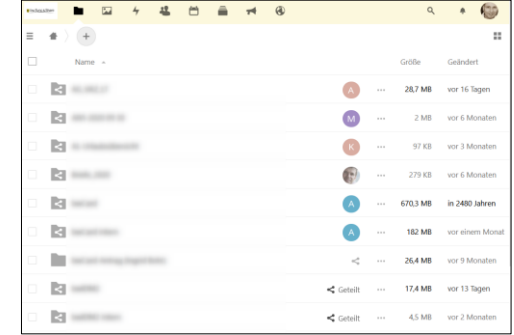
Service



RegApp AAI-SW

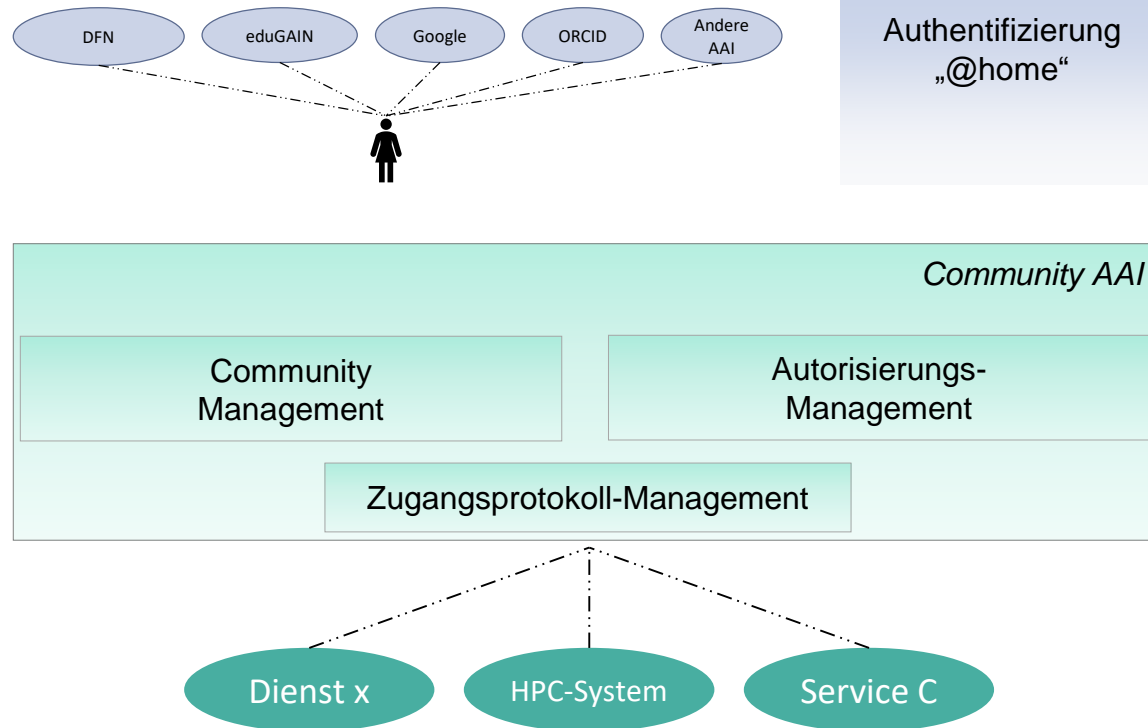


Heimat IdP

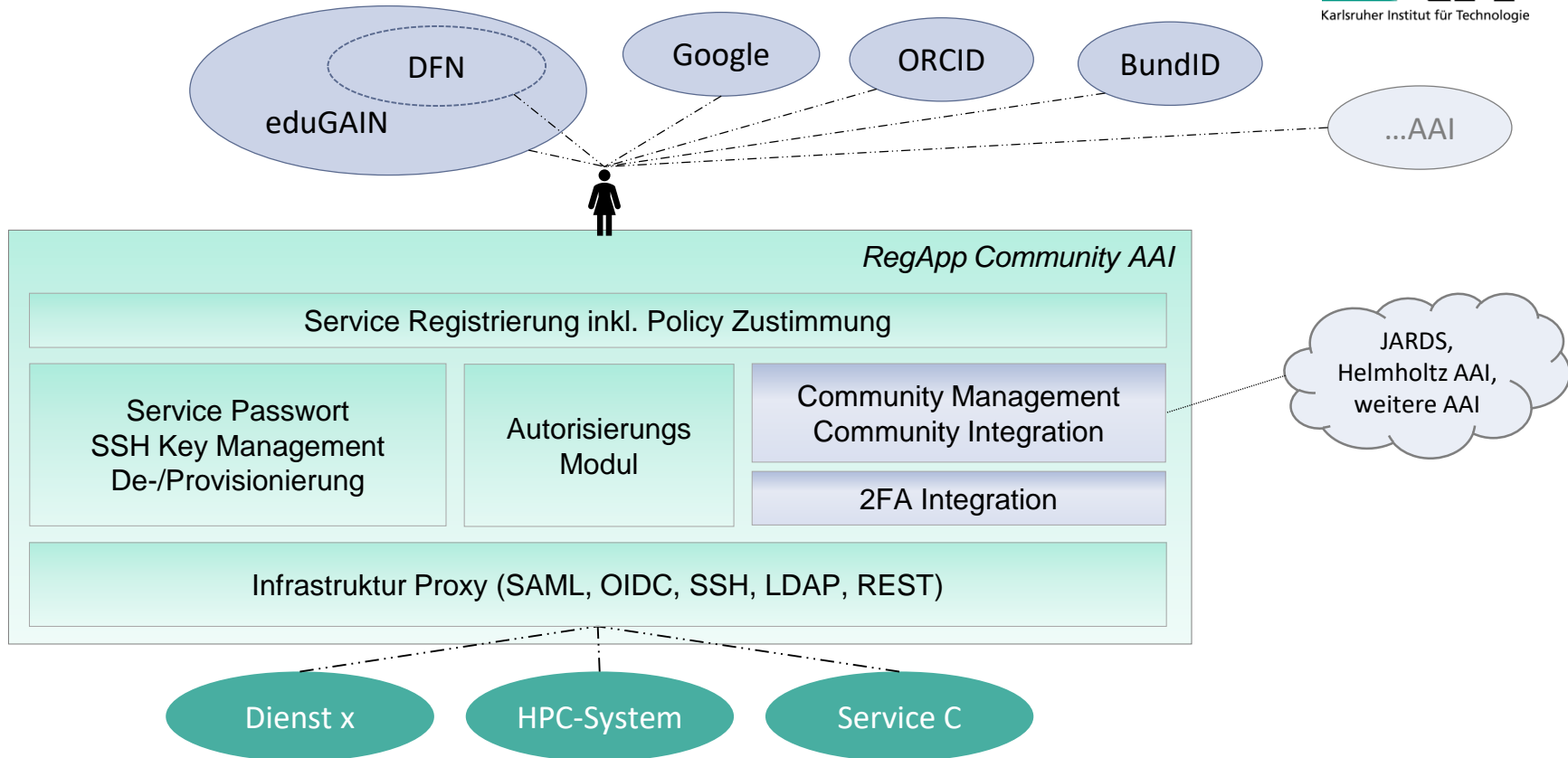


