

RegApp AAI – Community AAI, Infrastructure Proxy

regapp.nfdi-aai.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...

■ 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 A user 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 für Luft- und Raumfahrt e.V.
- Forschungszentrum Jülich GmbH (FZJ)
- GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel
- Helmholtz Zentrum München GmbH (HMGU)
- 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-DeBücker-Zentrum für molekulare Medizin

Heimatorganisation merken: ☐

FORTFAHREN

RegApp Instance

Service

Name	Größe	Erstellt
...	28,7 MB	vor 16 Tagen
...	2 MB	vor 6 Monaten
...	97 KB	vor 3 Monaten
...	279 KB	vor 6 Monaten
...	670,3 MB	in 2480 Jahren
...	182 MB	vor einem Monat
...	26,4 MB	vor 9 Monaten
...	17,4 MB	vor 13 Tagen
...	4,5 MB	vor 2 Monaten

Service

KIT

Impressum Datenschutz Barrierefreiheit Das SCC Stellenangebote

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:

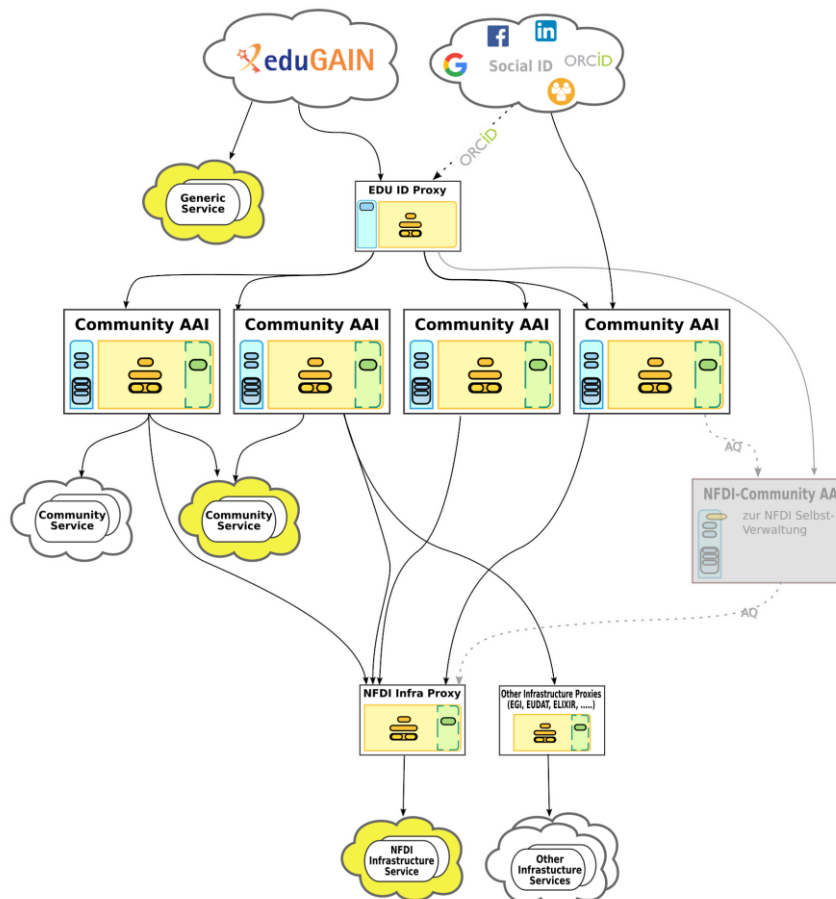
Wenn Ihr Computer in der KIT-Cloud vernetzt ist, können Sie sich mit Ihrem Windows-Konto anmelden.

Sie können auf der Folgende die Daten angezeigt, um deren Übermittlung der Serviceprovider bietet. Sie können dies bestätigen und damit den Vorgang fortsetzen oder durch Schließen des Fensters ablehnen. In beiden Fällen 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 links die entsprechende Option.

