

# RegApp AAI – Community AAI, Infrastructure Proxy

regapp.nfdi-aa1.de

M. Simon, U. Weiß, M. Bonn, F. Kaiser, M. Sayed



# Overview and History

## ■ Federated open source identity management system

- Started as an infrastructure proxy for federated LDAP access in 2012
- Enhanced to a full-featured multiprotocol identity proxy over the years...
- Gradually expanded to meet CAAI requirements
- Used at bwIDM, bwIDM2, NHR, Helmholtz Association, NFDI...

## ■ Mainly developed at the Scientific Computing Center (SCC) at KIT

- Able to react very flexibly to new requirements
- Established development team @KIT

## ■ Currently installed setup manages more than 50,000 registered users from various research institutions (DFN-AAI)

# Typical End User Experience

**bwSync & Share**

Anmeldeoptionen:

Mitglied im bwSync&Share-Verbund \*)

SSO Helmholtz Anwender account

Gast

Service

Federated Login Service

**Willkommen**

Sie wurden von einem Dienst hierher weitergeleitet um sich zu authentifizieren:

**bwSync&Share**

Föderation: Alle

Suchfilter:

Heimatorganisation:

- Deutsches Elektronen-Synchrotron DESY
- Deutsches Klimarechenzentrum GmbH (DKRZ)
- Deutsches Krebsforschungszentrum (DKFZ)
- DLR - Deutsches Zentrum fuer Luft- und Raumfahrt e.V.
- Forschungszentrum Jülich GmbH (FZJ)
- GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel
- Helmholtz Zentrum München GmbH (HMGM)
- Helmholtz-Zentrum Berlin für Materialien und Energie GmbH (HZB)
- Helmholtz-Zentrum Dresden-Rossendorf e.V. (HZDR)
- Helmholtz-Zentrum Potsdam Deutsches Geoforschungszentrum GFZ
- Helmholtz-Zentrum für Infektionsforschung GmbH [HZI]
- Helmholtz-Zentrum für Umweltforschung GmbH - UFZ IAP
- Karlsruher Institut für Technologie (KIT)
- Max-Deibüick-Centrum für molekulare Medizin

Heimatorganisation merken:

FORTFAHREN

RegApp Instance

**KIT**

Impressum Datenschutz Datenschutzerklärung

Das SCC [Stiftungsorgane](#)

Shibboleth Identity Provider

**Anmelden**

Sie wurden vom Serviceprovider **Föderierte Dienste am KIT** hierher weitergeleitet und befinden sich nun auf einem Server des KIT. Bitte melden Sie sich mit Ihrem KIT-Account (z.B. ab1234 als Mitarbeiter oder xxxxx als Student) und Ihrem Passwort an.

Benutzername:

Passwort:

Wenn Ihr Computer ein Shibboleth-Element als Ihre Heimatorganisation hat, können Sie sich mit Ihrem Shibboleth-Konto anmelden.

**ANMELDEN**

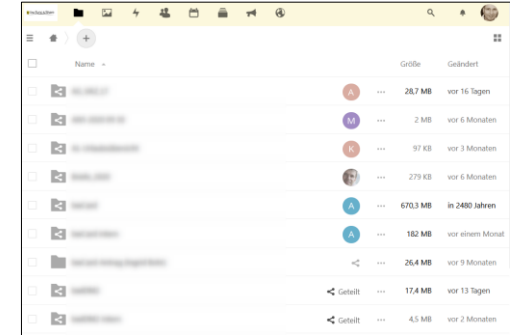
Die oben bezeichnete Webseite des Serviceanbieters bietet Sie, sich bei Ihrer Heimatorganisation anzumelden.

Sie bekommen auf der Folgebseite die Daten angezeigt, um deren Übermittlung der Serviceprovider bietet. Sie können dies bestätigen und damit den Vorgang fortsetzen oder durch Schließen des Fensters ablehnen. Haben Sie denselben Service bereits einmal genutzt, werden Sie nur dann erneut nach einer Bestätigung gefragt, wenn sich der Datenumfang oder der Name des Serviceanbieters geändert hat. Wenn Sie auf jeden Fall nochmal sehen möchten, welche Daten zur Übermittlung vorgesehen sind, aktivieren Sie bitte die entsprechende Option.

