



# HIFIS

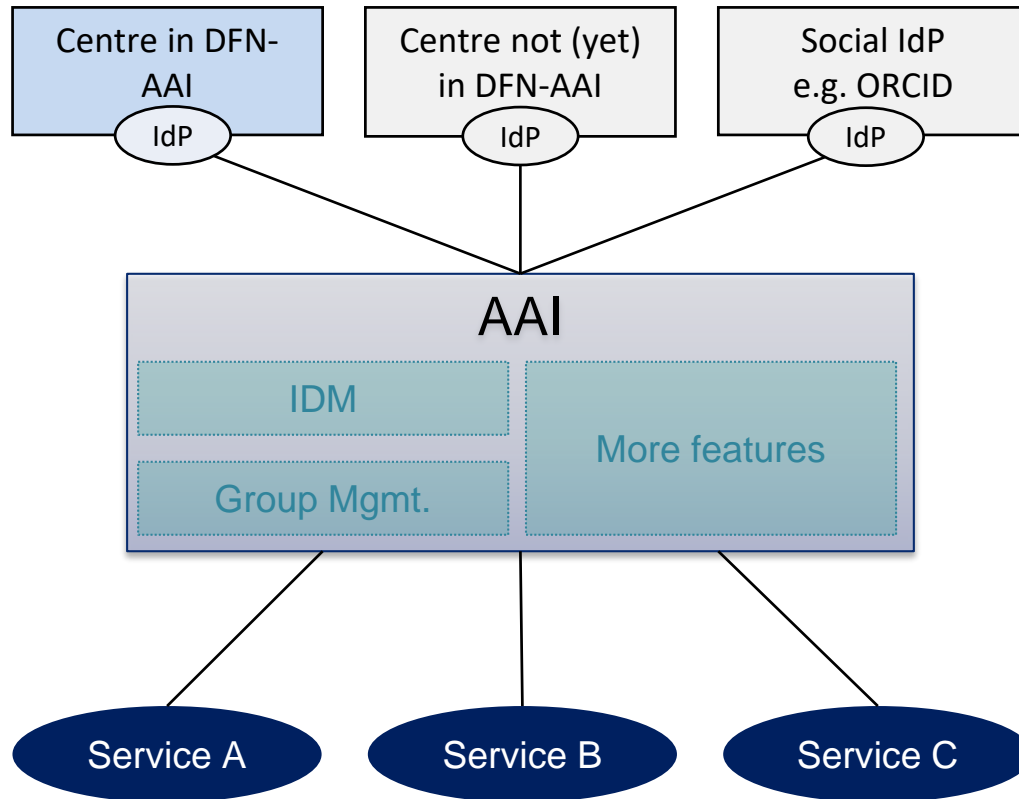
HELMHOLTZ  
FEDERATED  
IT SERVICES

## OVERVIEW OF AAI IN HELMHOLTZ

Sander Apweiler, Johannes Reppin, Uli Weiß

# Helmholtz Authentication & Authorization Infrastructure (AAI)

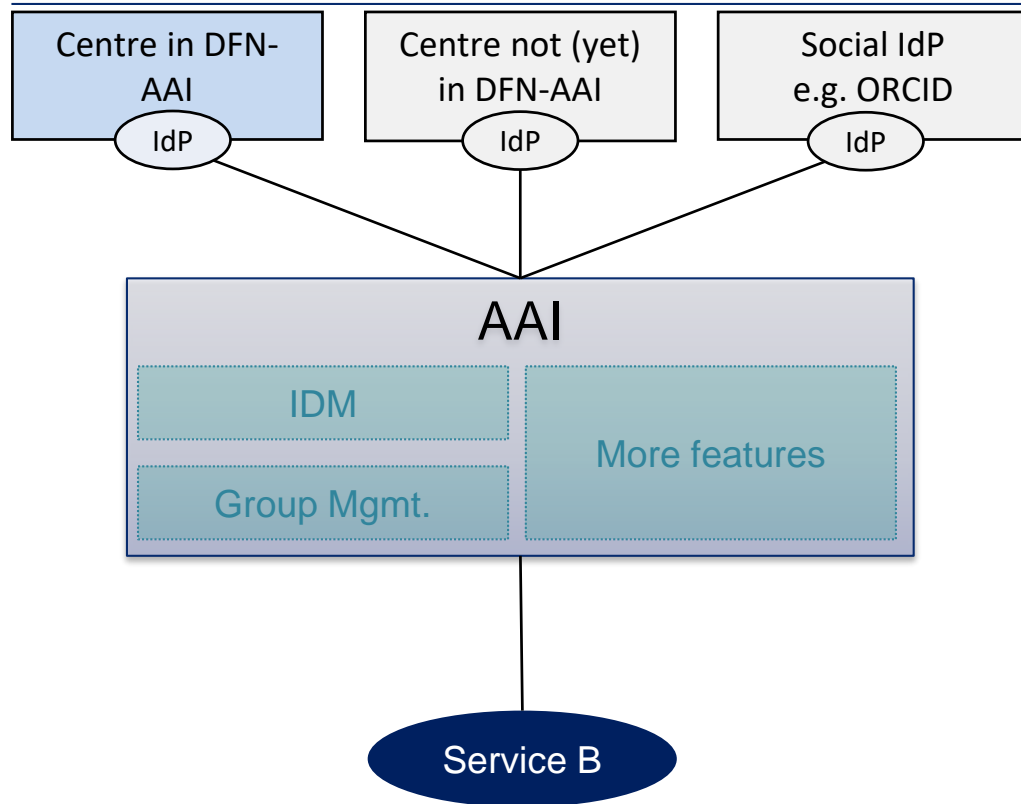
## Overview



- Helmholtz AAI is a proxy IdP (Identity Provider)
- Centre IdPs needs to be part of DFN AAI
- Temporary support of IdPs, which are not yet part of DFN AAI
- Social IdP as exception for users without centre IdP
  - User will have lower privileges

# Helmholtz Authentication & Authorization Infrastructure (AAI)

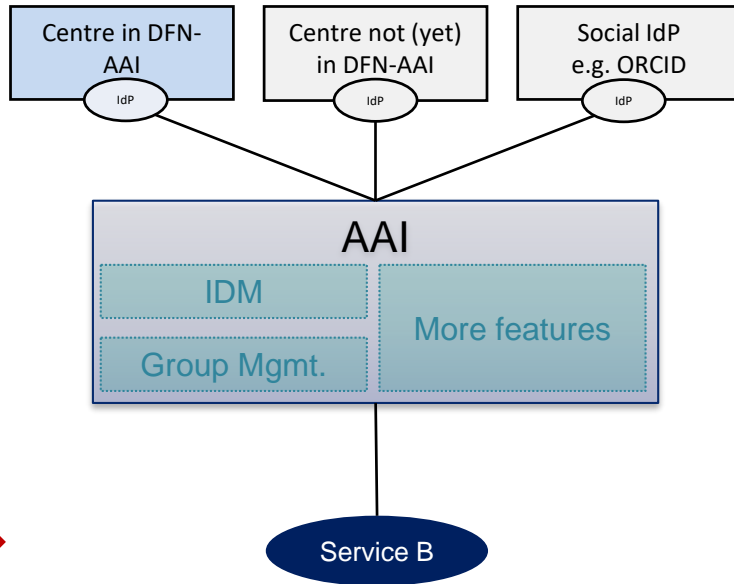
## Service provider option 1 - exclusive HIFIS service



