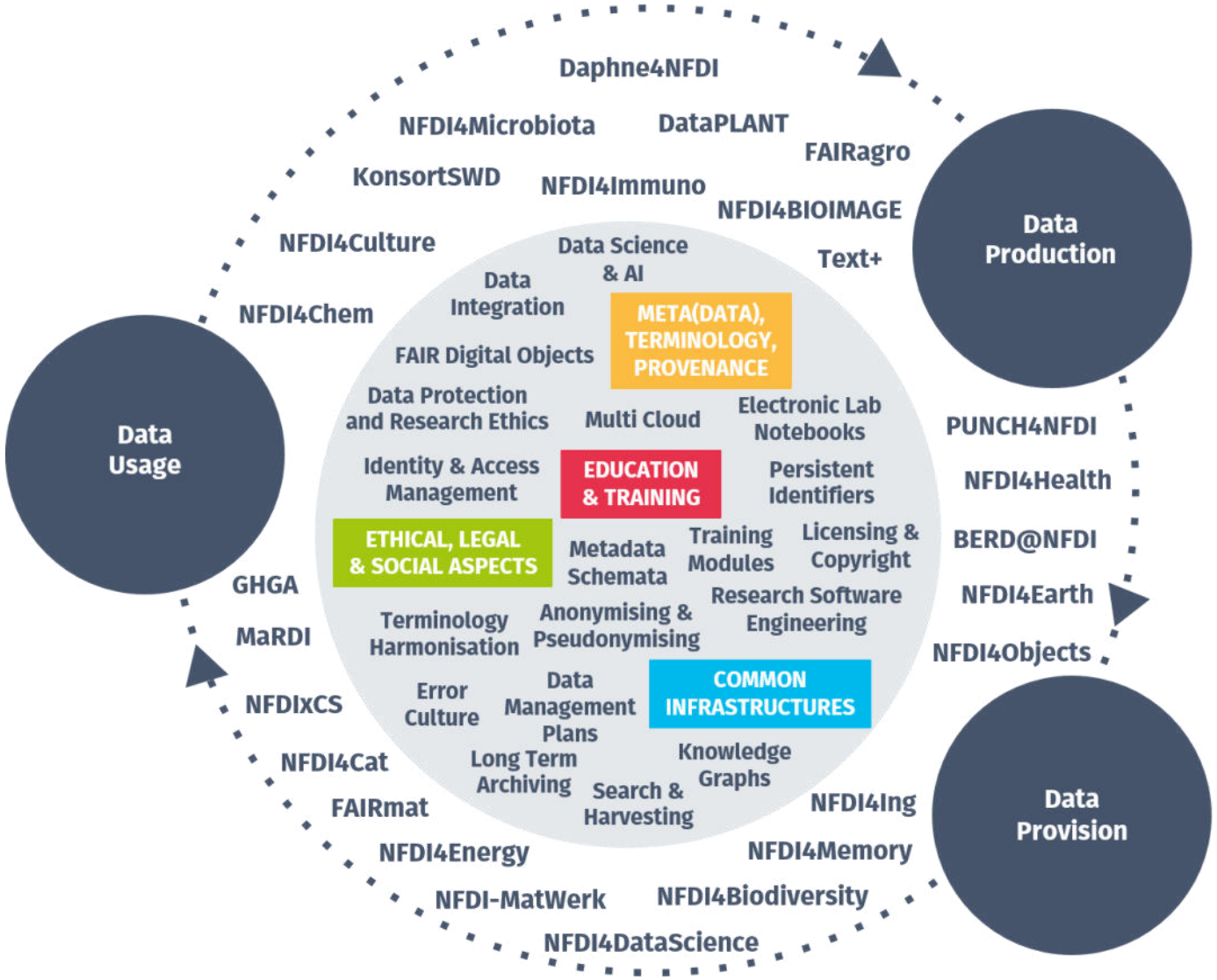
base4 nfdi Basic Services for NFDI

IAM4NFDI Workshop

IAM Basics #2

2023-08-24



base4 nfdi

Funded by **DFG** as part of **NFDI**.

Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

Contents

- Introduction
- Recap
- Overview Community-AAI solutions
- Community-AAI-as-a-Service
- Field report: RDMO integration

  -- Break –-
- Things you should know and be aware of when operating a Community-AAI
  - Authorization and VO Management
  - ~~Trust and Policies~~ *(canceled due to time constraints)*
  - ~~Security and Incident Response~~ *(canceled due to time constraints)*
  - Experiences of the CAAI-Operators
- Discussion
- Summary, next steps + wrap up

Introduction

base4nfdi

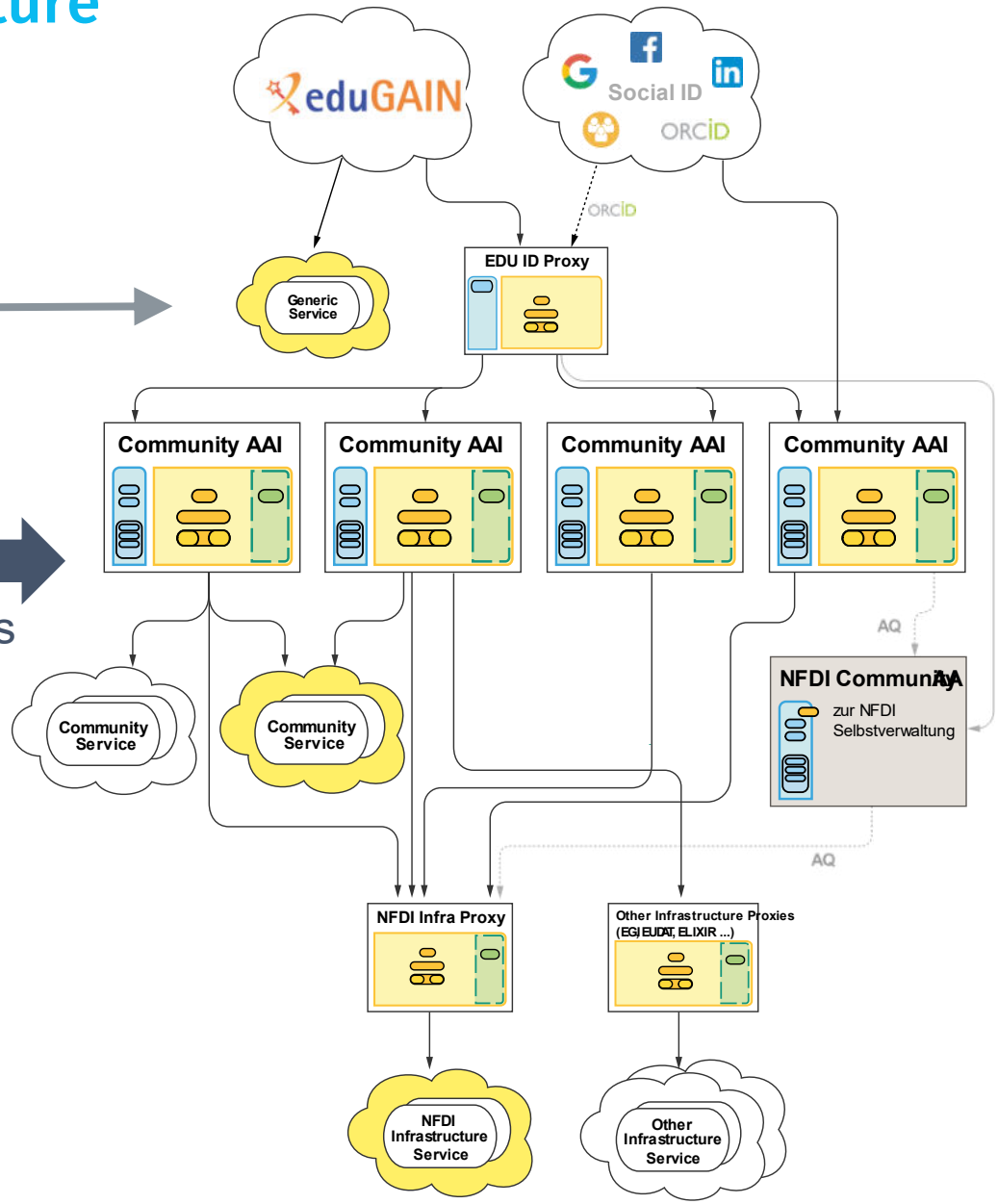
IAM4NFDI
Community Events

- **Provide basic IAM knowledge**
- **Information on all aspects of the Basic Service**
- **Gather Feedback**

NFDI-AAI Architecture

IAM Basics #1
Federated Identity Management
Federating Services

IAM Basics #2
Community AAI Solutions
Community Services
Virtual Organisations



Infoshare
IAM4NFDI – the big Picture
- Architecture
- Community AAIs
- Attribute Profiles
- Policy Framework

base4nfdi

Recap

- Concept of Community-AAI
- Architecture NFDI-AAI

base4nfdi

IAM in der Nationalen Forschungsdateninfrastruktur (NFDI)

Sander Apweiler, Matthias Bonn, Peter Gietz, Marcus Hardt, David Hübner, Thorsten Michels, Wolfgang Pempe, Christof Pohl, Marius Politze

Aug 2023

base4 nfdi

Base4NFDI-IAM Goals

(Based on requirement analysis run before proposal)

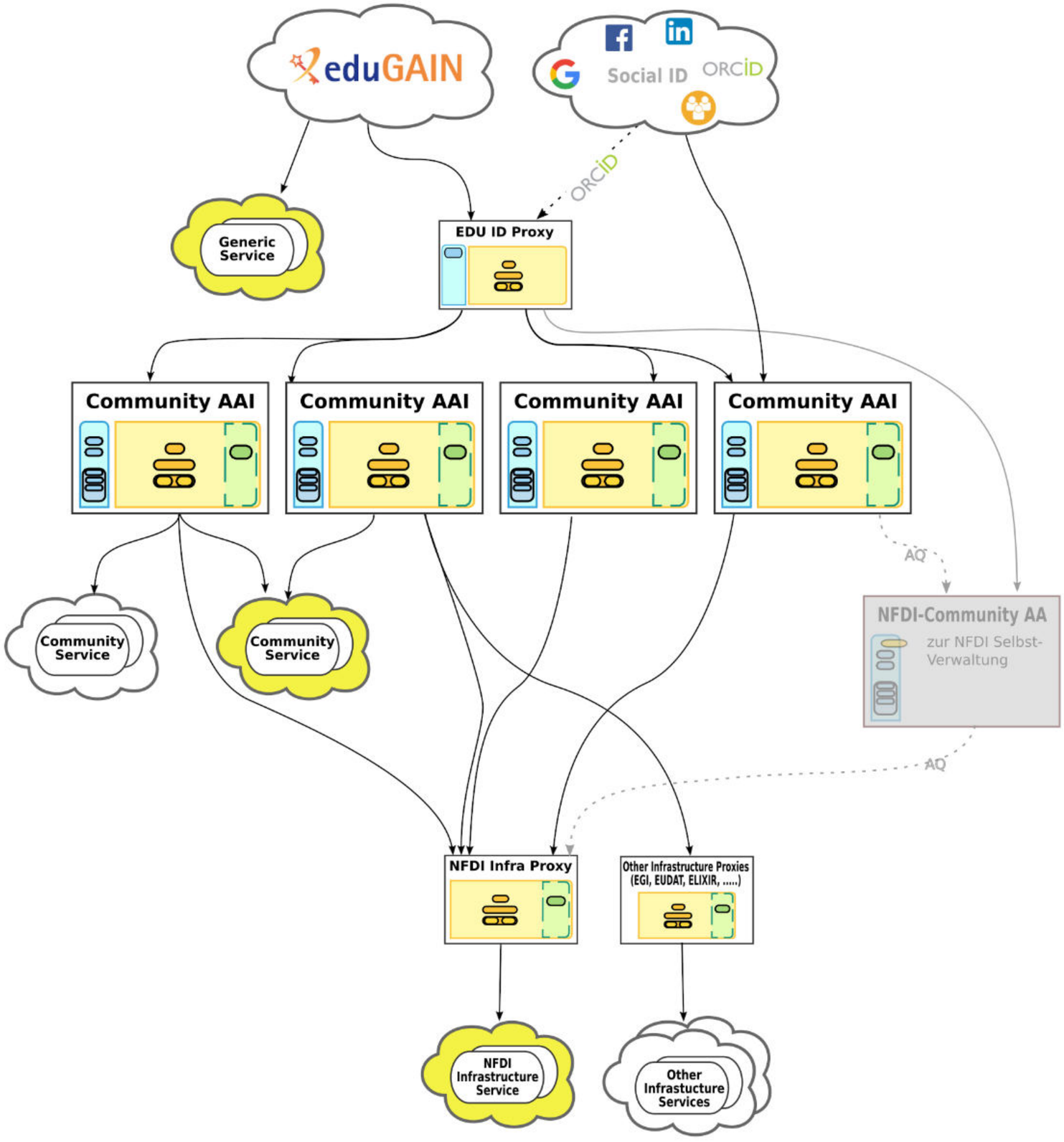
- **Provide state of the art IAM to all NFDI Consortia**
  - Use home organisation identity
  - Enable delegated group management (Virtual Organisations)
  - Open for NFDI and beyond
  - Compatible with AARC / EOSC
  - Community AAI as a Service!