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

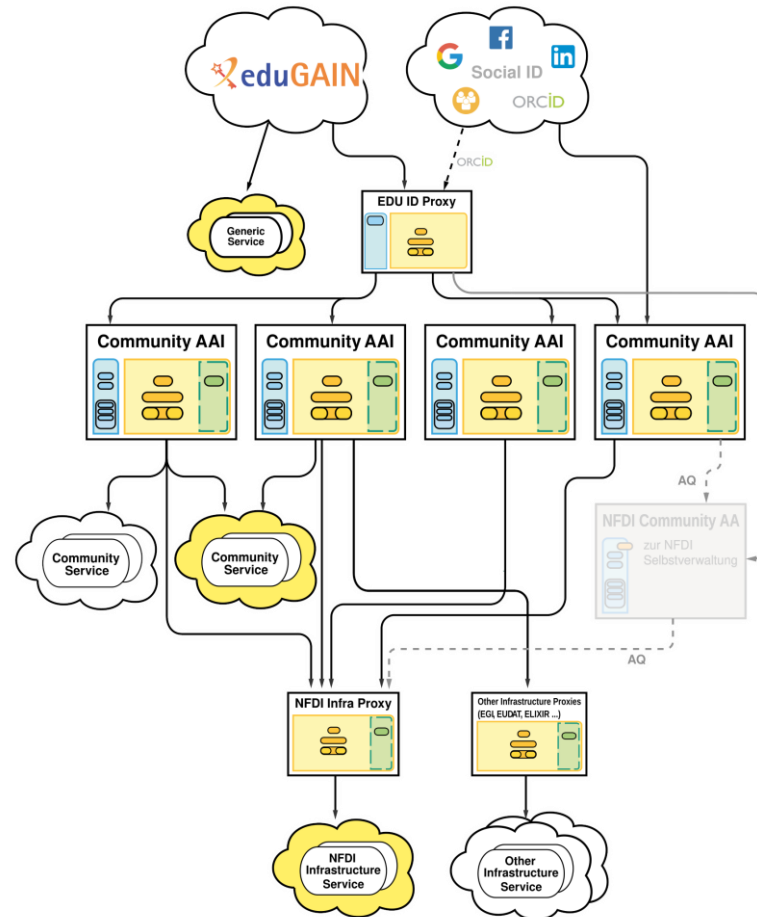
**ANMELDEN**

Home IdP

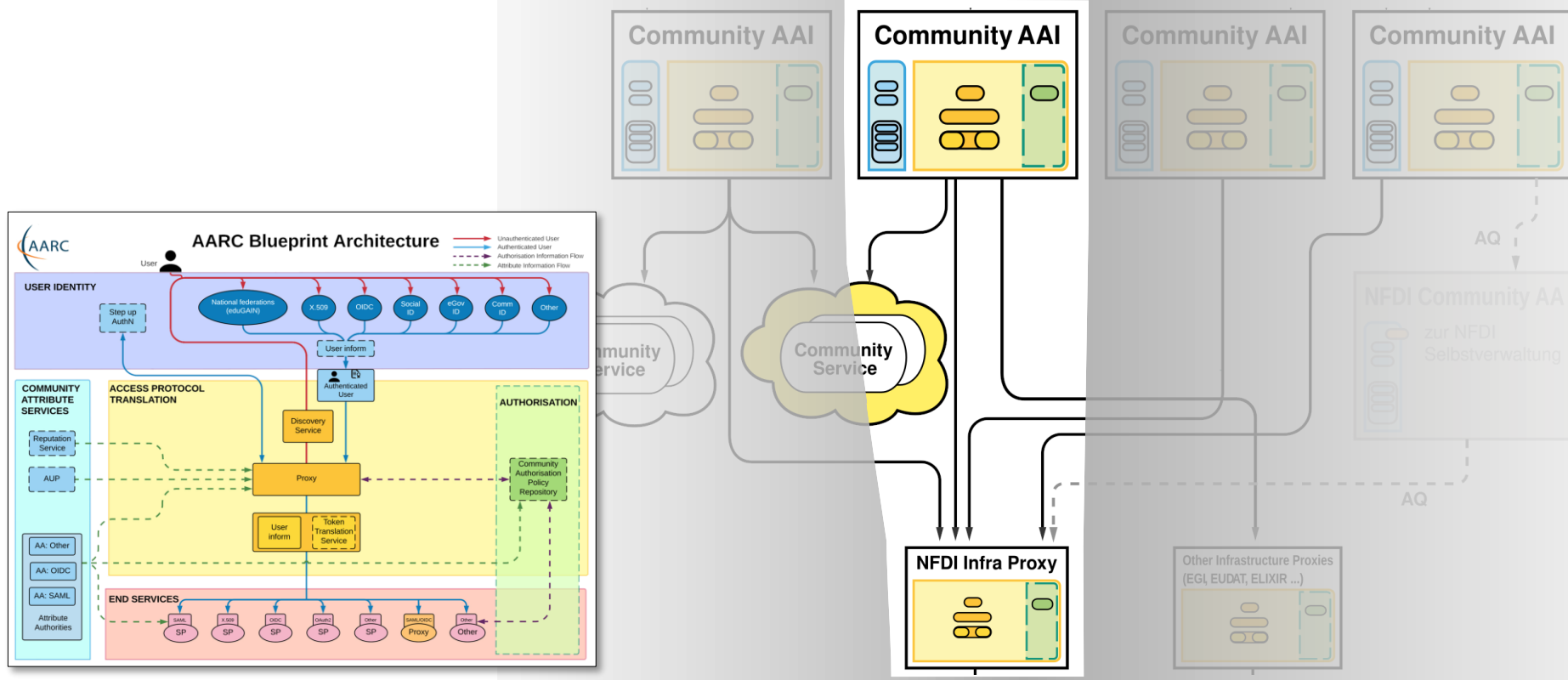


Service

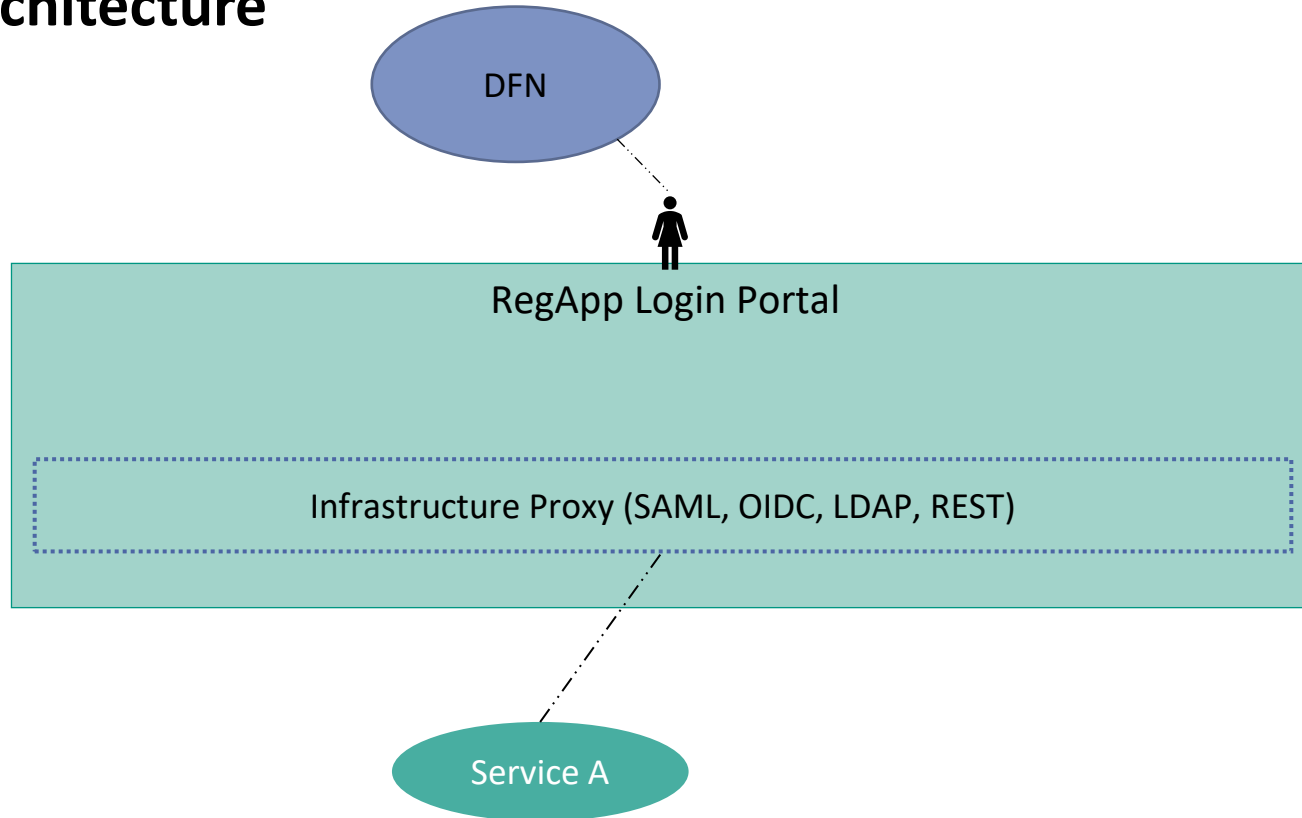
# Classification



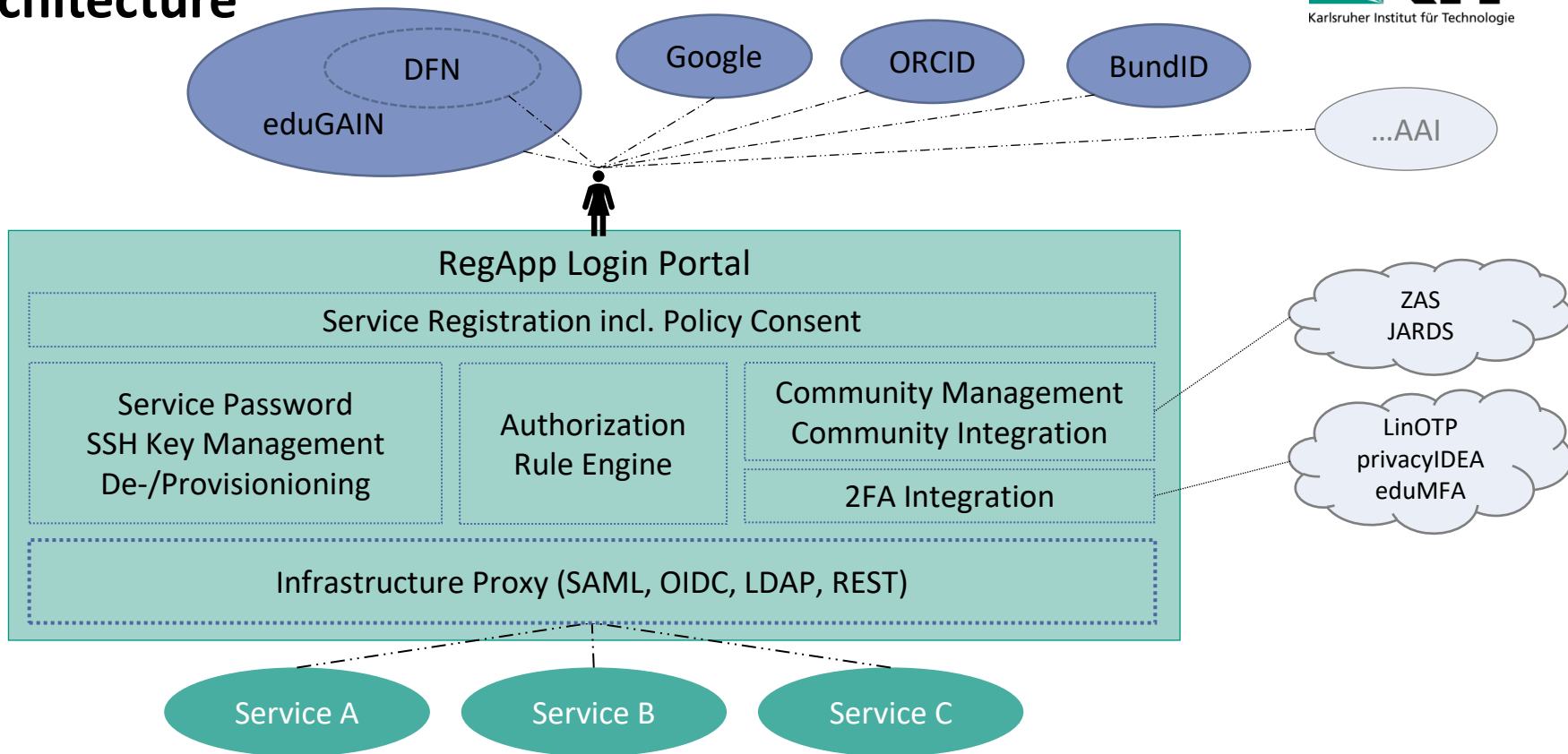