- Service is provided for Helmholtz members
- Service is only connected to Helmholtz AAI

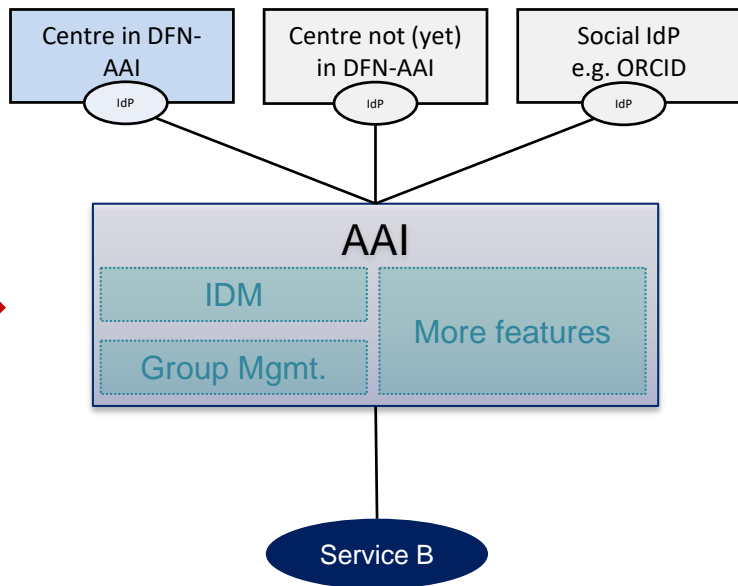
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 1 - exclusive HIFIS service - login flow



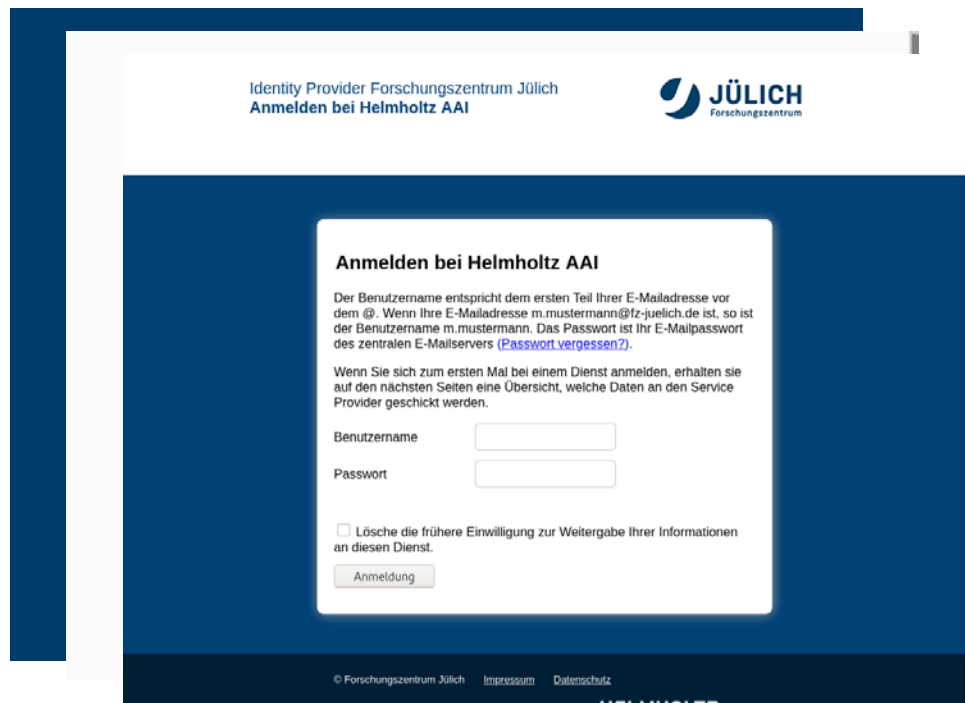
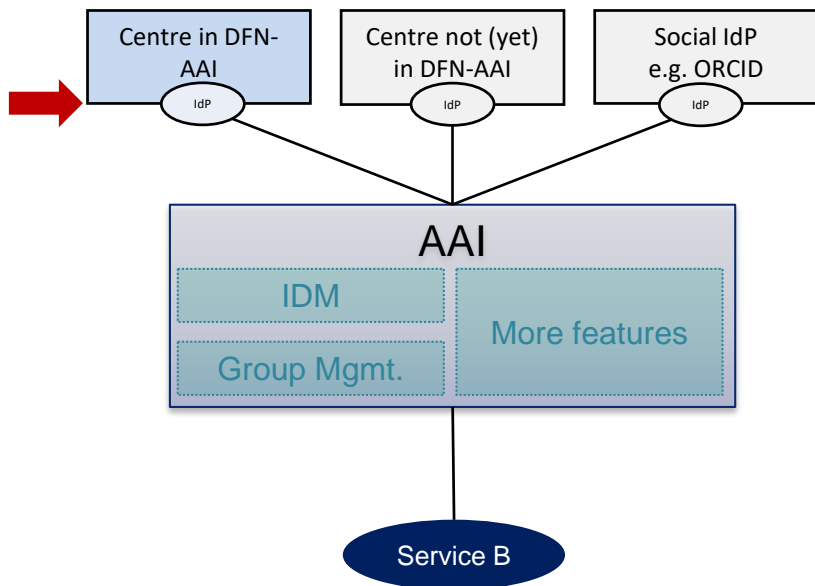
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 1 - exclusive HIFIS service - login flow



