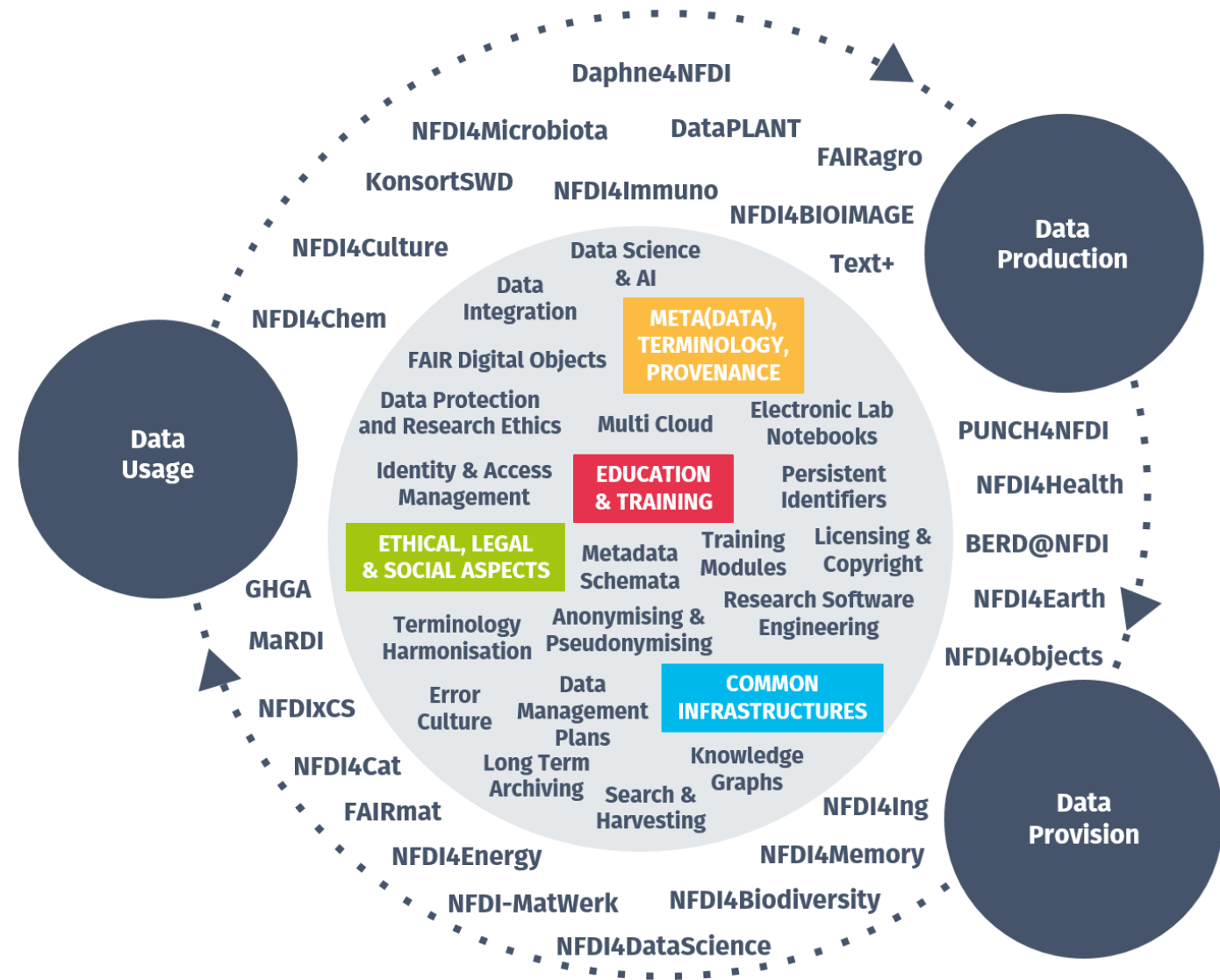


Infoshare IAM4NFDI

#1

2023-06-19



Agenda

- Introduction and Overview – Basic Concepts (W. Pempe)
- The Big Picture – NFDI and IAM (M. Hardt)
 - NFDI AAI and AARC Blueprint Architecture
 - Concept of Community AAls
 - Attribute/ Claim Profiles for NFDI AAI
 - Preview Policy Framework
- Community-AAI-as-a-Service (P. Gietz, Ch. Pohl)

Introduction and Overview

1. The Context: Federated Identity Management
2. AARC Blueprint Architecture and Community AAI
3. NFDI AAI

Wolfgang Pempe (pempe@dfn.de)

