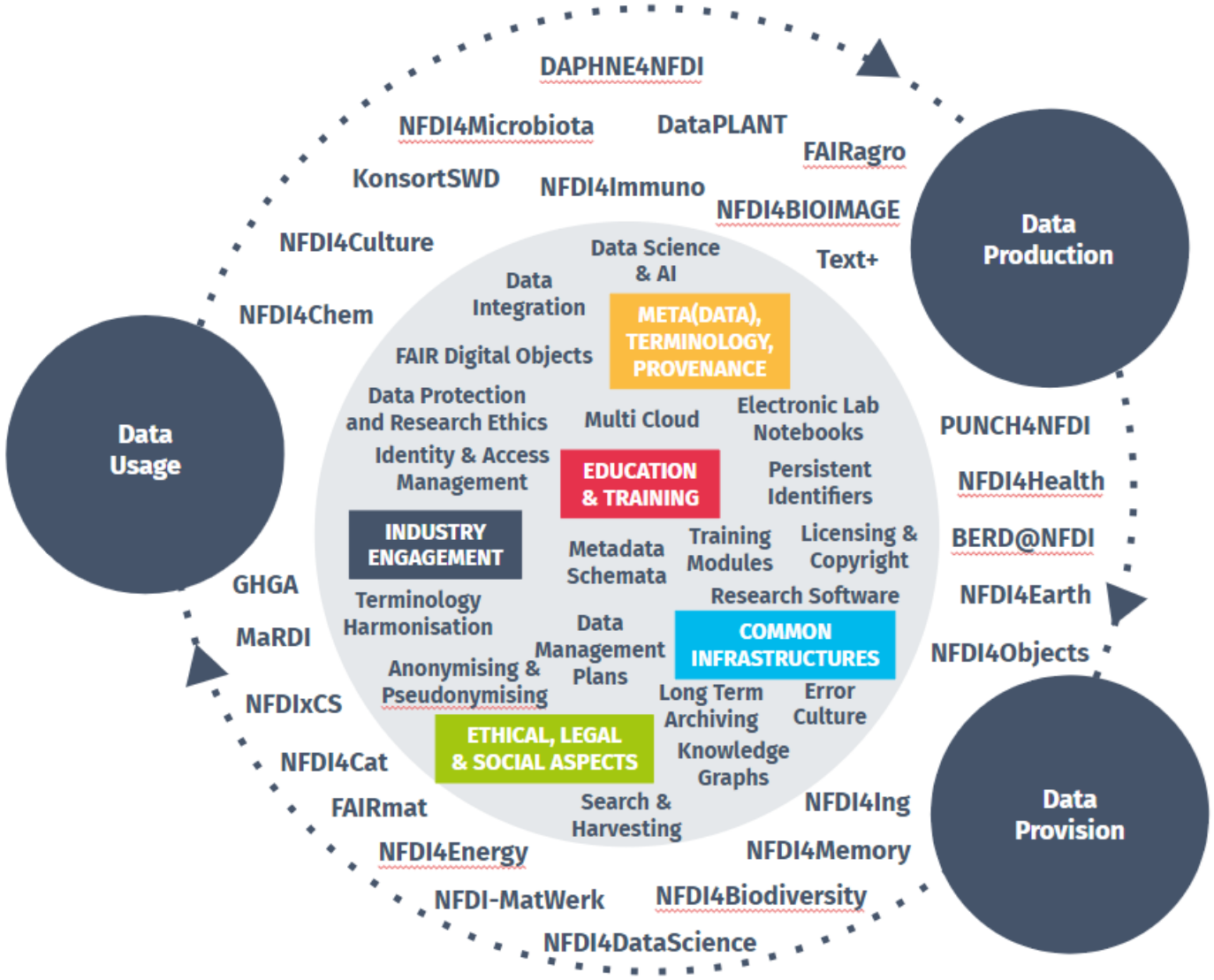
base4 nfdi Basic Services for NFDI

Federated Identity and NFDI-AAI

4.6.2024



base4 nfdi

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

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

Agenda

1. The Context: Federated Identity Management
2. AARC Blueprint Architecture and Community AAIs
3. NFDI-AAI and NFDI Basic Service Identity & Access Management

Wolfgang Pempe (pempe@dfn.de)

1. The Context: Federated Identity Management and Identity Federations

Service-specific Identities

User Id: **`lmuster`**
Passwd: ●●●●●●

User Id: **`ludmilla.muster@gmx.de`**
Passwd: ●●●●●●

User Id: **`lm1970`**
Passwd: ●●●●●●

Online Shop XY

Database YZ

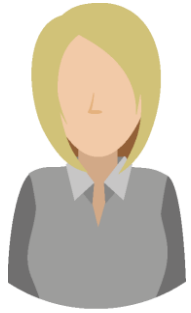
Publisher WX

base4 nfdi

Federated Identity

Home Organisation

User Id: `lmuster`
Passwd: ••••••



Online Shop XY

Database YZ

Publisher WX

base4 nfdi

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 Organisation)