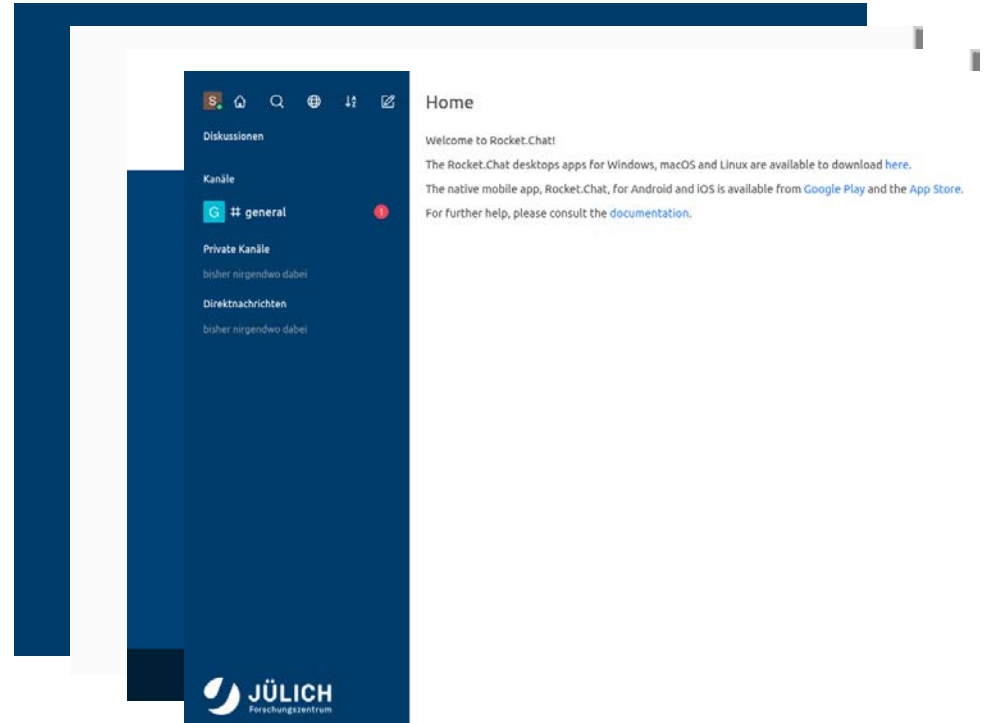
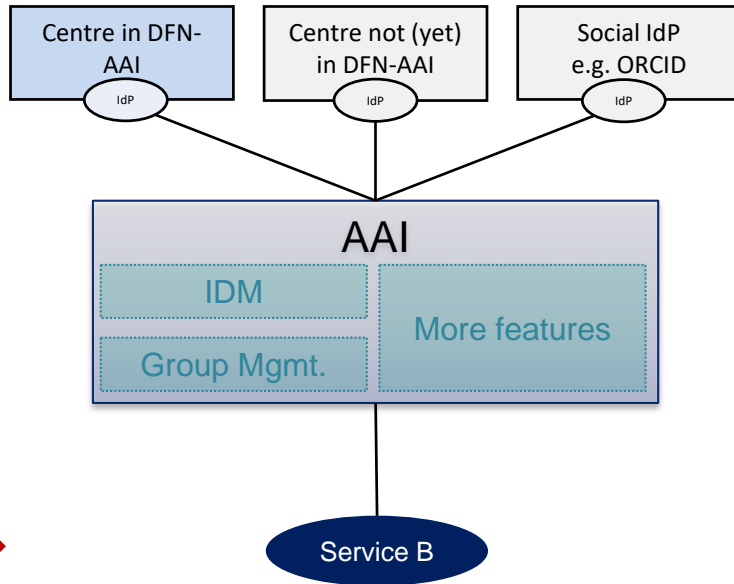
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 1 - exclusive HIFIS service - login flow



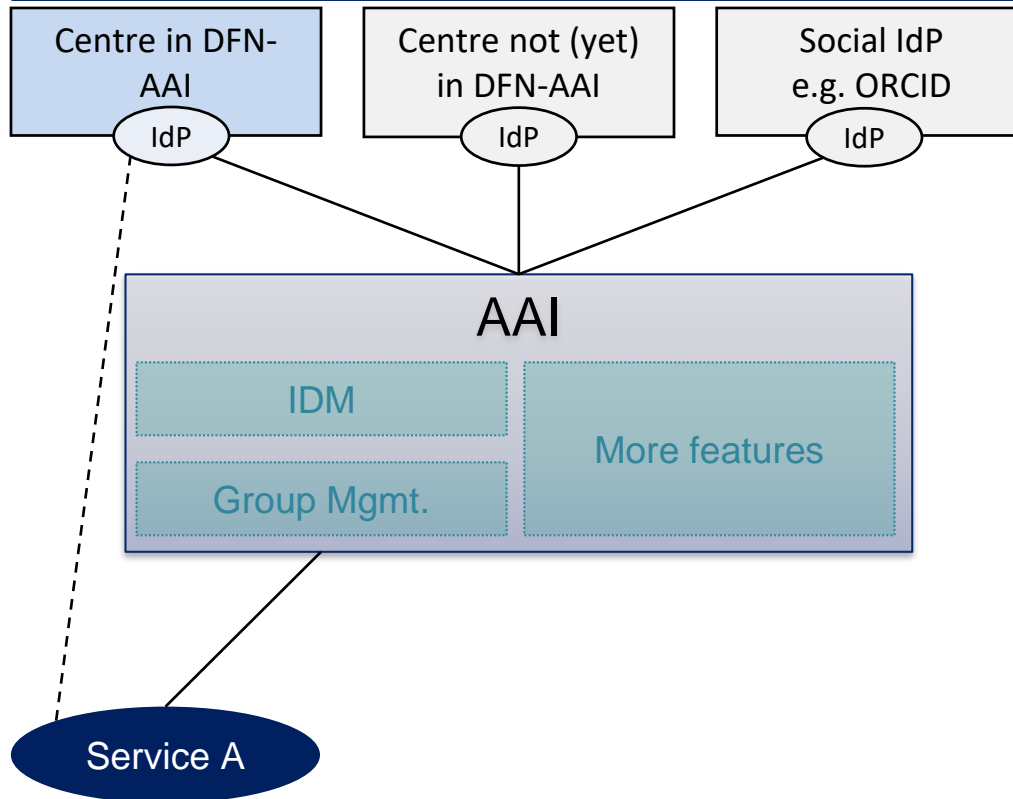
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 1 - exclusive HIFIS service - login flow



# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 2 - service extended to HIFIS

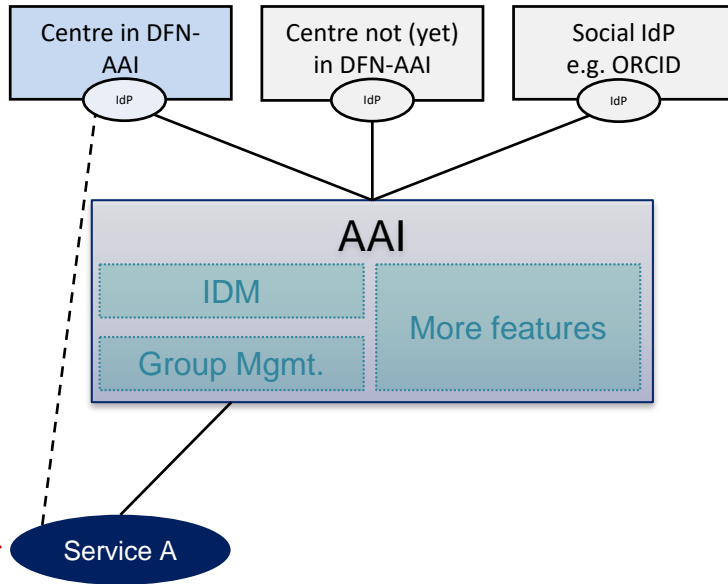


- Service is provided for the centre but extended to Helmholtz members
- Service offers multiple authentication mechanisms
- Helmholtz AAI is one of them



