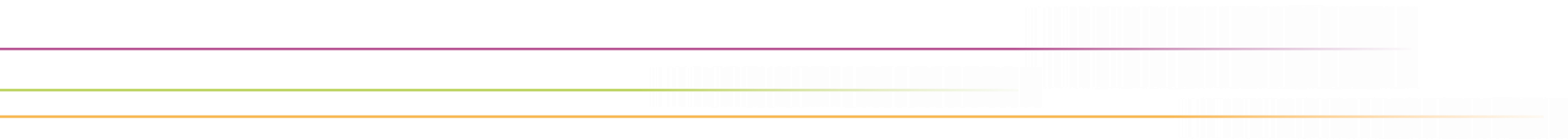


deutsches forschungsnetz

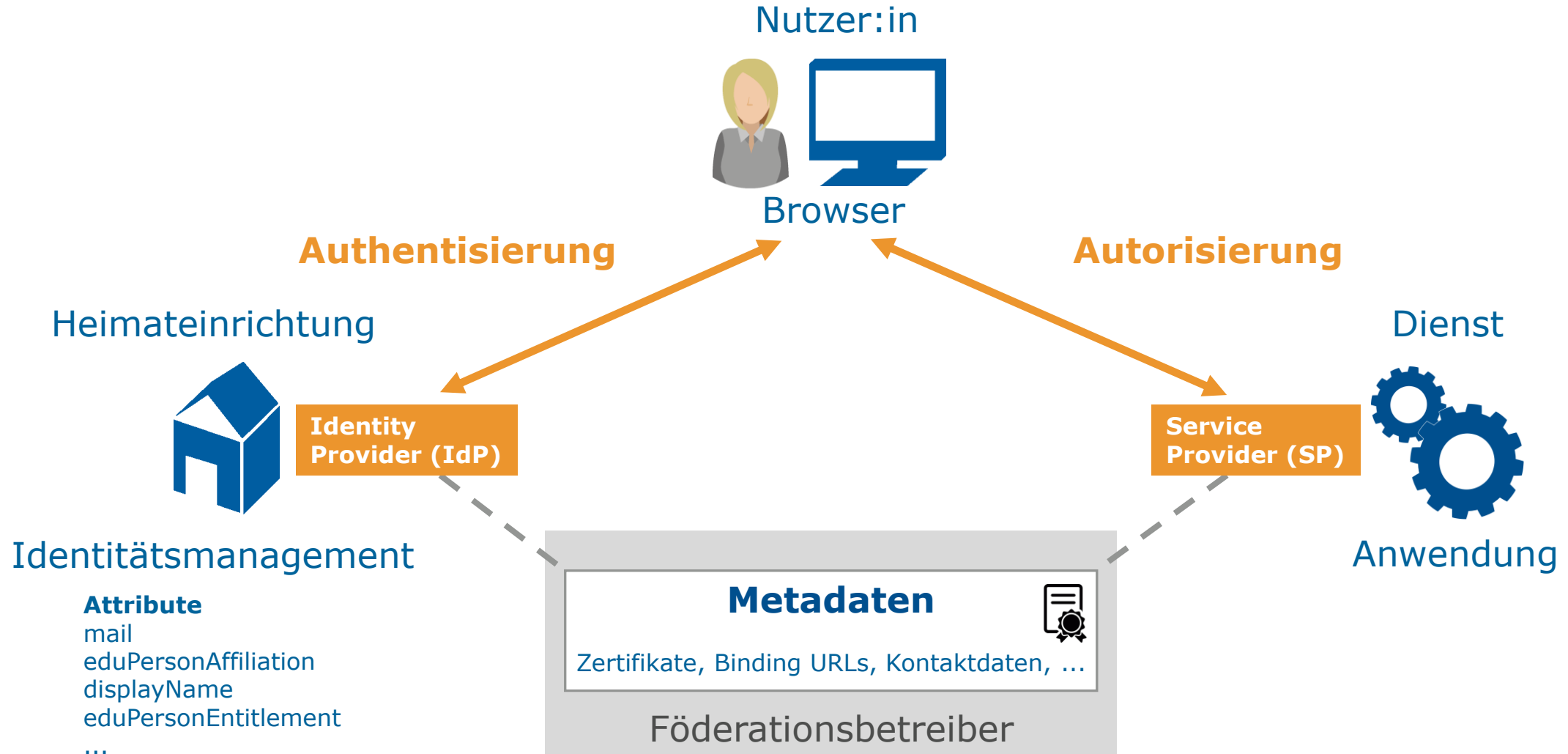


IDM.nrw und NFDI-AAI als Anwendungsfälle für das edu-ID-Konzept

Übergang zur Geschäftsstelle IDM.nrw | RWTH Aachen, 20. Mai 2026

Wolfgang Pempe (pempe@dfn.de)