Project has just started

- We have an architecture ✅
- We have a set of attributes ✅
- We have the initial set of policies ✅
- We have the initial documentation ✅

All documented at https://doc.nfdi-aai.de

Architecture


eduGAIN
Social ID
ORCID
ORCID
Generic Service
EDU ID Proxy
Community AAI
Community AAI
Community AAI
Community AAI
AQ
Community Service
Community Service
NFDI-Community AA
zur NFDI Selbst-Verwaltung
AQ
NFDI Infra Proxy
Other Infrastructure Proxies (EGI, EUDAT, ELIXIR, ...)
NFDI Infrastructure Service
Other Infrastucture Services

base4 nfdi

Information about

Users

base4 nfdi

Basic Attribute Profile

- User identifier (created by CAAI)
  - Non-reassignable
  - **and** persistent
  - **and** unique
- Name information
- Email information
- Home Organisation information
- Affiliation within the community
- Affiliation at the Home-Organisation
- Assurance

Extended Attribute Profile

- Groups and roles: **`eduPersonEntitlement`**
- Capabilities **`eduPersonEntitlement`** [AARC-G027]
- Assurance (see above)
- Agreement to policies
- ORCID identifier
- Supplemental Name Information
- Authentication Profiles
- External Identifier
- SSH-Keys

Attributes: Bottomline

- Services may know a lot about the user
- Services SHOULD [RFC2119] use these attributes (and not ask users for them)
- If this is insufficient for your community, contact us at:
  aai-kernteam@lists.kit.edu

base4 nfdi

Authorisation

aka “Virtual Organisation (VO) Concept”

- Common **ANTI**Pattern: VO named “`gitlab-kit`”
  - Wrong thought 1: “I want to know all my users”
  - Wrong thought 2: “I want **people** to sign up to my service”
- **CORRECT** Pattern:
  - **VO named “`global-ant-research`”**
  - The **service** `gitlab@kit` **may decide** to support the “`global-ant-research`” VO
  - Reason “I don’t need to know my users, this is the job of the VO!”
  - Consequence “I need to trust the VO, not an individual”
- If you want to know more, read the policies!

base4 nfdi

Common Caveats

- Some terms are defined differently in different communities
- Example:
  - The NFDI4Culture “Consortium” => AAI Speak: “Community”
    - Is subdivided into “Communities” => AAI Speak: “Virtual Organisation (VO)”

Policies

- Essential: Concept of **Policy Frameworks**
  - SIRTFI
  - SNCTFI
- Actual policies need to follow the Policy Framework
  - Top Level Infrastructure Policy (TLP)
  - Security Incident Response Policy (SIRP)
  - Policy on the Processing of Personal Data (PPPD)
  - Virtual Organization (VO) Membership Management Policy (VOMMP)
  - Virtual Organisation (VO) Life Cycle Management (VOLCM)
  - Service Access Policy (SAP)
  - Privacy Policy Template (PP (per VO / per Service))
  - Acceptable Use Policy Template (AUP (per VO / per Service))

base4 nfdi

base4 nfdi

NFDI AAI Documentation

News

23-02-14: Proposal for funding an NFDI IAM infrastructure submitted. Find the full proposal here.

Context

The NFDI AAI (architecture, policies, attributes, etc.) described in this context, is based on the work, the experience, and standardisation made in previous projects. In the European context these are most notably AARC and the EOSC-Taskforce on AAI Architecture.

In the German context, several different projects have contributed their experience to this AAI:

Overview Community-AAI Solutions

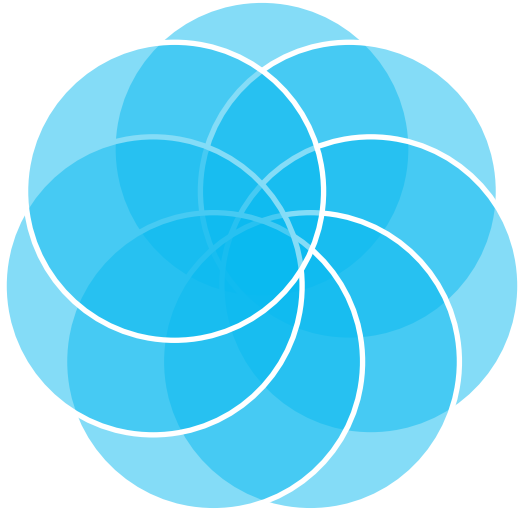
Academic ID, didmos, RegApp, Unity

base4nfdi

AcademicID – CAAI Solution

Powered by

AcademicID CAAI Solution



AcademicID

- Single Account for all AcademicID Communities

Support for 3rd-Party ID-Provider & Self-Registration

- Integration of "Homeless" Users

Single Sign-On (SSO)

- IdP- & SP-Proxy Support

Community, Organization & Group Management

- Service-Access, Quotas, Invitation-Workflow, ...

Identity Provisioning & Lifecycle Management

User Account Selfservice Portal

Multi-Factor-Authentication

- Tokens, Push, OTP, ...

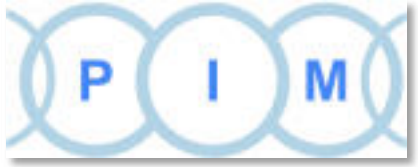
Key Features

- Support for individual instance and tenant-based operational models – tenants do not need to set up/operate their own CAAI instance.
- No vendor lock-in, lower overall costs and high compatibility to common standards through use of open-source components.
- Easy integration of external communities and AAIs (e.g. DFN-AAI, eduGain).
- Tenant-based CAAIs:
  - One single account for all AcademicID communities.
  - New and improved functionalities are immediately available for all AcademicID communities.
- Certified according to ISO 27001 (information security) and ISO 9001 (quality management).

Selected References

- Academic Cloud: (https://academiccloud.de)
- MPG-SSO, Max-Planck-Gesellschaft (MPG)
- Max Weber Stiftung (https://maxweberstiftung.de)
- GFBio (https://www.gfbio.org)
- DARIAH-DE (https://de.dariah.eu)
- MWW, Virtueller Forschungsraum (https://vfr.mww-forschung.de)
- Plattform für internationale Studienmobilität (https://pim.moses.tu-berlin.de/moses/index.html)
- …

Max Weber Stiftung
Deutsche Geisteswissenschaftliche Institute im Ausland

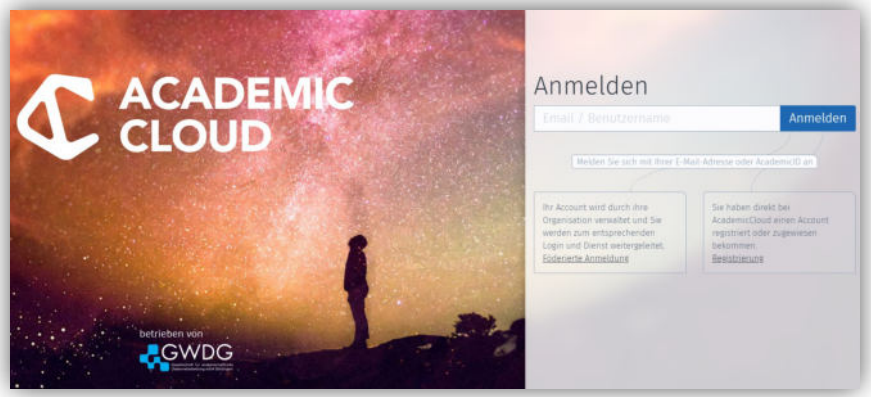


base4nfdi

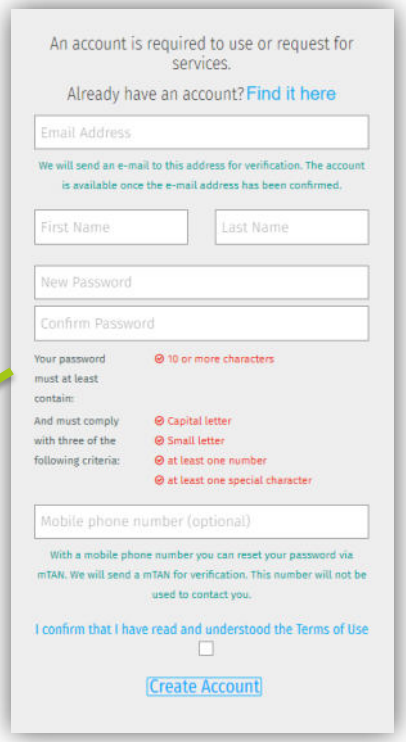
Example for Community AAI Customization

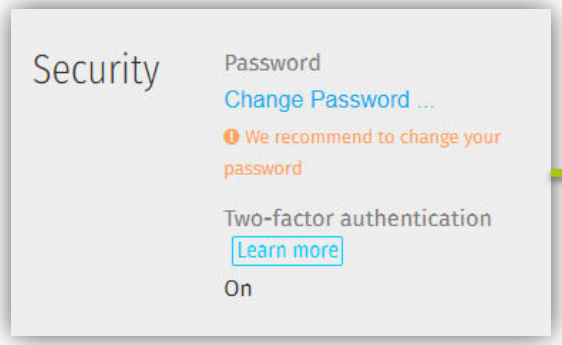
Academic Cloud for Universities in Lower Saxony

Single-Sign-On
(sso.academiccloud.de)



Self-Registration





Account/Profile Selfservice
(id.academiccloud.de)

AcademicID

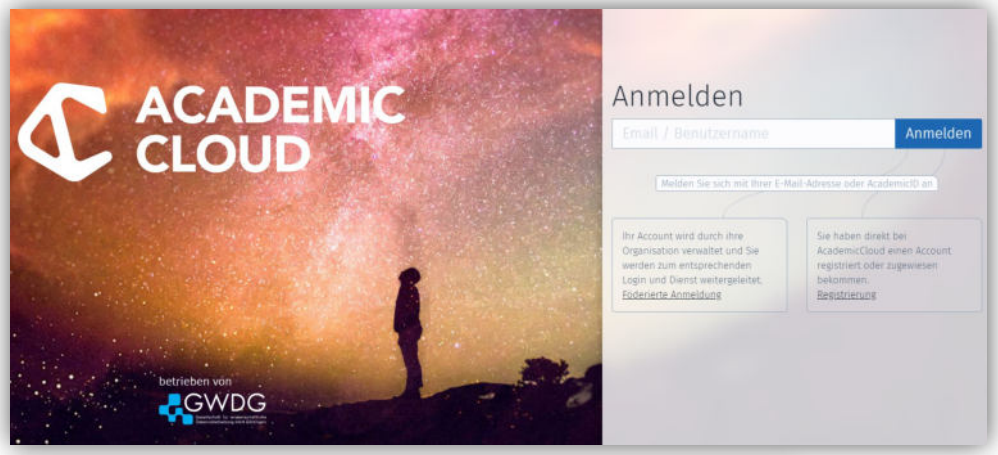
Components: Single-Sign-On (SSO)

Overview

- Central authentication platform for all services in a community
- Supports all common SSO protocols for connecting services to the community, e.g. SAML & OpenID Connect
- Multi-Factor Authentication (Hardware Tokens, Push-App, OTP, …)
- Authentication through connected AAI infrastructures (e.g. eduGain or DFN-AAI etc. or connected identity providers (e.g. other communities)
- Compliance to common standards (AARC, REFEDS, …)
- Support for external ID-Providers (e.g. ORCID, eduID, BundID)

Components: Single-Sign-On (SSO)

Customizing Examples

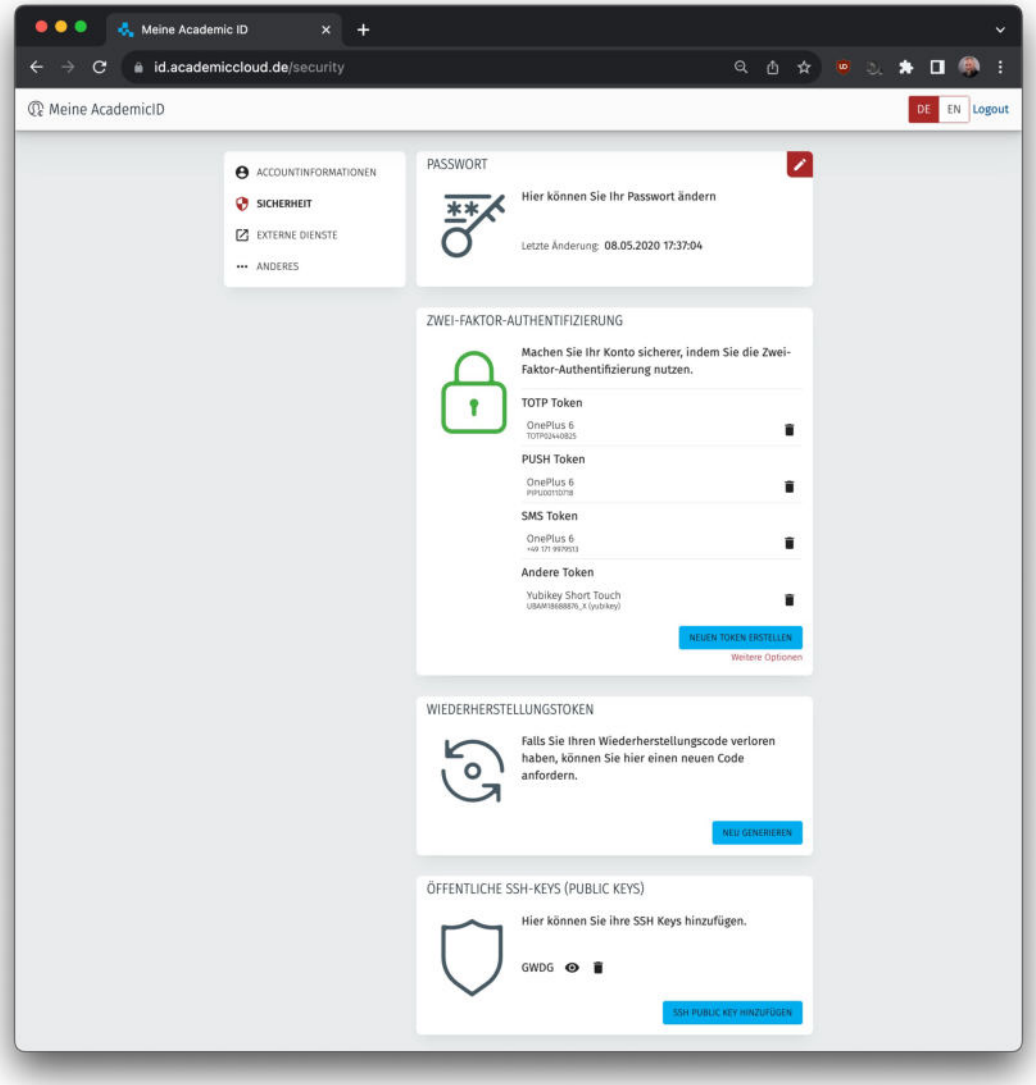


SSO-Proxy

Connection of external AAIs or ID-Providers

User Account Selfservice Portal

- Management of account/user information (self-service)
  - Check/apply for membership with communities or institutions
  - External email addresses, postal addresses, phone numbers
- Security settings
  - MFA token registration and recovery function, change/reset password, SSH keys
- Customization: individual logo/colours/design



Community, Organization & Group Management

Overview

- Service access (rights) and quota can be assigned to a community, organization units (OU) or groups by administrators.
- Administration of a community, OU and groups can be delegated to appropriate users.
- Users can be invited to a community/OU/group or apply for membership.