# Classification



# Architecture



# Architecture



# Feature Overview

## ■ Community AAI for Single Sign On Environments

- Transparent connection of SAML federations
- Provisioning and deprovisioning (linked user accounts, with SAML AQtS)
- End user portal for service registration and group management
- Infrastructure proxy for non web services (LDAP, REST)
- SSO protocol proxy OIDC ↔ SAML



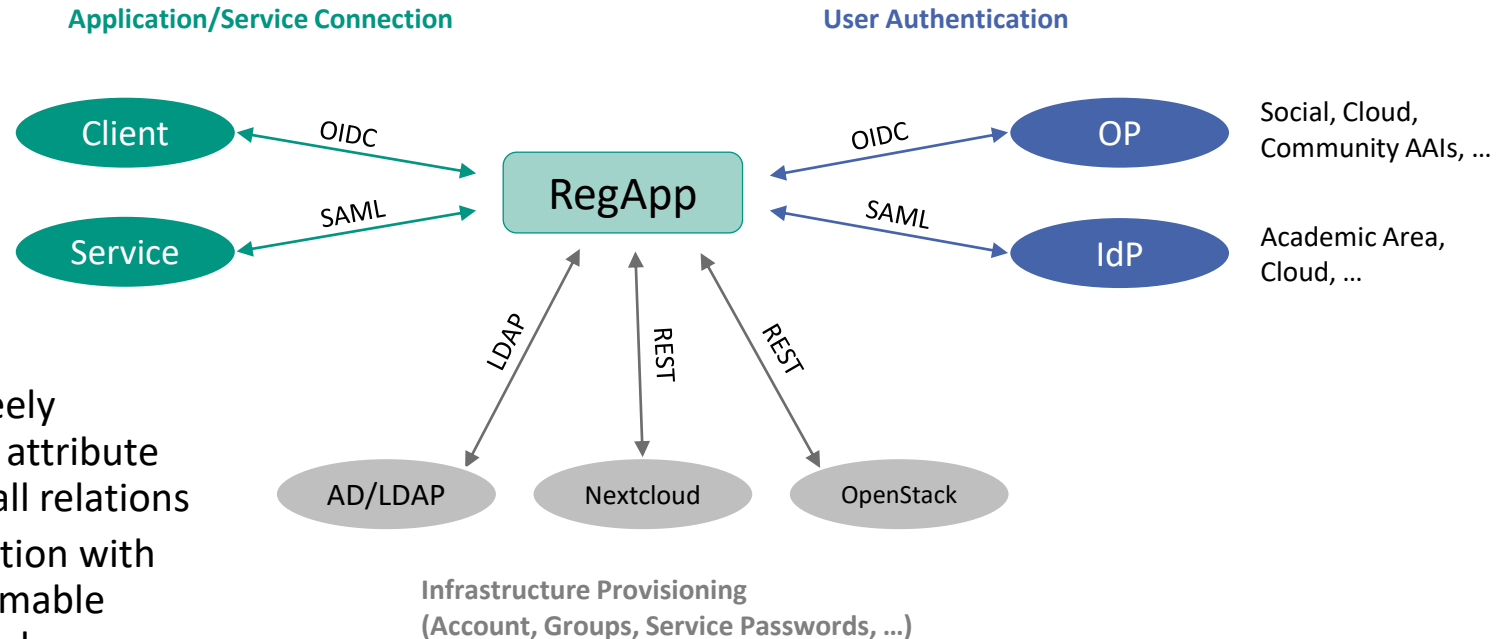
Authentication and Authorisation for  
Research and Collaboration  
<https://aarc-project.eu/>

## ■ Additional features

- Management of SSH keys and service passwords (CLI/HPC login)
- Multifactor authentication (TOTP, also available for CLI/HPC logins)
- **Freely programmable authorization rules and attribute processing**