Exkurs vorab: AAI und Föderationen



Beispiel DFN-AAI

- **Föderationsbetreiber**

DFN-Verein

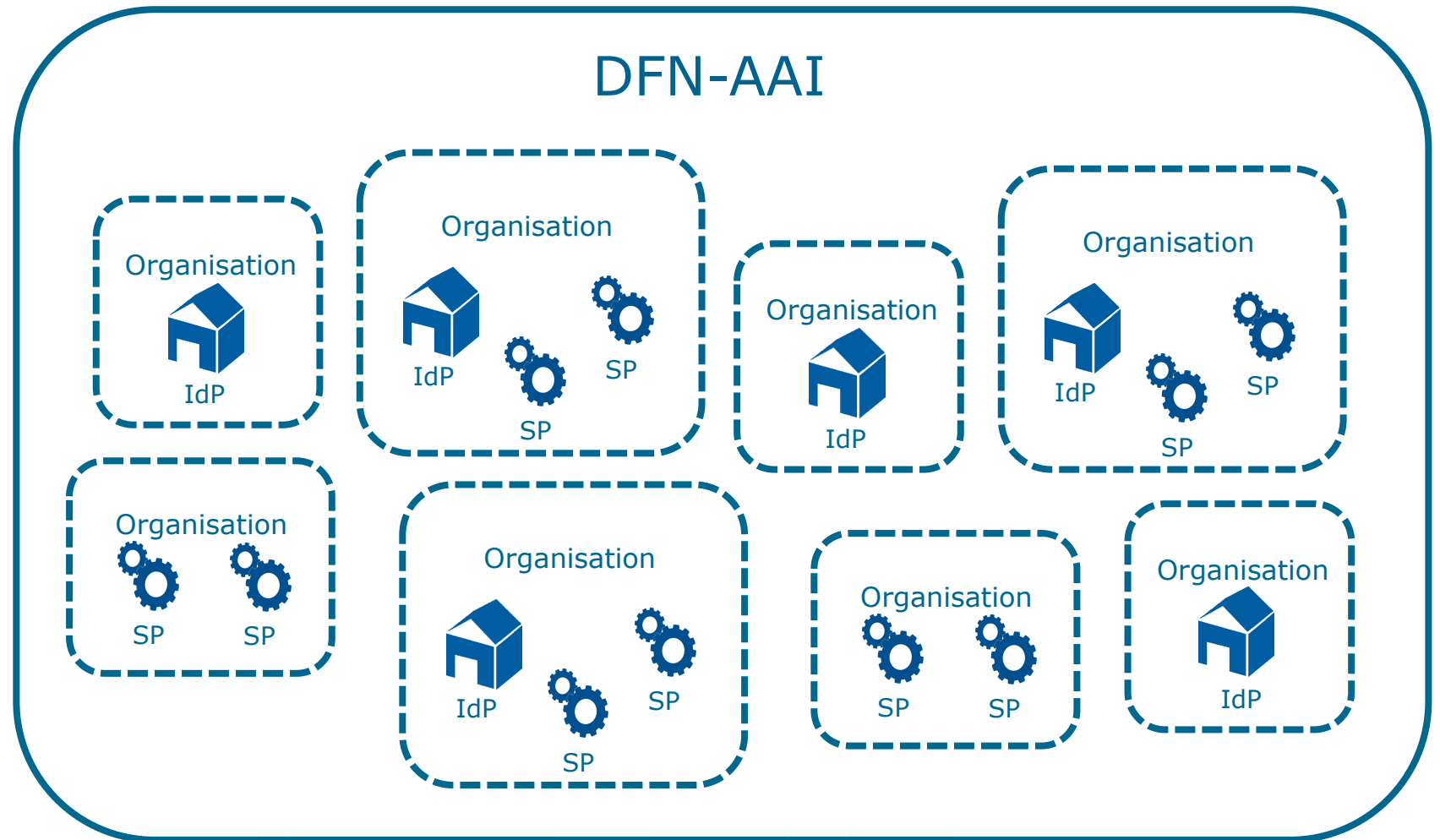
- **Vertrauen**

Verträge mit allen
Teilnehmern, Policies,
Levels of Assurance

- **Technik**

Metadatenverwaltung
und -Signierung

Aktuell 427 teilnehmende
Einrichtungen und 1017 Dienste
(zzgl. ~2200 lokale SP)