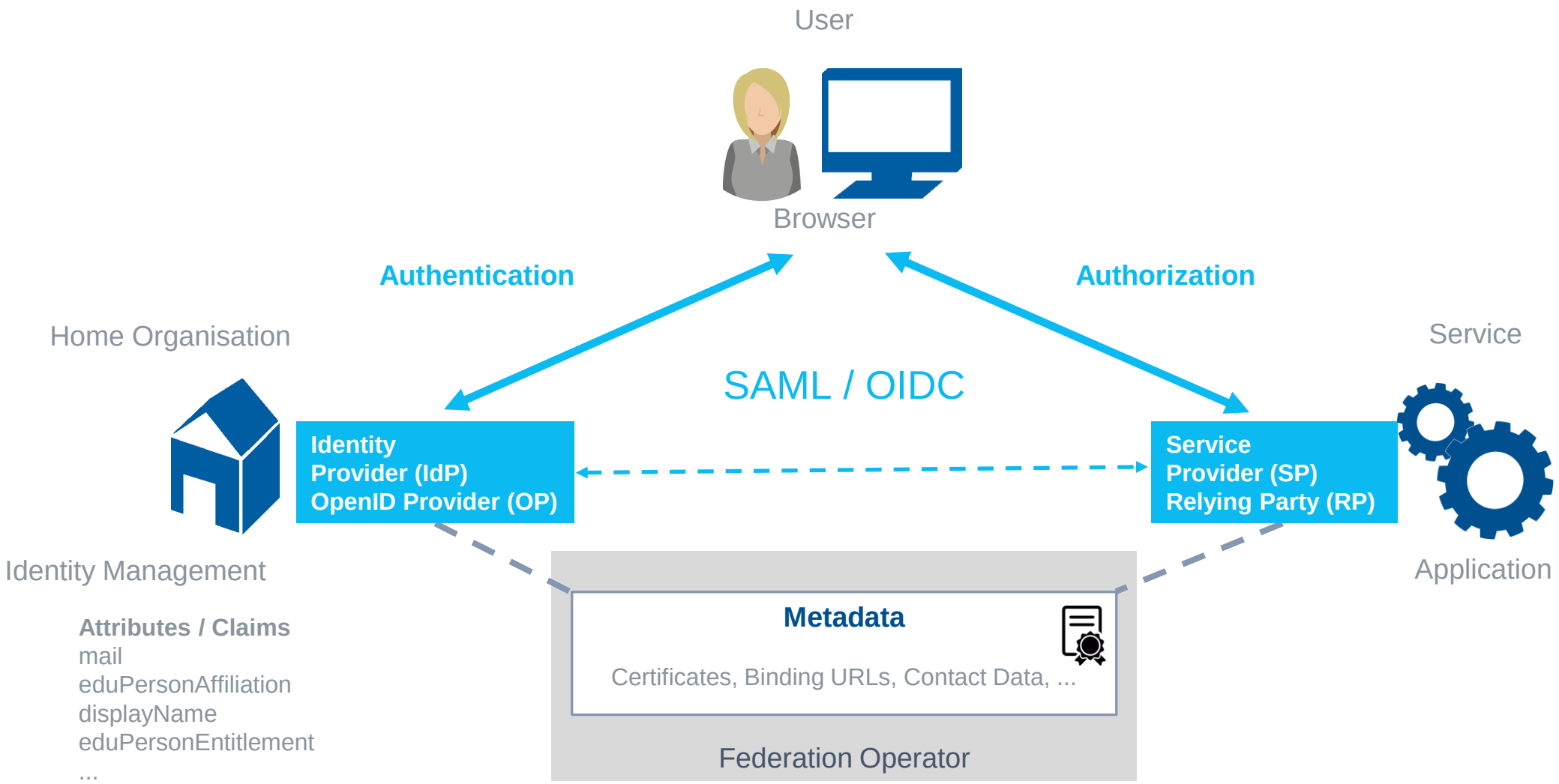
AAI = Authentication and Authorization Infrastructure

- 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

How does a federation work?