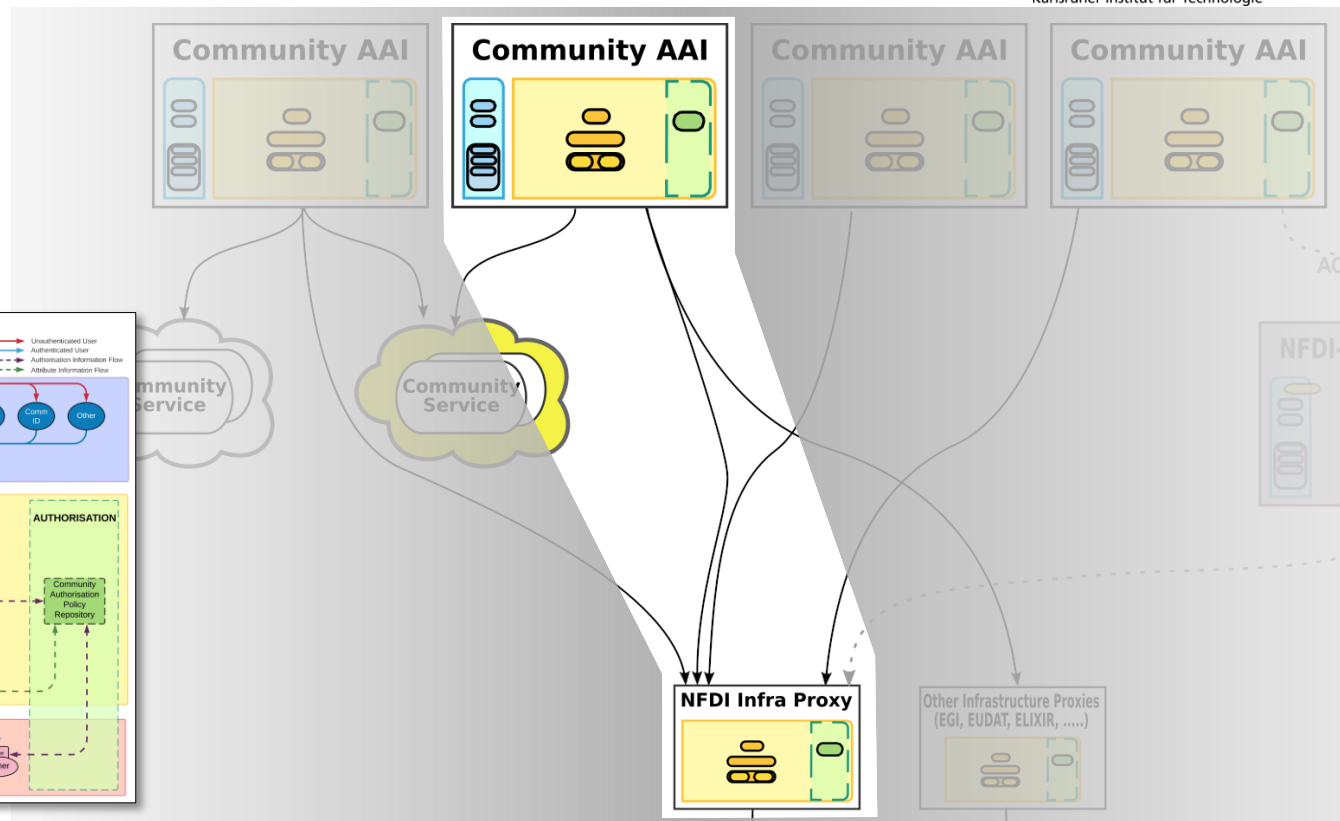
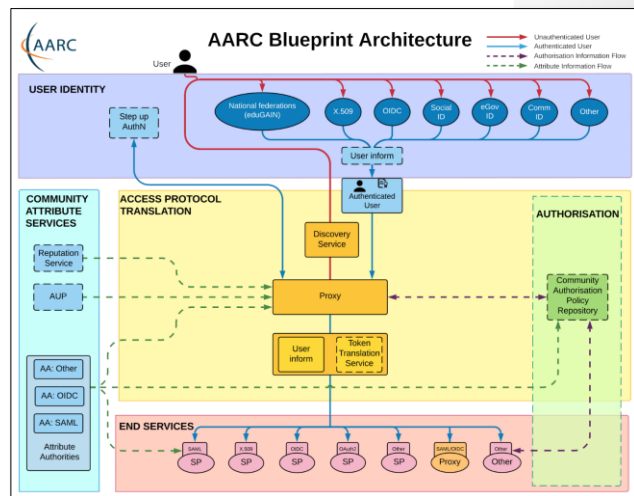
☐ Bitte zeige mir für diesen Serviceprovider erneut an, welche Daten gesendet werden sollen.