Konzept virtuelle Subföderation

- ▶ **Föderationsbetreiber**

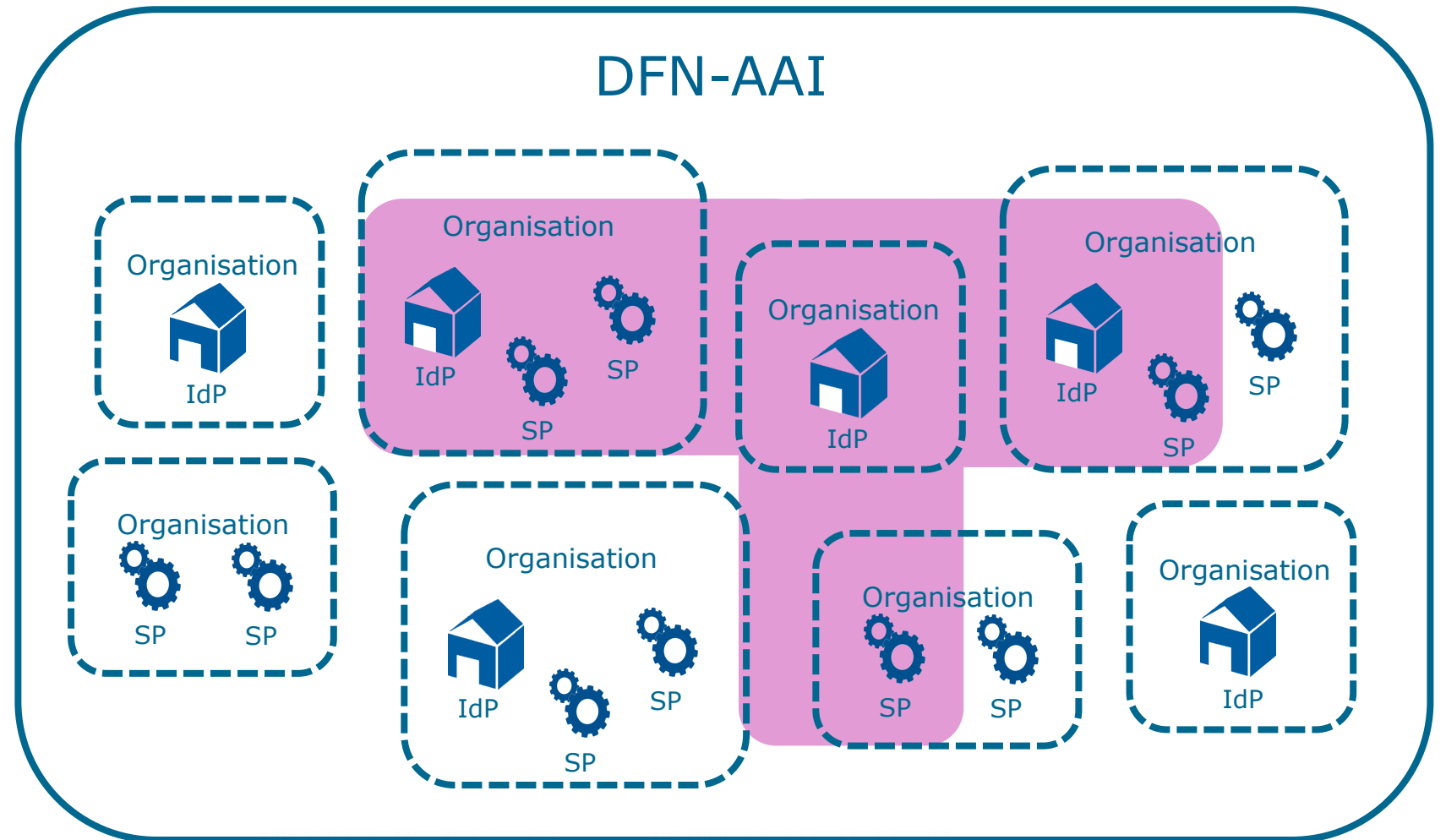
(Landes-)Projekt

- ▶ **Vertrauen**