# Helmholtz Authentication & Authorization Infrastructure (AAI)

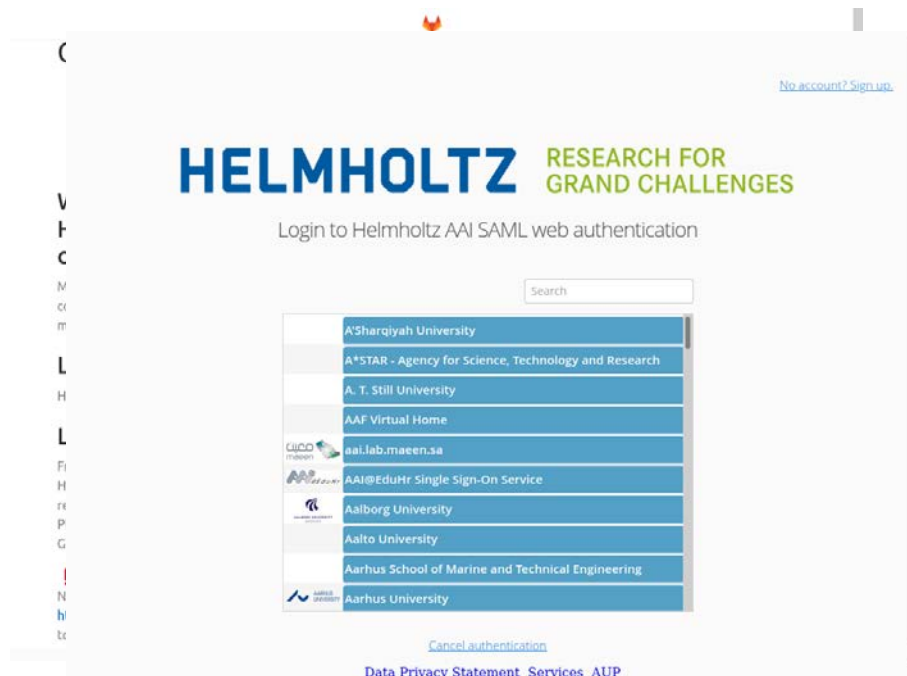
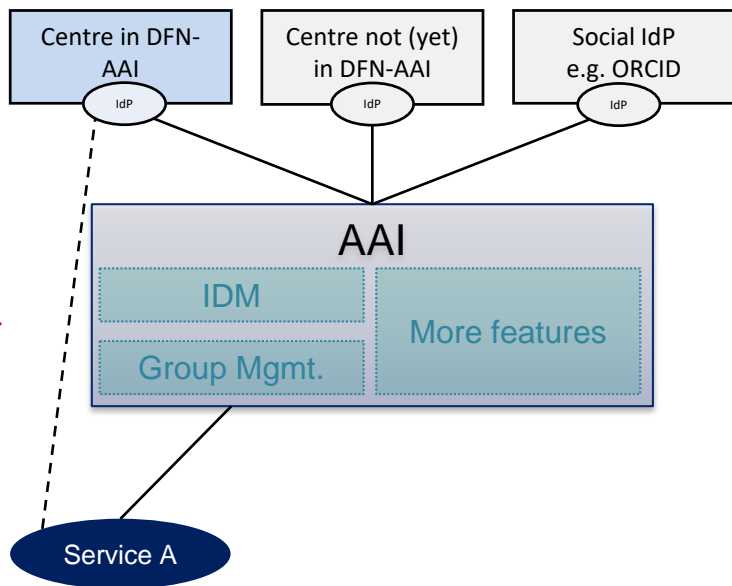
## Service provider option 2 - service extended to HIFIS - login flow



The screenshot shows the GitLab@HZDR login interface. At the top left, it says 'GitLab@HZDR' with the HZDR logo (HELMHOLTZ ZENTRUM DRESDEN ROSSENDORF). The main heading is 'Welcome to the GitLab Web Service at HZDR, a software to collaborate on code.' Below this is a brief description of GitLab's capabilities. There are two main sections for login: 'Login for HZDR Members' and 'Login for external users'. The 'Login for HZDR Members' section includes a form with fields for 'HZDR Username' and 'Password', a 'Remember me' checkbox, and a green 'Sign in' button. The 'Login for external users' section includes a 'Sign in with' section with buttons for 'GitHub', 'Shibboleth (Deprecated)', and 'Helmholtz AAI', along with a 'Remember me' checkbox. A warning message states: 'Login via Shibboleth is deprecated and will be removed on November 19th. Please configure another login mechanism via <https://gitlab.hzdr.de/profile/account>. Otherwise you will not be able to sign-in to GitLab after that date.' At the bottom right, there are links for 'Privacy | Imprint | Support'.

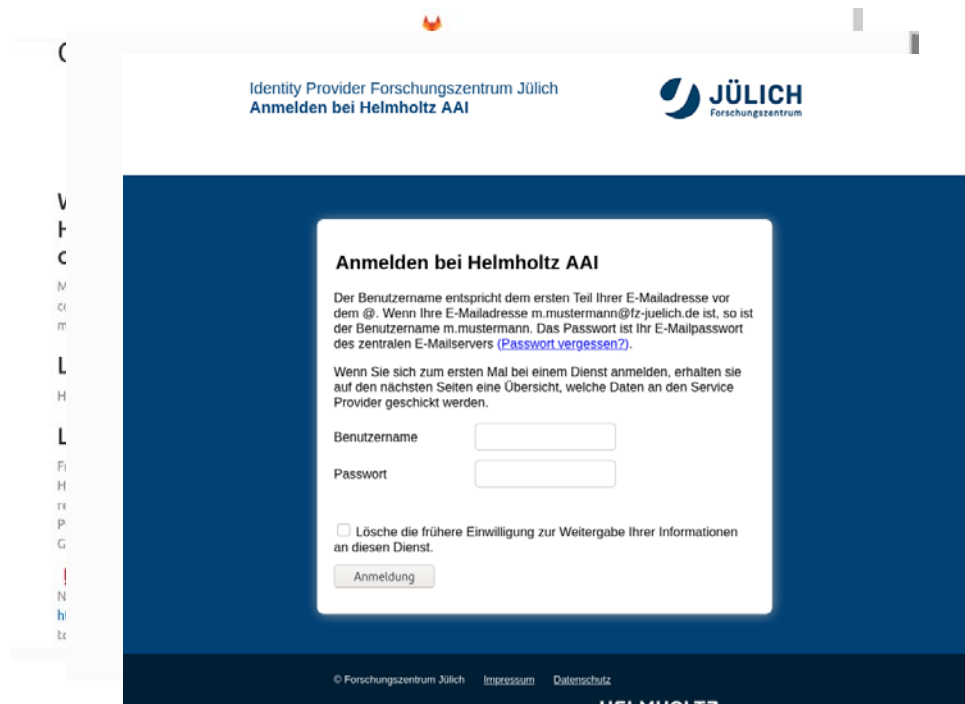
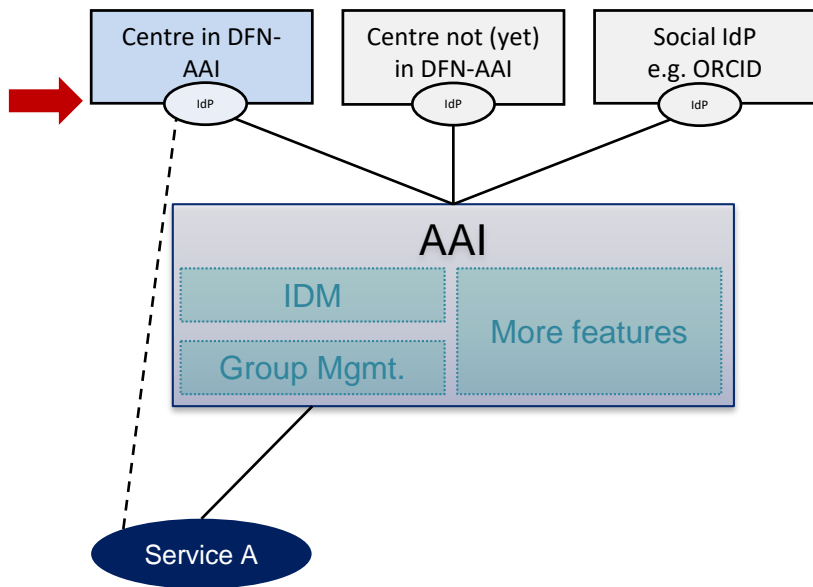
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 2 - service extended to HIFIS - login flow