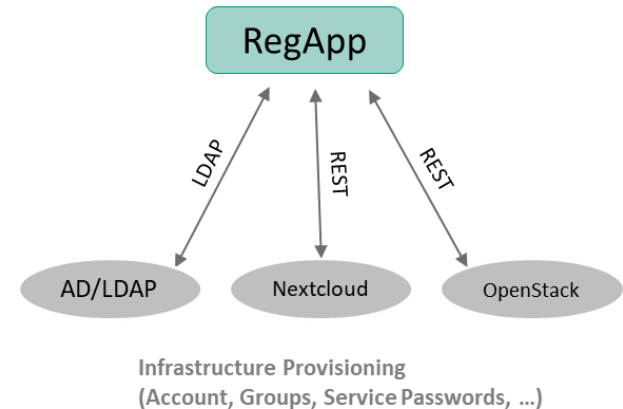
# Multiprotocol Proxy



- Flexible and freely programmable attribute processing on all relations
- Service connection with freely programmable authorization rules

# Infrastructure Proxy

- Wide provisioning AND deprovisioning
- Current modules
  - LDAP (attributes with templates or scripted)
  - Samba
  - OpenStack
  - Nextcloud
  - Powerfolder
- In development
  - Gitlab
- If needed: **We can provide NFDI LDAP as a service**



# End user's view: Login

## ■ Select home organization

- DFN AAI
- Other AAI's
- Social

## ■ Selection can be stored for a faster next login




Federated Login Service

### 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  
karl

	Karlsruher Institut für Technologie (KIT)
	Hochschule Karlsruhe
	PH Karlsruhe
	DHBW Karlsruhe
	FIZ Karlsruhe

Oder nutzen Sie einen alternativen Anbieter:



HIFIS  
Helmholtz AAI



ORCID ID






KIT  
Karlsruhe Institute of Technology  
Karlsruher Institut für Technologie (KIT)

# End user's view: MFA

- **MFA and token management integrated in RegApp**
  - Home IdPs without MFA
  - Services which need MFA but cannot do it by themselves
- **Self-service registration** (via QR-codes), Backup TANS, TOTP
- Supported backends: LinOTP, privacyIDEA, eduMFA

### Liste zweiter Faktor

 <p>Tokenotyp: Backup TAN Liste Aktiv: Ja</p>	 <p>Tokenotyp: Smartphone App Aktiv: Ja</p>	 <p>Tokenotyp: Hardware TOTP Aktiv: Ja</p>
--	---	---

# End user's (PI) view: Project Management

## Projekte

ID	Kurzname	Name ↑↓
1276221	agropro	AgroPro
1249981	bip1	Big Important
1243701	calc1	Calc Projekt 1
1276825	testproject001	Test Projekt 00

Neues Projekt anlegen

## Lokales Projekt (SSH-Test Service): AgroPro

**Eigenschaften**

ID: 1276221

Name: AgroPro

Gruppenname: agropro

Dienste: SSH-Test Service (ACTIVE)  
bwDataArchive Test (ACTIVE)

**Aktiv verbunden**

Das Projekt ist mit dem Dienst verbunden.