Basic Service IAM – IAM4NFDI

Initialization Phase

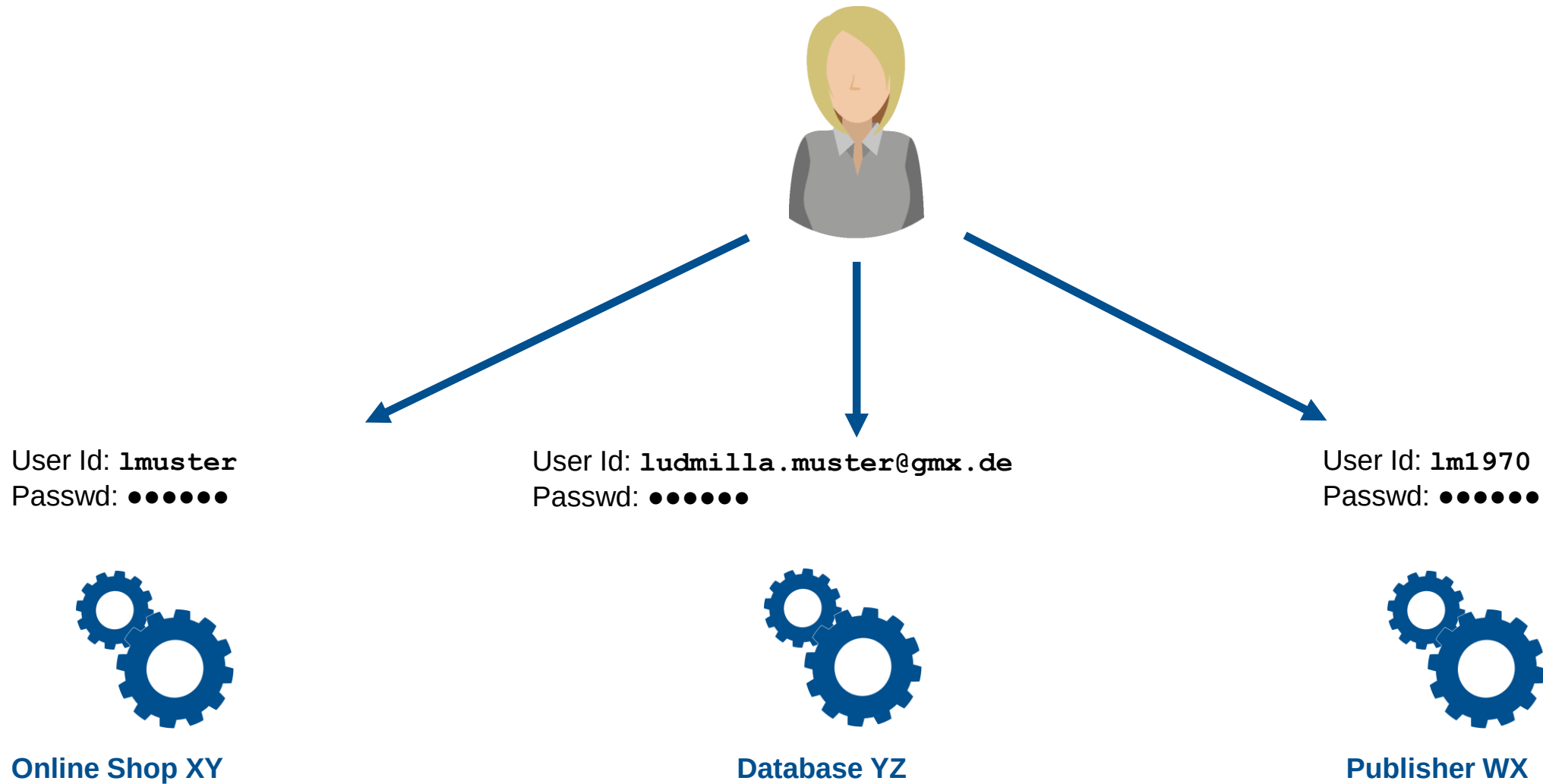
- May 2023 – October 2023

Work Packages

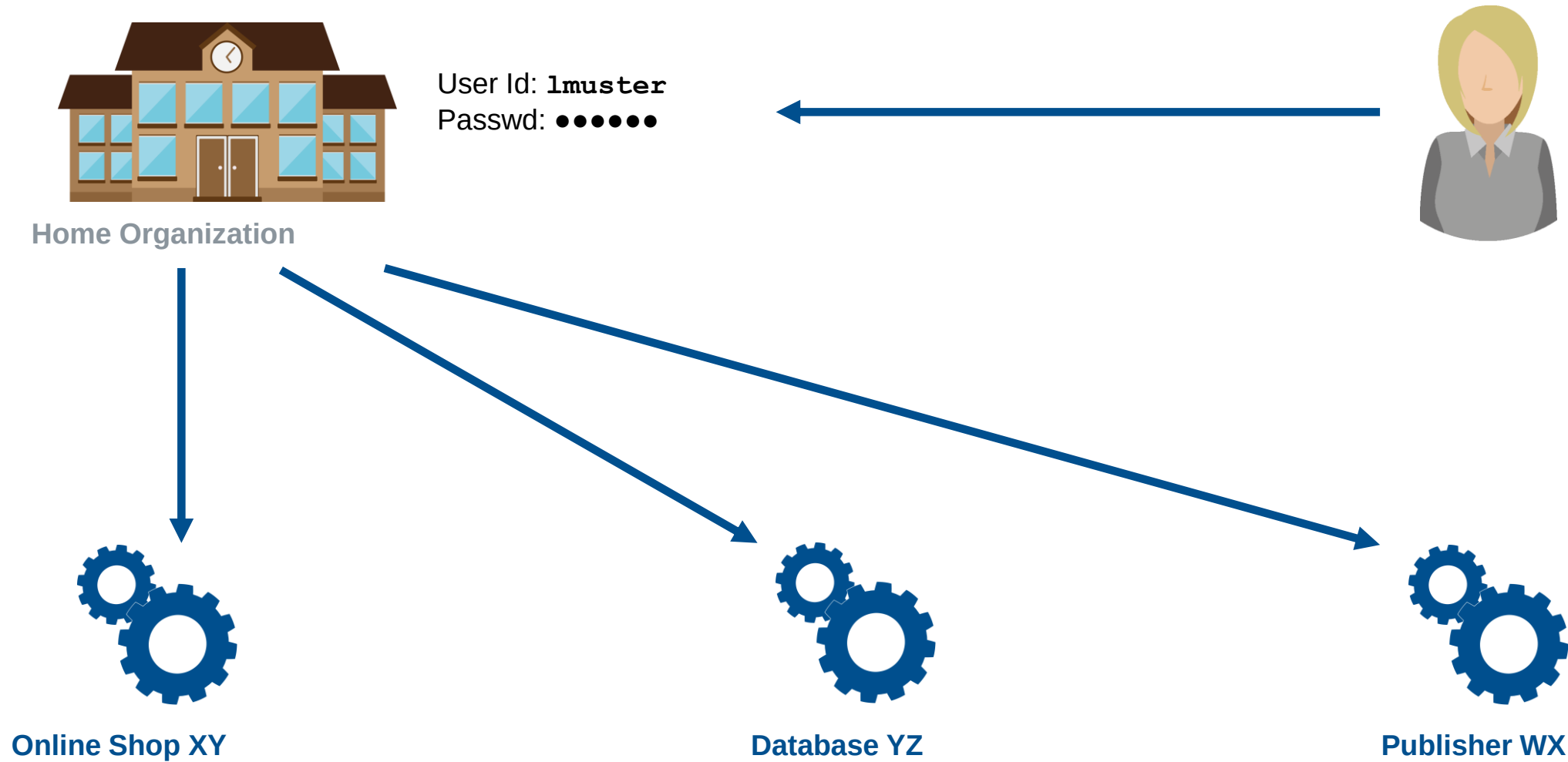
- WP1: Policy, Governance, and Legal Aspects
- WP2: AAI Architecture and Implementation (-> NFDI AAI)
- WP3: Incubator
- WP4: Operations
- WP5: Dissemination, Training, and Community Engagement

1. The Context: Federated Identity Management and Identity Federations

Service-specific Identities



Federated Identity



Some Terminology...