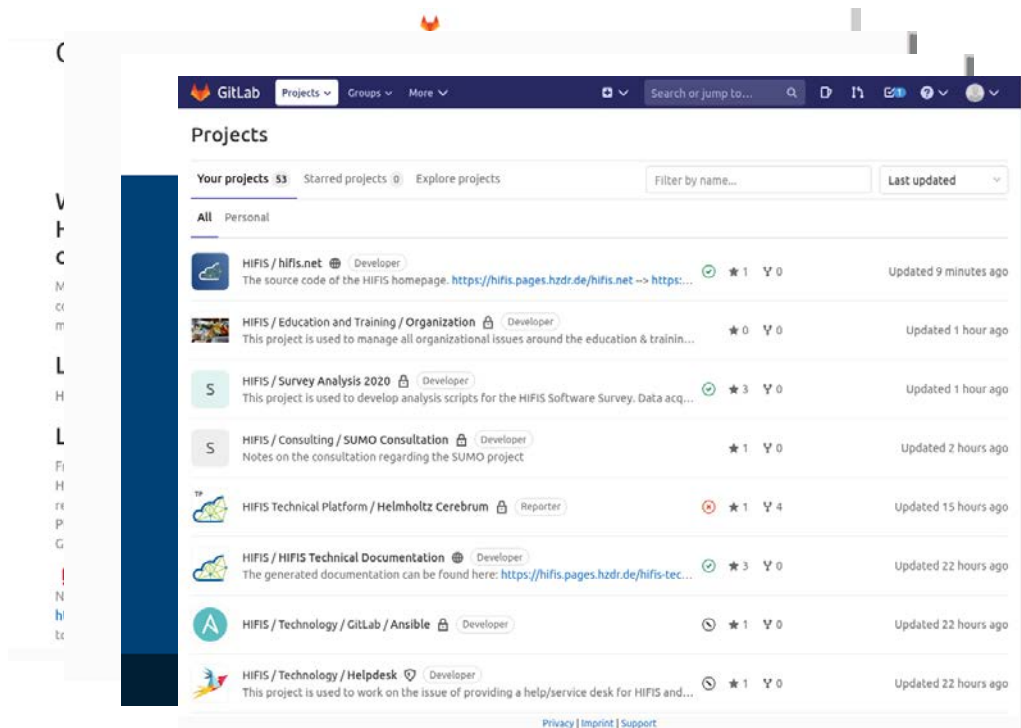
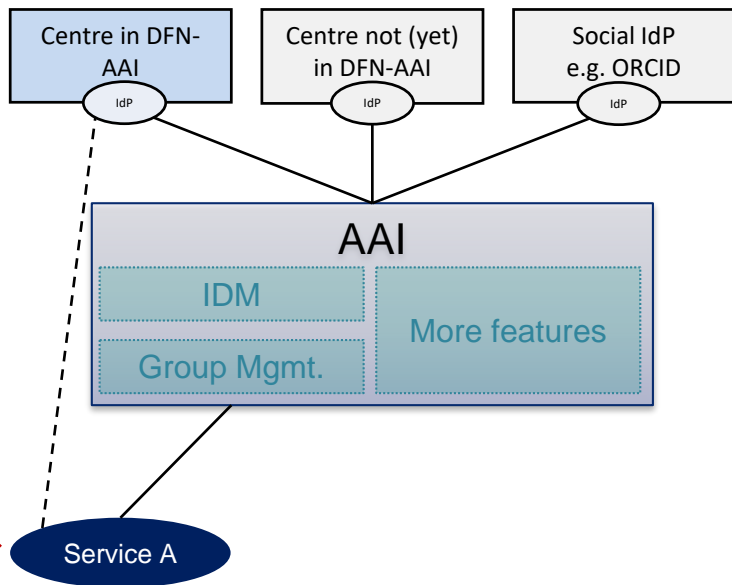
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 2 - service extended to HIFIS - login flow



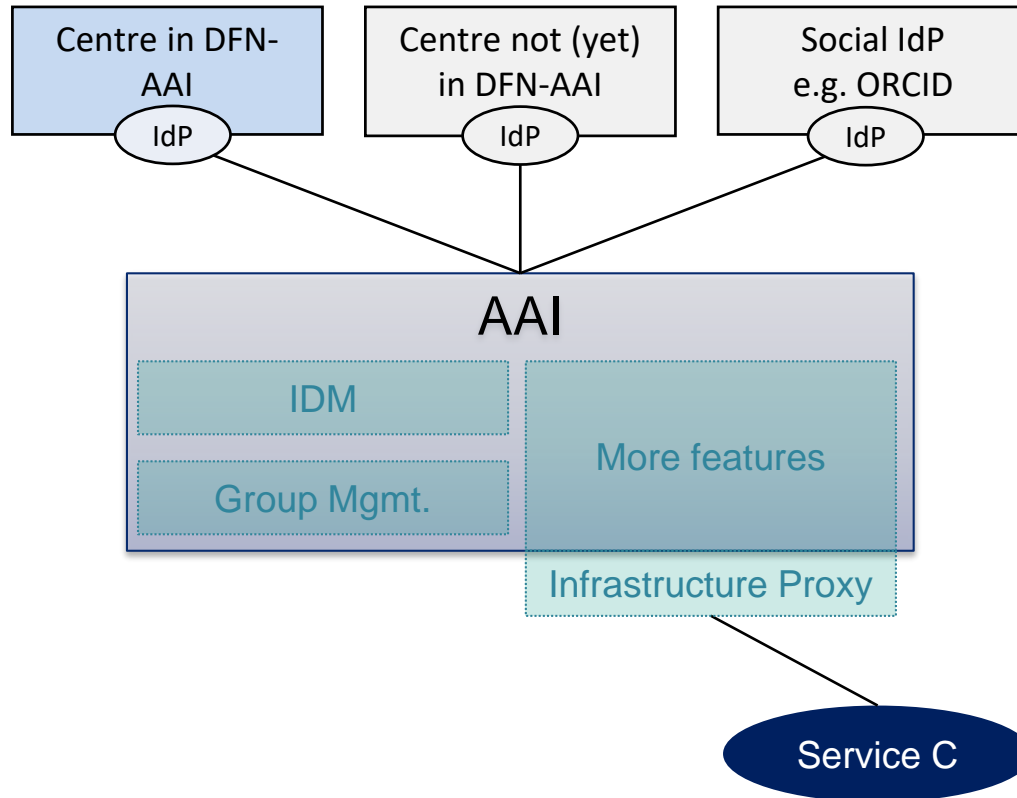
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 2 - service extended to HIFIS - login flow