Home IdP

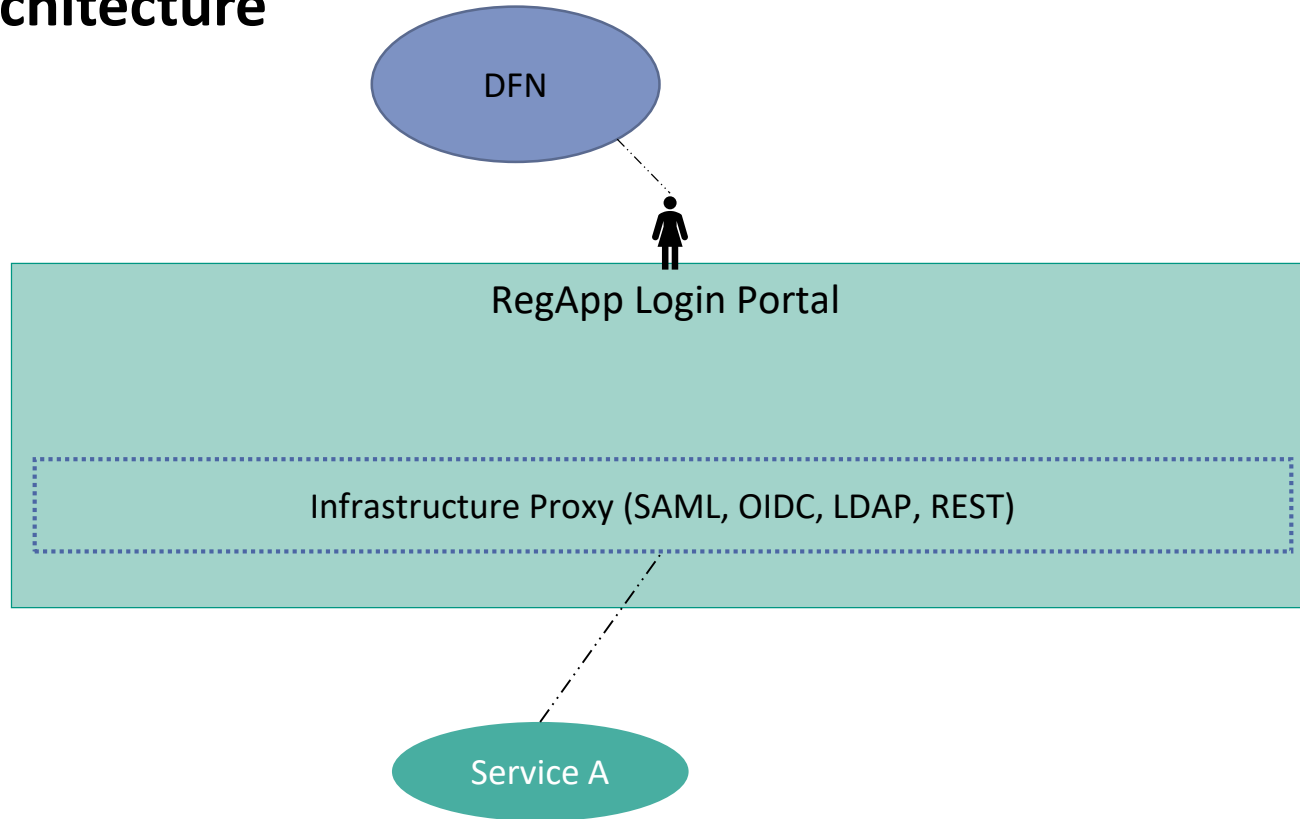
Classification



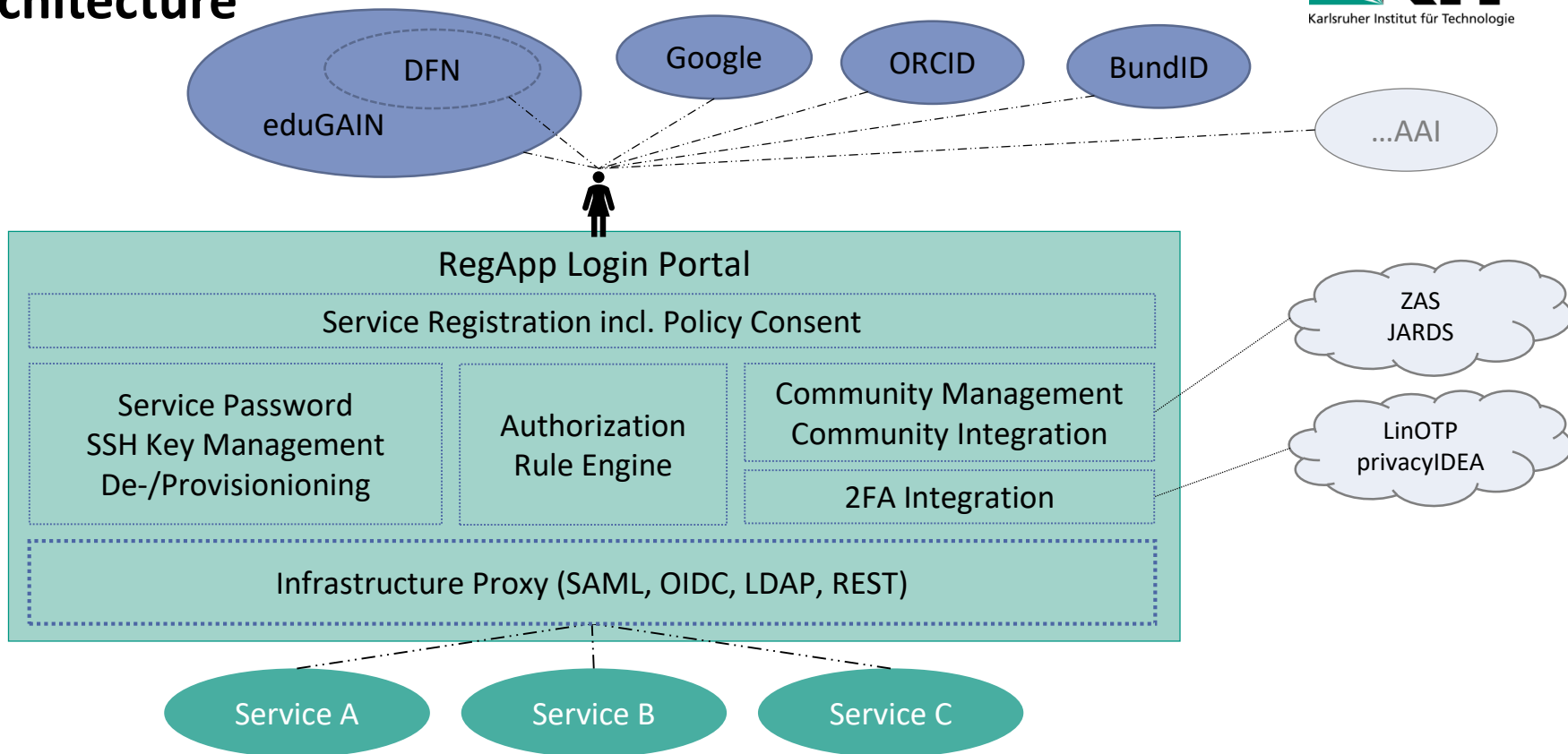
Classification



Architecture



Architecture



Feature Overview

■ Community AAI for Single Sign On Environments

- Transparent connection of SAML federations
- Provisioning and deprovisioning (linked user identities, 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