Federated Identity Management

- Exchange of identity data across service and organisational boundaries
- Avoidance of service-specific identities/accounts and credentials
- One identity source as leading system (usually the IdP of the Home Organization)

AAI = Authentication and Authorization Infrastructure

- The technical and organizational framework for federated identity management

AAI enables Single Sign-On (SSO)

- Log in once to access all services I'm entitled to use
- Usually relevant for web-based applications, but there are also solutions for non-web szenarios

Federation

Federated identity management requires a central instance (“trusted third party”): Federation Operator

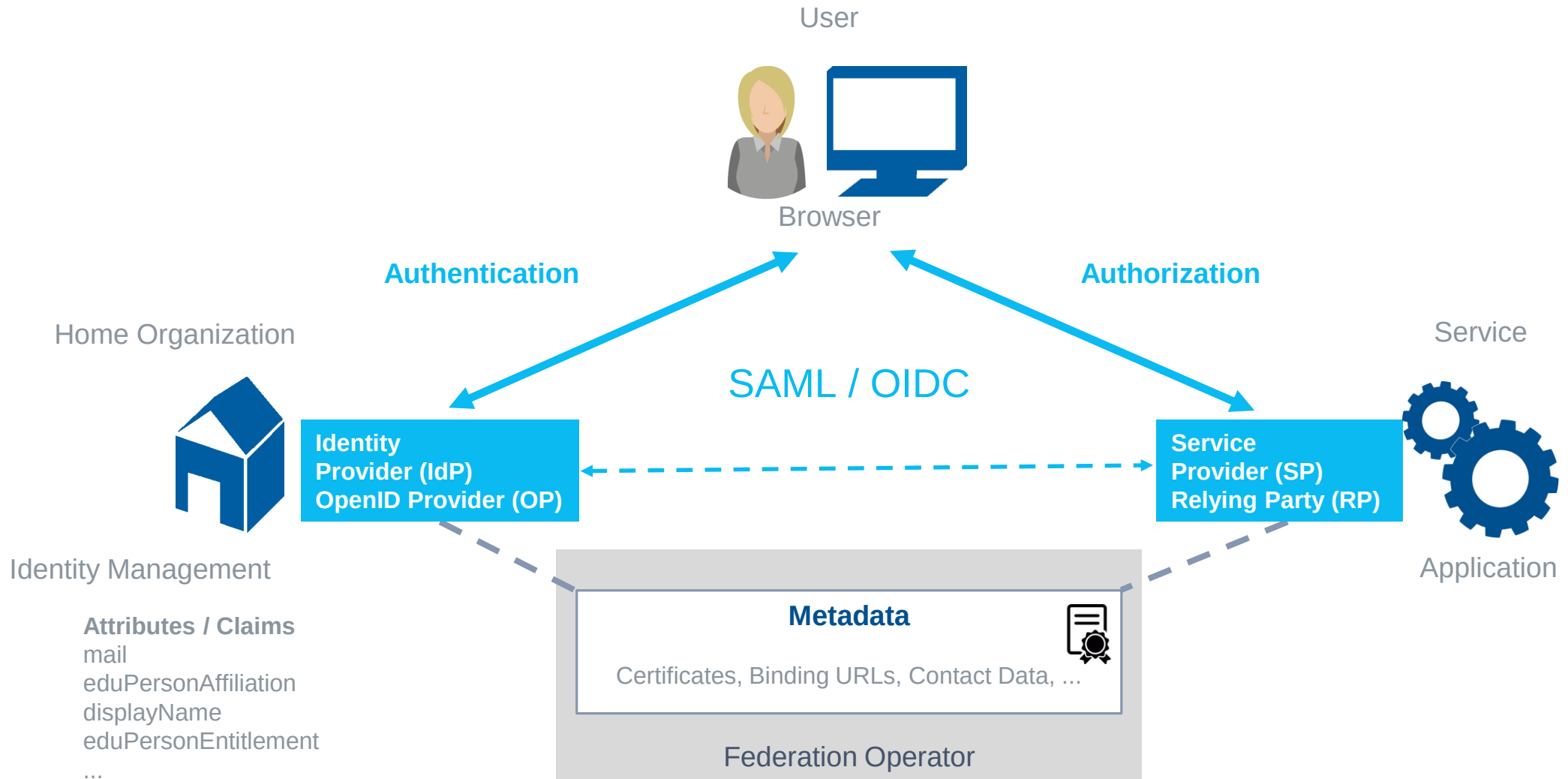
- Defines the organizational, technical and legal framework conditions
- ensures/enforces compliance with them
- and establishes the relationship of trust within the federation