Example DFN-AAI

Federation Operator

DFN-Verein

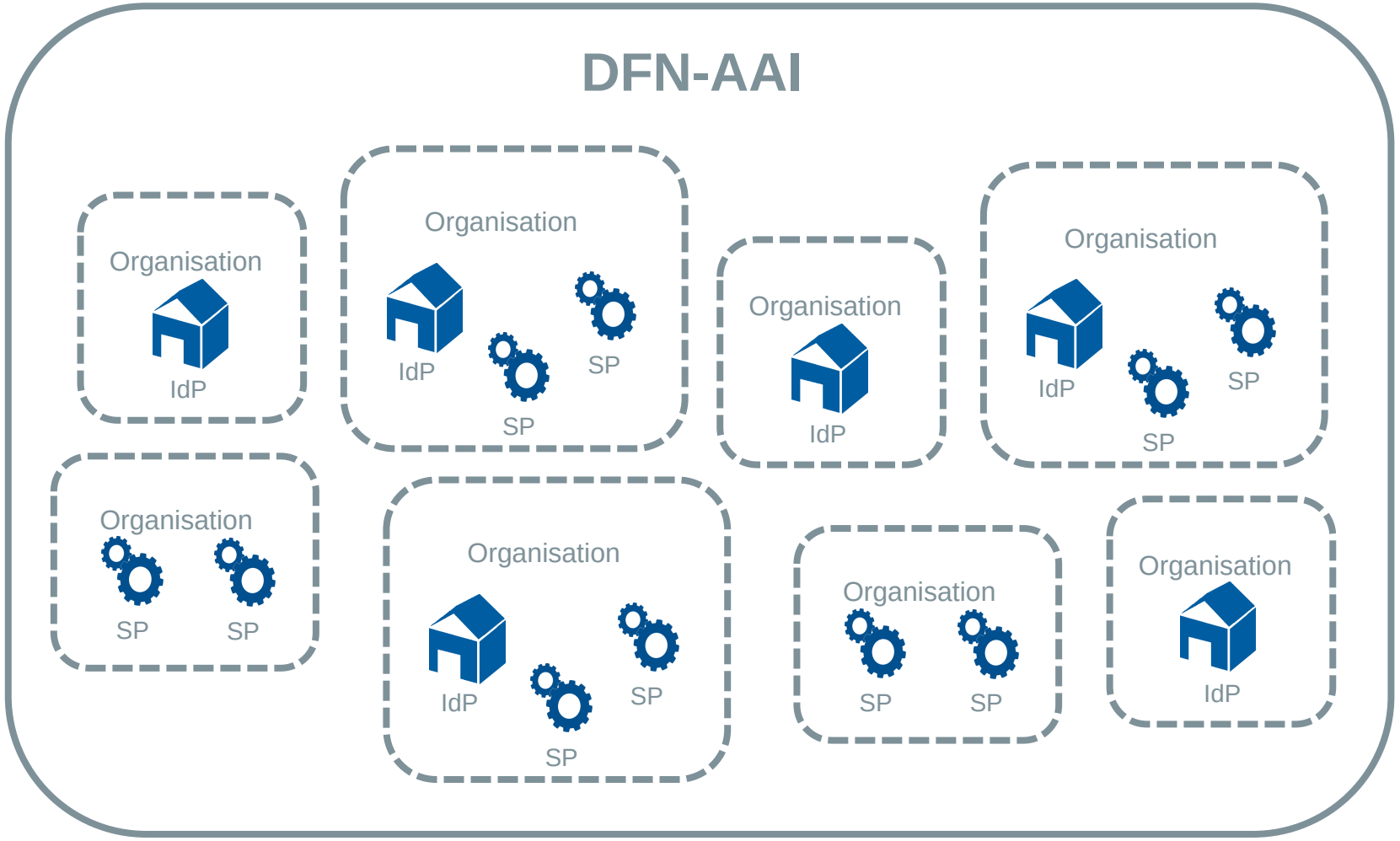
Trust

Contracts with all Participants, Policies, Levels of Assurance

Technical

Metadata Management and Distribution

Currently approx. 400 actively participating Home Orgs and 840 Services
(plus ~1710 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

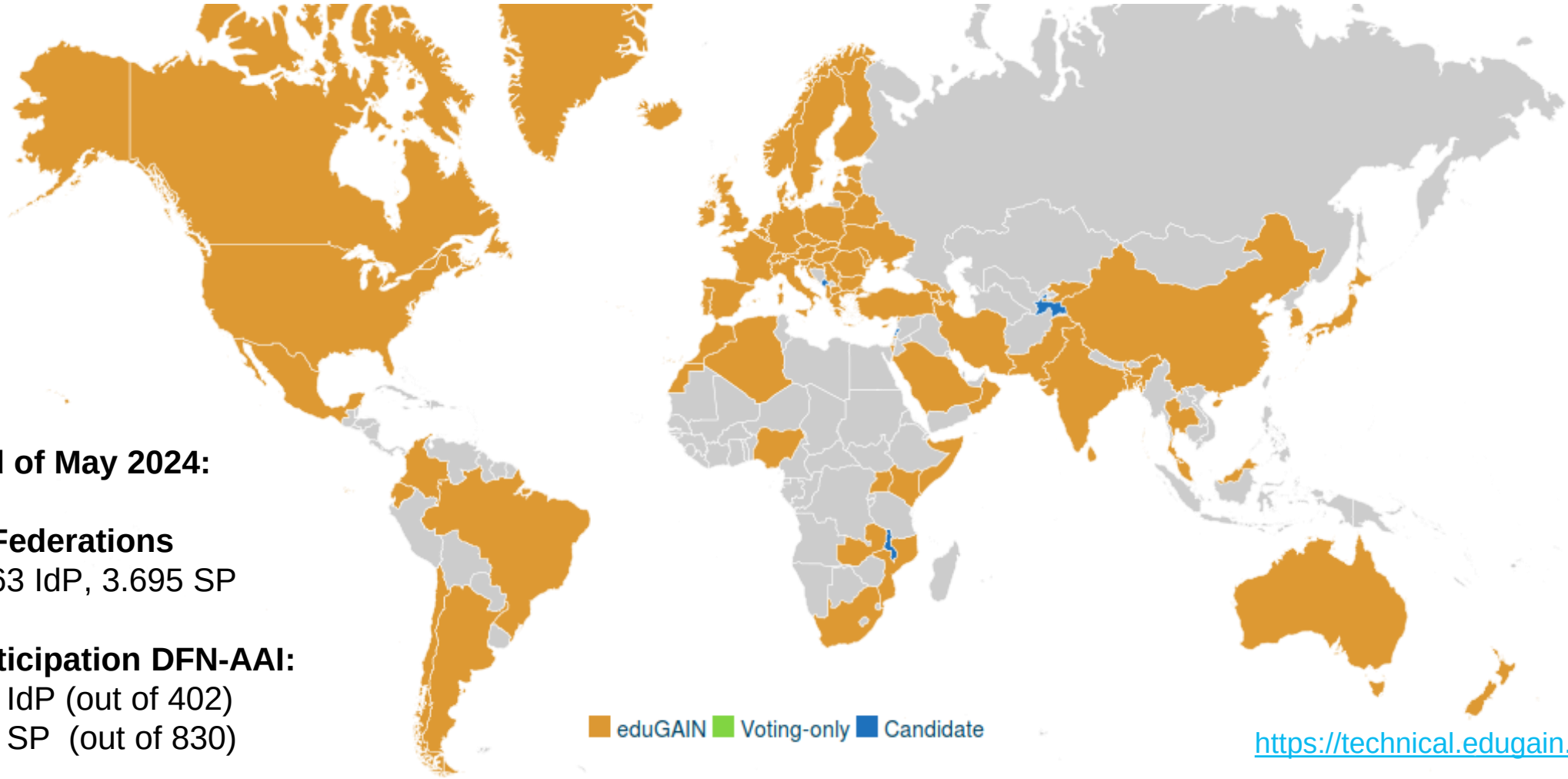
Basically a metadata exchange service:

- Aggregation of the metadata of the member federations
- Member federations are resposible 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



End of May 2024:

79 Federations
5.663 IdP, 3.695 SP

Participation DFN-AAI:
356 IdP (out of 402)
163 SP (out of 830)

https://technical.edugain.org

base4 nfdi

2. AARC Blueprint Architecture and Community AAIs

The power of proxies

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

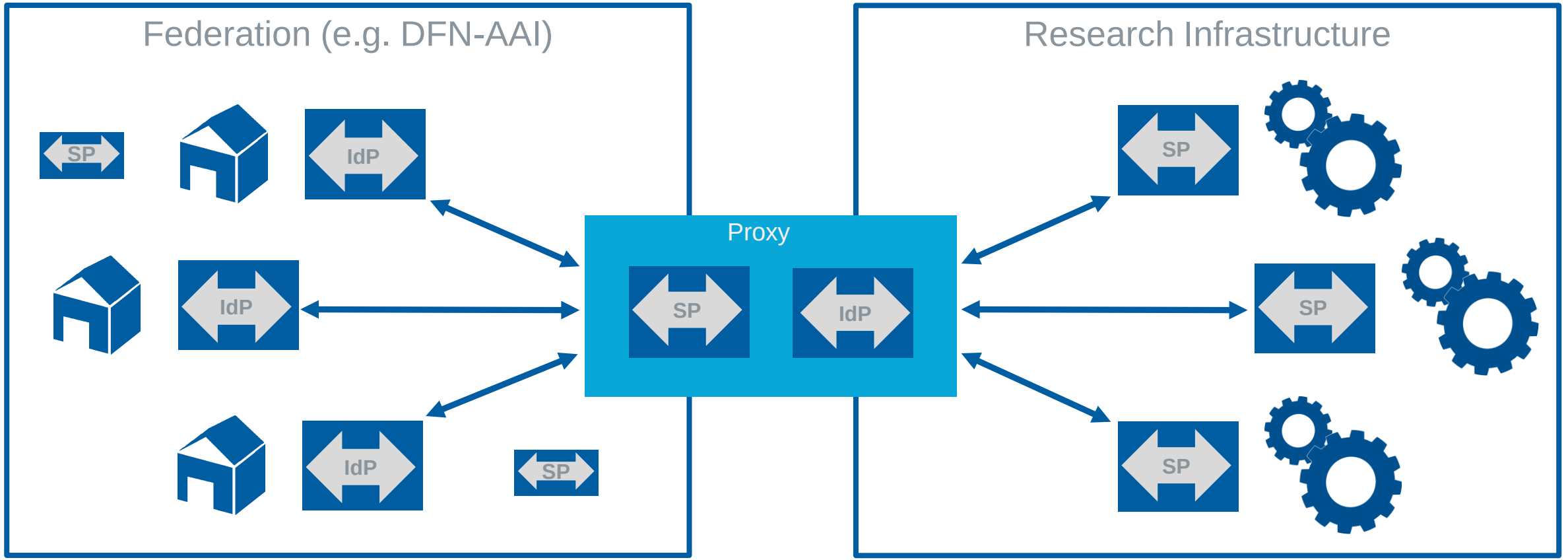
„[...] as a way to simplify and control [...] complexity. Proxies were invented to add structure and encapsulation to distributed systems."