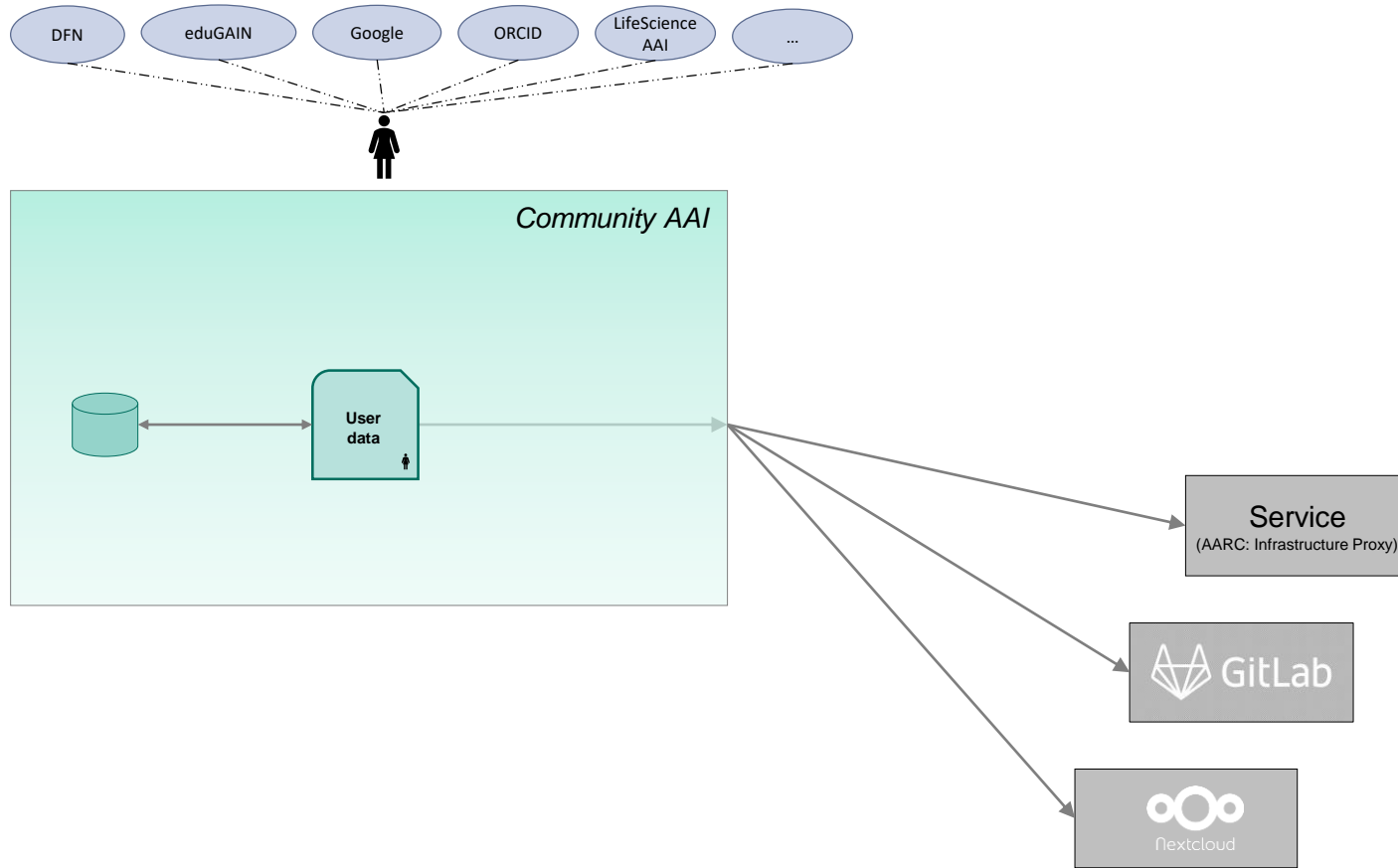
Service

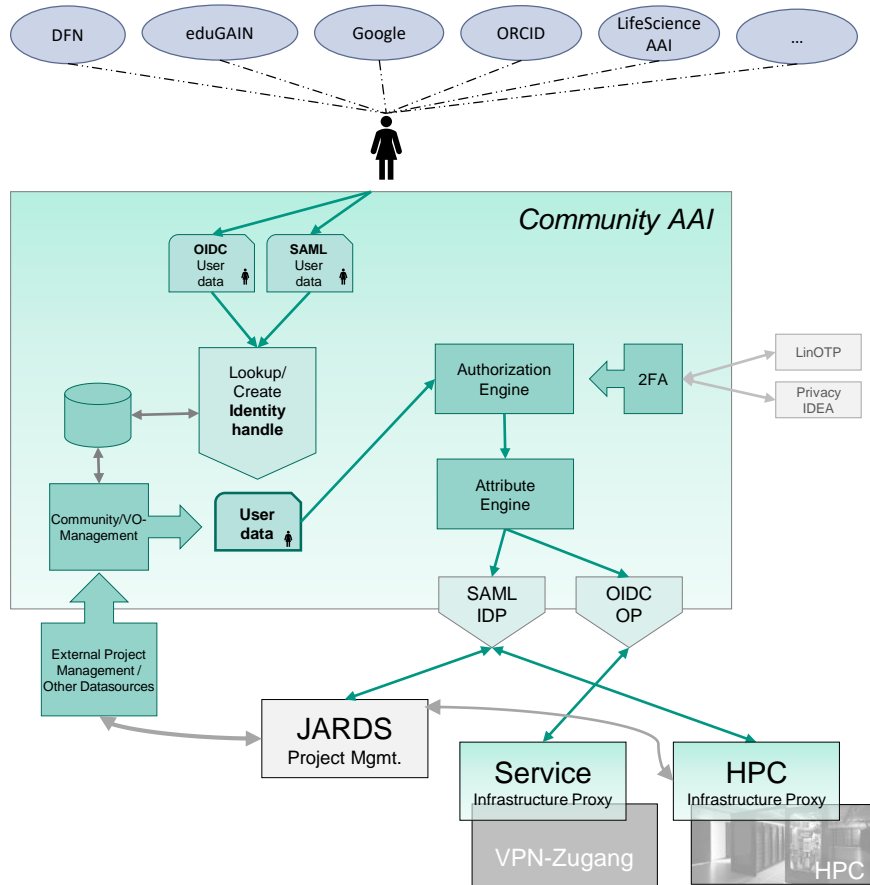
Community Authentifizierungs- und Autorisierungs-Infrastruktur (CAAI)