DFN Association is operator of the cross-institutional federation DFN-AAI

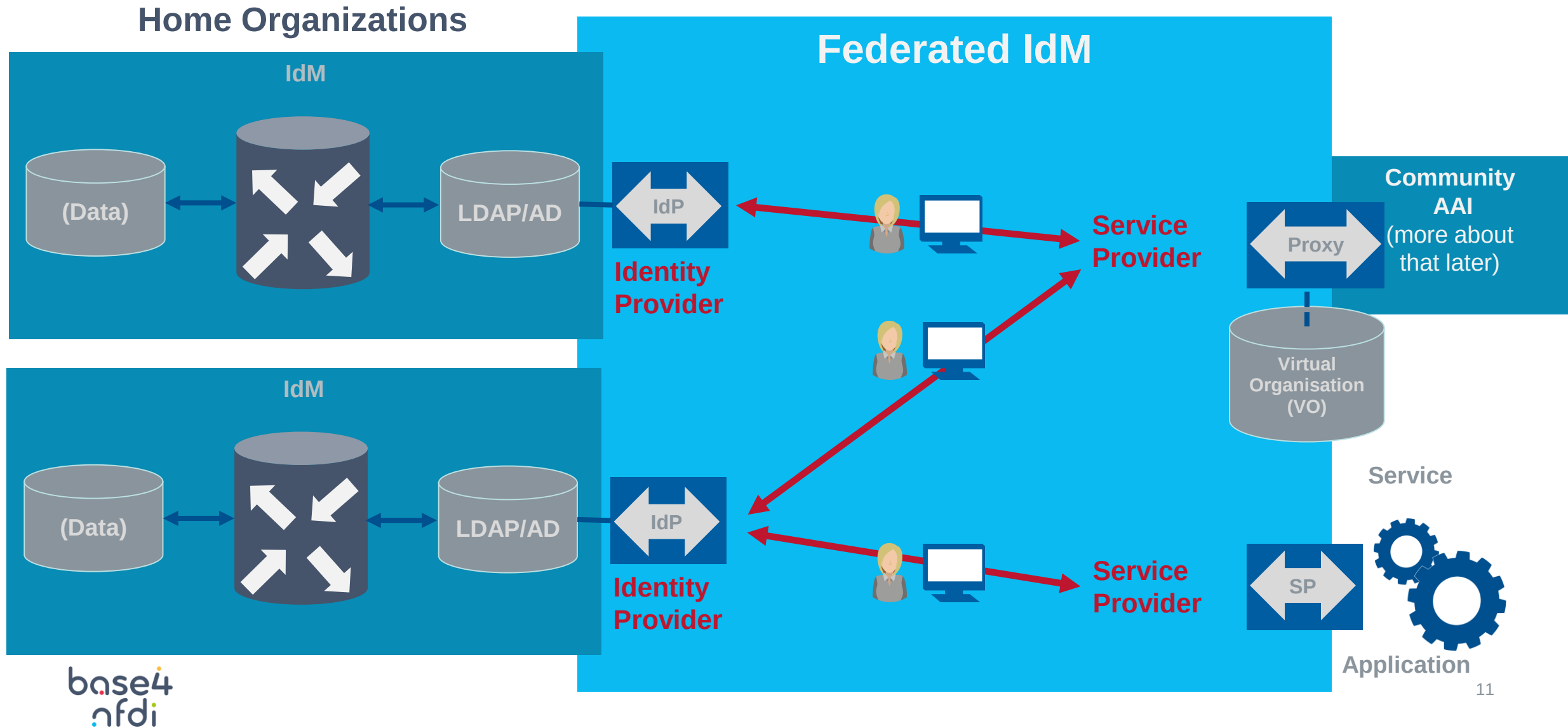
- Target group: Higher education and research institutions
- DFN holds contracts with about 420 Research and Education Institutions
- plus more than 200 contracts with external Service Providers (commercial and non-commercial)

The concept of Federation allows for hierarchies:
inter-federation (eduGAIN), sub-federations (bwIDM, IDM.nrw, ...)

How does a federation work?



The big picture



Example DFN-AAI

Federation Operator

DFN-Verein

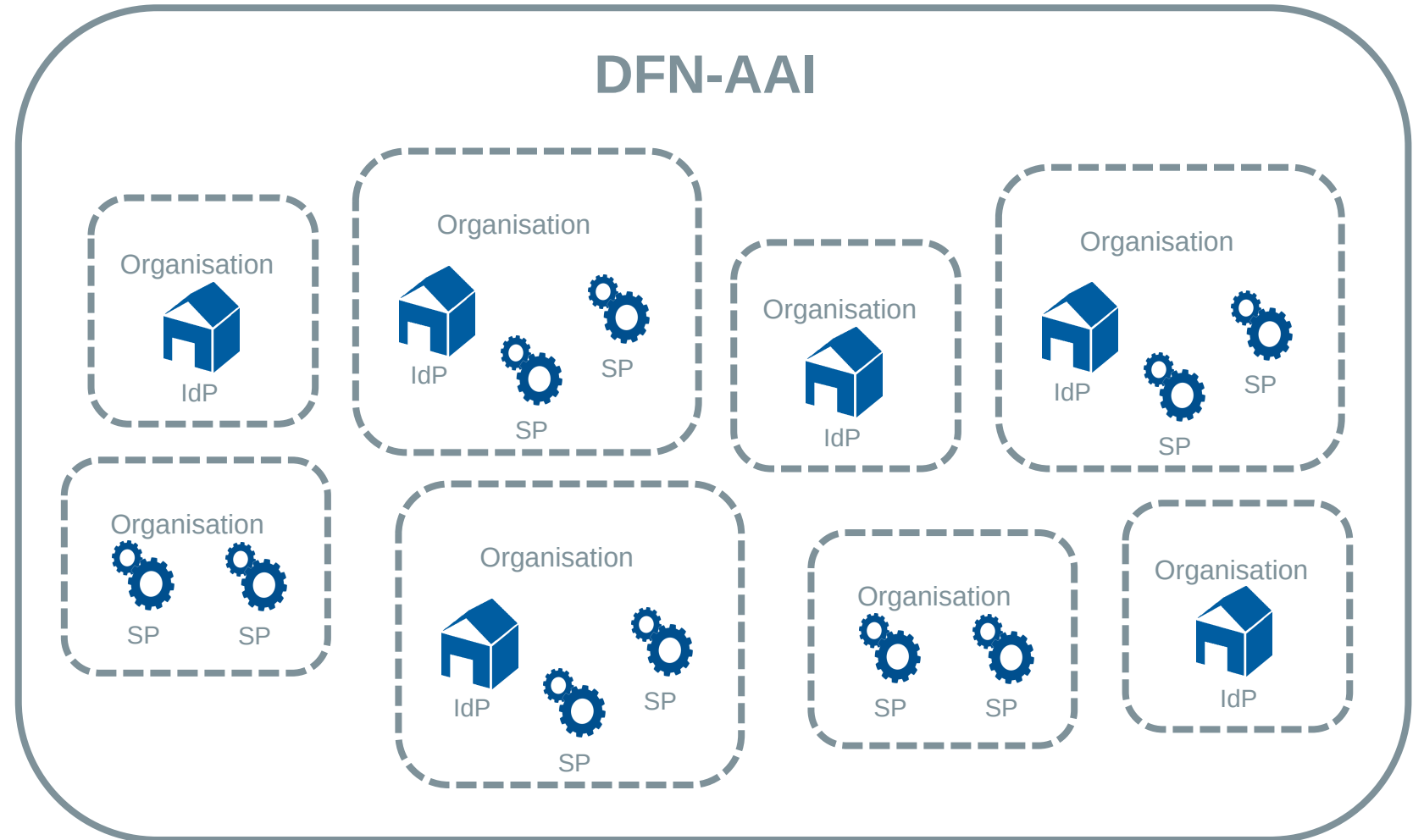
Trust

Contracts with all
Participants, Policies,
Levels of Assurance

Technical

Metadata Management
and Distribution

Currently 385 actively participating
Home Orgs and 760 Services
(plus ~1490 local SPs)



eduGAIN

eduGAIN is a global Inter-Federation

- Enables cross-federation AAI, i.e. collaboration between entities (IdP/SP) from other federations

Operated by GÉANT, in production since end of 2011

- DFN is one of the very first eduGAIN members

Basically a metadata exchange service:

- Aggregation of the metadata of the member federations
- Member federations are responsible for distributing the metadata within their constituency

No contracts between DFN and IdPs/SPs from other federations(!)