Federated Identity Management for Research Communities

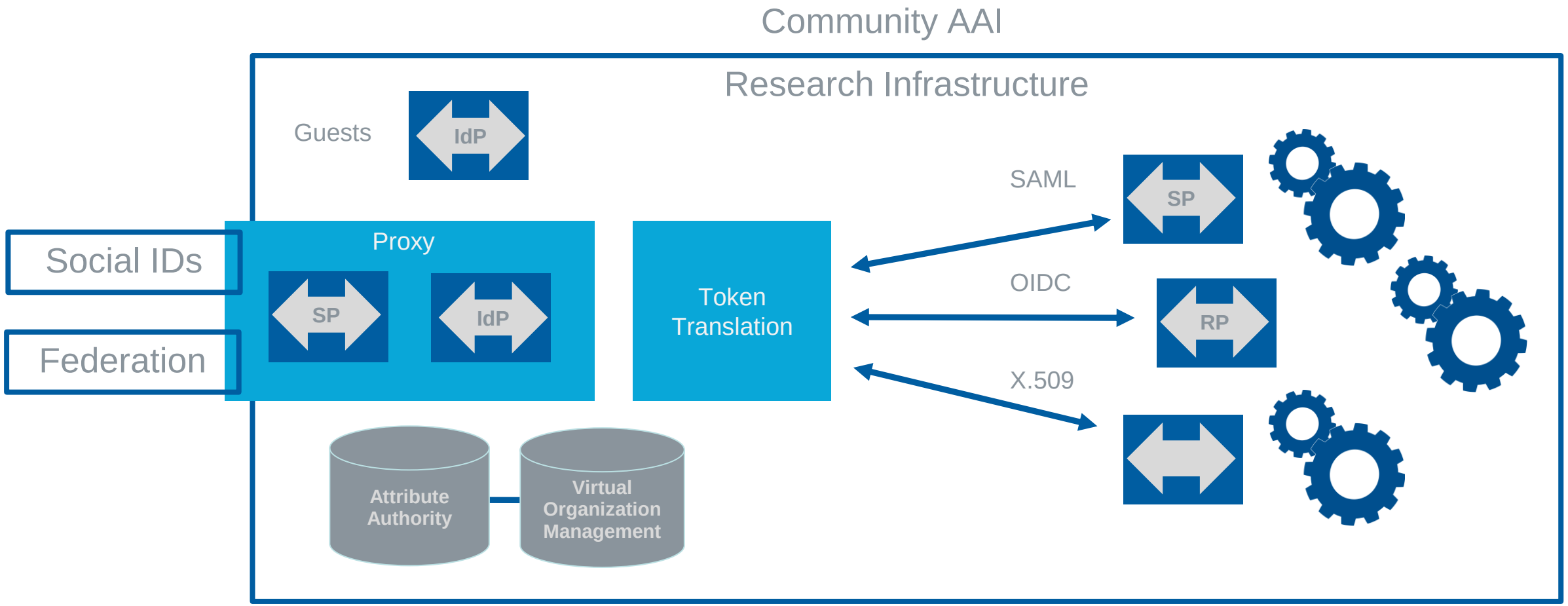
- One well-defined interface of a Community AAI to an Identity Federation
  --> services behind the proxy (no need to register each service with a federation)
- Support for several protocols and standards (not only SAML)
- Virtual Organization Management (access management by the reseach community)
- Integration of further technical components and authentication sources