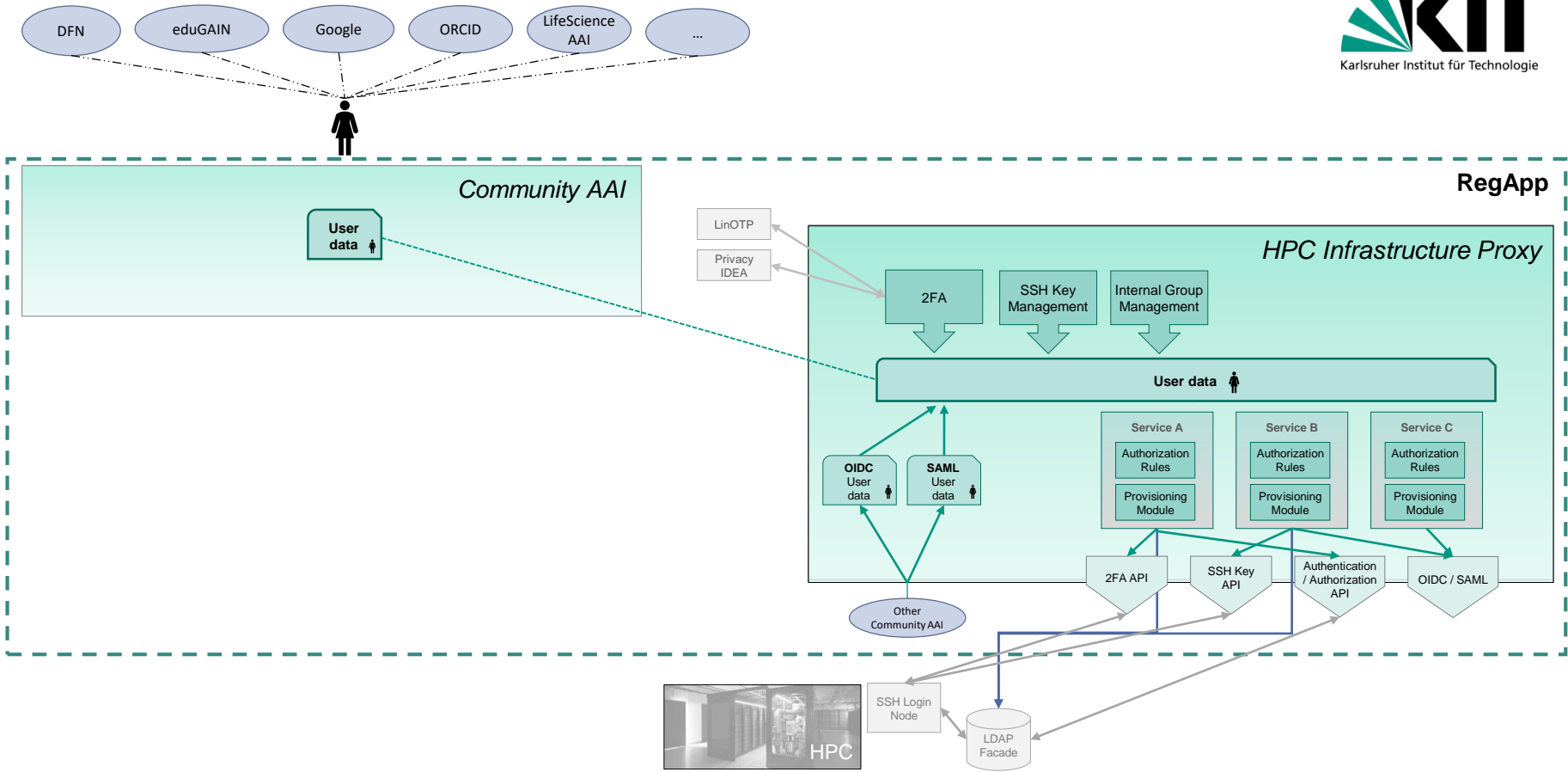


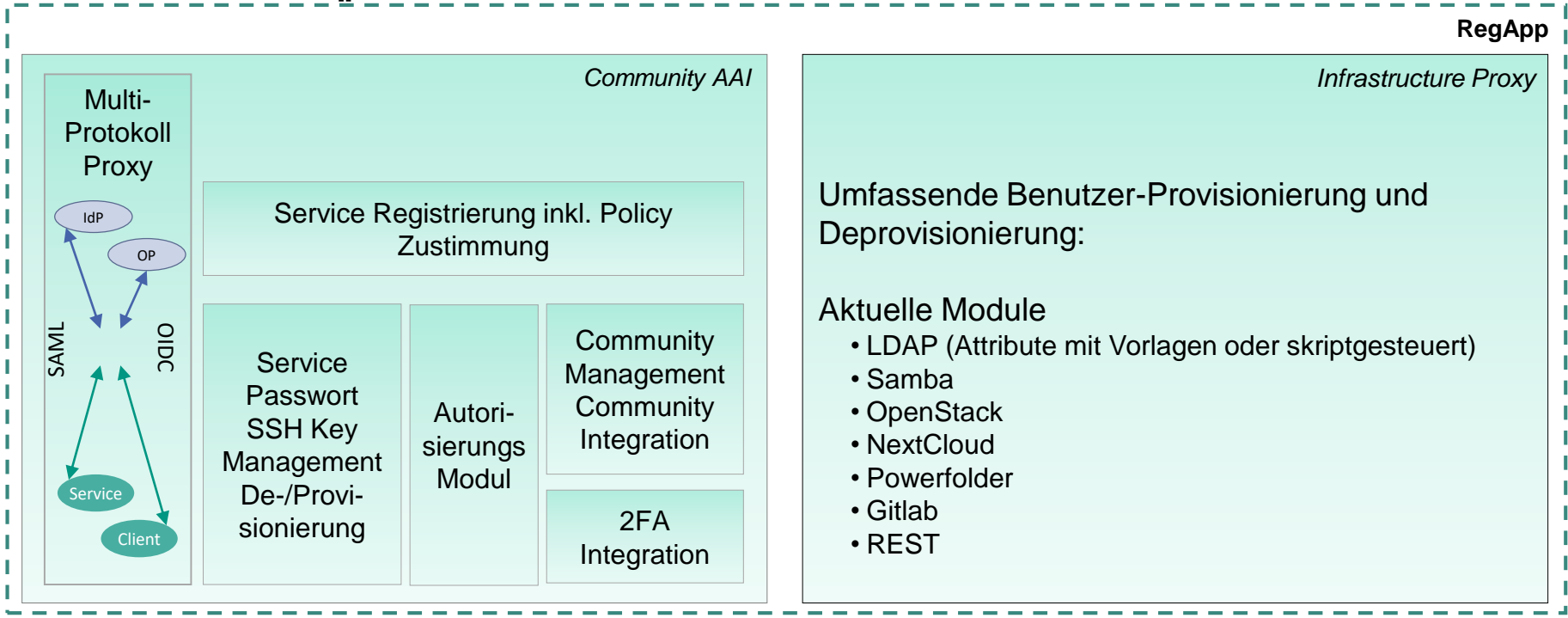
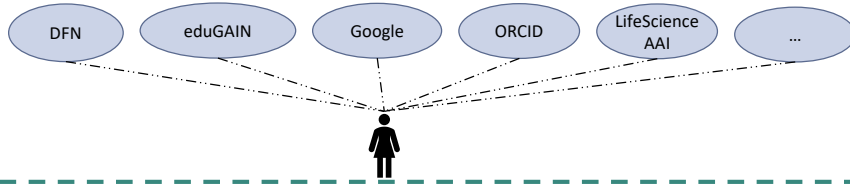
RegApp CAAI