- Establishing inter-federation trust is still an issue...

eduGAIN – participating Federations

June 2023:

79 Federations

5.373 IdP, 3.615 SP

Participation DFN-AAI:

340 IdP (out of 385)

164 SP (out of 760)

■ eduGAIN ■ Voting-only ■ Candidate

<https://technical.edugain.org>

2. AARC Blueprint Architecture and Community AAls

The power of proxies

Wikipedia (https://en.wikipedia.org/wiki/Proxy_server):

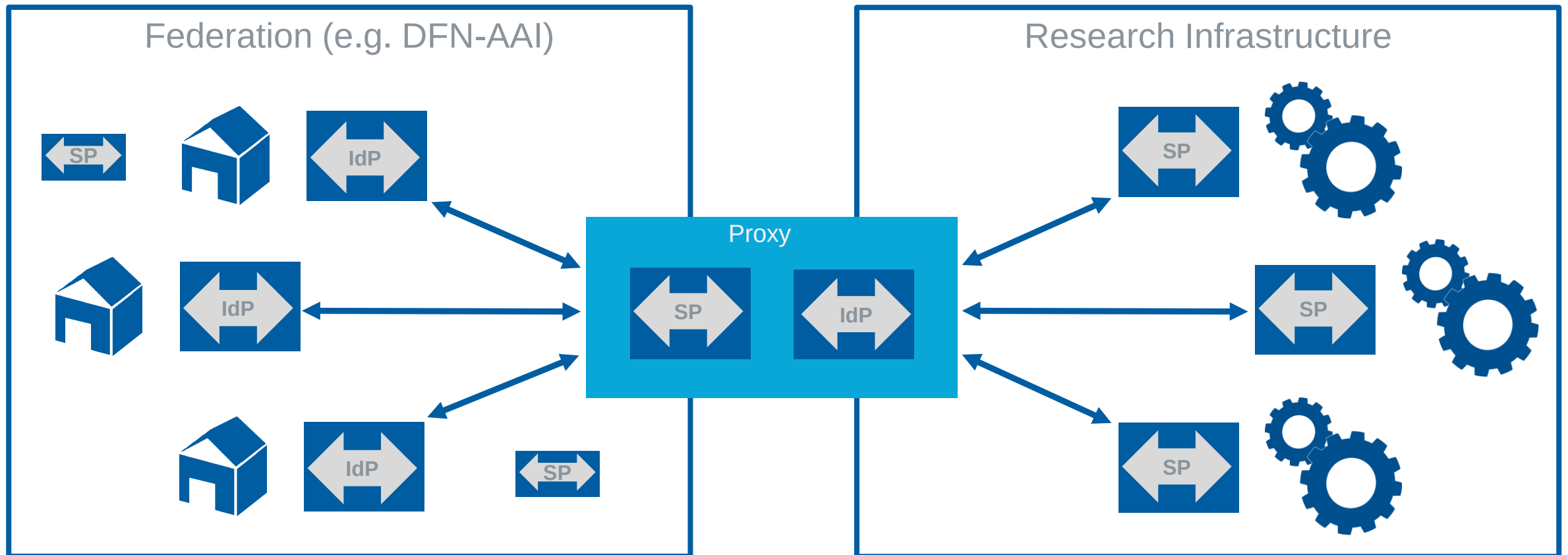
„[...] as a way to simplify and control [...] complexity. Proxies were invented to add structure and encapsulation to distributed systems.”

Federated Identity Management

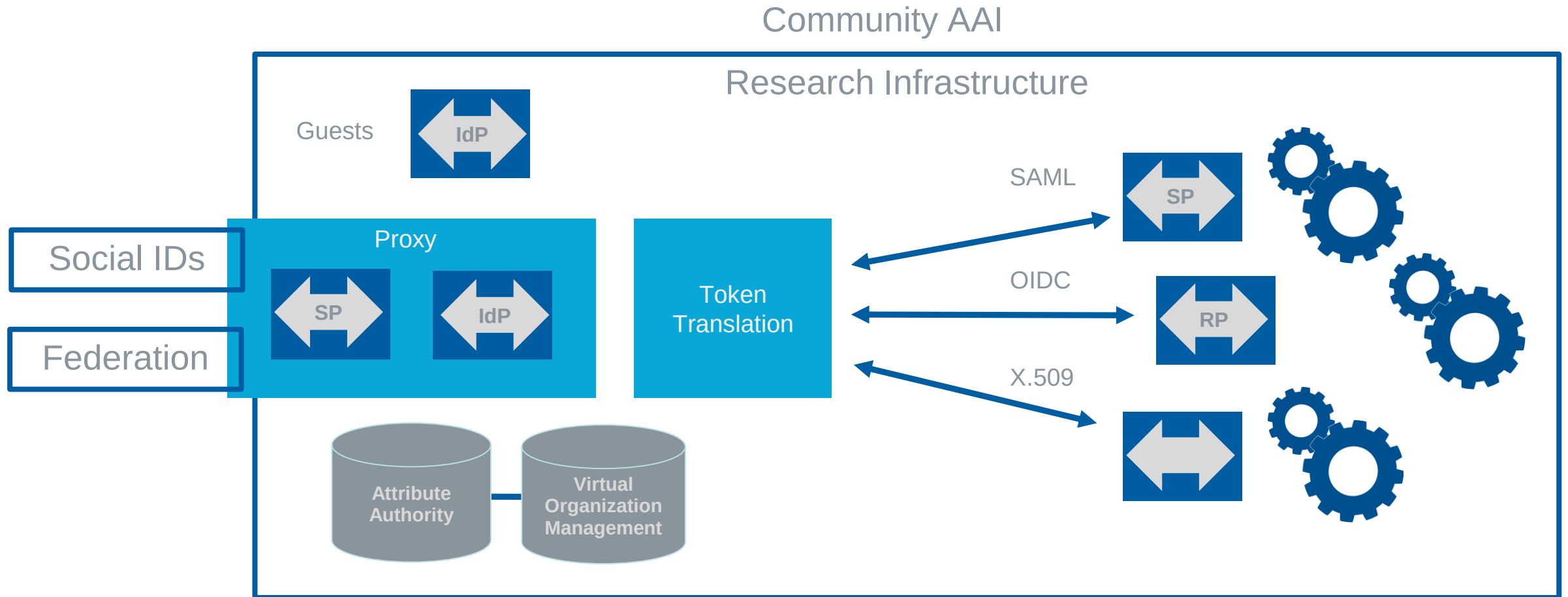
- One well-defined interface of a Community AAI to an Identity Federation
--> services behind the proxy
- Support for several protocols and standards
- Community VO Management
- Integration of further technical components