Spezifischer Gruppenname für das Projekt und den Dienst: ssh-project-agropro

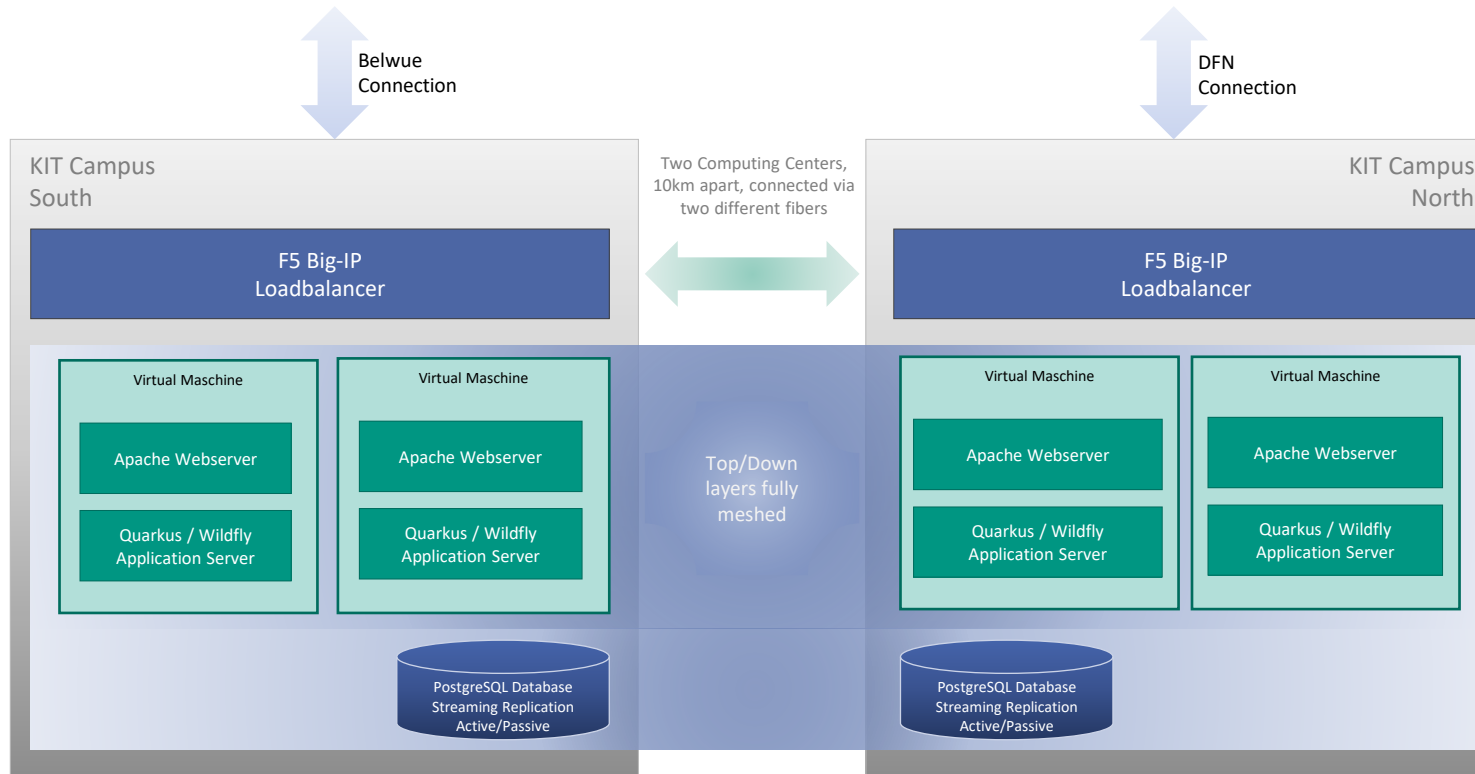
**Projekt Administratoren**

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

**Projekt Mitglieder**

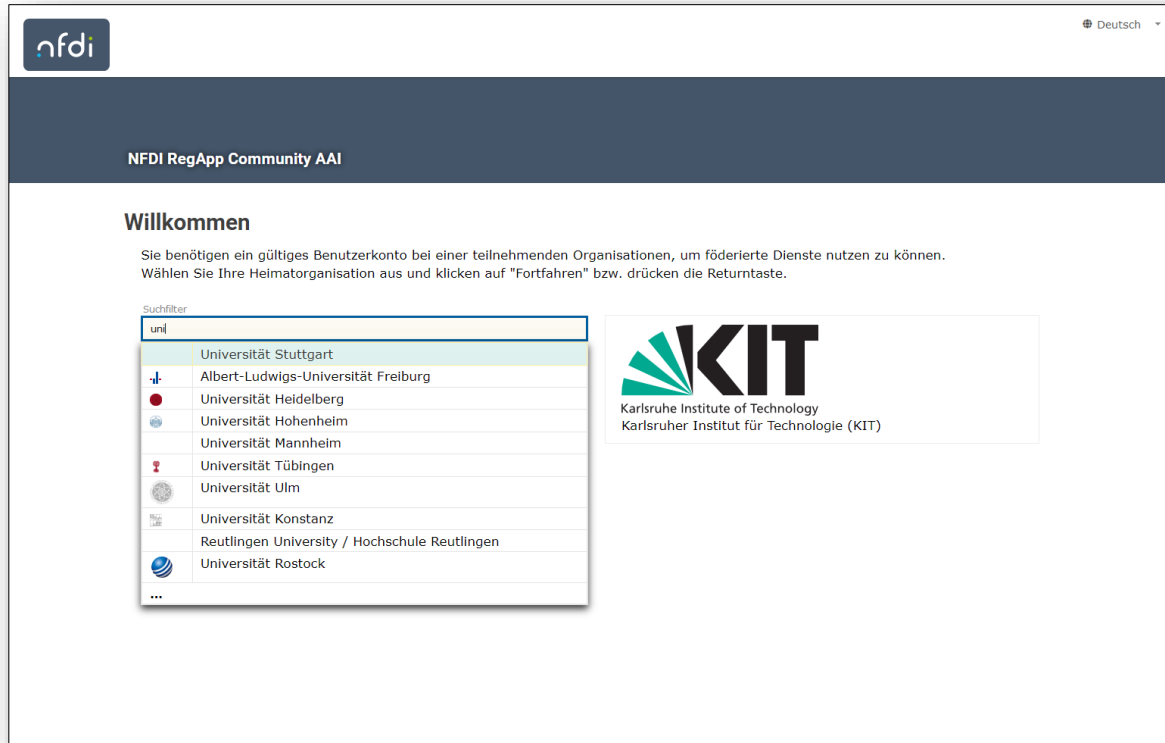
ID	Name ↑↓	Nachname ↑↓	Vorname ↑↓	Typ
1208133	<input type="text"/>	<input type="text"/>	<input type="text"/>	MEMBER

# RegApp for NFDI: 4 Servers / 2 Locations



Setup architecture approved since 2013 in bwIDM with ~50k users, connected to HPC systems and standard services

# RegApp for NFDI: Customized Frontend



The screenshot shows the NFDI RegApp Community AAI interface. At the top left is the 'nfdi' logo, and at the top right is a language selector set to 'Deutsch'. Below the header is a dark blue bar with the text 'NFDI RegApp Community AAI'. The main content area starts with a 'Willkommen' (Welcome) section, followed by a paragraph explaining that a valid user account is needed and that users should select their home organization. Below this is a search filter box containing 'uni', which has triggered a dropdown list of German universities. To the right of the search filter is a placeholder for the Karlsruhe Institute of Technology (KIT) logo and name.

nfdi Deutsch











NFDI RegApp Community AAI


## Willkommen

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

Suchfilter

uni

	Universität Stuttgart
	Albert-Ludwigs-Universität Freiburg
	Universität Heidelberg