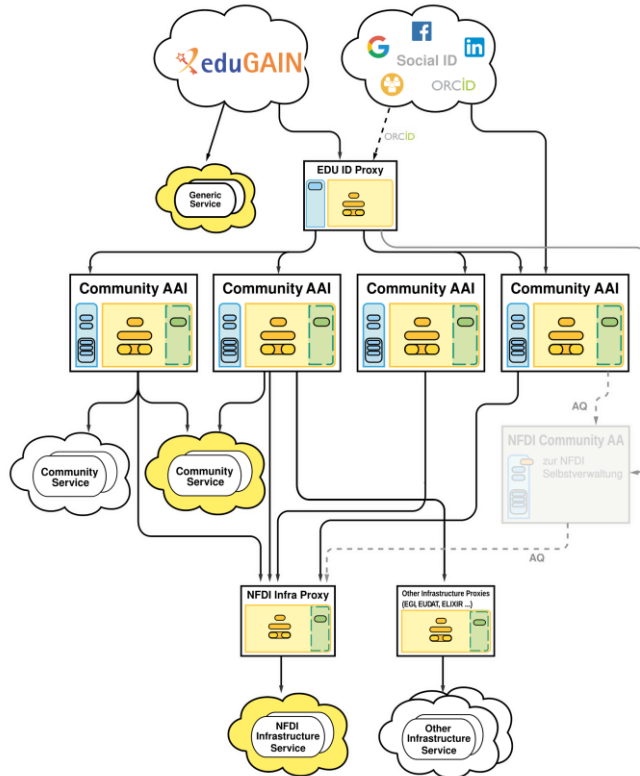






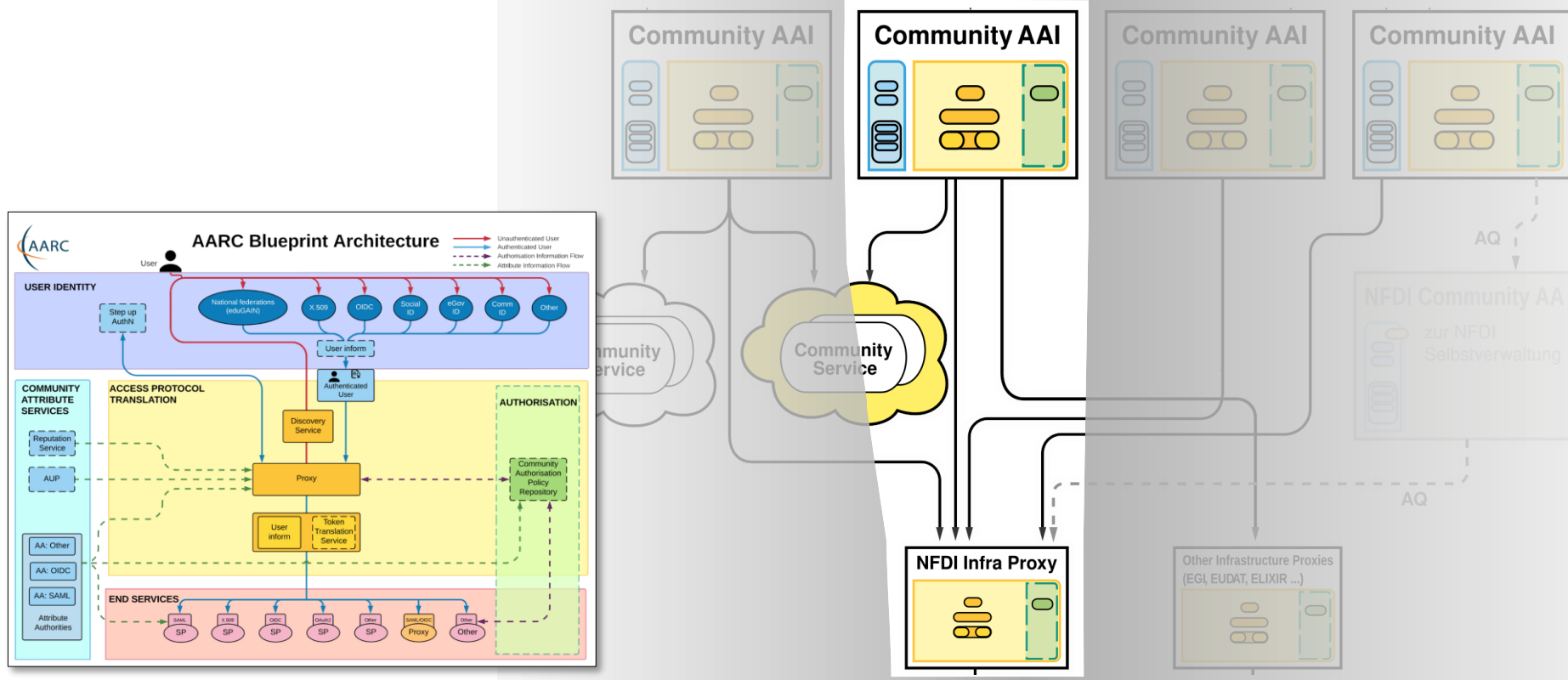


AARC Blueprint Architecture



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

AARC Blueprint Architecture (4NFDI)

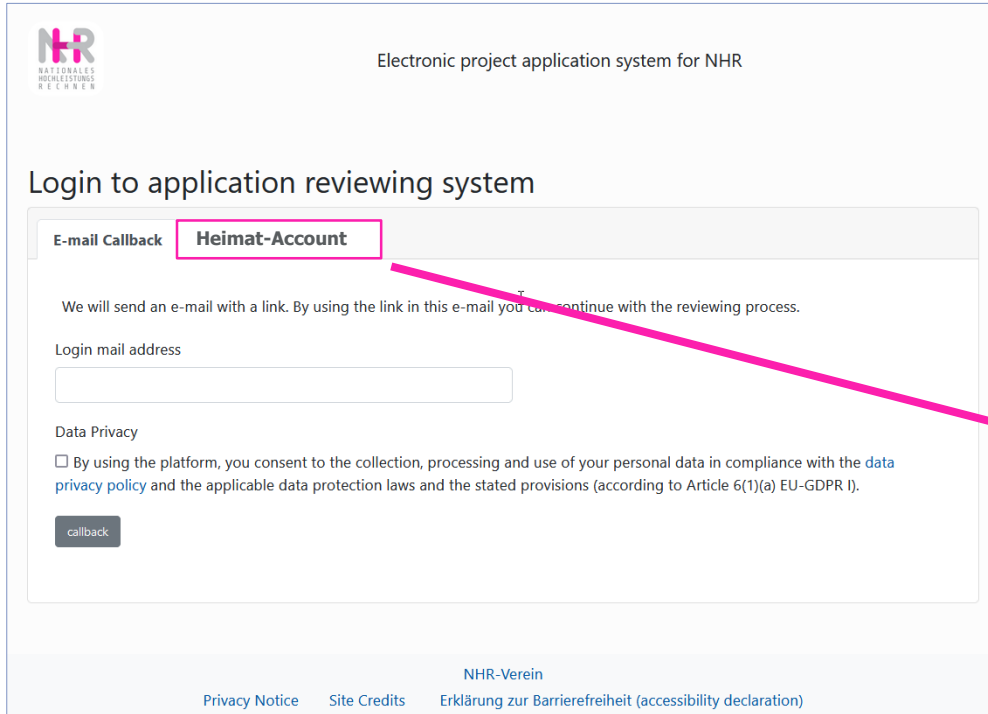


RegApp Funktionalitäten

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)



NHR
NATIONALES
HIGHLIGHTS
RECHNER

Electronic project application system for NHR

Login to application reviewing system

E-mail Callback **Heimat-Account**

We will send an e-mail with a link. By using the link in this e-mail you can continue with the reviewing process.

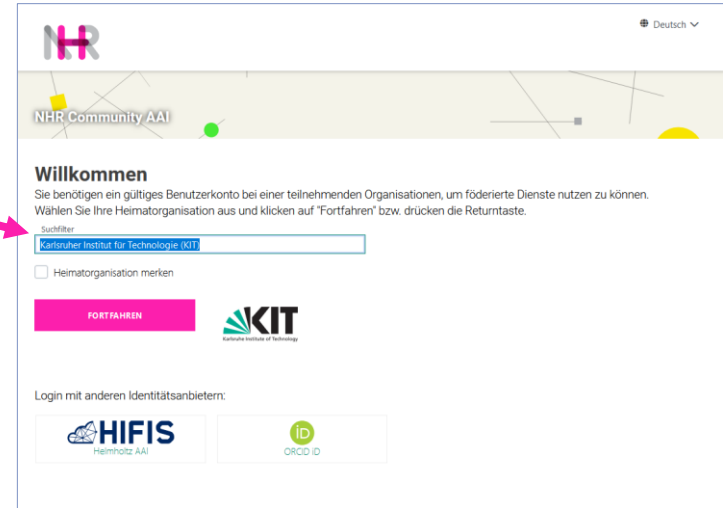
Login mail address

Data Privacy

By using the platform, you consent to the collection, processing and use of your personal data in compliance with the [data privacy policy](#) and the applicable data protection laws and the stated provisions (according to Article 6(1)(a) EU-GDPR I).