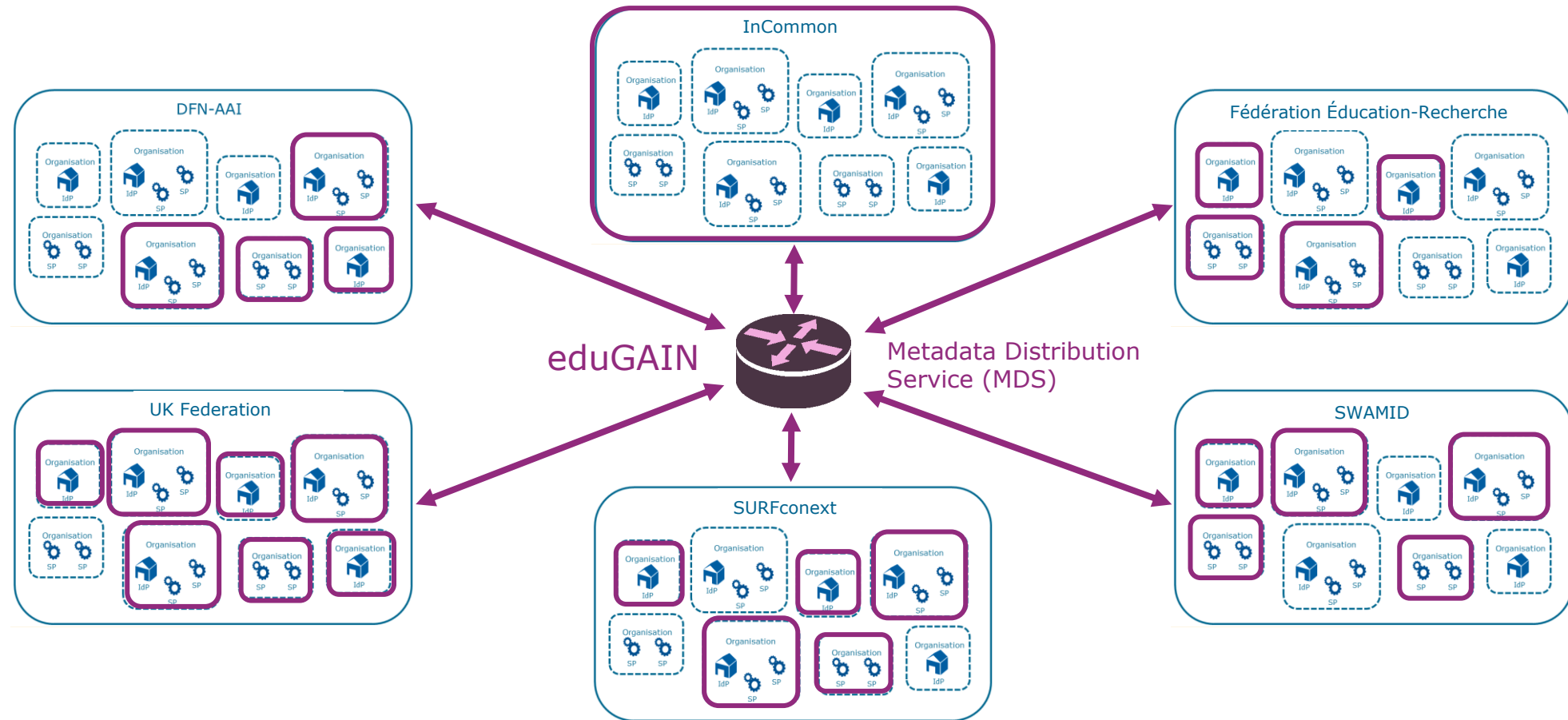
Verträge / Code of Conduct

- ▶ **Technik**

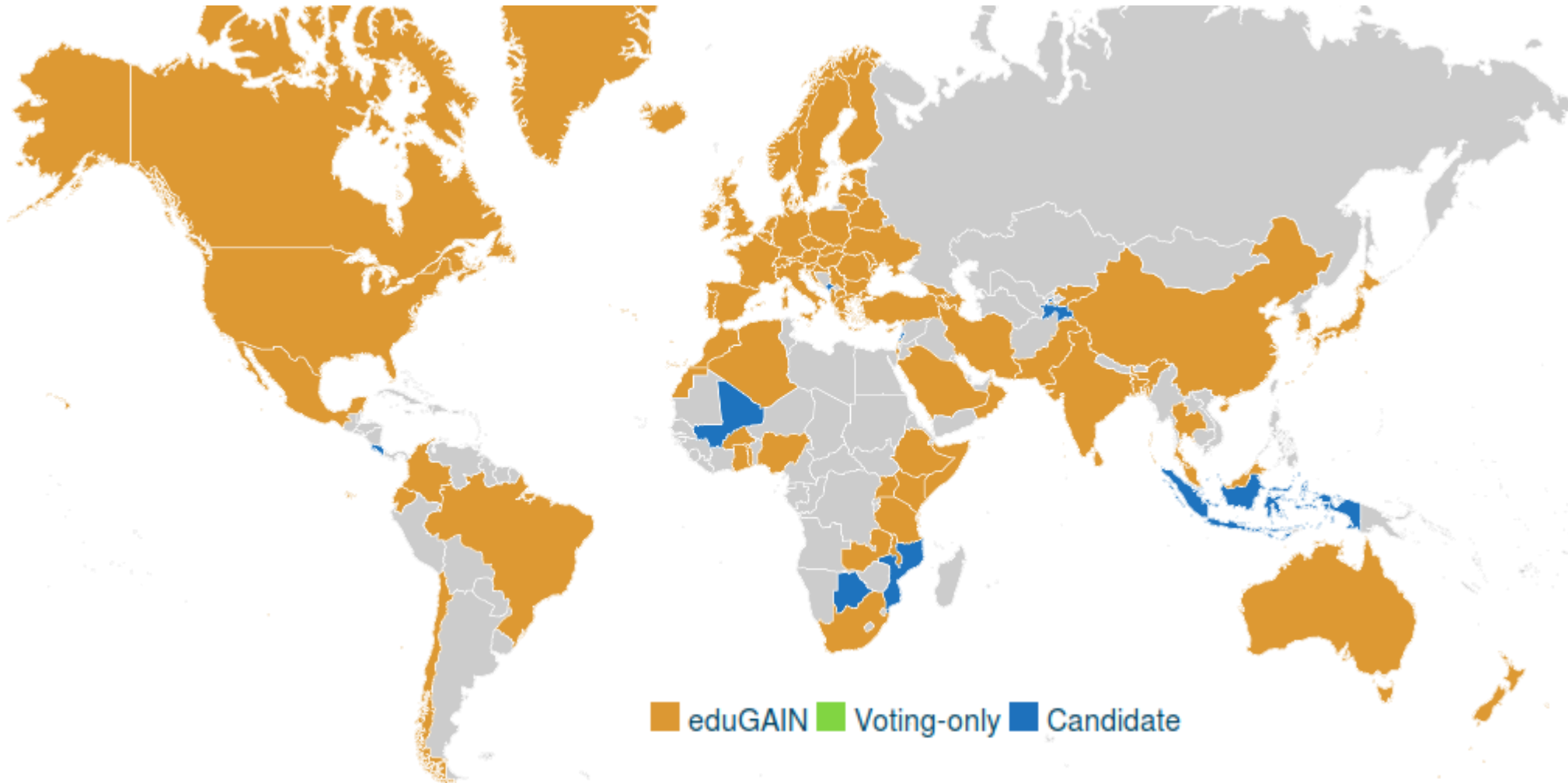
- ▶ **Entity Category**, Vergabe durch Projektleitung
- ▶ **Einheitliches Attributprofil**
- ▶ Metadatenverwaltung und –Signierung durch DFN-Verein