Community, Organization & Group Management

Invitation Process

- Community X wants to add a bunch of members and let them use community services:
  - Community X sends users an invitation email including a login link and invitation code.
  - Users open the link and log in with their respective home organization or register a new account.
  - The invitation code can be entered by users during registration or login.
  - Users will automatically get access rights and quota to services as specified by Community X.

Community, Organization & Group Management

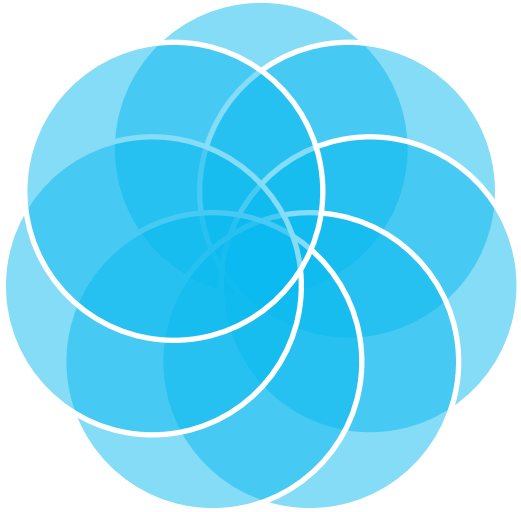
Administration

- Administrators of a community, organization or group can manage user accounts within their respective realm.
- Example: Community administrators can:
  - set new passwords for users,
  - edit user information, and
  - assign access rights and quota for services either for all users of a (sub-)realm or for individual accounts.

AcademicID CAAI Solution

AcademicID
- Single Account for all AcademicID Communities

Support for 3rd-Party ID-Provider & Self-Registration
- Integration of "Homeless" Users



Single Sign-On (SSO)
- IdP- & SP-Proxy Support

Community, Organization & Group Management
- Service-Access, Quotas, Invitation-Workflow, ...

Identity Provisioning & Lifecycle Management

User Account Selfservice Portal

Multi-Factor-Authentication
- Tokens, Push, OTP, ...

Contact:
christof.pohl@gwdg.de
sascha.krull@gwdg.de

Powered by

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

base4nfdi

didmos as a Community AAI solution

Basic Service Identity & Access Management: Workshop IAM Basics #2

David Hübner
DAASI International GmbH

didmos

- A standardised IAM system so flexible it is able to address all customer needs no matter how specific
- Successfully implemented for more than nine customers
- It is very difficult to develop a software which meets all requirements. Hence, didmos consists of several modules for different tasks.
- didmos also allows for plugin interfaces in many places to allow for extensions
- The development of didmos relied on well-established open source products such as OpenLDAP, RabbitMQ, SATOSA, and many more
- Available as Docker Images

DAASI International

didmos

DAASI International

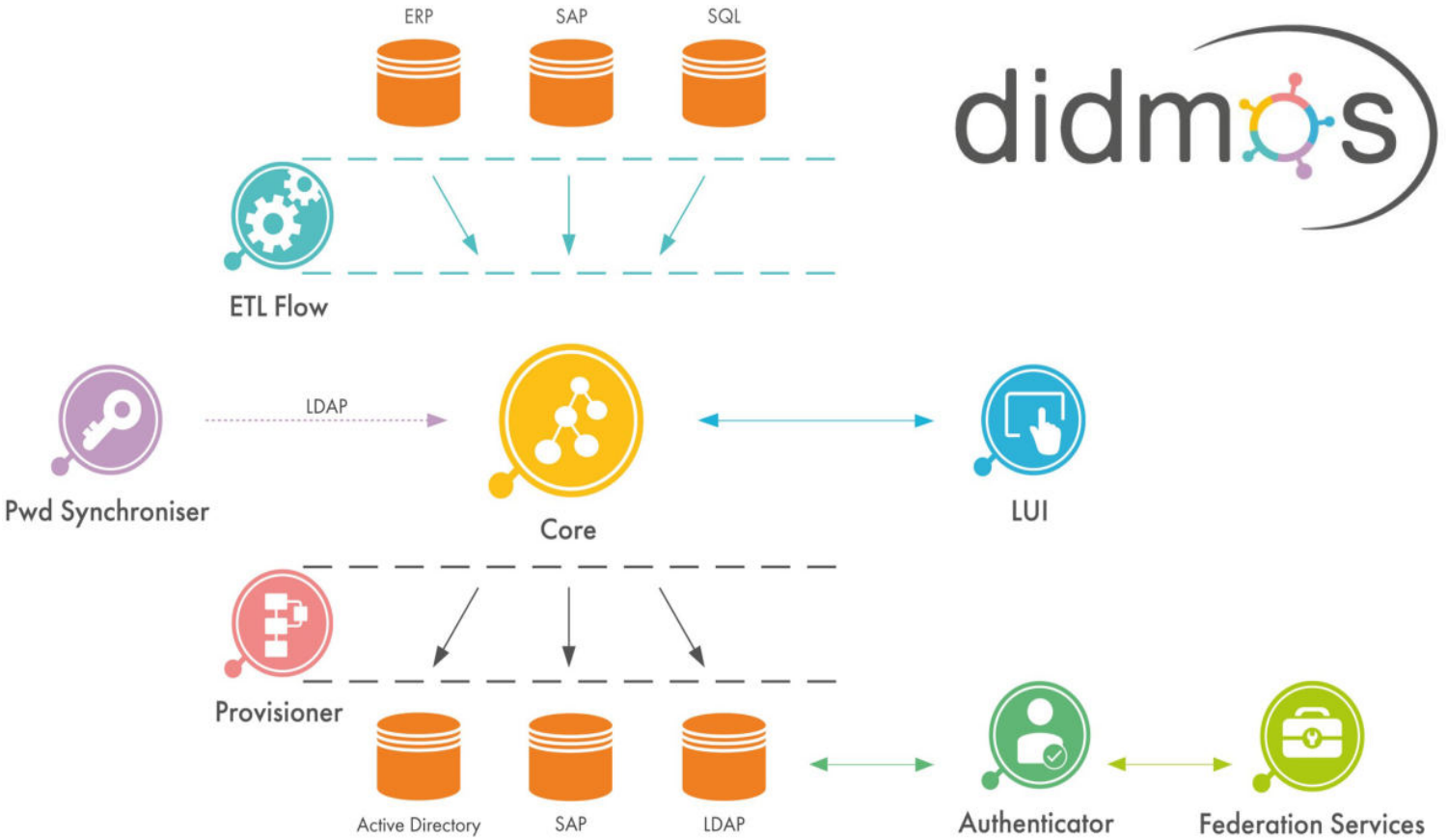
Identity

Management with

Open

Source

didmos - Overview



didmos

DAASI International

didmos Core

- Core consists of two components:
  - OpenLDAP server as metadirectory
  - Backend/API server for data access and background processes (based on Django/Python)
- The API server consists of several modules (called “apps” in Django), which respectively provide a modern REST API via which data can be shared as JSON
  - Access to IdM via SCIM
  - Workflow management
  - Policy Decision Point (PDP) / RBAC
  - MFA token management with privacyIDEA
- Multi tenant capable both in LDAP and API server

didmos LUI

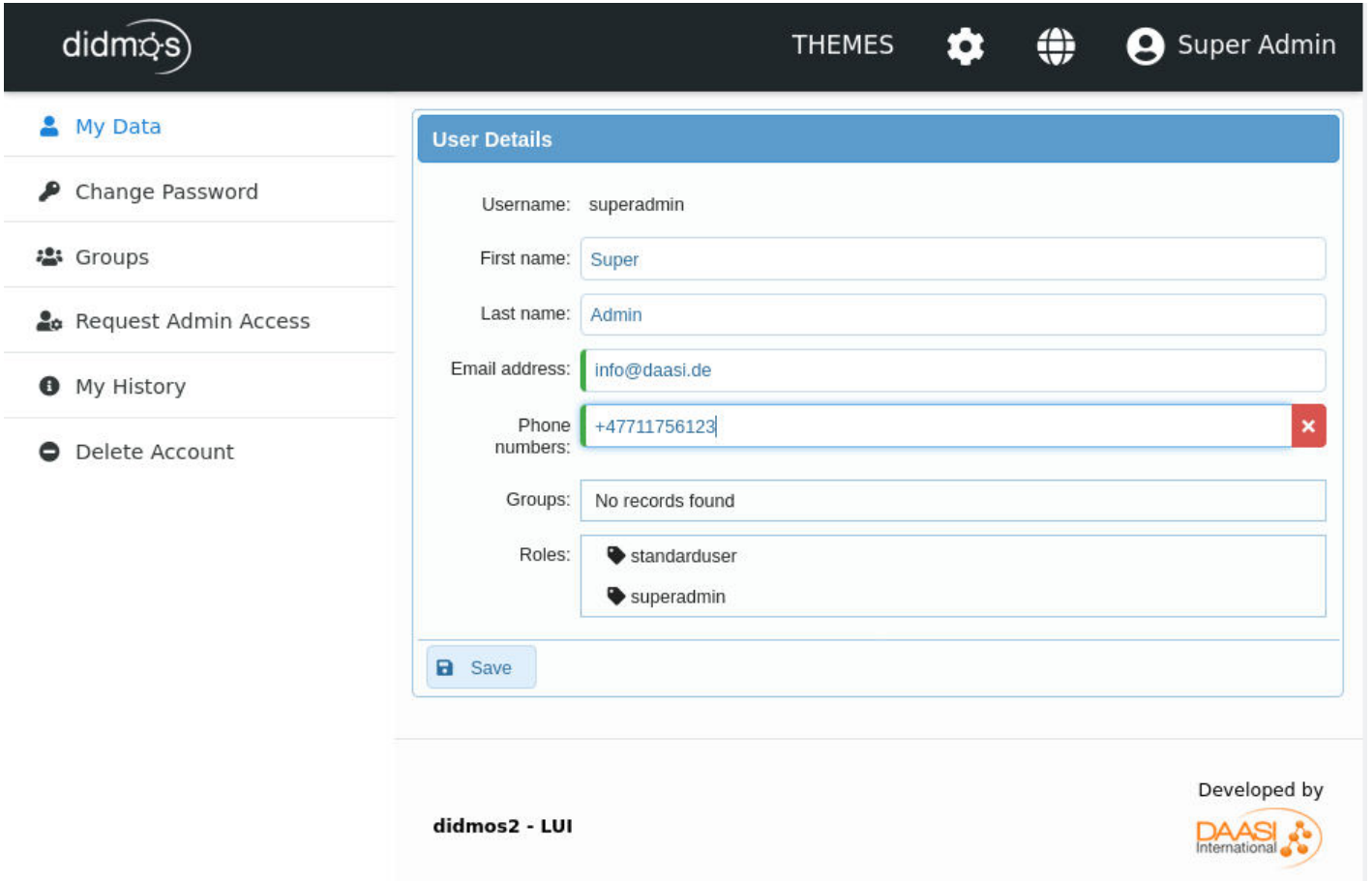
Frontend entirely based on JavaScript (Angular)

- Responsive Single-page application
- Mobile app (PWA) capable
- Authentication with OIDC
- Adjustable, both for layout and functionality (we have various standard modules in a shared library and can create custom modules)
- Both for selfservice and admin functionality