[Privacy Notice](#) [Site Credits](#) [NHR-Verein](#) [Erklärung zur Barrierefreiheit \(accessibility declaration\)](#)

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



NHR Deutsch


NHR Community AAI

Willkommen


Sie benötigen ein gültiges Benutzerkonto bei einer teilnehmenden Organisation, um förderierte Dienste nutzen zu können. Wählen Sie Ihre Heimatorganisation aus und klicken auf "Fortfahren" bzw. drücken die Return-Taste.


Suchfilter

Heimatorganisation merken

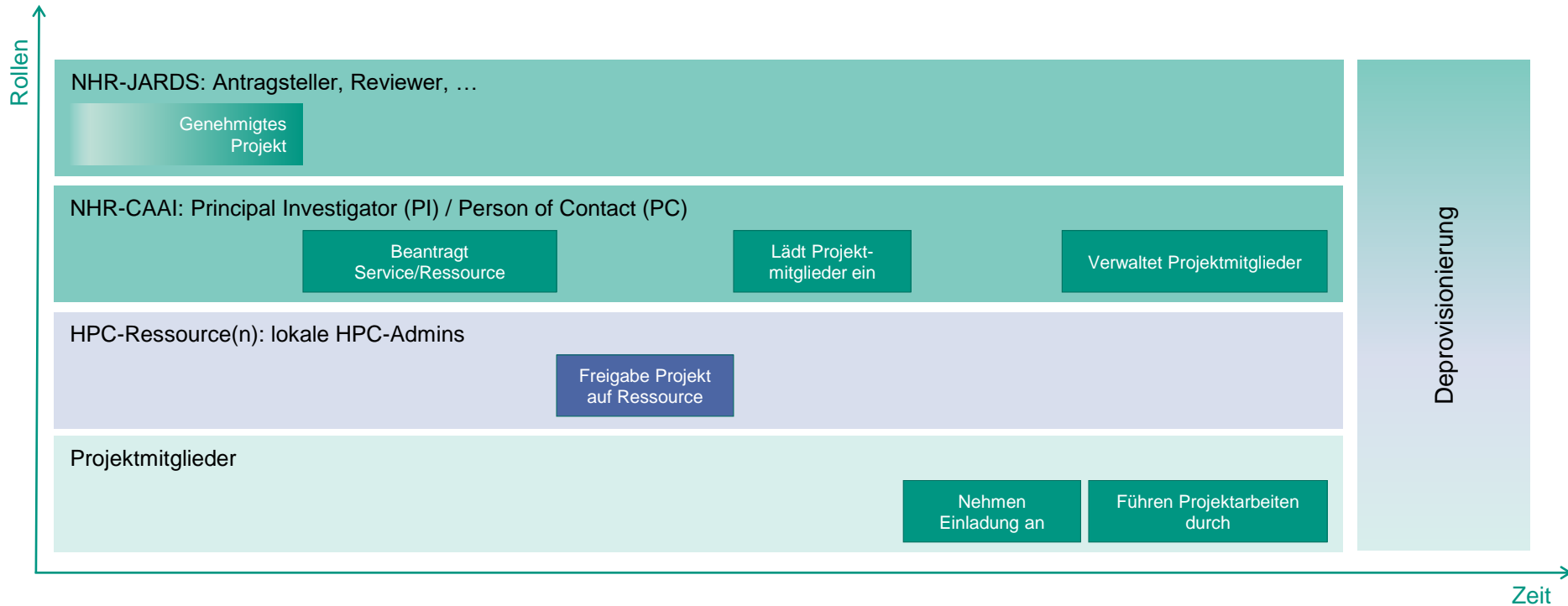


Login mit anderen Identitätsanbietern:

 **HIFIS**
Helmholtz AAI

 **ID**
ORCID ID

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 *	<input type="text" value="Test für Communitymanagement"/>
Kurzname *	<input type="text" value="tfc"/>
Gruppenname *	<input type="text" value="tfc"/>
Kurze Beschreibung	<input type="text" value="RegApp-Communitymanagement"/>
Beschreibung des Projekts	<input type="text" value="Verschachtelte Communities mit delegierten Verantwortlichen als Basis für Dienstzugänge."/>
Selbst Mitglied werden	<input checked="" type="checkbox"/>

ABBRECHEN

SPEICHERN

Community Management: Service Registration

Lokales Projekt: Test für Communitymanagement

ID: 1284310
Name: Test für Communitymanagement
Gruppenname: tfc
Dienste:

[Mit Dienst verbinden](#) Hier können Sie die Nutzung einer Resource für

[Mitglieder einladen](#) Laden Sie Mitglieder für Ihr Projekt ein. Die Einla

[Projekt löschen](#) Öffnet eine neue Seite, auf der das Projekt gelö

[Zurück](#)

Projekt Mitglieder

Name ↑↓	Nachname ↑↓	Vorname ↑↓
<input type="text"/>	<input type="text"/>	<input type="text"/>
kd1927@kit.edu	Weiß	Ulrich

Projekt Administratoren

Name ↑↓	Nachname ↑↓	Vorname
<input type="text"/>	<input type="text"/>	<input type="text"/>

Dienstnutzung für Projekt: Test für Communitymanagement

ID: 1284310
Name: Test für Communitymanagement

Dienste auswählen:

- SSH-Test Service
- Nextcloud Test
- Dummy Service 1
- bwDataArchive Test

Dienste:

Wählen Sie die Dienste aus, die Sie im Rahmen Ihres Projekts verwenden wollen. Mit Klick auf den Button, wird die Nutzung einem Projektadmin des jeweiligen Dienstes zur Begutachtung und Freigabe vorgelegt.

SSH Project Connect Policy - v1

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Ich habe die Nutzungsbedingungen gelesen und bin einverstanden.

Community Management: User Management

Mitglieder einladen: Test für Communitymanagement

Laden Sie Mitglieder zu Ihrem Projekt ein.

Token	E-Mail-Adresse
Keine Datensätze gefunden.	

Einladung per E-Mail

Sie können eine Projekteinladung erstellen, die in Ihrem Projekt an den Mitgliedern an Ihrem Projekt teilnehmen kann.

E-Mail Adresse der einzuladenden Person

Name der einzuladenden Person

Absender E-Mail

Absender Name

EINLADUNG SCHICKEN

[Zurück](#)

Projekteinladung

Bitte kopieren Sie den Token aus der Einladungs-E-Mail, die Sie vom PI (Project Investigator) erhalten haben.

Token

f5kk2f5a67l3336mqjro064d37

Sie wurden zur Teilnahme an einem Projekt eingeladen:

Big Important Project 1

Möchten Sie die Einladung annehmen?

Das Projekt hat Nutzungsbedingungen, denen Sie zustimmen müssen, um teilzunehmen.

SSH Project Member Join Policy - v1.3

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Ich habe die Nutzungsbedingungen gelesen und bin einverstanden.