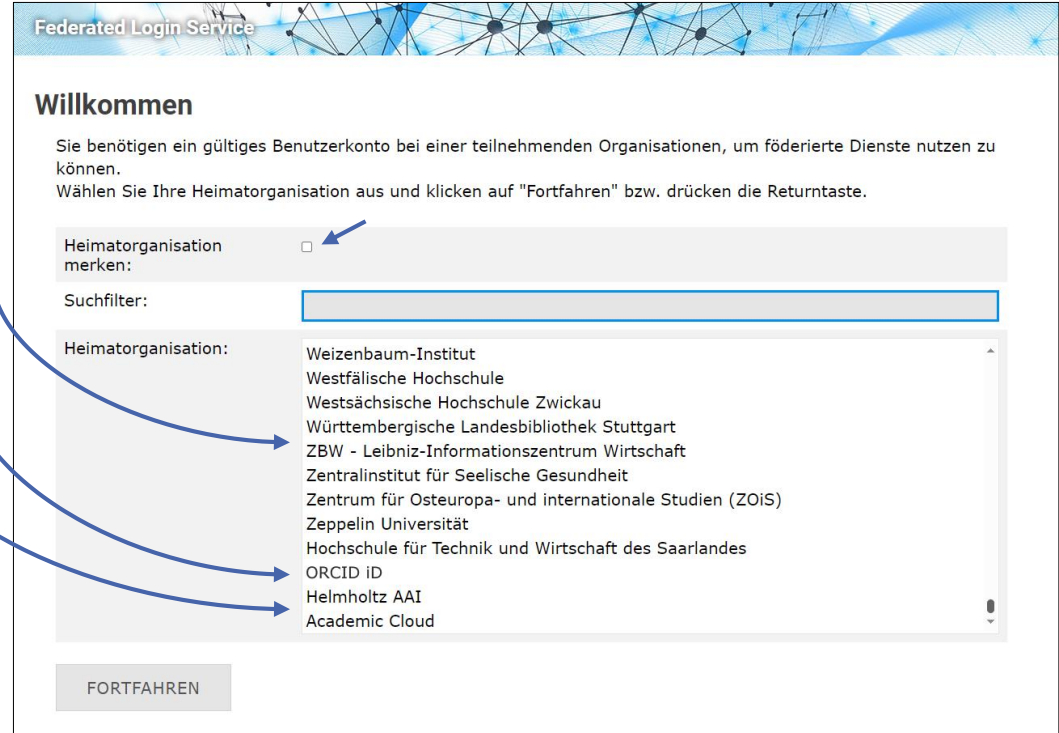
- Management of SSH keys and service passwords (CLI/HPC login)
- Multifactor authentication (LinOTP/privacyIDEA, also available for CLI/HPC logins)
- **Freely programmable authorization rules and attribute processing**

End user's view: Login

■ Select home organization

- DFN AAI
- Social
- Other AAI's

■ 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 Heimorganisation aus und klicken auf "Fortfahren" bzw. drücken die Returnstaste.

Heimorganisation merken: ☐

Suchfilter:

Heimorganisation:

- Weizenbaum-Institut
- Westfälische Hochschule
- Westsächsische Hochschule Zwickau
- Württembergische Landesbibliothek Stuttgart
- ZBW - Leibniz-Informationszentrum Wirtschaft
- Zentralinstitut für Seelische Gesundheit
- Zentrum für Osteuropa- und internationale Studien (ZOIS)
- Zeppelin Universität
- Hochschule für Technik und Wirtschaft des Saarlandes
- ORCID iD
- Helmholtz AAI
- Academic Cloud

FORTFAHREN

End user's view: Stored Data

View of the stored Data

- RegApp internal/generated attributes
- Details about attributes delivered by home IdP
- Group and project memberships

Meine Daten
Shibboleth
Gruppen
Projekte

Hier können Sie alle Daten einsehen, die über Sie gespeichert sind. Sollten diese Daten für eine Korrektur bei der Organisation veranlassen, von der die Daten geliefert werden.
Daten von: **Karlsruher Institut für Technologie (KIT)**

Name	Bonn, Matthias
E-Mail-Adresse	matthias.bonn@kit.edu
eduPersonPrincipalName	
Persistente ID	
Lokale UserID-Nummer	
Lokale primäre Gruppe	scc (12345)
Identityprovider	Karlsruher Institut für Technologie (KIT)

Meine Daten
Shibboleth
Gruppen
Projekte

Diese Daten wurde aus folgender SAML Datenlieferung von Ihrem Shibboleth Identity Provider erzeugt. Die letzte Aktualisierung erfolgte am 24.01.2024 08:34