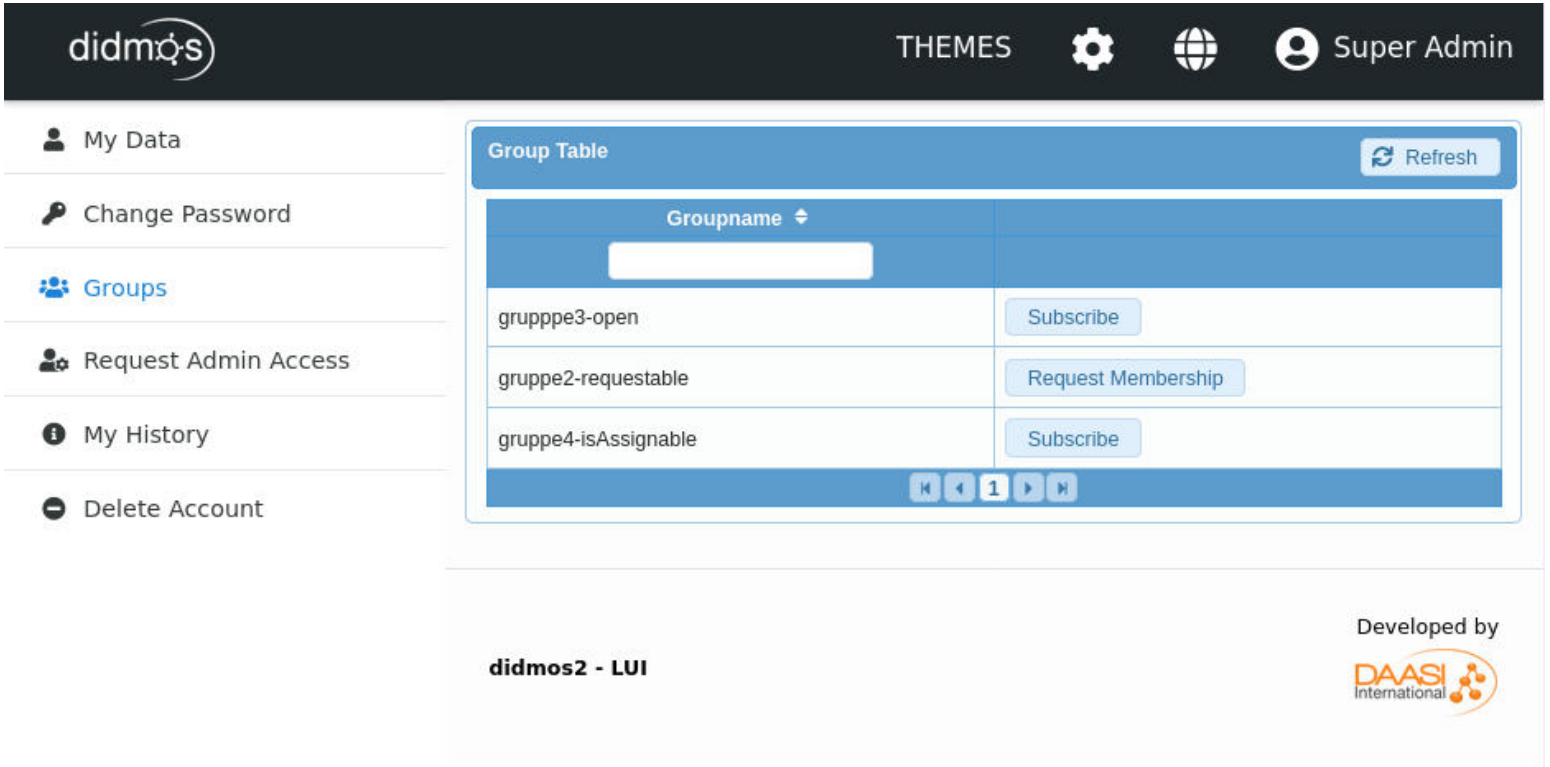
Extensive usage of SCIM

- Only Core is responsible for the manipulation of LDAP objects
- SCIM calls protected by OAuth2 bearer tokens
- Menu items can be controlled via permission assignment from Core to LUI

didmos LUI
- Self-Service – User Information

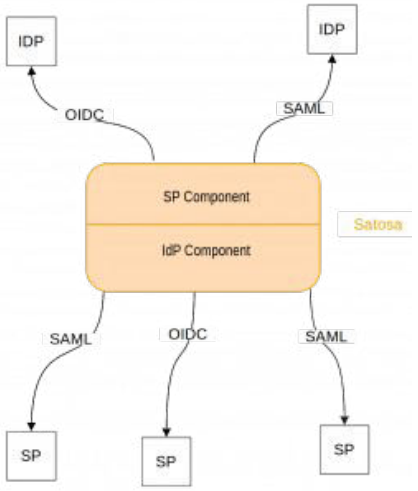


didmos LUI
- Customer – Edit Groups



didmos Authenticator

- Acts as an SSO proxy and supports multiple protocols by default
  - Acts as an IdP/OP for SAML2 and OIDC
  - Acts an an SP/Client for various protocols/services such as OIDC, SAML2, Social IdPs, Orcid, etc.
- Queries additional attributes, such as entitlements from didmos Core via SCIM API
- Various optional microservices for functionality such as MFA, Consent, etc.
- Users with external accounts are created in didmos as „Shadow accounts“ without passwords and can be managed in the VO
- Also support authentication with local accounts (i.e. users with passwords in didmos)



didmos ETL Flow

- **E**xtract **T**ransform **L**oad
- Typical flow (simplified):
  - Read and convert (multiple) data sources (e.g. ldapsearch)
  - Identify against IdM
  - Merge identical data sets within one data source if necessary
  - Merge multiple data sources
  - Calcluate diff against IdM
  - Install changes
- Typically used for either one-time data migration or regular synchronization from source systems
- The workflow is configured via LDAP objects (=configuration)

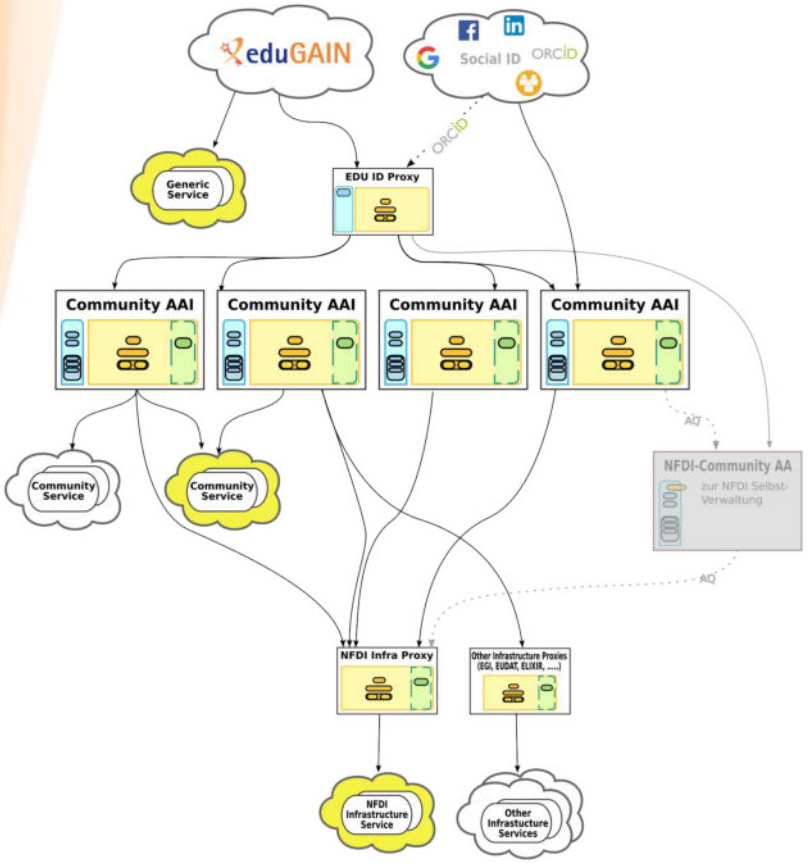
DAASI International

didmos Provisioner

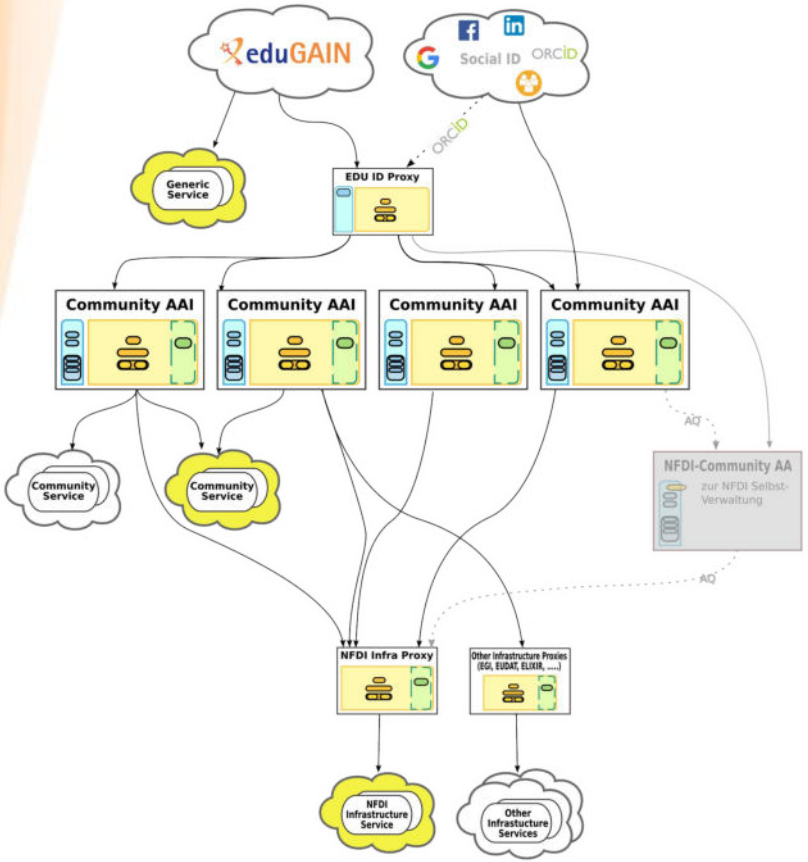
- Real-time transfer of identity information to connected target systems
  - Reads change information in the OpenLDAP accesslog
  - Architecture is inspired by SPML, however it can implement SCIM as well
- Changes are recorded in JSON documents which are inserted into the queuing system RabbitMQ
- A dedicated worker then installs them in the target system and reports back to didmos Core
- We have workers for
  - LDAP, Active Directory
  - SCIM2
  - Gluu
  - Other proprietary systems of customers

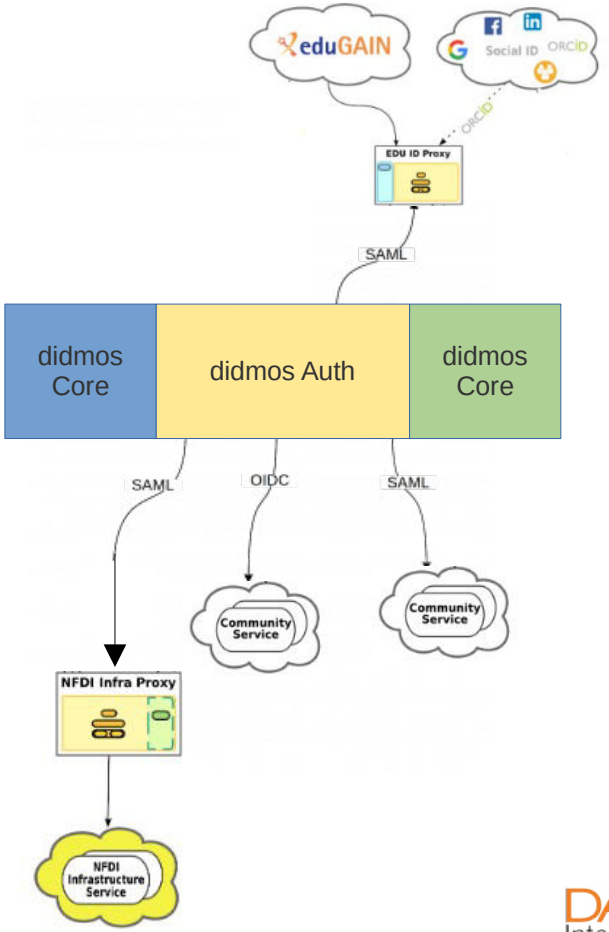
DAASI International

NFDI integration



NFDI integration





What we’re working on

- We’re currently implementing the NFDI attribute model into our default config and refining our CI/CD processes
- We’re setting up a demonstrator that consists of our main components to implement the integration scenario shown on the previous page
  - didmos Core, didmos LUI and didmos Auth
- The multi tenancy capabilities of didmos can be used to onboard different communities
- Once the Edu ID system is available, we will connect to that. For now we integrate eduGAIN directly
- We can create and deploy individual deployments for more complex projects, either on-premise or as a SaaS solution
  - In such projects we can also add didmos ETL Flow to sync existing user data and didmos Provisioner for systems that do not support SSO ...
  - ... or to support push (de)provisioning in addition to SSO

DAASI International

Thank you for listening.

David Hübner

DAASI International

email: david.huebner@daasi.de

Karlsruher Institut für Technologie

RegApp AAI – Community AAI, Infrastructure Proxy

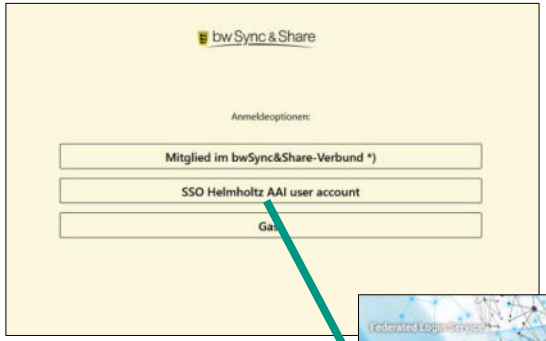
regapp.nfdi-aai.de

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

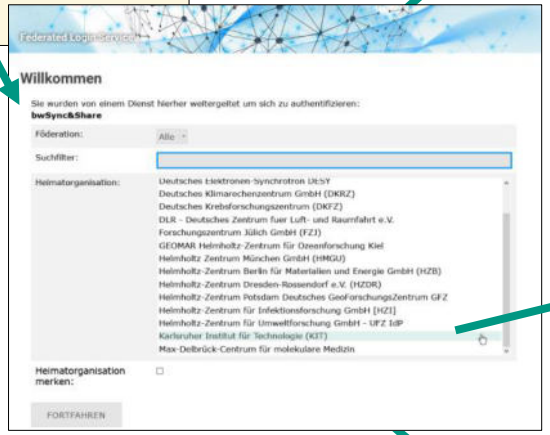
Overview and History

- 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…
  - Used at bwIDM, bwIDM2, NHR, Helmholtz Association…
- Mainly developed at the Steinbuch Centre for Computing (SCC) at KIT
- Currently installed setup manages more than 40,000 registered users from various research institutions (DFN-AAI)