ANNEHEMEN

ABLEHNEN

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)

Shibboleth Identity Provider

Anmelden

Sie wurden von dem Serviceprovider als **KIT-Account** (z.B. ab1234 als Mitarbeiter)

Benutzername:

Passwort:

ANMELDEN

Die oben bezeichnete Webseite des Service

Sie bekommen auf der Folgeseite die Möglichkeit fortsetzen oder durch Schließen des Dialogs abgefragt, wenn sich der Datenumfang oder die Übermittlung vorgesehen sind, aktivieren Sie

Bitte zeige mir für diesen Serviceprovider erneut an, welche Daten gesendet werden sollen.

ANMELDEN

Shibboleth Identity Provider

Token-basierter Login

Token code:

ANMELDEN

Registrierte Tokens für Account kd1927:

- yubico (UBCM00058C44)
- TOTP (TOTP00017291)
- TOTP (TOTP0001A97F)
- HMAC (OATH00018724)

Federated Login Service

Login mit zweitem Faktor


Um die angeforderte Aktion durchzuführen, muss ein zweiter Faktor eingegeben werden. Bitte geben Sie einen beliebigen zweiten Faktor aus der unten stehenden Liste ein um fortzufahren.

Aktueller code:

PRÜFEN


UBCM00058C44

Yubikey




TOTP00017291

Smartphone App




TOTP0001A97F

Smartphone App

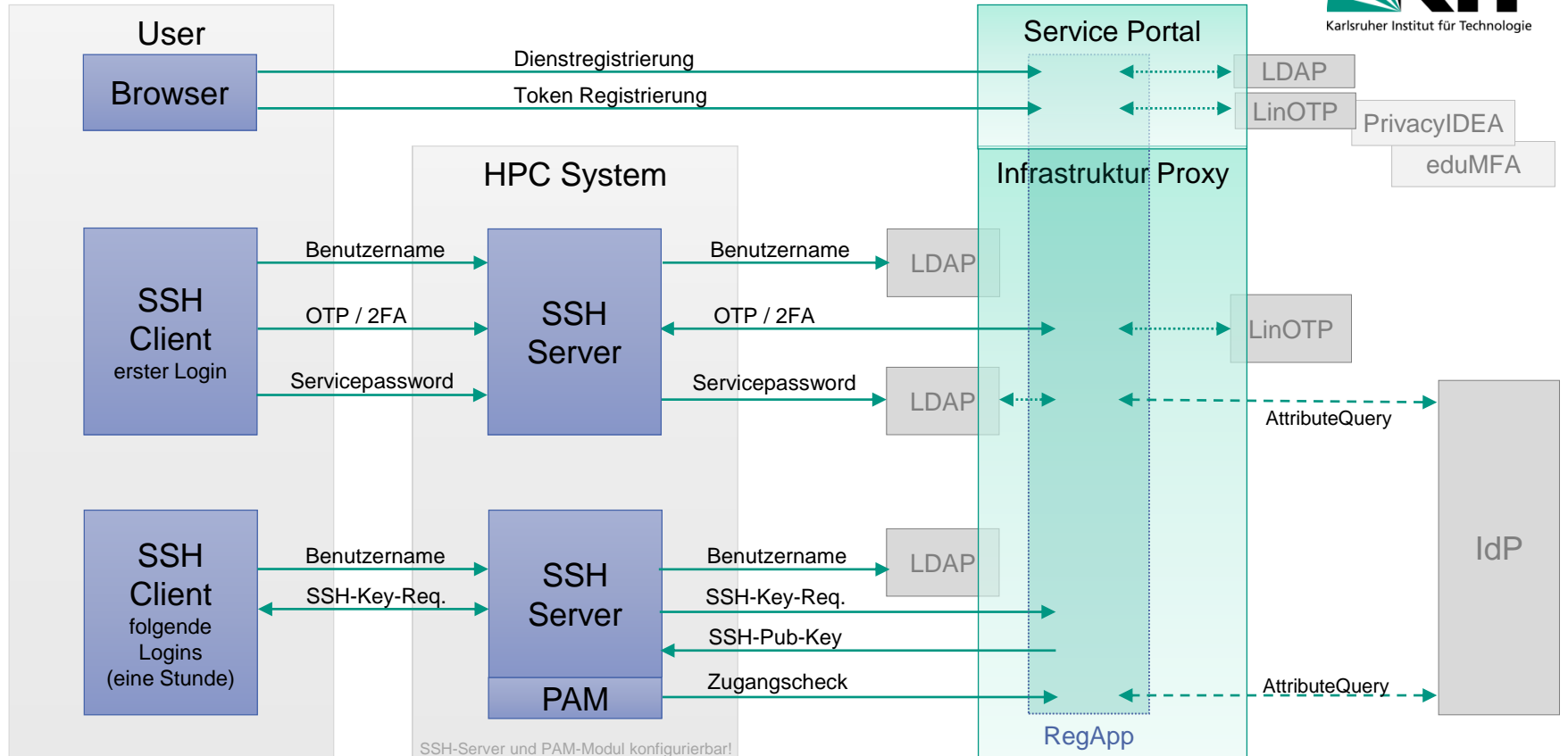


OATH00018724

Backup TAN Liste



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



Erweiterung der föderierten Login-Dienste

Federated Login Service - FeLS (TEST)

Willkommen

Sie benötigen ein gültiges Benutzerkonto bei einer teilnehmenden Organisationen, um föderierte Dienste nutzen zu können.
Wählen Sie Ihre Heimatorganisation aus und klicken auf "Fortfahren" bzw. drücken die Returnntaste.

Suchfilter

-  Karlsruhe Institute of Technology (KIT) - Test
Heimatorganisation merken

FORTFAHREN

Oder nutzen Sie einen alternativen Anbieter:



Google

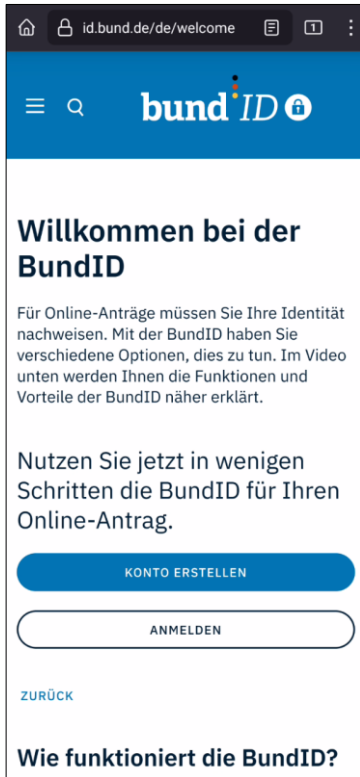


bund ID
BundID



ID
ORCID

Nutzende – Login mit BundID



id.bund.de/de/welcome

Willkommen bei der BundID

Für Online-Anträge müssen Sie Ihre Identität nachweisen. Mit der BundID haben Sie verschiedene Optionen, dies zu tun. Im Video unten werden Ihnen die Funktionen und Vorteile der BundID näher erklärt.

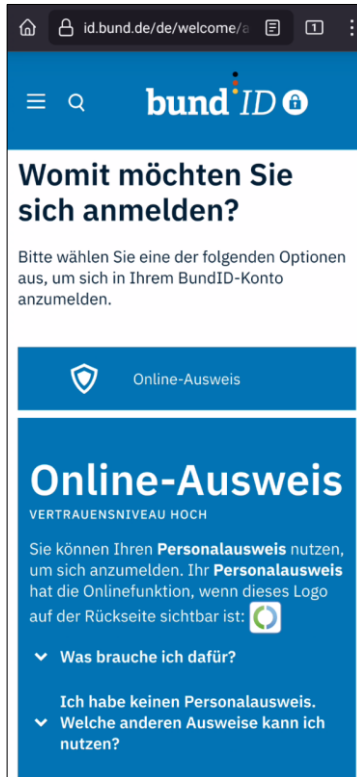
Nutzen Sie jetzt in wenigen Schritten die BundID für Ihren Online-Antrag.