Proxy – a simple model

The simplest variant consists only of an IdP and an SP component

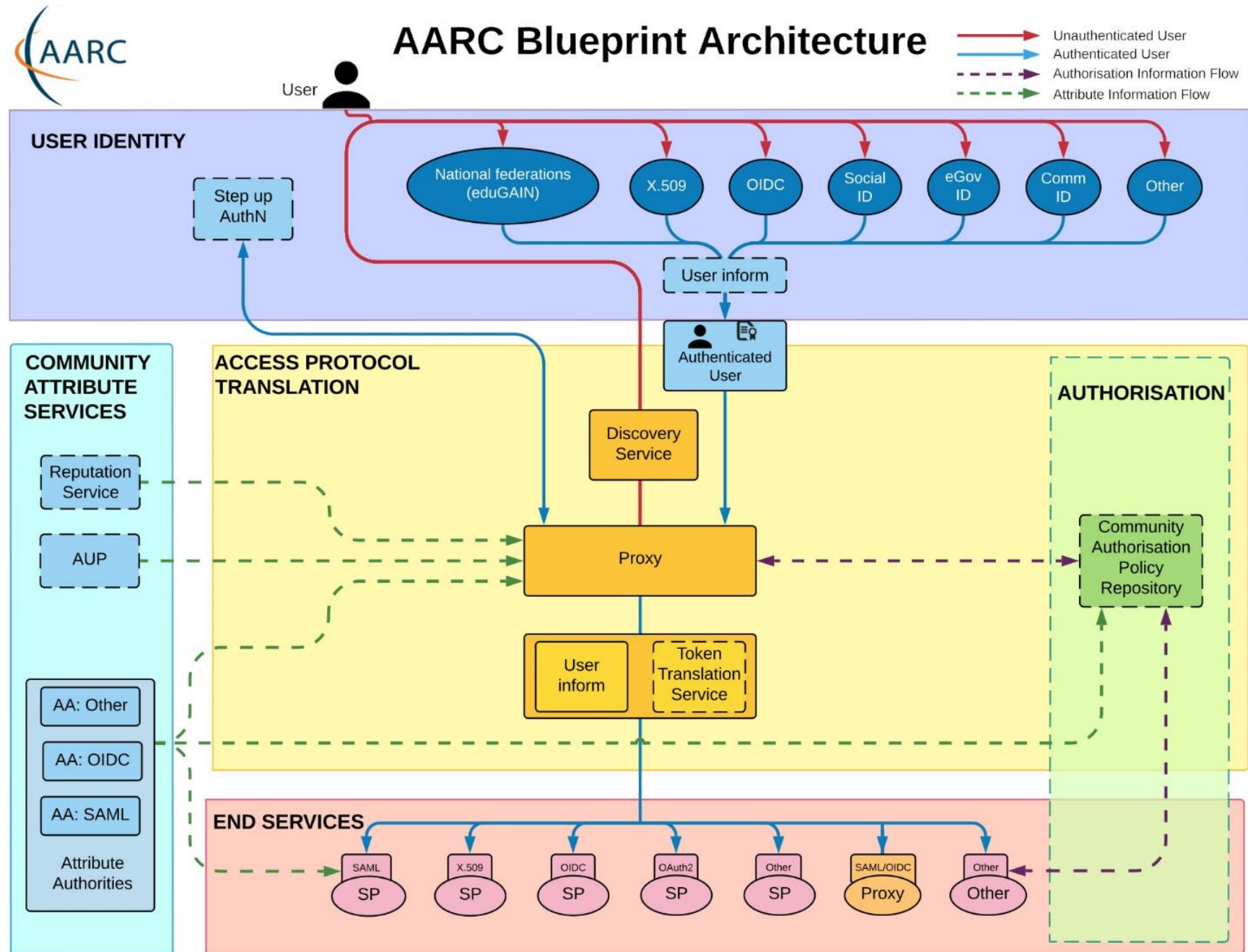


... that can be easily extended



And here we are:

AARC = Authentication and Authorization
for Research and Collaboration
<https://aarc-community.org/>