	Universität Hohenheim
	Universität Mannheim
	Universität Tübingen
	Universität Ulm
	Universität Konstanz
	Reutlingen University / Hochschule Reutlingen
	Universität Rostock
...	



Karlsruhe Institute of Technology  
Karlsruher Institut für Technologie (KIT)

Production-ready  
setup for NFDI  
[regapp.nfdi-aa1.de](https://regapp.nfdi-aa1.de)

# Current and Future Developments

- **Improving the community functionality (well progressed)**
  - Project and virtual organization management
  - Active group membership provision
  - Invitation of external persons by email/link
  - Improve user experience when linking accounts
- **Support of modern authentication methods (planned)**
  - FIDO2 keys for SSH login
  - Webauthn/Passkeys for user-/passwordless web login
- **Internal redesign/modularisation (ongoing...)**
  - Wildfly, J2EE 8 → Quarkus framework, Jakarta EE 10
  - Server-rendered management webpages → SPA with Angular





# Further Information

## ■ RegApp

- Deutsch: <https://www.scc.kit.edu/dienste/regapp>
- English: <https://www.scc.kit.edu/en/services/regapp>

## ■ Downloads

- Gitlab: <https://gitlab.kit.edu/kit/reg-app/regapp>
- Docker: <https://gitlab.kit.edu/kit/reg-app/regapp-docker>

## ■ References

- In NFDI context: <https://regapp.nfdi-aa.de>

## ■ Contact

- [regapp-support@lists.kit.edu](mailto:regapp-support@lists.kit.edu)
- [uli.weiss@kit.edu](mailto:uli.weiss@kit.edu) and [michael.simon@kit.edu](mailto:michael.simon@kit.edu)