eduGAIN - Interföderation



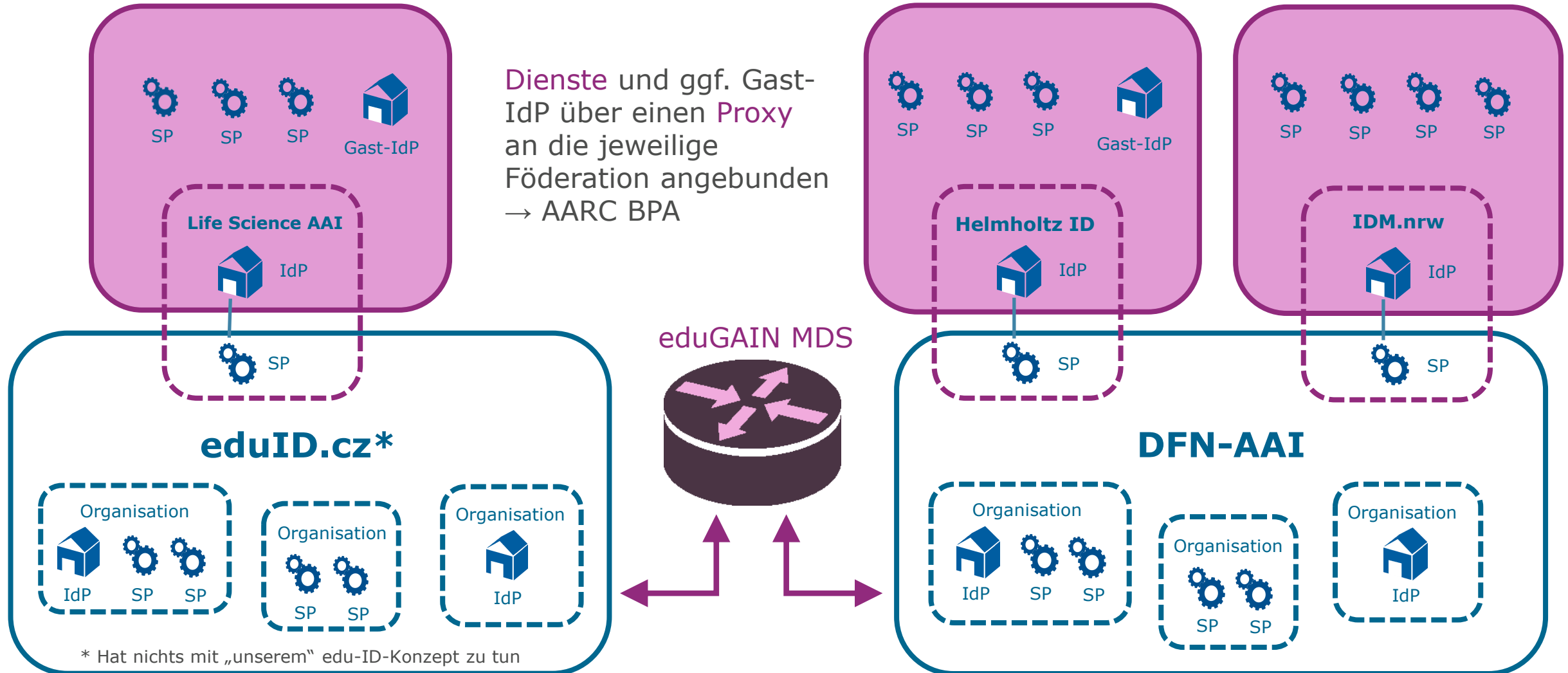
eduGAIN – weltweite Abdeckung



Aktuell 84 teilnehmende Föderationen mit 6357 IdPs und 4005 SPs, siehe <https://technical.edugain.org>