# Helmholtz Authentication & Authorization Infrastructure (AAI)

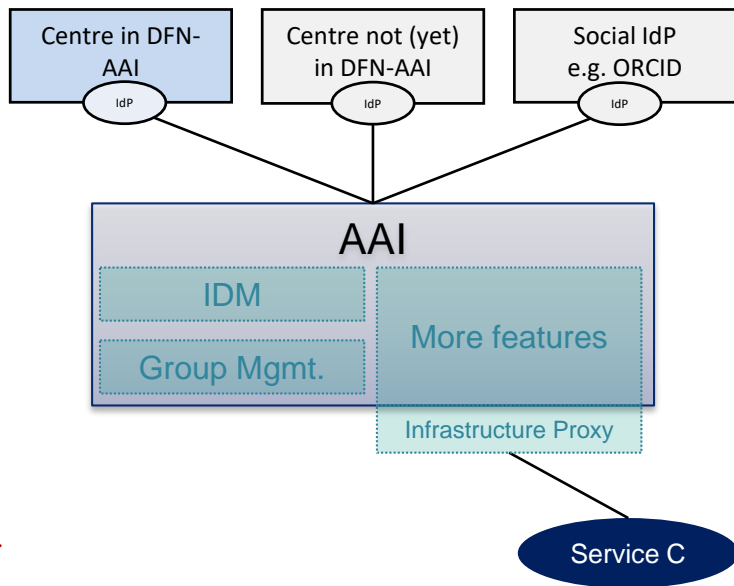
## Service provider option 3 - connected with infrastructure proxy



- Service is connected with a infrastructure proxy
  - e.g. to provide non web accounts
  - e.g. mapping different logins (of one user) to same account

# Helmholtz Authentication & Authorization Infrastructure (AAI)

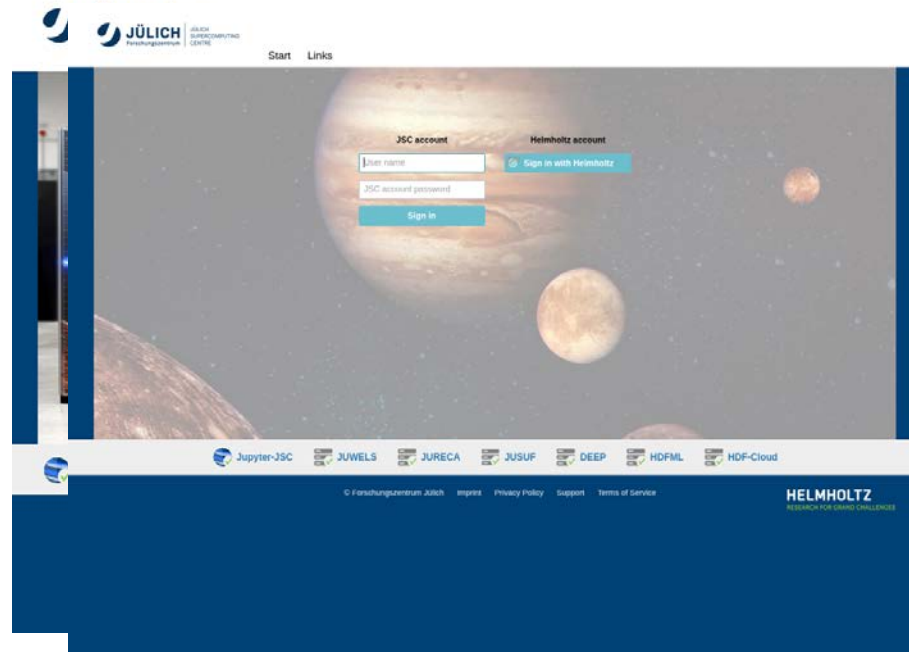
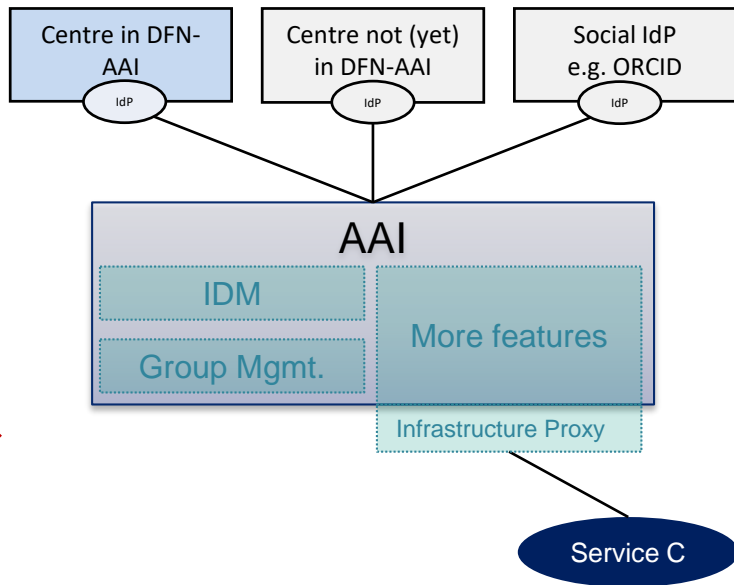
## Service provider option 3 - connected with infrastructure proxy - login flow



The screenshot shows the Jupyter-JSC login page. At the top left is the JÜLICH Forschungszentrum | JÜLICH SUPERCOMPUTING CENTRE logo. Below it are 'Start' and 'Links' links. The main content area features a 'Next-Generation Notebook interface' banner with a description of Jupyter-JSC. To the right, under 'Jupyter-JSC', there is a section titled 'Supercomputing in Your Browser' with a detailed description and a 'Please use your JSC account to log in or register if you have not already done so. It's also possible to log in via Helmholtz AAI.' section. Below this is a 'Login' button with a user icon and a 'Register' button. At the bottom, there is a navigation bar with logos for Jupyter-JSC, JUWELS, JURECA, JUSUF, DEEP, HDFML, and HDF-Cloud. The footer contains copyright information for Forschungszentrum Jülich and links for Imprint, Privacy Policy, Support, and Terms of Service, along with the HELMHOLTZ RESEARCH FOR GRAND CHALLENGES logo.