Proxy – a simple model

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

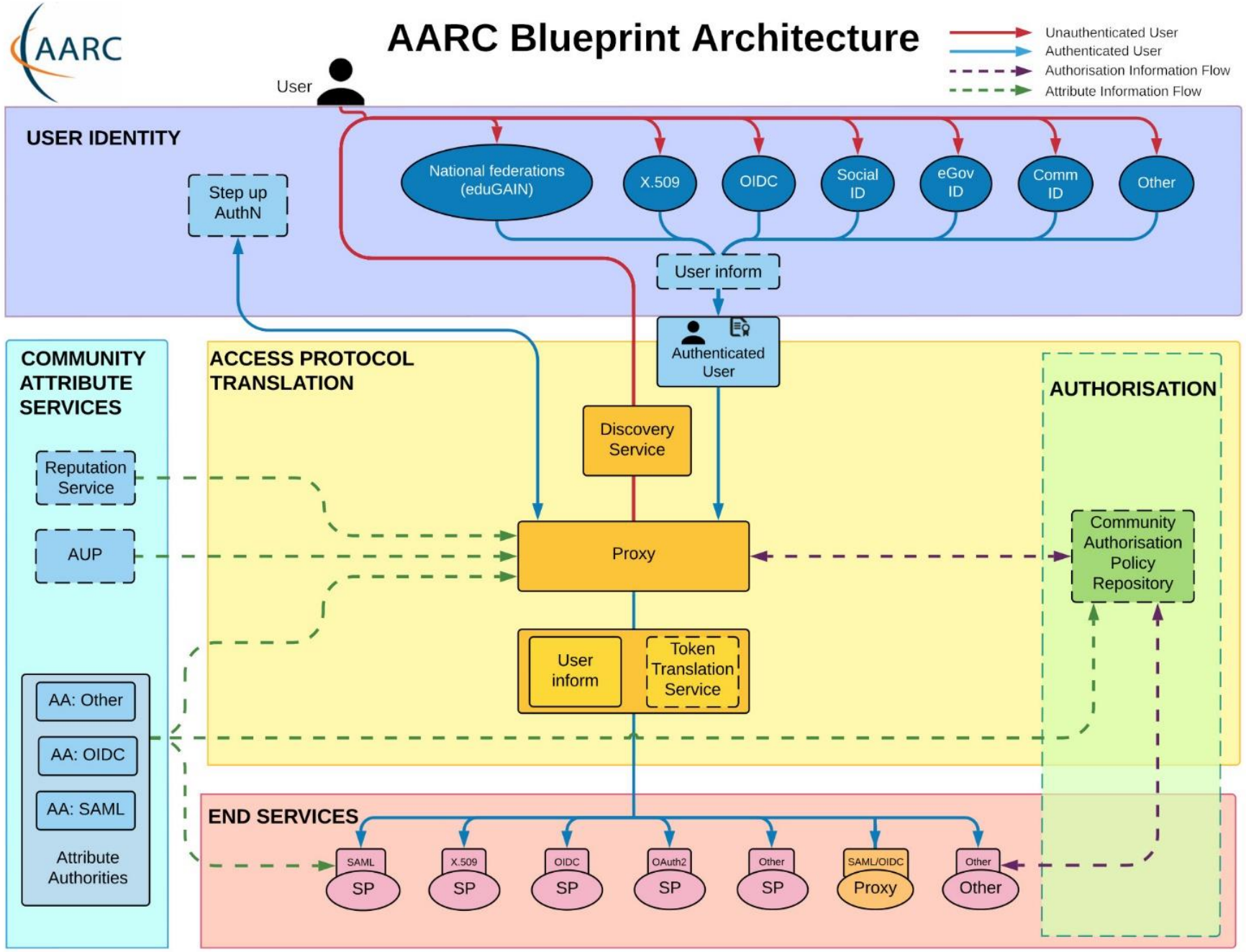


… that can be easily extended



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/

Managing Virtual Organizations
(VO Management)

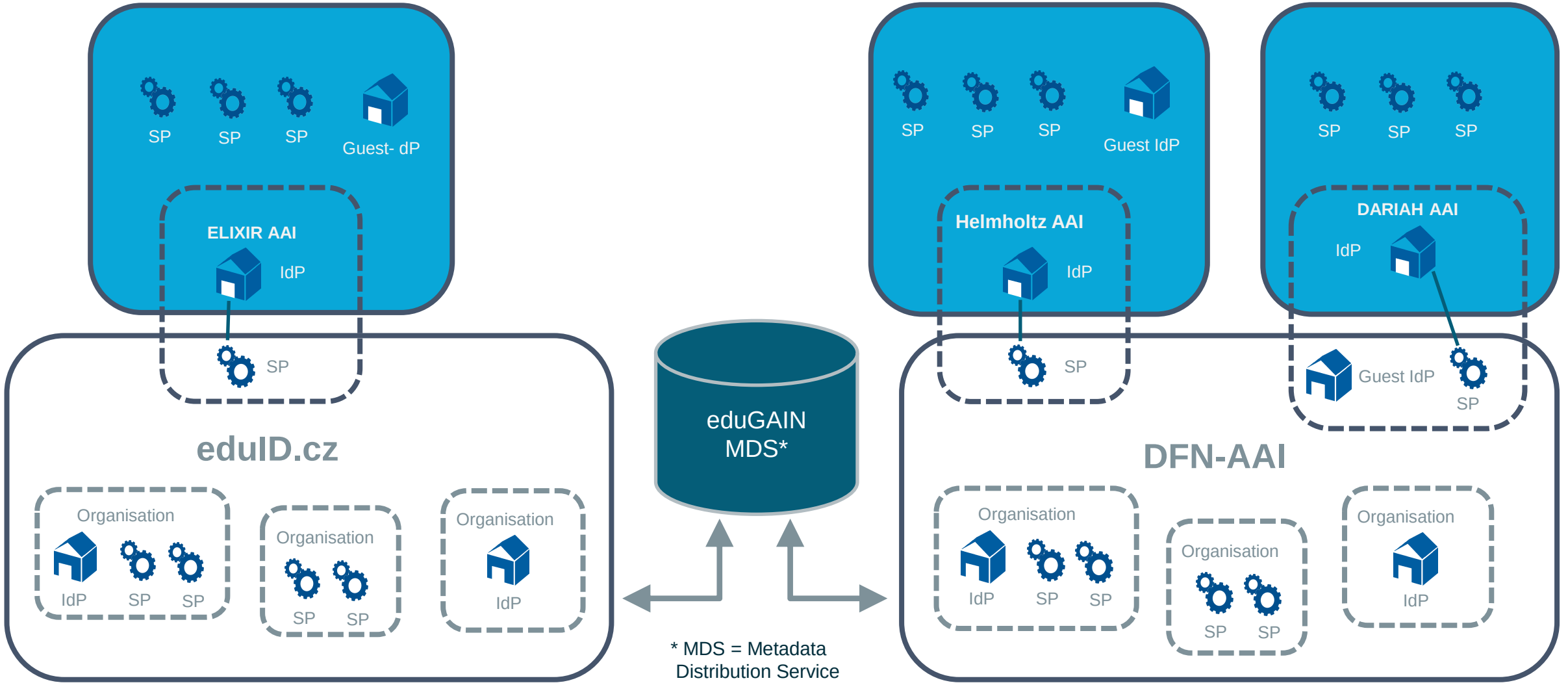
A Virtual Organization is a scalable way to organize Access Management

- A VO is a group of one or more Users, not necessarily bound to a single institution, organized with a common purpose, jointly granted access to one or more Services
- A VO unites the users of a specific research community represented by one or more of the NFDI consortia
- Service Providers are no longer required to implement their own access management
- Definition of structures and processes about who decides who can access which resources, when and to what extent → governance