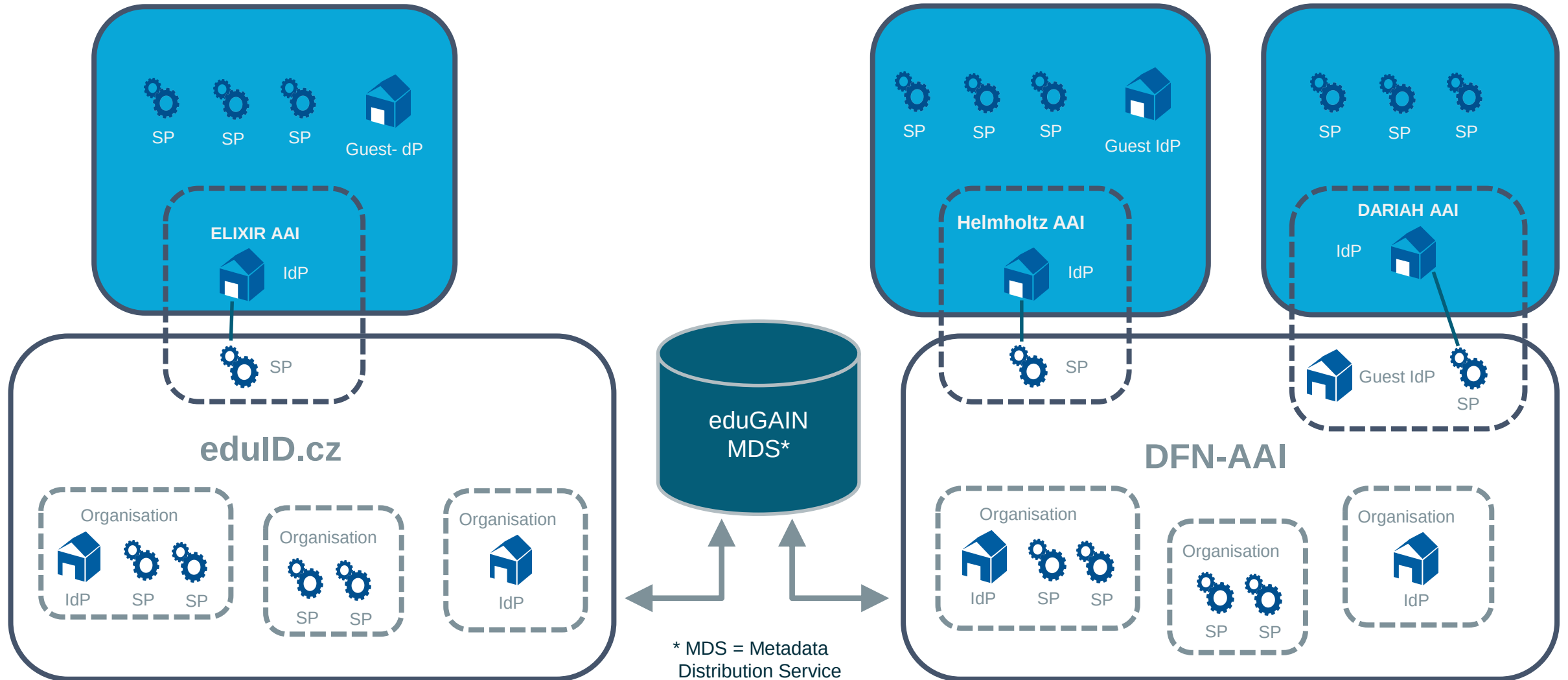
AARC Blueprint Architecture

Five components that can be combined to implement federated IAM solutions for (international) research collaborations:

- User Identity: Authentication via AAI, Social Media IDs, ORCID, etc.
- Community Attribute Services: Rights, Roles, VO Management
- Access Protocol Translation: IdP-/SP-Proxy, Token Translation, ...
- Authorisation: Authorization, management of access to services/resources
- End-services: the actual services and resources

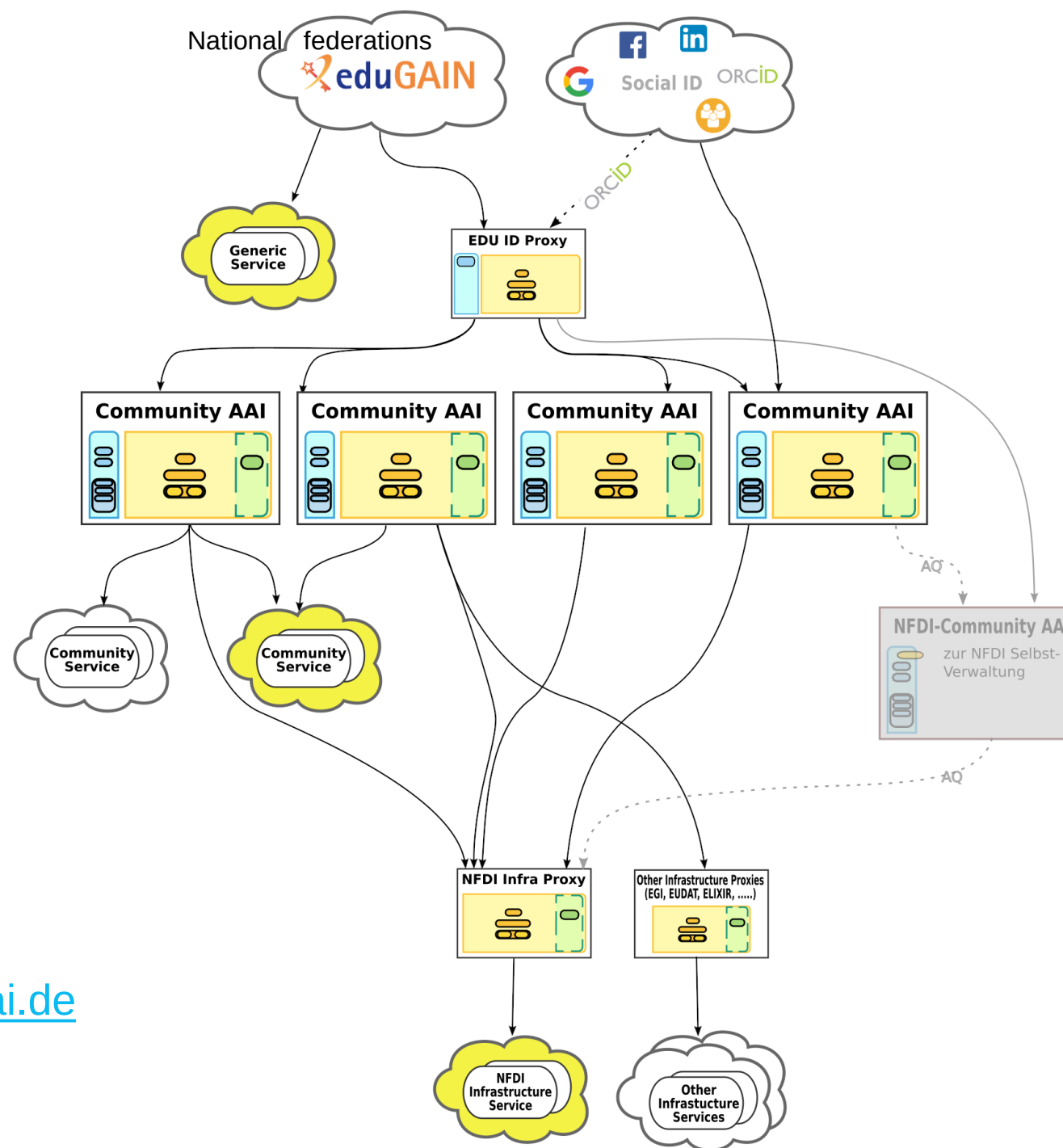
<https://aarc-community.org/architecture/>