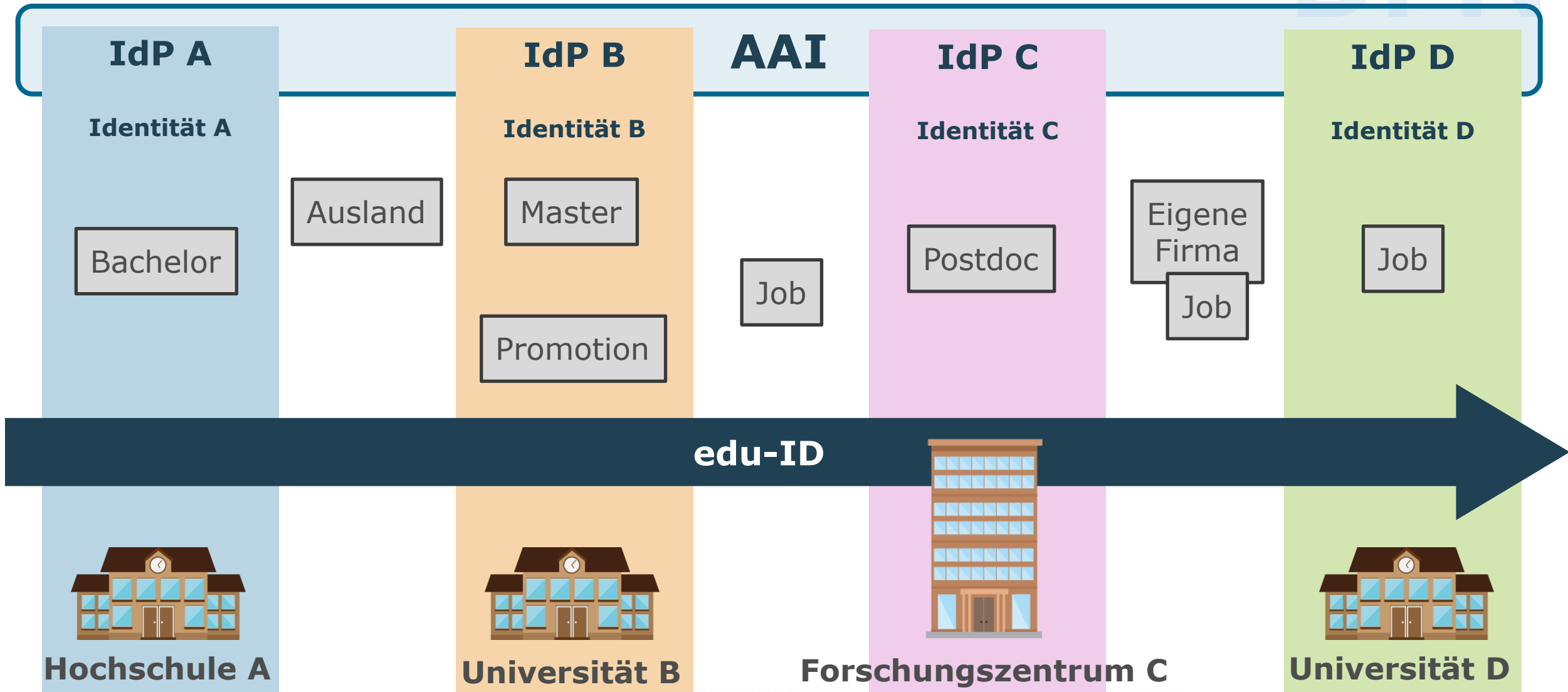
Föderationen und Community-AAIs

DFN



edu-ID: Eine lebensbegleitende digitale Identität

DFN



Das edu-ID-Konzept

- ▶ Kontinuität:

Eine lebenslange, global eindeutige digitale Identität für den Forschungs- und Bildungssektor