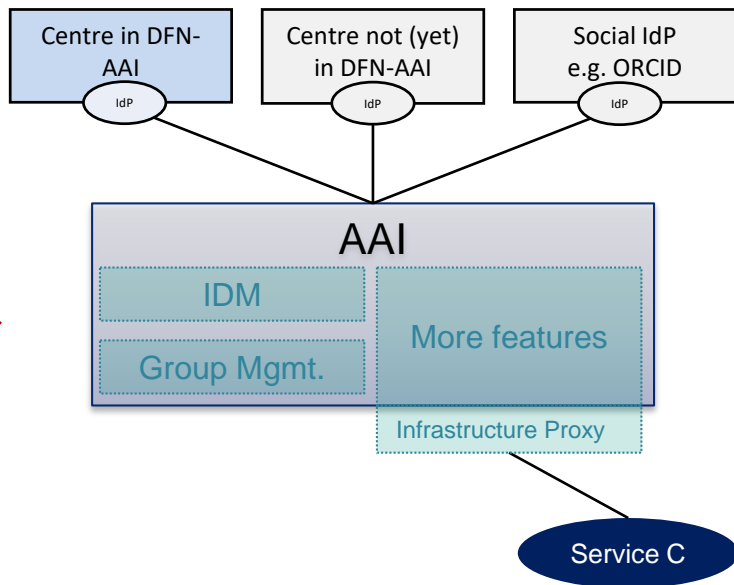
# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 3 - connected with infrastructure proxy - login flow



# Helmholtz Authentication & Authorization Infrastructure (AAI)

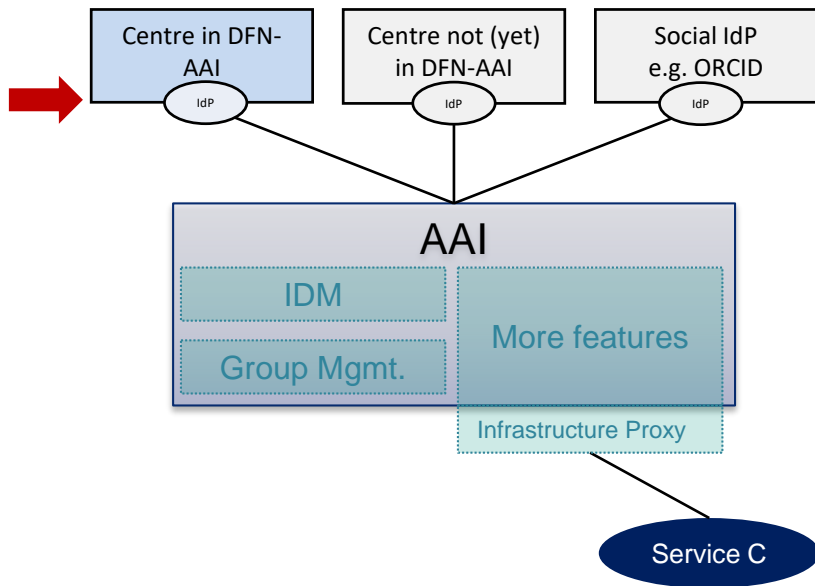
## Service provider option 3 - connected with infrastructure proxy - login flow





# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 3 - connected with infrastructure proxy - login flow



Identity Provider Forschungszentrum Jülich  
Anmelden bei Helmholtz AAI

**JÜLICH**  
Forschungszentrum

### Anmelden bei Helmholtz AAI

Der Benutzername entspricht dem ersten Teil Ihrer E-Mailadresse vor dem @. Wenn Ihre E-Mailadresse m.mustermann@fz-juelich.de ist, so ist der Benutzername m.mustermann. Das Passwort ist Ihr E-Mailpasswort des zentralen E-Mailservers ([Passwort vergessen?](#)).

Wenn Sie sich zum ersten Mal bei einem Dienst anmelden, erhalten sie auf den nächsten Seiten eine Übersicht, welche Daten an den Service Provider geschickt werden.

Benutzername

Passwort

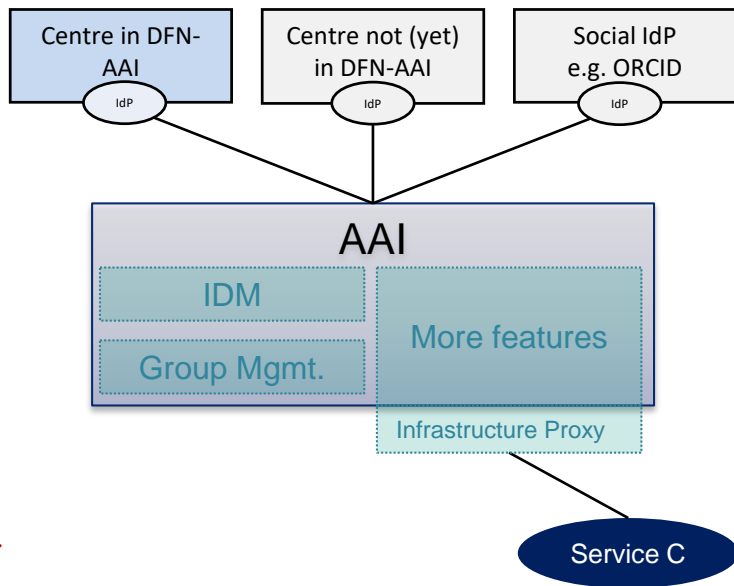
Lösche die frühere Einwilligung zur Weitergabe Ihrer Informationen an diesen Dienst.

Anmeldung

© Forschungszentrum Jülich [Impressum](#) [Datenschutz](#)

# Helmholtz Authentication & Authorization Infrastructure (AAI)

## Service provider option 3 - connected with infrastructure proxy - login flow



The screenshot shows the Jülich Supercomputing Centre (JSC) user interface. The header includes the Jülich logo and navigation links: 'Start', 'Links', 'Last login: 12:11:00 2020-10-15', 'sa.apweiler@fz-juelich.de', and 'Logout'. The main content area is titled 'Configurations' and contains instructions: 'Please give each of your configurations a name. This way you can run multiple instances at the same time. Supported characters are a-z, 0-9 and "."'. Below this is a form with a text input 'Name your JupyterLab' and a button 'Add new JupyterLab'. A table below the form has columns: 'Name', 'System', 'Account/Image', 'Project', 'Partition', 'Reservation', 'Resources', and 'Actions'. The footer features logos for 'Jupyter-JSC', 'JUWELS', 'JURECA', 'JUSUF', 'DEEP', 'HDFML', and 'HDF-Cloud', along with copyright information for '© Forschungszentrum Jülich' and links for 'Imprint', 'Privacy Policy', 'Support', and 'Terms of Service'. The 'HELMHOLTZ RESEARCH FOR GRAND CHALLENGES' logo is also present.

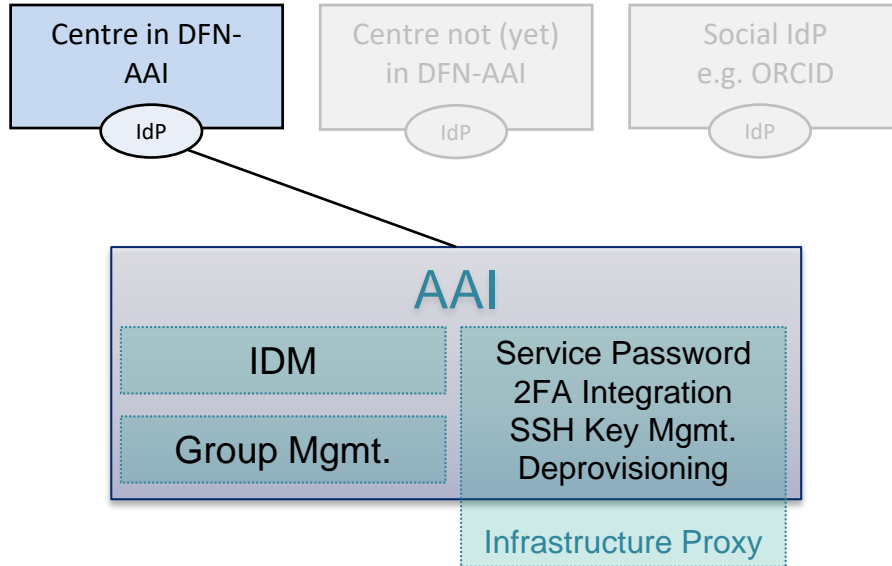
# Achievements

---

- Helmholtz AAI consists of different modules and (two) software stacks
- First services are integrated
- More Identity Providers of Helmholtz Centres became part of the DFN AAI
- Policies are written: [www.hifis.net/mission/publications.html](http://www.hifis.net/mission/publications.html)