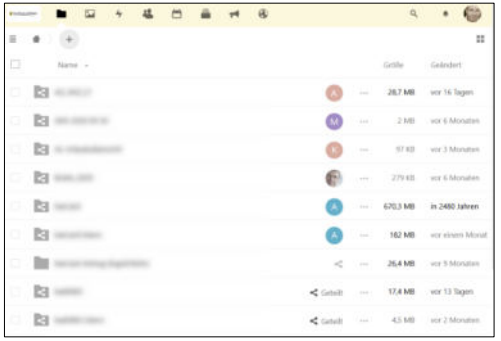
Typical Login Process



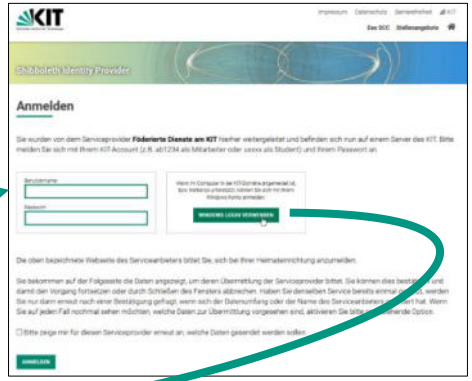
Service



RegApp Instance

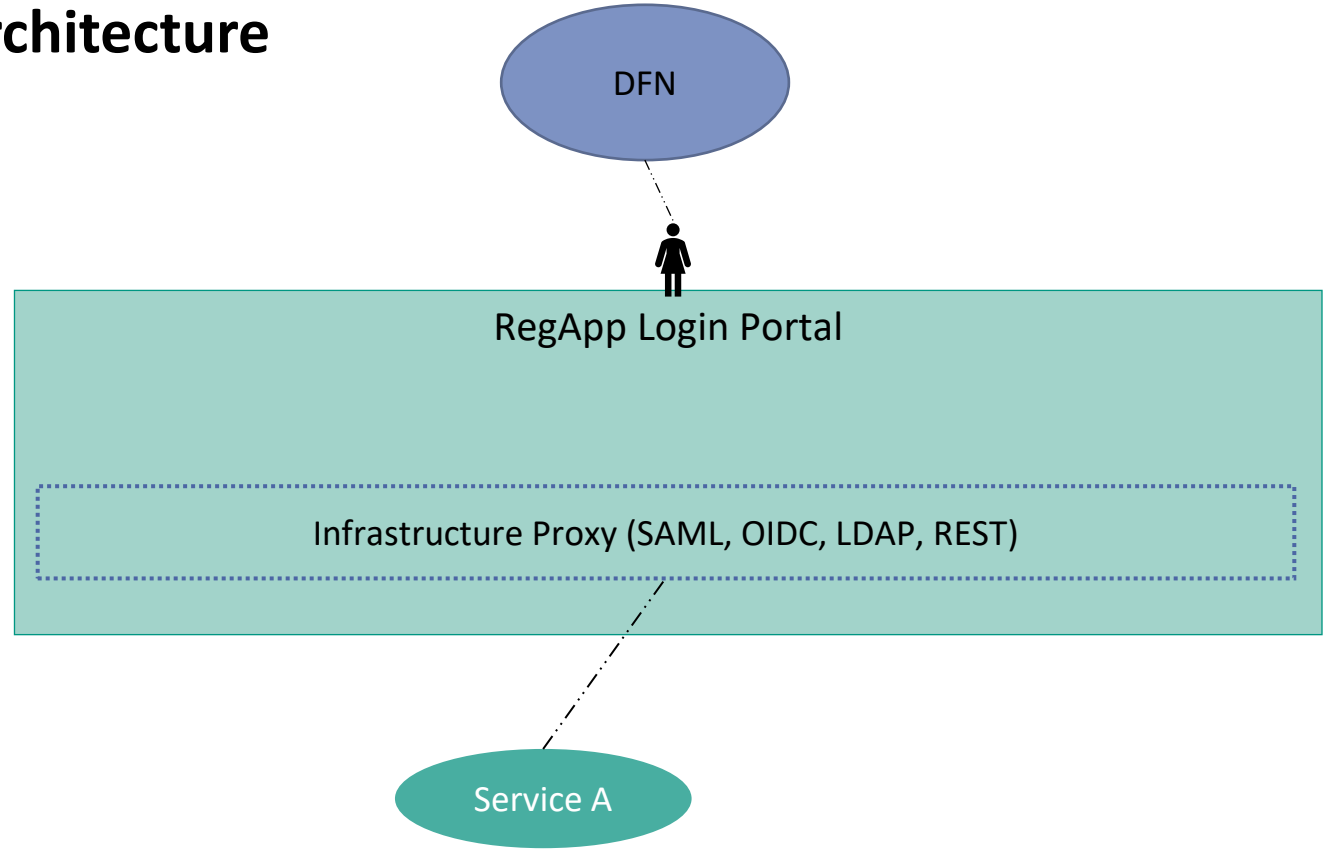


Service

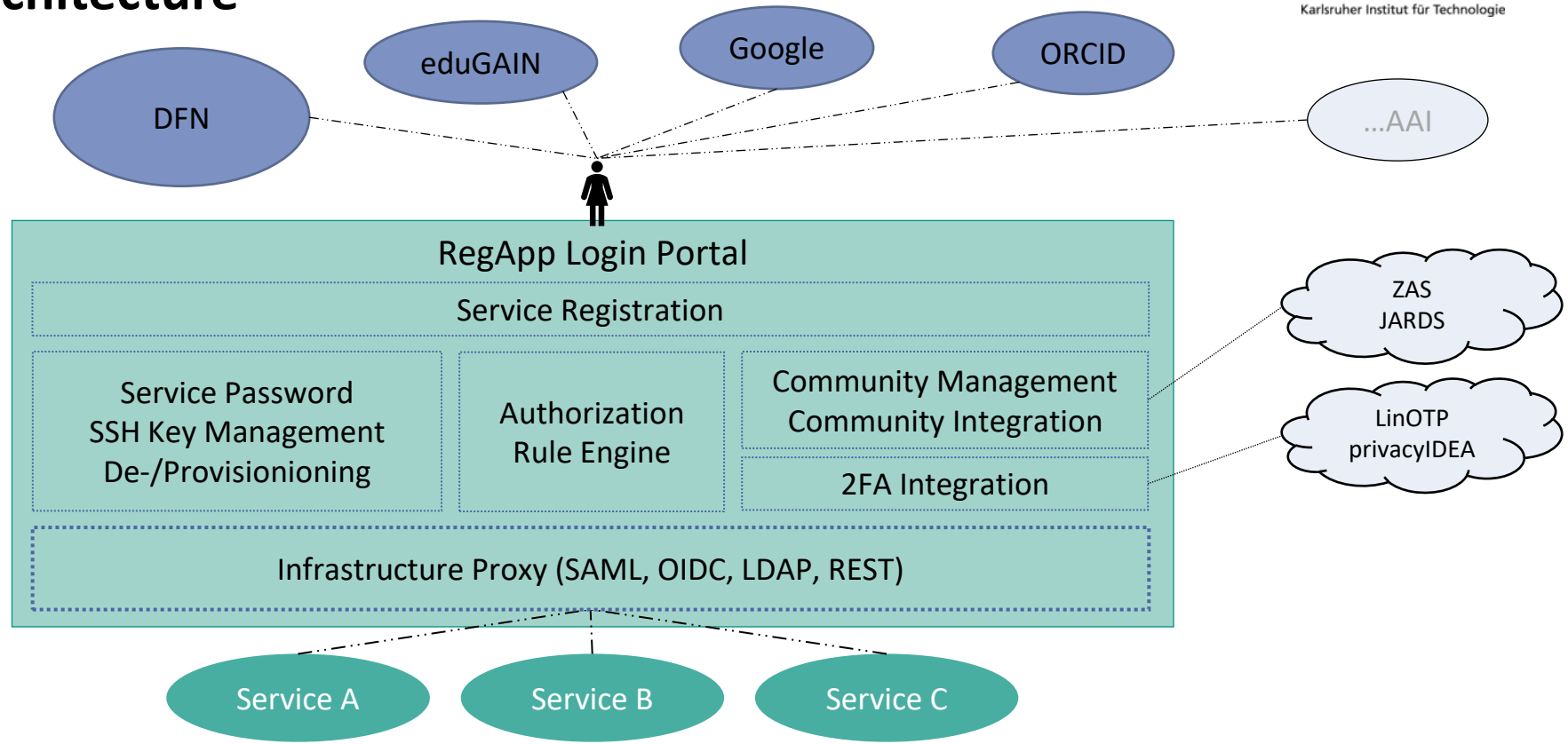


Home IdP

Architecture



Architecture



Features

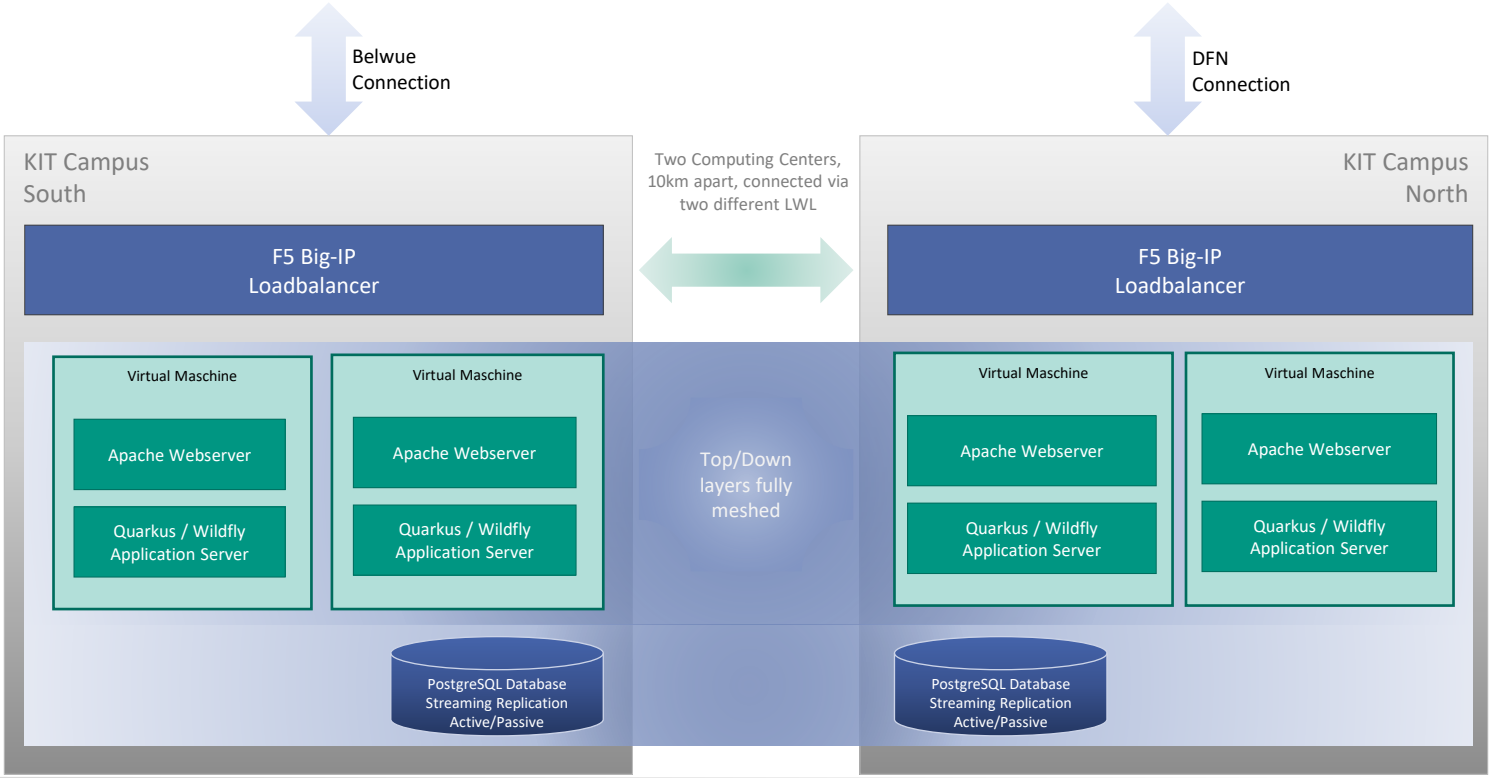
- **Core funcionality: Community AAI for Single Sign On Environments**
  - Transparent connection of SAML federations
  - Provisioning and deprovisioning (linked user identities, with SAML AQs)
  - SSO protocol proxy OIDC ↔ SAML
  - Infrastructure proxy for non web service (LDAP, REST)

- **Additional functions**
  - End user portal for service registration and group management
  - Management of SSH keys / service passwords (CLI/HPC login)
  - Multifactor authentication (LinOTP/privacyIDEA, also available for CLI/HPC logins)
  - Freely programmable authorization rules and attribute processing/release

AARC compliant

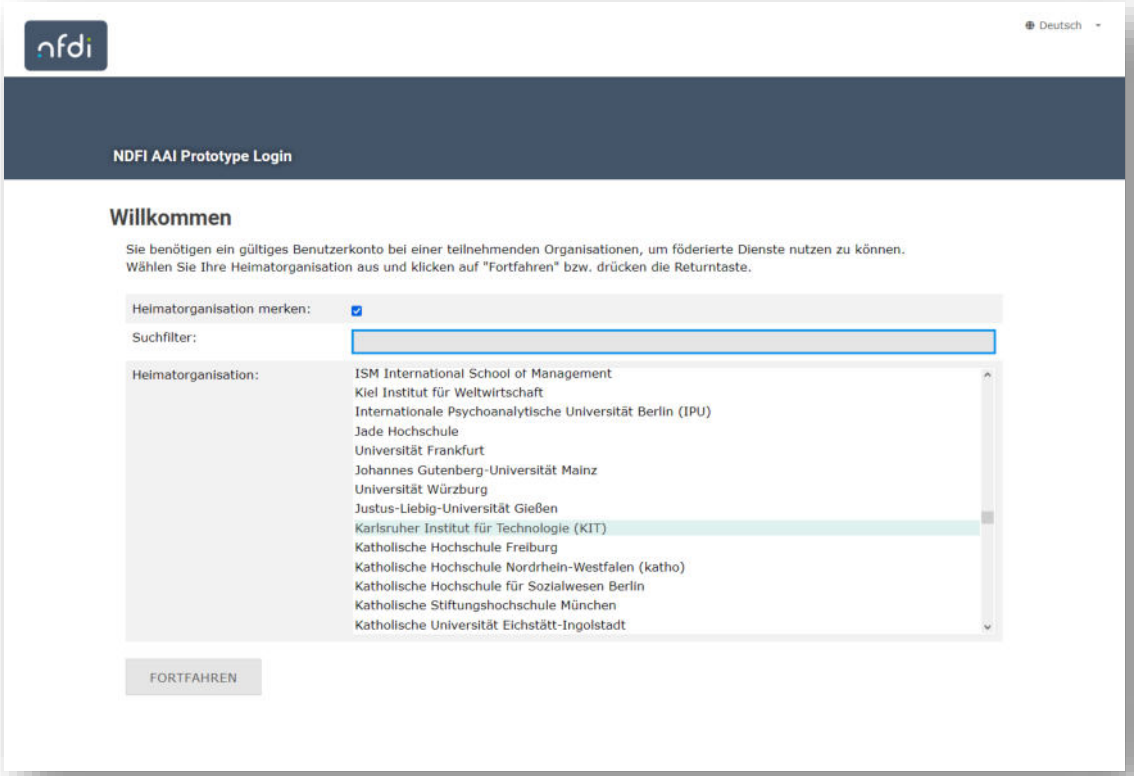
Authentication and Authorisation for Research and Collaboration
https://aarc-project.eu/