BPA Implementations (Community AAIs) provide tools for VO Management

base4 nfdi

Interoperability:
Federations and Community AAIs



* MDS = Metadata Distribution Service

base4 nfdi

3. NFDI-AAI

... and NFDI Basic Service Identity & Access Management –

IAM4NFDI

NFDI Basic Service IAM4NFDI

Integration Phase

- February 2024 – January 2026

Project Goals

- Provide state-of-the-art IAM to the NFDI consortia
- Use Home Organization Identity
- Enable delegated group/access management (Virtual Organizations)
- Interoperability, connect to EOSC
- Community-AAI-as-a-Service

base4nfdi

NFDI-AAI
Architecture

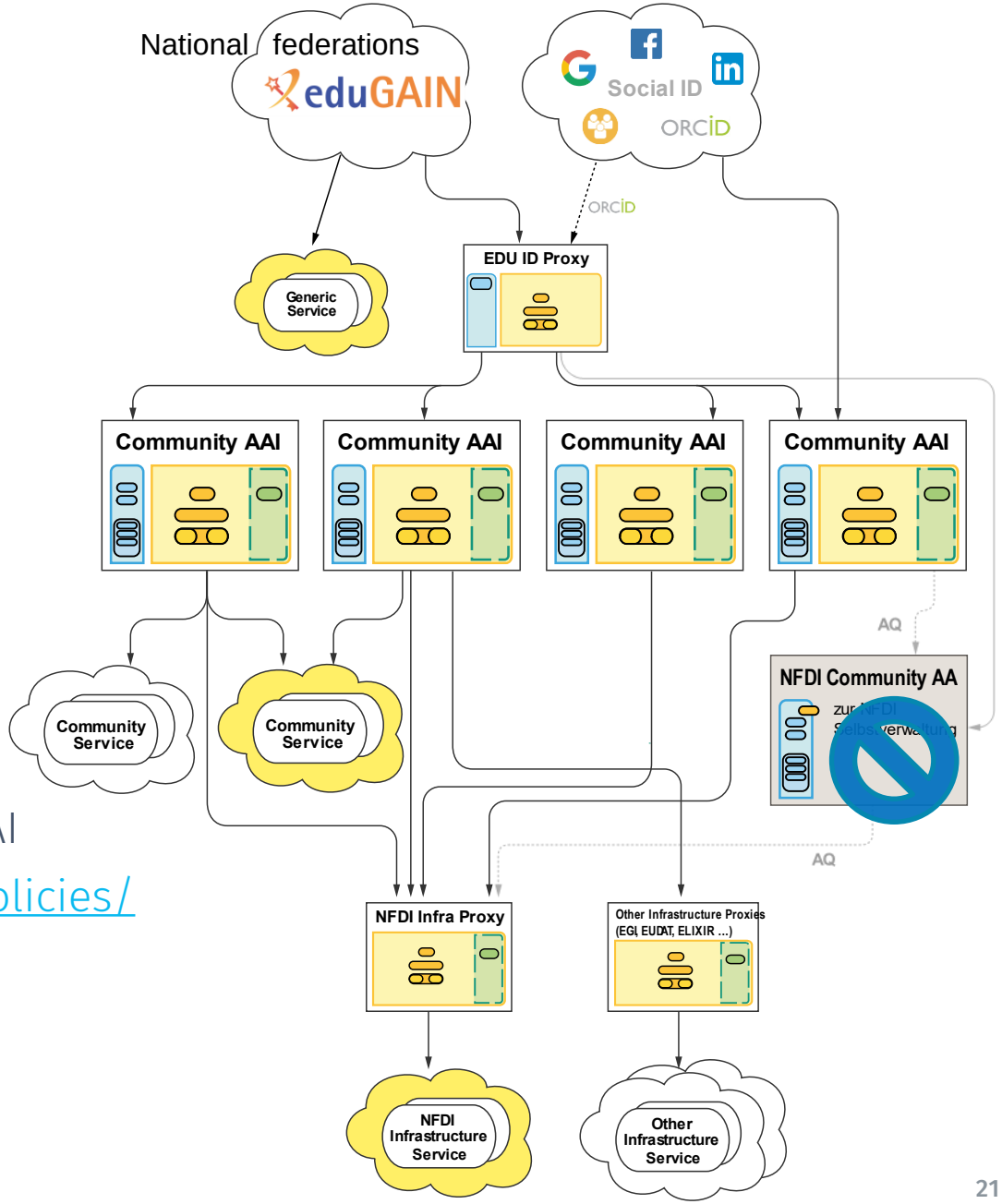
Design of the NFDI-AAI Architecture aims at interoperability between

- Community AAIs
- 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, cf. https://doc.nfdi-aai.de/policies/
- …

See https://doc.nfdi-aai.de



NFDI-AAI

NFDI Consortia supposed to use a Community AAI

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)
- edu-ID Proxy (lifelong self-managed ID, Guest IdP, Attribute Aggregation, Account Linking

NFDI-AAI: Additional Components

- edu-ID Proxy
  - Lifelong, self-managed digital identity, unchangeable identifier attributes/claims
  - Attribute aggregation and account linking from different sources like Home IdPs and ORCID
  - Central Guest IdP
  - Not part of the project (upcoming DFN service, cf. https://doku.tid.dfn.de/de:aai:eduid:start)
- Infrastructure Proxy
  - Integration of services that address more than one community
    → enabling access for users from different identity sources: eduGAIN, ORCID, Social IDs and CAAIs
  - Forwards attributes from the VO Management(s), especially entitlements
  - In exceptional cases, it can make authorization decisions for services that are unable to reject users without the required attributes.
  - Identity Linking between Community AAIs and/or other identity sources.