KONTO ERSTELLEN

ANMELDEN

ZURÜCK

Wie funktioniert die BundID?



id.bund.de/de/welcome/

Womit möchten Sie sich anmelden?

Bitte wählen Sie eine der folgenden Optionen aus, um sich in Ihrem BundID-Konto anzumelden.

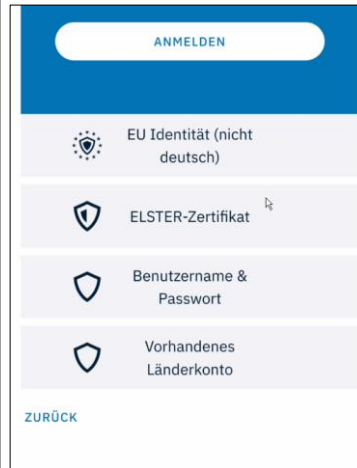
Online-Ausweis

Online-Ausweis

VERTRAUENSNIVEAU HOCH

Sie können Ihren **Personalausweis** nutzen, um sich anzumelden. Ihr **Personalausweis** hat die Onlinefunktion, wenn dieses Logo auf der Rückseite sichtbar ist:


- Was brauche ich dafür?
- Ich habe keinen Personalausweis.
- Welche anderen Ausweise kann ich nutzen?



ANMELDEN

- EU Identität (nicht deutsch)
- ELSTER-Zertifikat
- Benutzername & Passwort
- Vorhandenes Länderkonto

ZURÜCK



id.bund.de/de/welcome/

Haben Sie alles für die Anmeldung?

Bitte halten Sie Folgendes bereit, um sich mit Ihrem Online-Ausweis anzumelden. Unsicher wie es geht? [Hier finden Sie ein Erklärvideo dazu.](#)

- Ihren Online-Ausweis
- Ihre persönliche 6-stellige PIN oder die 5-stellige Transport-PIN
- Ihr Smartphone oder Kartenlesegerät
- Installierte und geöffnete AusweisApp auf Ihrem Smartphone und Ihrem Laptop/PC



id.bund.de/de/welcome/

Ihren Online-Ausweis

Ihre persönliche 6-stellige PIN oder die 5-stellige Transport-PIN

Ihr Smartphone oder Kartenlesegerät

Installierte und geöffnete AusweisApp auf Ihrem Smartphone und Ihrem Laptop/PC

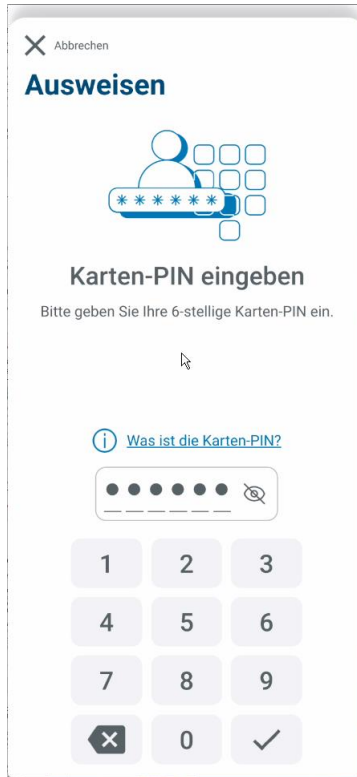
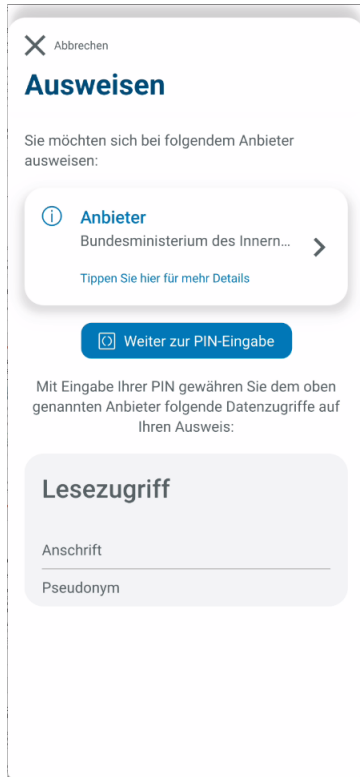
In einer anderen App öffnen

Möchten Sie Firefox verlassen, um diesen Inhalt anzuzeigen?

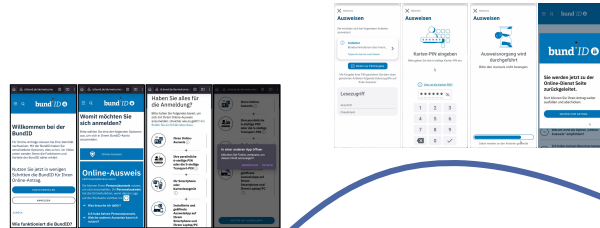
ABBRECHEN ÖFFNEN

WEITER MIT AUSWEISAPP

Nutzende – Ausweis-App



Service Provider – angebundener Dienst



Gelieferte Attribute & Werte des Personalausweis	
Name	Wert
Unbekanntes Attribut	VI...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

Dienstverbindung aus Nutzendensicht

Scientific Computer Center

Änderung des Passworts für Ihr KIT-Benutzerkonto

Sie haben Ihr Passwort zu Ihrem KIT-Benutzerkonto vergessen? Sie können entweder zum SCC-ServiceDesk gehen, sich dort ausweisen und Ihr Kennwort zurücksetzen lassen, oder alternativ die Anmeldung mit Personalausweis durchführen.

Wenn Sie Ihr KIT-Benutzerkonto bereits mit der BundID verknüpft haben, können Sie Ihr Passwort nach Anmeldung mit BundID im Folgedialog neu setzen.

MIT BUNDID ANMELDEN

RegApp (transparent)
Weiterleitung Bund-Id

RegApp (transparent)
Mapping KIT-Account
Attribute an SP

Scientific Computing Center

kd1927 abmelden

Änderung des Passworts für Ihr KIT-Benutzerkonto

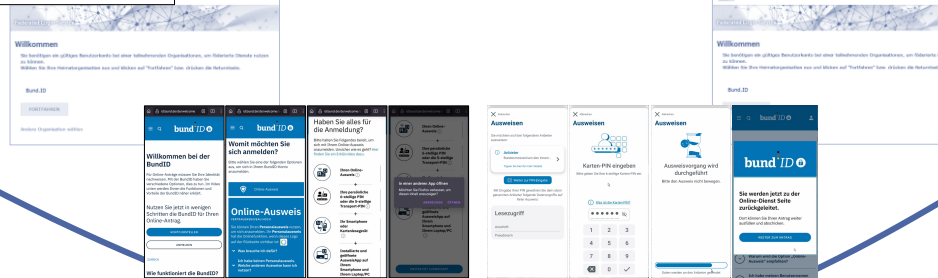
Passwortänderung

Benutzerkennung:

Neues Passwort:

Neues Passwort (Wiederholung):

Ändern



Erweiterung der föderierten Login-Dienste

Federated Login Service - FeLS (TEST)

Willkommen

Sie benötigen ein gültiges Benutzerkonto bei einer teilnehmenden Organisationen, um föderierte Dienste nutzen zu können.
Wählen Sie Ihre Heimatorganisation aus und klicken auf "Fortfahren" bzw. drücken die Returnntaste.