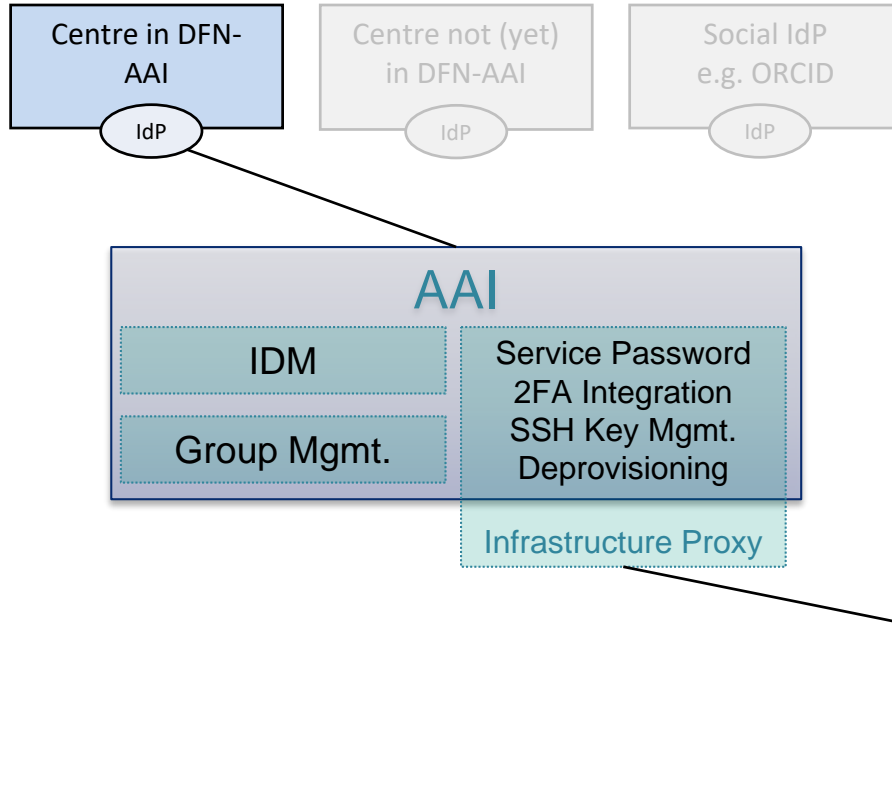
# Achievements

## HAICORE – Access Since July 2020



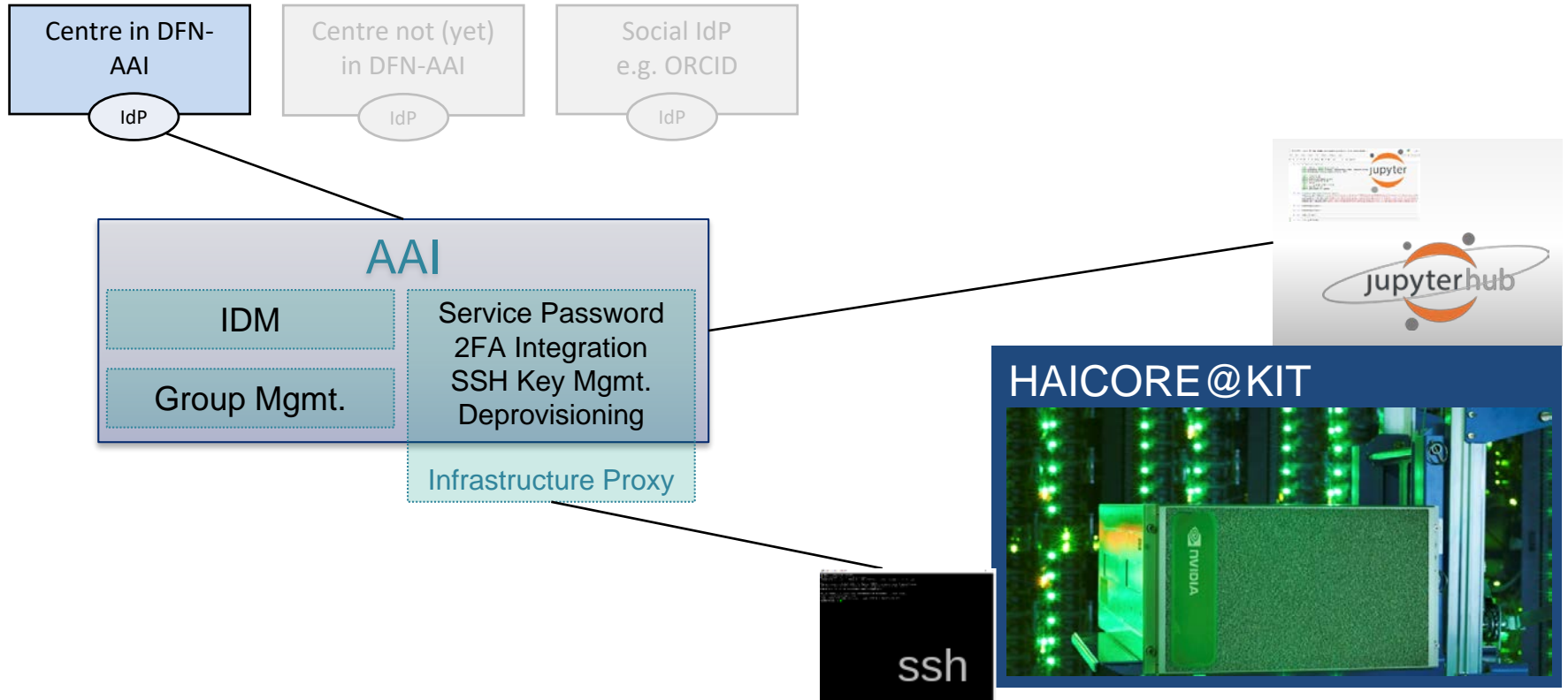
# Achievements

## HAICORE – Access Since July 2020



# Achievements

## HAICORE – Access Since July 2020



# Achievement / Outlook

---

- Available now
  - Group / community management
  - Service password management
  - Secure SSH key management
  - 2FA
  - Deprovisioning (not yet in all modules)
  - Different integration technologies (SAML, OpenID Connect, SSH, LDAP, API, etc.)
- Some work to do in all modules / components
  - Full support of deprovisioning (incl. service providers)
  - Support chain for 2FA