Support Services for the NFDI Communities

… provided by the IAM4NFDI Project Team

Community-AAI-as-a-Service (CAAIaaS)

- Active support for 4 different technical solutions that are already in productive use in one or more NFDI community
- Single-instance or tenant-style CAAI operation by the IAM4NFDI project partners, depending on the CAAI solution

Incubator Projects

- Supporting the NFDI communities in implementing AAI/IAM use cases, e.g.
  - Connecting services to a CAAI, deeper integration of complex services
  - Development of new features
  - … and more - just ask (call for incubators every 6 months)

Summary

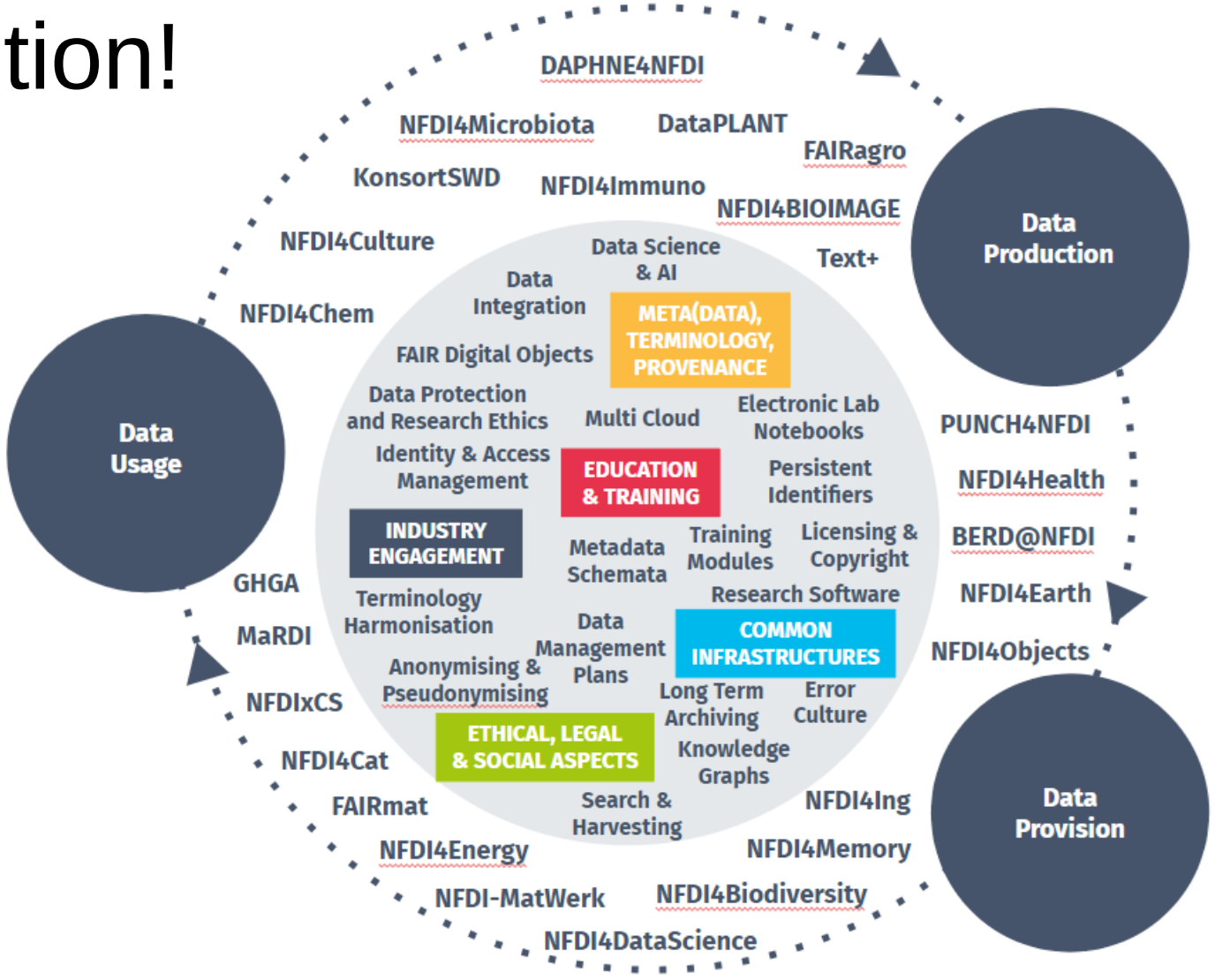
- IAM4NFDI does *not* re-invent the wheel
- Builds upon existing solutions
- Based on well-established Standards and Best Practices
  - SAML, OIDC, AARC Guidelines, EOSC Architecture, ...
- Enables Interoperability
- Aims to integrate existing components in the best possible way
  - In cases where additional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

For a detailed overview on IAM4NFDI and the concept of Community-AAI-as-a-Service see https://doc.nfdi-aai.de

base4 nfdi

Thanks for your attention!

Questions?



Contact: aai-kernteam@lists.kit.edu

base4nfdi

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

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

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

- https://doku.tid.dfn.de/de:aai:eduid:start

Federation

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

- Defines the organisational, 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 all participants

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

Basic Service IAM – IAM4NFDI

Integration Phase

- February 2024 – January 2026

Work Packages

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

edu-ID Proxy

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