Suchfilter

-  Karlsruhe Institute of Technology (KIT) - Test
Heimatorganisation merken

FORTFAHREN

Oder nutzen Sie einen alternativen Anbieter:

 Google

 bund ID
BundID

 ORCID

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

→ Ausführung auf Smartphone
erforderlich

Account-Linking

Konto auswählen:

- ▶ **Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt**
- ▶ Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu)

Konto auswählen:

- ▶ Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt
- ▶ **Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)**

Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

Konfigurierbare Heuristik zur
Erkennung von potenziell zu
verknüpfenden Accounts

Account-Linking

Konto auswählen:

- ▶ **Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt**
- ▶ Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu)

Meine Daten Shibboleth Gruppen Projekte

Fehlerhafte Daten können nur bei der Organisation **Karlsruher Institut für Technologie (KIT)**

Name	Weiß, Ulrich
E-Mail-Adresse	ulrich.weiss@kit.edu
eduPersonPrincipalName	kd1927@kit.edu
Persistente ID	YC3[redacted]TcVA=
Lokale UserID-Nummer	900043
Lokale primäre Gruppe	scc (50[redacted]0)
Identityprovider	Karlsruhe Institute of Technology (KIT) - Test

Konto auswählen:

- ▶ Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt
- ▶ **Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)**

Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

Account-Linking

Konto auswählen:

- ▶ **Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt**
- ▶ Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu)

Meine Daten Shibboleth Gruppen Projekte

Fehlerhafte Daten können nur bei der Organisation **Karlsruher Institut für Technologie (KIT)** korrigiert werden.

Name	Weiß, Ulrich
E-Mail-Adresse	ulrich.weiss@kit.edu
eduPersonPrincipalName	kd1927@kit.edu
Persistente ID	YC3[redacted]TcVA=
Lokale UserID-Nummer	900043
Lokale primäre Gruppe	scc (50[redacted])
Identityprovider	Karlsruhe Institute of Technology (KIT) - Test

Konto auswählen:

- ▶ Karlsruhe Institute of Technology (KIT) - Test (kd1927@kit.edu) - Aktuell eingeloggt
- ▶ **Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)**

Helmholtz AAI (gnk2181@fels-test.scc.kit.edu)

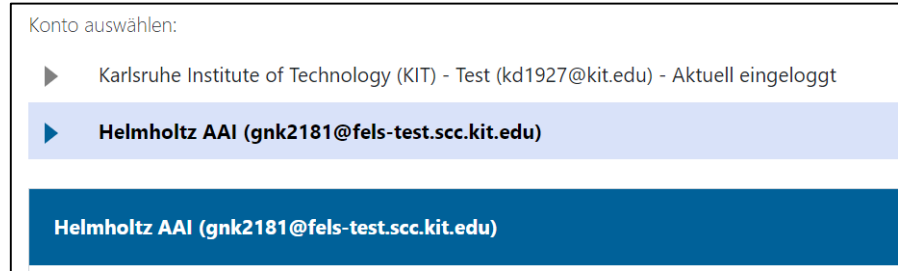
Meine Daten OIDC Gruppen Projekte

Fehlerhafte Daten können nur bei der Organisation **Helmholtz AAI** korrigiert werden.

Name	Weiß, Ulrich
E-Mail-Adresse	ulrich.weiss@kit.edu
eduPersonPrincipalName	gnk2181@fels-test.scc.kit.edu
Subject ID	bc[redacted]01e
Lokale UserID-Nummer	9[redacted]14
Lokale primäre Gruppe	kit (5[redacted]7)
OIDC OP	Helmholtz AAI

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)



UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

EBERTHARD KARLS
UNIVERSITÄT
TÜBINGEN



universität freiburg



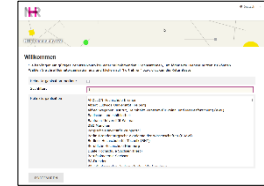
bwIDM



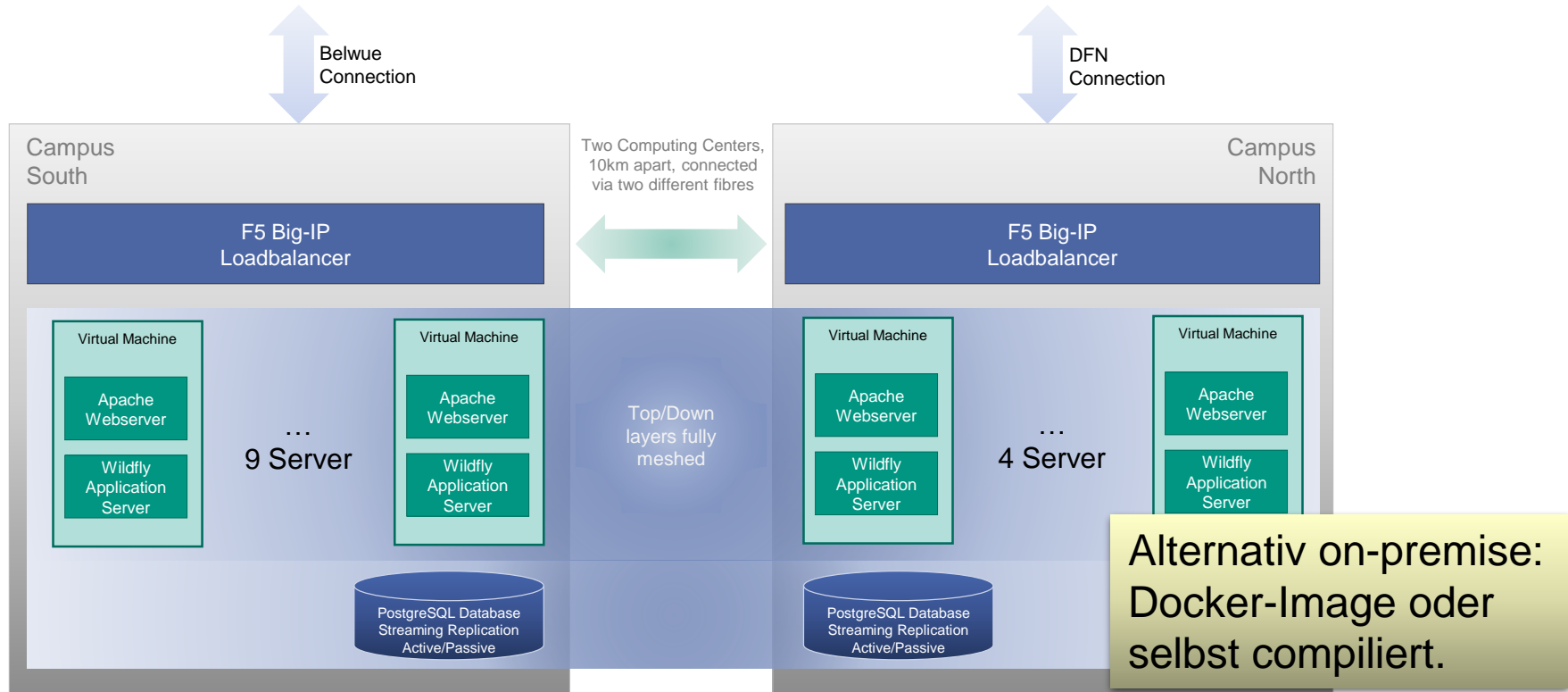
NFDI4ing



nfdi Nationale
Forschungsdaten
Infrastruktur



Mandantenfähiger Betrieb am KIT (2023)



(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