Name	Wert
urn:oid:0.9.2342.19200300.100.1.3	matthias.bonn@kit.edu
urn:oid:0.9.2342.19200300.100.1.1	
urn:oid:2.5.4.42	Matthias
urn:oid:1.3.6.1.4.1.25178.1.2.9	kit.edu
urn:oid:2.5.4.11	SCC
http://bwidm.de/bwidmOrgId	ka
urn:oid:1.3.6.1.4.1.5923.1.1.1.16	https://orcid.org/0000-0002-7867-8004
urn:oid:1.3.6.1.1.1.1.0	
urn:oid:1.3.6.1.1.1.1.1	12345
urn:oid:1.3.6.1.4.1.5923.1.1.1.11	https://refeds.org/assurance/IAP/local-enterprise;https://refeds.org/assurance;https://refeds.org/assurance/ATP/ePA-1m;https://refeds.org/assurance/IAP/low;https://refeds.org/assurance/IAP/medium;https://refeds.org/assurance/ID/eppn-unique-no-reassign;https://refeds.org/assurance/profile/cappuccino;https://refeds.org/assurance/ID/unique;https://refeds.org/assurance/ATP/ePA-1d
urn:oid:1.3.6.1.4.1.5923.1.1.1.13	
urn:oid:1.3.6.1.4.1.57378.1.2	
urn:oid:1.3.6.1.4.1.57378.1.4	2024-08-31
urn:oid:2.5.4.4	Bonn
urn:oid:1.3.6.1.4.1.57378.1.1	kit.edu
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	
urn:oid:1.3.6.1.4.1.5923.1.1.1.9	employee@kit.edu;member@kit.edu
urn:oid:1.3.6.1.4.1.5923.1.1.1.7	http://bwidm.scc.kit.edu/entitlement/lsdf-dis;http://bwidm.de/entitlement/bwUniCluster;http://bwidm.de/entitlement/bwGRiD;http://bwidm.de/entitlement/bwLSDF-FileService;http://bwidm.de/entitlement/bwLSDF-SyncShare;urn:geant:kit.edu:res:fels:ldp-admin

Klicken Sie hier, um alle persönlichen Daten löschen zu lassen. Der Link öffnet eine neue Seite mit einer Erklärung, was genau gelöscht wird.
[Alle Meine Daten löschen](#)

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 and privacyIDEA

Liste zweiter Faktor

 Backup-TAN-Liste	 Smartphone-App	 Hardware-TOTP
 Tokenotyp: Backup TAN Liste Aktiv: Ja	 Tokenotyp: Smartphone App Aktiv: Ja	 Tokenotyp: Hardware TOTP Aktiv: Ja

End user's view: Account Linking

- User driven, by clicking „Add account...”
- Semi-automatic by specified rules

Choose account:

ls1947@kit.edu - Karlsruhe Institute of Technology (KIT) - Test (???currently_logged_id???)
mar8138@fels-test.scc.kit.edu - ORCID

Meine DatenShibbolethGruppenProjekte

Hier können Sie alle Daten einsehen, die über Sie gespeichert sind. Sollten diese Daten fehlerhaft sein können Sie eine Korrektur bei der Organisation veranlassen, von der die Daten geliefert werden.
Daten von: **Karlsruher Institut für Technologie (KIT)**

Name	Simon, Michael
E-Mail-Adresse	michael.simon@kit.edu
eduPersonPrincipalName	ls1947@kit.edu
Persistente ID	uxkAz855MQSerV3iacrxcAOd2DA=

Community Management: Typical Workflow



VO Manager / Principal Investigator (PI)

Creates Project

Requests
Service/Resource

Invites Project
Members

Manages Project Members

HPC Admin (e.g. HoreKa)

Release Project
to Resource

Service Admin (e.g. LSDF, Gitlab)

Release Project
to Resource

Project Members

Accept Invitation

Do Project Work

Community Management: Projects and Services

Föderierte Dienste am KIT (TEST)

Lokales Projekt: Big Important Project 1

Eigenschaften

ID:	1249981
Name:	Big Important Project 1
Gruppenname:	bip1
Dienste:	

Hier können Sie die Nutzung einer Resource für Ihr Projekt bearbeiten.

Laden Sie Mitglieder für Ihr Projekt ein. Die Einladung erfolgt über...

Zurück

Projekt Mitglieder

Name	Nachname	Vorname
Keine Datensätze gefunden.		

Projekt Administratoren

ID	Name
1208133	

Föderierte Dienste am KIT (TEST)

Dienstnutzung für Projekt: Big Important Project 1

Eigenschaften

ID:	1249981
Name:	Big Important Project 1
Dienste auswählen:	☒ SSH-Test Service
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 Invitation

Föderierte Dienste am KIT (TEST)

Mitglieder einladen: Big Important Project 1

Laden Sie Mitglieder zu Ihrem Projekt ein.

Token	E-Mail-Adresse	Gültig bis
eo3j80sgubfi4fp4aq5irmv7n2		2023-05-30 11:17

Einladung per E-Mail

Sie können eine Projekteinladung erstellen, die in Ihrem Namen per E-Mail mit dem sie oder er an Ihrem Projekt teilnehmen kann.