RegApp for NFDI: 4 Servers / 2 Locations



Setup architecture approved since 2011 in bwIDM with ~40k users, connected to HPC systems and standard services

RegApp for NFDI: Customized Frontend



Production-ready setup for NDFI

Future Developments

- Improving the community functionality (in progress)
  - Project and virtual organization management
  - Active group membership provision
  - Invitation of external persons by email/link
- Support of modern authentication methods (planned)
  - FIDO2 keys for SSH login
- Internal redesign/modularisation (ongoing…)
  - Wildfly J2EE → Quarkus framework
  - Server-rendered management webpages → SPA with Angular

Further Information

- **RegApp**
  - Deutsch: www.scc.kit.edu/dienste/regapp
  - English: www.scc.kit.edu/en/services/regapp
- **Downloads**
  - Gitlab: https://git.scc.kit.edu/reg-app/reg-app
  - Docker https://git.scc.kit.edu/reg-app/regapp-docker
- **References**
  - In NFDI context: regapp.nfdi-aai.de
- **Contakt**
  - uli.weiss@kit.edu and michael.simon@kit.edu

Unity basics

- First release was already 2015
- Was developed in context of UNICORE and became a spin-of company Bixbit
- Fully open-source
- Is based on Java
- Already used on several places around EOSC:

base4 nfdi

Unity instances at Forschungszentrum Jülich

- EUDAT B2ACCESS
  - AAI with following SP-IdP Proxy concept
  - Started 2015
- Helmholtz AAI
  - Started in Helmholtz Data Federation (HDF) Projekt and continued in Helmholtz Federated IT Services (HIFIS)
  - AAI following SP-IdP Proxy concept without local user accounts
- FURMS
  - User and Resource provisioning tool in FENIX
- JSC login Service
  - Started as translation from LDAP to OIDC
  - Becoming a full SP-IdP-Proxy in JSC
  - Streamline access to local services, independent to the user origin

base4 nfdi

Unity Features

- Fulfilling AARC BPA
- Offers upstream authentication based on SAML, OAuth2/OIDC, LDAP
- Supporting SAML federations out of the box
- Pre-configured “social” IdPs
- Offers accounts to “homeless” user based on X.509 or username/password
- SCIM API for updating user information
- Build-in extensions for account linking, policy management, group management, MFA using TOTP or FIDO
- Powerful configuration makes it easy to follow multiple standards and guidelines like SAML2, OAuth2/OIDC, AARC, ...

base4 nfdi

Upcoming enhancements

- Bringing deprovisioning agent (external tool) in production
  - Successfully tested on development instance
  - Notifying services needs to be implemented
- Improving MFA
  - Signaling MFA usage to services based on protocol standards
  - Honoring MFA from upstream IdPs
- Continuous enhancements based on user feedback
  - Gathering feedback from users and recurring problems in tickets and provide this to Bixbit
  - Next release contains improvements in sending bulk group invitations

base4 nfdi

Community-AAI-as-a-Service

base4nfdi

Goals of IAM4NFDI for CAAIaaS

- Provide documentation and serivces to enable NFDI Consortia to
  - either use an existing instance of a CAAIs as a ***tenant,*** *or*
  - get professional services to install, configure, customize and support an ***individual instance*** of either CAAI solution and
  - get professional hosting environments for operating ***individual instances*** of the CAAI solutions.

- Disclaimer: the CAAI solution of your choice may not support both deployment models (tenant/individual instance).

base4 nfdi

Generic Procedure for setting up a CAAI for NFDI Consortia

- Analysis and documentation of the NFDI Consortium requirements for its CAAI.
- Selection of the CAAI solution e.g. on the basis of a criteria catalog for required features.
- Providing/choosing a hosting environment for the CAAI (individual instance only).
- Basic installation and configuration of the CAAI solution (individual instance only).
- Implementation and roll-out of community-specific requirements.
- Preparations for productive operation: e.g. providing 1st and 2nd level support for community members.

Comparison of Deployment Models

Multi-tenant Deployment

- Operation of infrastructure and CAAI solution as well as 2nd/3rd level support is taken over by the CAAI provider.
- Limited possibilities for individual customizing of CAAI solution.

Deployment of Individual Instance

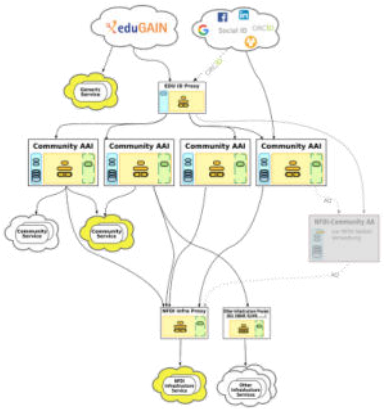
- Own hosting environment is required.
- Common operational aspects need to be addressed, e.g. backup, monitoring, load balancing, failover, support
- Outsourcing of all or specific hosting/operational parts to a third-party provider is possible.
- Extensive possibilities for individual customizing of CAAI solution.

Current State & Next Steps for CAAIaaS

- For the four CAAI solutions in IAM4NFDI, there are already productive examples in which a multi-tenant and/or individual deployment is used for some communities.
- For each of the four CAAI solutions, a demo instance will be set up and operated as part of IAM4NFDI, which NFDI consortia can use to evaluate the solutions.
- The implementation, hosting and operation of tenants or instances of CAAI solutions for NFDI consortia are *not* part of the IAM4NFDI project.
- DAASI and GWDG will offer professional (paid) services for the implementation, hosting and operation of CAAI solutions for the NFDI consortia.

Field Report: RDMO Integration

base4nfdi

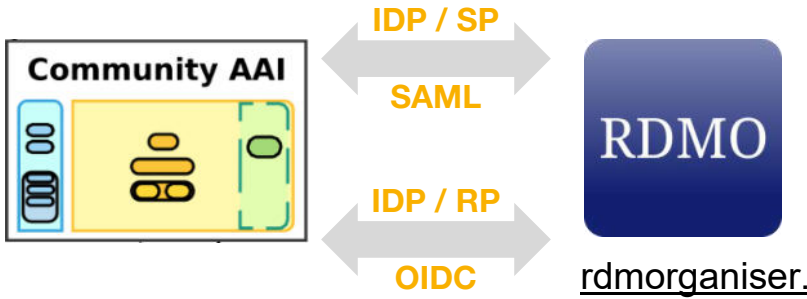


https://doc.nfdi-aai.de

Recap: Workshop IAM Basic #1

Community AAIs would solve our problem to support both SAML and OIDC users

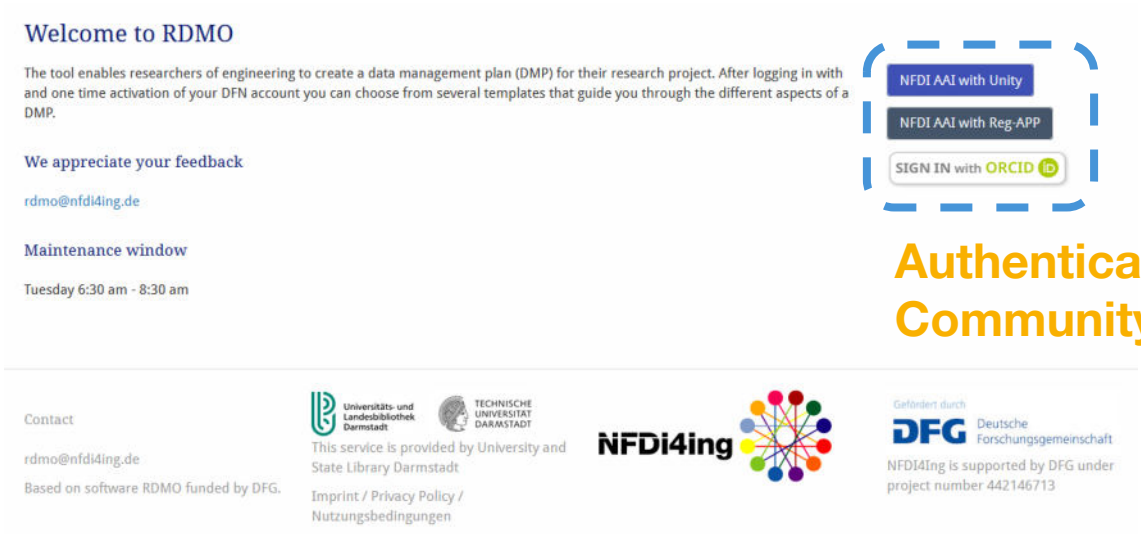
- Implementation in RDMO would be straightforward because of OIDC
- Looking forward to authentication via a Community AAI (CAAI) !



rdmorganiser.github.io/

Web service

RDMO NFDI4Ing test instance



Authentication with a Community AAI

Also currently in-use in the productive instance **rdmo.nfdi4ing.de/**

Overview of how-to connect a service with a Community AAI

Starting point: doc.nfdi-aai.de/

Information:

- Ideally, there are docs provided by the specific CAAI providers.

Registration, Policy and Security Contacts:

- Registration of the service
- Provide the required legal documents and/or references
  - the service needs a valid Data Privacy Statement (!)
- Provide admin and security contacts

Technical implementation:

- Re-use an existing OIDC/SAML solution that is compatible with your service?
- Consider the user authentication and sign-up flow
- Existing user accounts?
- Staging and production instances

Implementation: registration

Register your service as an OIDC client in the CAAI

Information:

- This example is for the CAAI type Unity provided by the Helmholtz AAI
- Docs: hifis.net/doc/helmholtz-aai/howto-services/

Registration, Policy and Security :

- Self-registration, submit a request to register a new client.
  - Organizational: Name, description, contact, Data Privacy Statement, logo
  - Technical: **client ID** and **secret** (username/pass), redirect URLs
- Request will be reviewed by the CAAI admins.
- Client can be used when the request is accepted.

Take-away for your service:

- the **client ID** and **secret** will be used by your service
  - store them in a secure place! (eg. password manager)
- redirect URLs, one could add localhost for local debugging

Implementation: technical aspects in general

Technical implementation depends on software framework of the service

Information:

- Look for existing solutions?
  - OIDC certified libraries: openid.net/certified-open-id-developer-tools/
  - or uncertified: uncertified-openid-connect-implementations/
  - Via web search “OIDC client” or “social authentication” for your framework

Configuration:

- **client ID** and **secret**, deploy with environment variables?
- **server URL,** one URL of the CAAI can used to build the required OIDC endpoints
  - URL to the metadata of the OP configuration
- **scope**, defines the sets of user attributes that the service requests from the OP
  - Important for which attributes your service requires
  - doc.nfdi-aai.de/attributes/, emails are verified

RDMO implementation: Django web framework

A django PROJECT

The Django allauth library supports any OIDC compatible provider

Information:

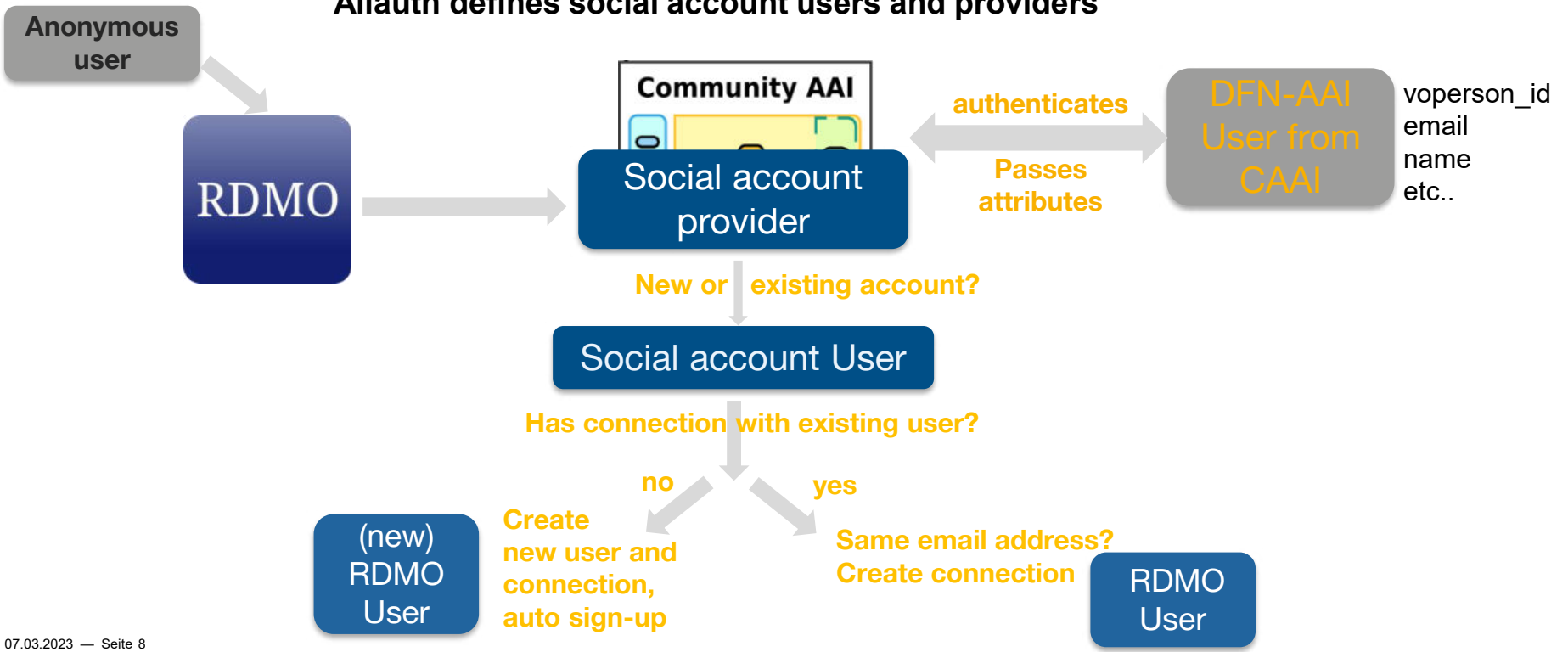
- Widely used and long-lived Django app, django-allauth.readthedocs.io/
- Supports any OIDC compatible provider, as well as many OAuth 1.0/2.0 and SAML 2.0, providers/
- Integrated with User Model, configurable authentication flows