Interoperability: Federations and Community AAls



3. NFDI AAI

NFDI AAI Architecture



<https://doc.nfdi-aa.de>

NFDI AAI

NFDI Consortia supposed to operate (or have operated) Community AAls

NFDI AAI Architecture as connecting element --> interoperability

Three-layered Service Model

- Generic services --> Federation (DFN-AAI)
- Community services --> Community AAI
- Infrastructure services --> Infrastructure Proxy

Additional components

- NFDI Infrastructure Proxy (simplify connection to services, AuthZ, ID linking)
- NFDI Attribute Authority (NFDI-internal rights management)
- edu-ID Proxy (lifelong self-managed ID, Guest IdP, Attribute Aggregation, Account Linking)

Interoperability

The design of the NFDI AAI Architecture aims at interoperability between

- Community AAI
- NFDI AAI
- EOSC AAI
- Infrastructures like EGI
- eduGAIN and national R&E Federations

AARC Guidelines (BPA etc.) and the EOSC AAI Architecture

- Mandatory attribute + claim profiles for NFDI AAI
- Policy Framework
- ...

(Interim) Summary

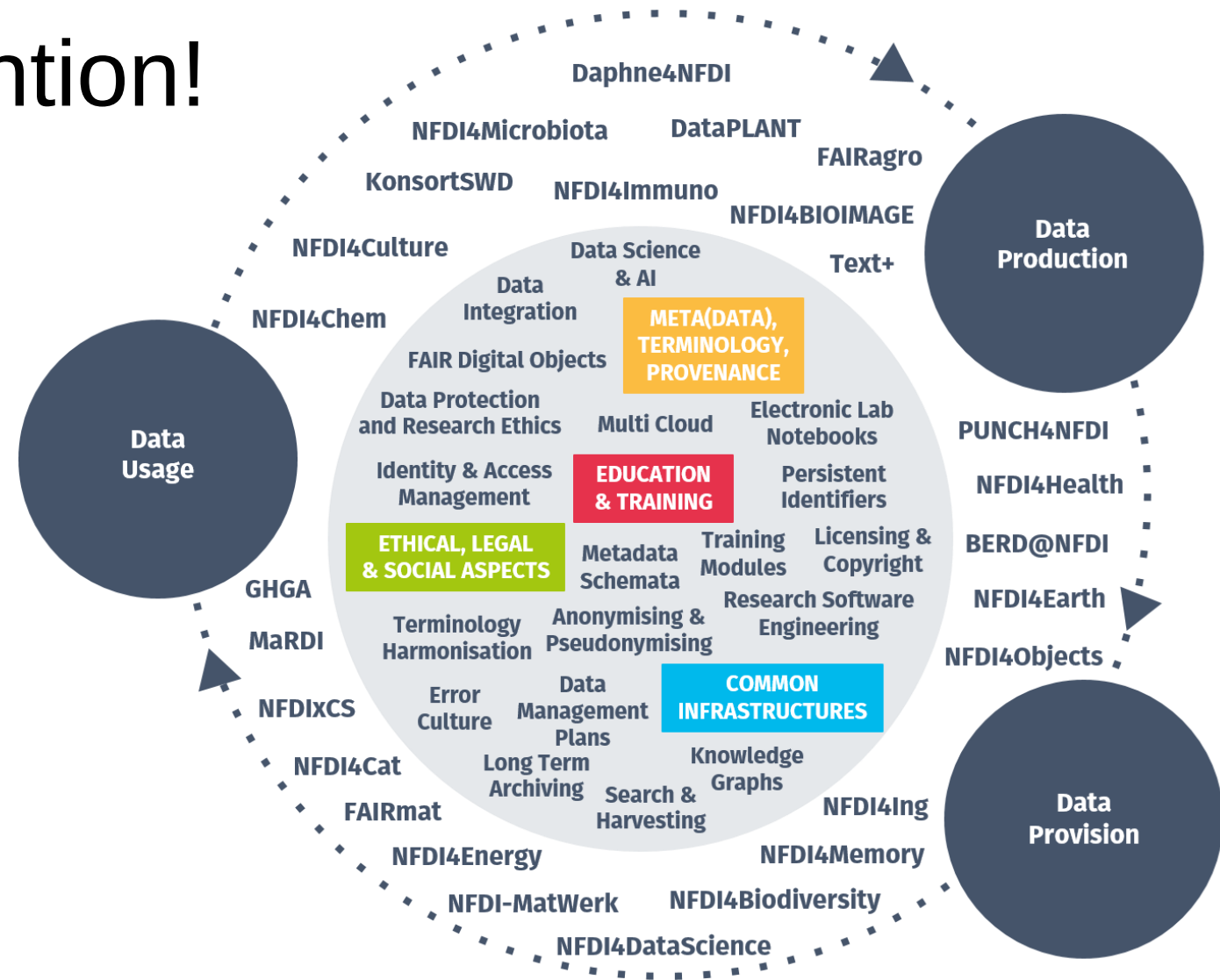
- IAM4NFDI does **not** re-invent the wheel
- Builds upon existing solutions
- Based on well-established Standards and Best Practices
 - SAML, OIDC, AARC Guidelines, EOSC Architecture, ...
- Enables Interoperability
- Aims to integrate existing components in the best possible way
 - In cases where additional development should be necessary --> WP3: Incubator

For a detailed overview on IAM4NFDI and the concept of Community-AAI-as-a-Service see the next presentations...

Thanks for your attention!

Questions?

Contact: aai-kernteam@lists.kit.edu



References

AARC Blueprint Architecture and Guidelines

- <https://aarc-community.org>

Section Common Infrastructures – WG IAM

- https://drive.google.com/drive/folders/1U4sjXzfk1G0TgKN-eQwWTK_xgjkLF6Ov
- <https://lists.nfdi.de/postorius/lists/section-infra-wg-iam.lists.nfdi.de/>

NFDI AAI, IAM4NFDI

- <https://doc.nfdi-aai.de>

edu-ID Proxy

- Life-long user-centric digital Identity
- Attribute Aggregation (Home IdP, ORCiD, ...)
- Homeless / Guest IdP („edu-ID IdP“)