E-Mail Adresse

Empfänger

Absender E-Mail

Absender Name

Einladung Schicken

Föderierte Dienste am KIT (TEST)

Projekteinladung

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

Token

fskk2f5a6713336mjr064d37

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.

Annehmen

Ablehnen

Community Management: Group management

■ Manage group memberships

- Standard operations
- Search/Filter operations
- Subgroups possible

Föderierte Dienste am KIT

Interne Gruppe (Dummy Service 1): test1112

Eigenschaften

Name	test1112
GID	501363
Status	ACTIVE
Dienste	Dummy Service 1

MITGLIEDER ANPASSEN

Mitglieder

eduPersonPrincipalName	E-Mail-Adresse	Nachname	Name

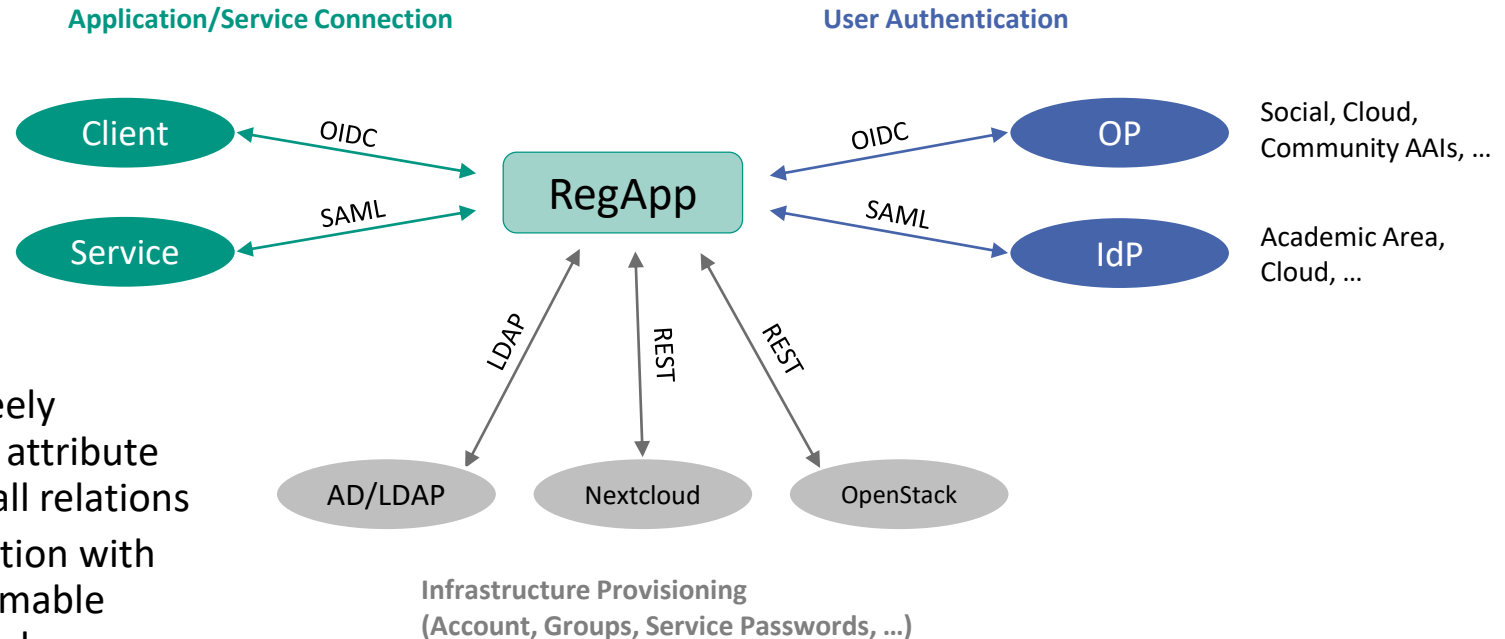
Untergruppen:

Effektive Mitglieder:

Werkzeuge

GRUPPE LÖSCHEN

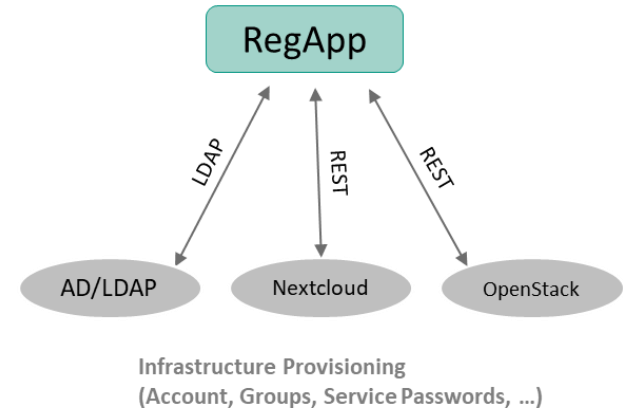
Multiprotocol Proxy



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

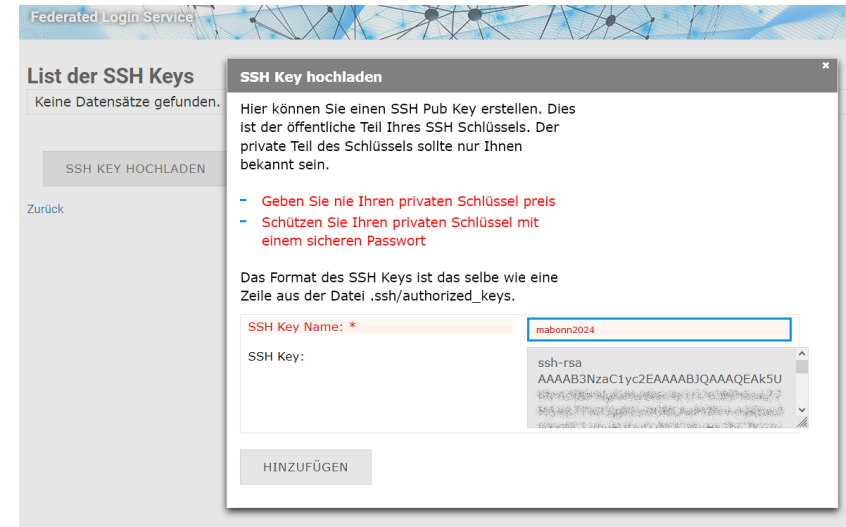
Infrastructure Proxy

- 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**

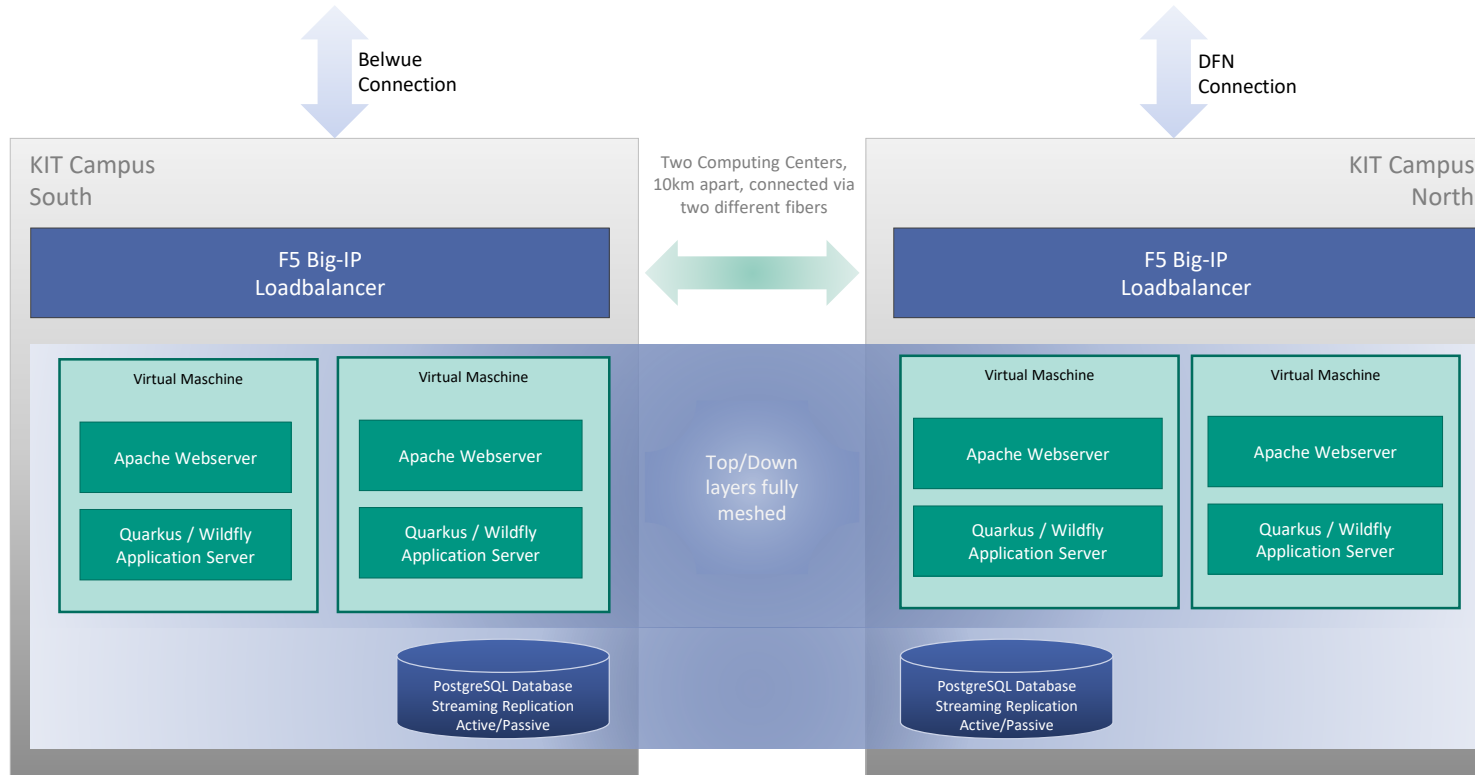


One more thing: uncategorized Features

- More focus on account linking in the near future
 - Identity can have multiple accounts
- More self-service for project owners (current development)
 - Create OIDC credentials for a project
 - Manage subprojects
- Policies for project participants
 - Managable by project owners
- Generic attribute sources for additional account info
 - HTTP plain text or JSON
 - LDAP
- S/MIME signed e-mails
- User managed ssh-keys (used for login to HPC systems, can also run combined with MFA)