Configuration:

- Implementing of the CAAI requires minimal adaption (if at all) of existing code.
- In the latest version, new OIDC providers can be added directly via the web admin UI without any codebase adaptation.
- Extraction or mapping of attributes
  - uid as voperson_id, take only verified emails

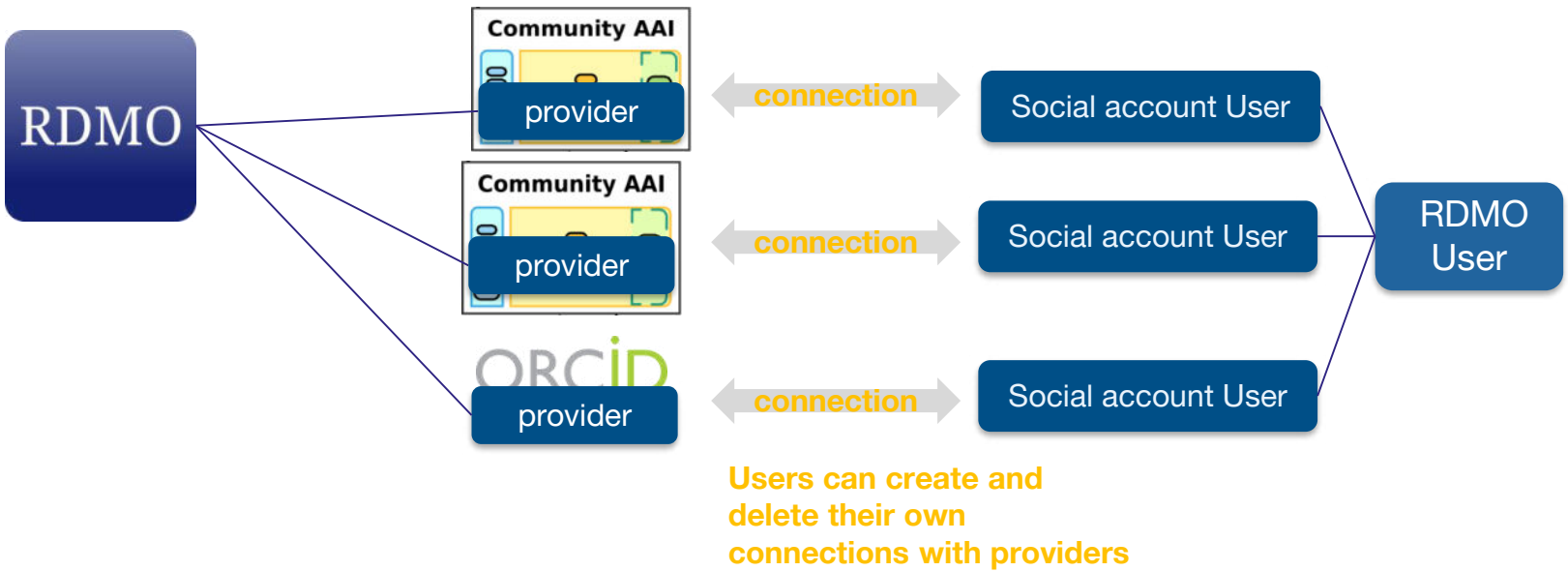
RDMO implementation: allauth and user flow

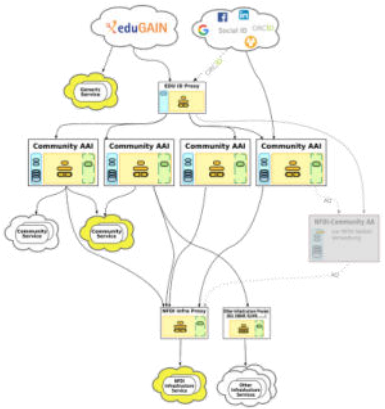
Allauth defines social account users and providers



RDMO implementation: multiple providers

Allauth allows for the use of multiple providers in parallel



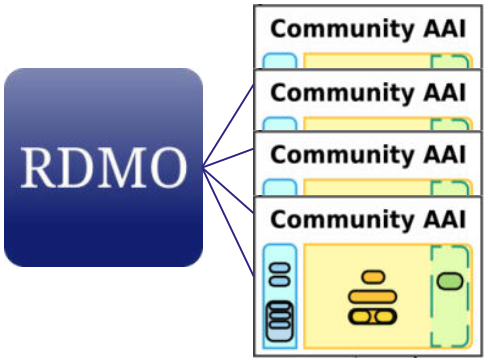


https://doc.nfdi-aai.de

Conclusion of field report and outlook

Community AAIs provide a straightforward authentication service

- ☑ documentation available for the service provider
- ☑ service registration via online form
- ☑ support for OIDC and SAML
- ☑ uniform user attributes, email verification
- ☑ user profile self service in CAAI
- Button logos like shibboleth?



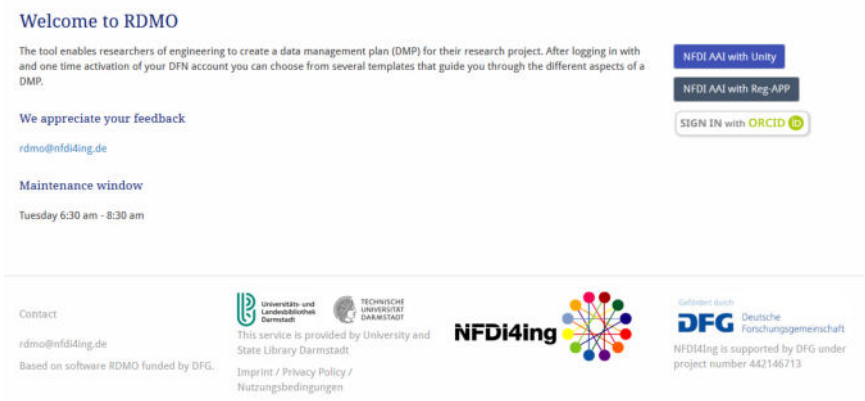
Unity ☑

RegApp ☑

didmos ➔ in September

AcademicID ➔ in September

Thank you for your kind attention!



David Wallace
Forschungsdaten-Services
ULB Darmstadt
david.wallace@tu-darmstadt.de

BREAK

Things you should know and be aware of when operating a Community-AAI

Authorization and VO Management

base4nfdi

Identity / User Management
Where do users come from?

- DFN-AAI, Edugain, Google, …?
- Discovery Service: Is a restricted list (of home institutions or of NFDI communities) useful?
- Can the same user come from several sources?
    - If yes: How do you match identities? (Name, date and place of birth, ….)
    - Don‘t use the email address as primary key to identify users!
    - Will most likely become easier with the Edu-ID-Proxy.
- If using Google or other social media accounts: Do you need and have sponsors?
    - → Principal Investigators / VO-Managers
- On existing systems: Migration of users to a new login way.

base4 nfdi

Identity / User Management
Deprovisioning

- Who clears the service of users that are no longer members?
- Can you do this via AttributeQuery (cf. https://doku.tid.dfn.de/de:shibidp:config-deprovisionierung)? (Will also get easier with the Edu-ID-Proxy.)
- Can you check whether necessary attributes (values) are still present?
- Can you lock users temporarily or permanent?
- What happens when a user is deprovisioned?
    - Which data of the user can or must be deleted?
    - Which data should stay (we are an NFDI…) and for how long?
    - Who takes care of these?

Authorization

- Who decides about the rules for access to the system?
- How can you implement these rules?
  - Do you get all the neccesary attributes (values) from the IdPs?
  - Do these have to get transformed? Are there standards for entitlement values?
- Who can set attribute values manually, if necessary?
- Can there be manual additions to user objects by service admins? If yes:
  - Who are the service admins?
  - Who confirms service admins or informs about personnel changes?
  - Does the service have / need admin groups?

Technical aspects

- How gets a service connected technially (SAML, OIDC, LDAP, ...)?
  - If LDAP: Does the service has its own LDAP that needs to be filled by the CAAI?
    Or does the CAAI have to provide an LDAP (-tree)?
  - Does the service need a certain tree structure? Special groups?
- When SSL certificates are changed (on the service or the CAAI): Can the certificates be provisioned automatically, e.g. via DFN-AAI metadata administration?
- Reporting and audit

Organisatorial aspects

- Who are the contact persons for a service?
- Is there a service description for the users? Who writes this?
- Who gives user support on which level?
- For all persons who decide things: Is there a substitute, e.g. during holidays?
- Reporting and audit
- Bug hunting in multi-stage system like this needs coordination
  - There are at least three stages: IdP → CAAI → Service (+ the user)
  - Up to five stages:
    IdP → Edu-Id-Proxy → CAAI → Infrastructure Proxy → Service (+ the user)

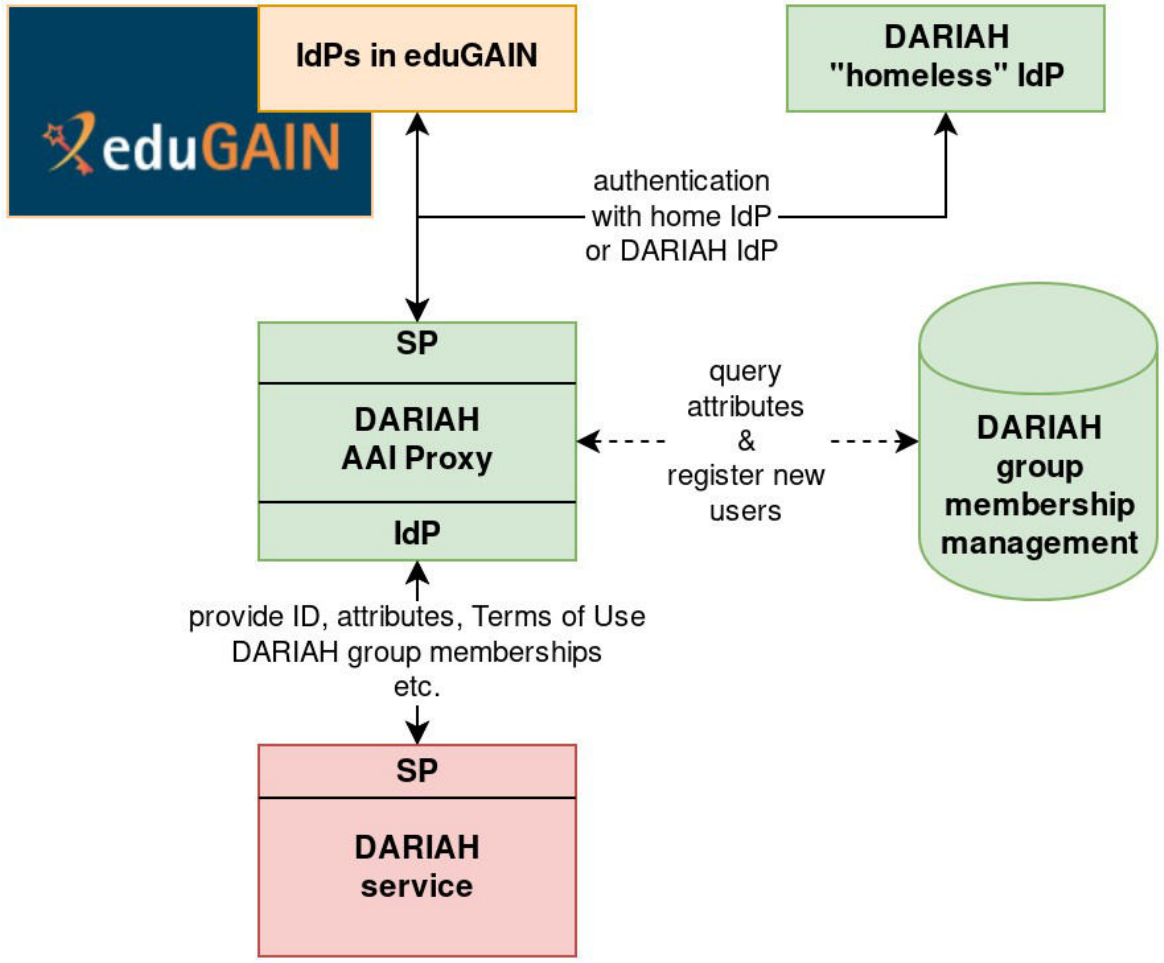
Things you should know and be aware of when operating a Community-AAI

Experiences of the CAAI-Operators

base4nfdi

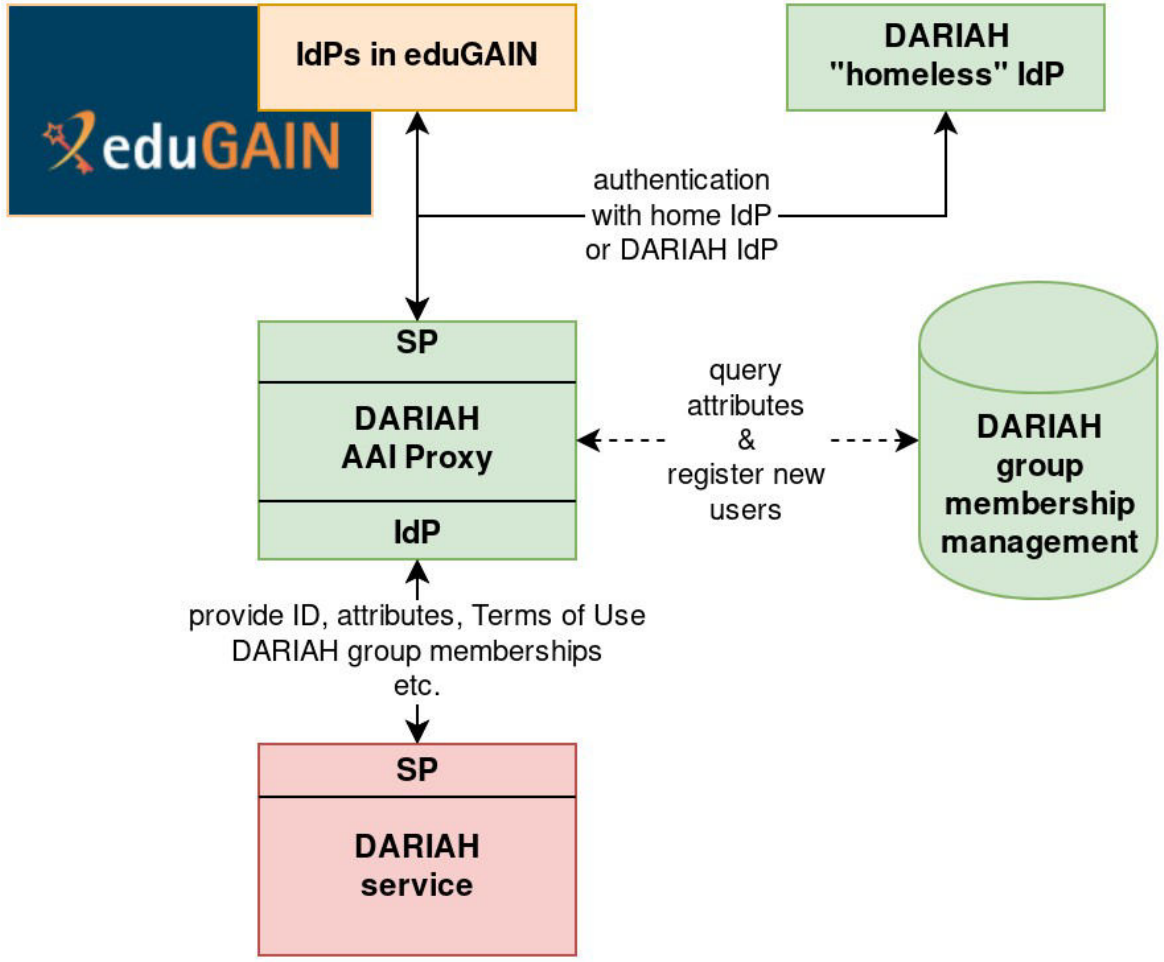
Operating the DARIAH-AAI

- In the DARIAH-AAI we offer a “homeless” IdP for users with no HO IdP identity from eduGAIN. This poses additional challenges.
- A lot of users do not have a HO IdP for various reasons (e.g. guest researchers)
- For these users vetting of identities is difficult, since we can’t rely on the information provided by the HO
- We use a combination of whitelisted email domains from known organisations and manual vetting based on information provided by the researchers
- Due to the DARIAH homeless IdP being in the DFN-AAI federation this vetting process is particularly important



Operating the DARIAH-AAI

- Service operators sometimes struggle to implement federated authentication (SAML or OIDC) in their applications
- To assist them, we provide documentation, incl. “How-To” tutorials for e.g. Shibboleth SP, technical trainings and workshops
- We set up and operated a Helpdesk:
  - for technical questions, including service integrations
  - for end users, including account vetting on the “homeless” IdP
- Due to open standards (SAML2, OIDC, AARC guidelines, etc.) the actual technical solution is of less importance. We changed the AAI proxy component from Shibboleth to SimpleSAMLPHP without much problems
- Generally, sustainable and pemanent funding is needed for operating the service, which usually is difficult in research projects



Operating unity

- Used at EUDAT B2ACCESS, Helmholtz AAI, Clarin IdP, …
- Offers upstream authentication based on SAML, OAuth2/OIDC, LDAP
- Pre-configured “social” IdPs
- Offers accounts to “homeless” based on X.509 or username/password
- Build-in extensions for account linking, Policy management, group management, MFA using TOTP or FIDO
- Powerful configuration makes it easy to follow multiple standards and guidelines like SAML2, OAuth2/OIDC, AARC, ...

base4 nfdi

Operating unity

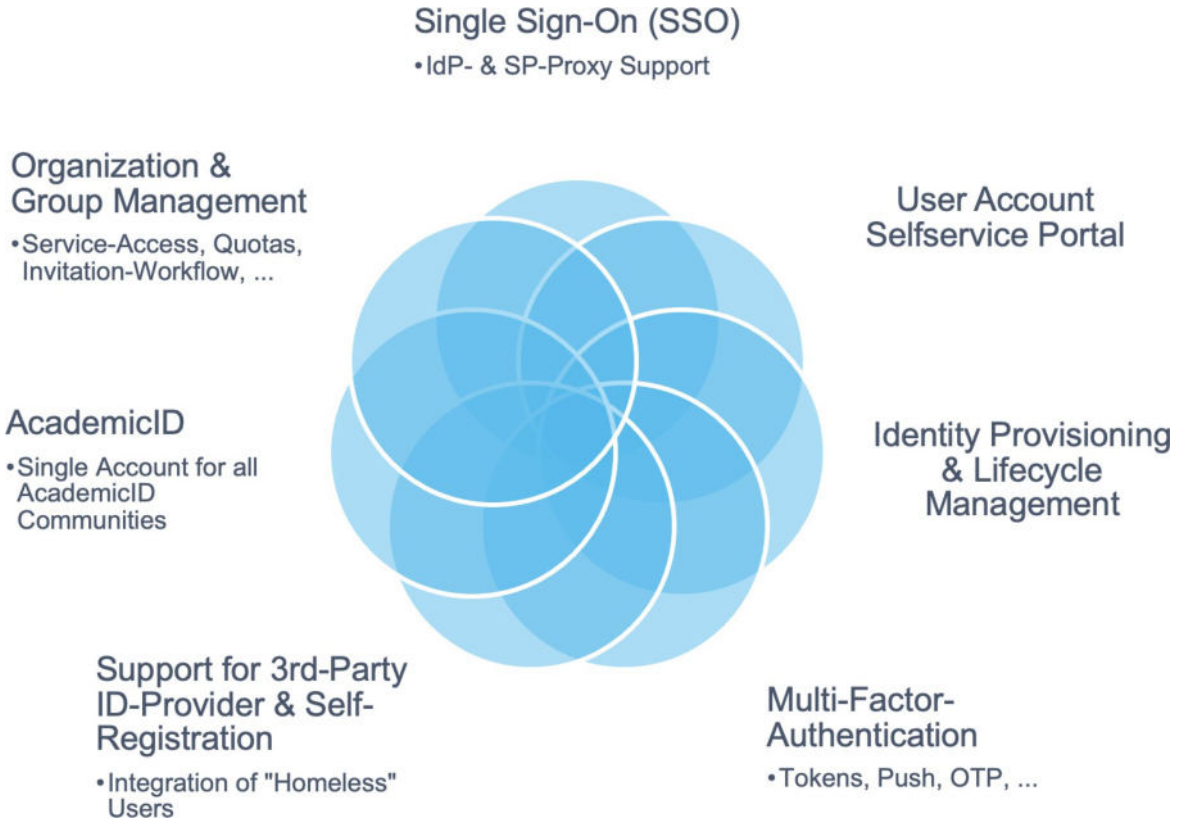
- X.509 handling is difficult since DN changes in renewal and can’t rely on information provided by the HO
- “Social” IdPs deliver different information and not all guarantee persistent identifiers
- Linked accounts are tricky in deprovisioning, if resources were bound to one of the upstream identities
- Deprovisioning based on an additional tool
- MFA needs some improvements in signaling and honoring MFA from upstream IdPs

base4 nfdi

Experiences of operating AcademicID

- Availability Management
  - Authentication & authorization services need to be available 24/7. Any interruption of these services needs to be fixed ASAP, otherwise no user can access any IT service. Operation of these services should cover: load-balancing, failover, monitoring (geo-)redundancy, backup, testing
  - Identity (de)provisioning and lifecycle services are less critical, since only a small number of users will usually be affected by an interruption.
- Security
  - IAM infrastructures are “crown juwels” that need a high level of security protection.
  - Restrict administrative access: use MFA, dedicated administration workstations and networks/VPNs, ...
  - Document and regularly audit critical changes, e.g. to administrative accounts.

AcademicID CAAI Solution



DISCUSSION

Questions?

Suggestions?

Solutions to open problems?

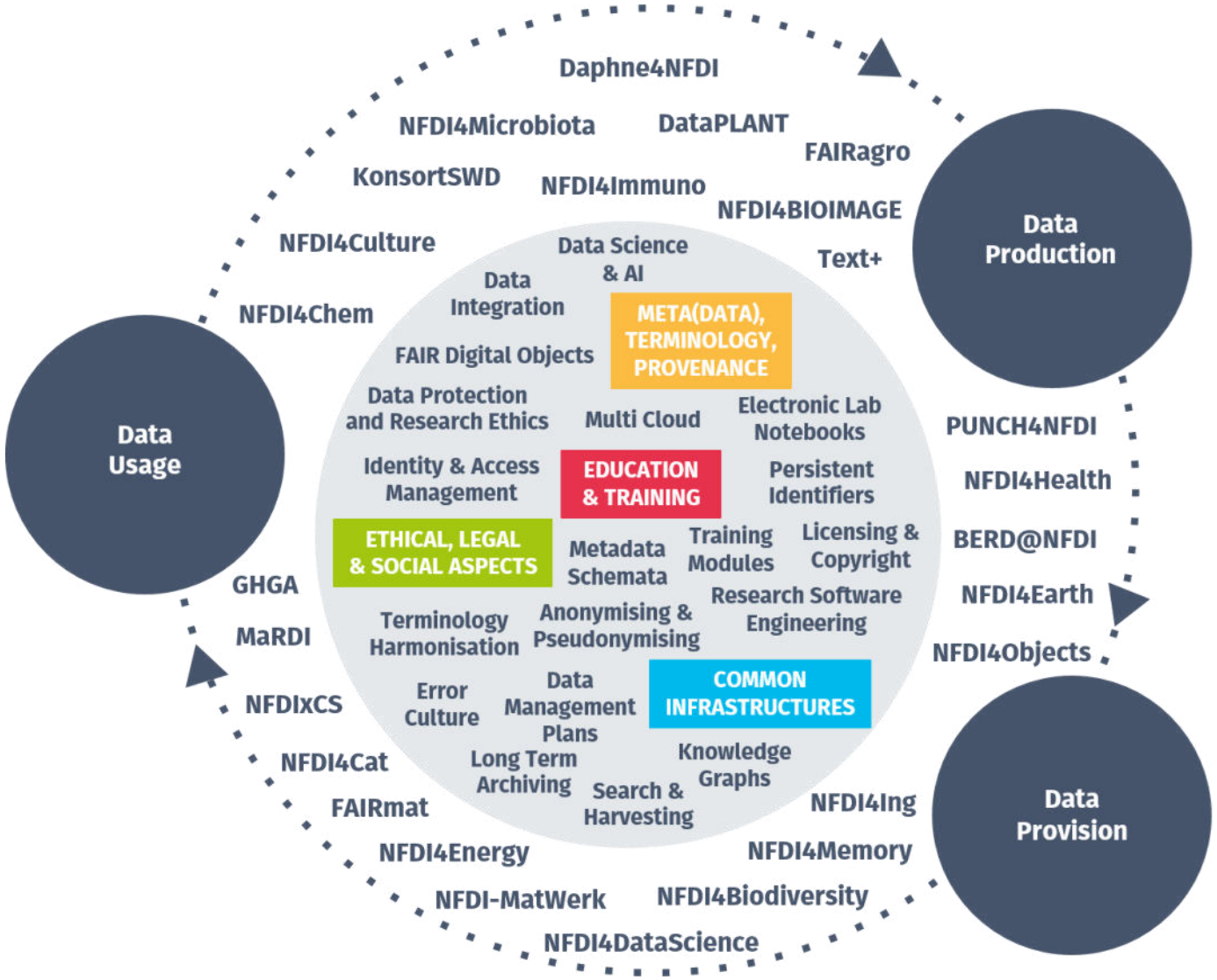
Experiences?

Summary, next steps & wrap up

base4nfdi

Next steps

- 3rd Workshop for the skipped topics: Trust and Policies, Security and Incidence Response
- Workshops for each of the four CAAI solutions
- Test instances of the four CAAI solutions to test integration of services and validating attribute release: ca. Q4 2023
- Approval of Policy Framework
  - Establishing a governance structure
- Infrastructure Proxy ca. Q3 2024
- Community-AA ca. Q4 2024
- Gather experience on connecting frameworks and technology to the CAAIs (e.g. Django)
- Incubator projects: Deeper integration of complex services, development of new features, based on community feedback: Starting sometime in 2024.



base4 nfdi

Funded by **DFG** as part of **NFDI**.

Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232