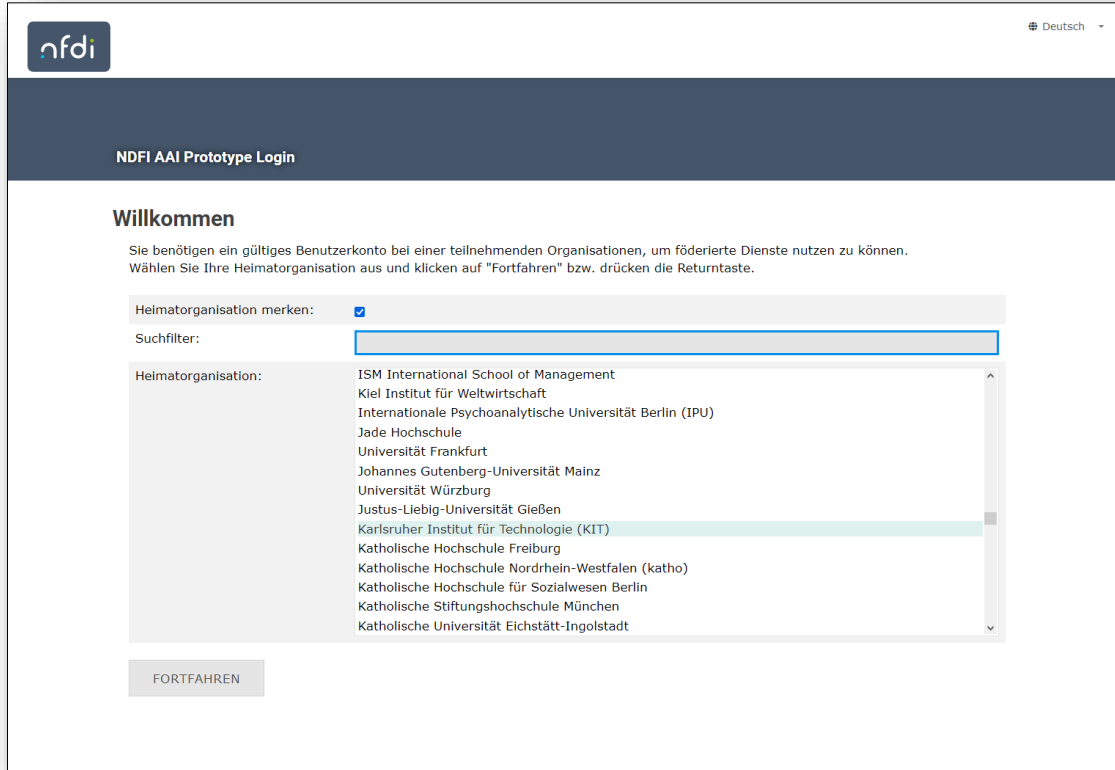


RegApp for NFDI: 4 Servers / 2 Locations



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 AAI Prototype Login' page. At the top left is the 'nfdi' logo, and at the top right is a language selector set to 'Deutsch'. Below the header, the page title 'NFDI AAI Prototype Login' is displayed. The main section is titled 'Willkommen' and contains a welcome message: '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 Returntaste.' Below this, there is a form with a checkbox 'Heimatorganisation merken:' which is checked. A search filter input field is labeled 'Suchfilter:'. Below the search filter is a list of participating organizations under the label 'Heimatorganisation:'. The list includes: ISM International School of Management, Kiel Institut für Weltwirtschaft, Internationale Psychoanalytische Universität Berlin (IPU), Jade Hochschule, Universität Frankfurt, Johannes Gutenberg-Universität Mainz, Universität Würzburg, Justus-Liebig-Universität Gießen, Karlsruher Institut für Technologie (KIT) (highlighted in light green), Katholische Hochschule Freiburg, Katholische Hochschule Nordrhein-Westfalen (katho), Katholische Hochschule für Sozialwesen Berlin, Katholische Stiftungshochschule München, and Katholische Universität Eichstätt-Ingolstadt. At the bottom of the form is a button labeled 'FORTFAHREN'.

nfdi

Deutsch

NFDI AAI Prototype Login

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 Returntaste.

Heimatorganisation merken: ☒

Suchfilter:

Heimatorganisation:

- ISM International School of Management
- Kiel Institut für Weltwirtschaft
- Internationale Psychoanalytische Universität Berlin (IPU)
- Jade Hochschule
- Universität Frankfurt
- Johannes Gutenberg-Universität Mainz
- Universität Würzburg
- Justus-Liebig-Universität Gießen
- Karlsruher Institut für Technologie (KIT)
- Katholische Hochschule Freiburg
- Katholische Hochschule Nordrhein-Westfalen (katho)
- Katholische Hochschule für Sozialwesen Berlin
- Katholische Stiftungshochschule München
- Katholische Universität Eichstätt-Ingolstadt

FORTFAHREN

Production-ready
setup for NFDI
regapp.nfdi-aai.de

Current and Future Developments

■ Improving the community functionality (in progress)

- 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-aai.de>

■ Contact

- regapp-support@lists.kit.edu
- uli.weiss@kit.edu and michael.simon@kit.edu