- ▶ Digitale Souveränität:

Die edu-ID-Identität wird von den Nutzenden selbst verwaltet

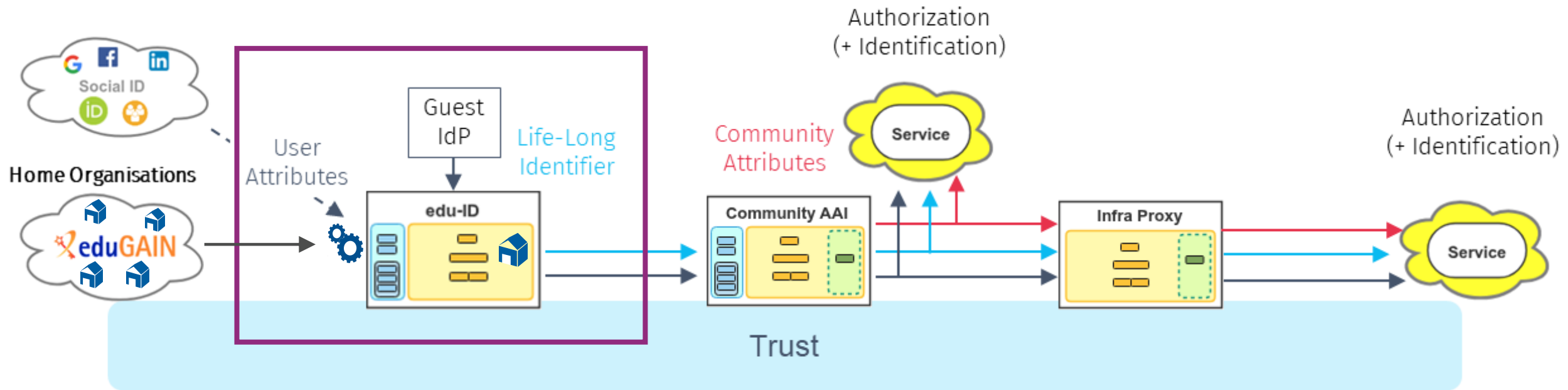
- ▶ Interoperabilität:

Verknüpfung mit anderen digitalen Identitäten: Heimateinrichtungen, ORCiD, MyAccessID (zukünftig evtl. auch bundID)

- ▶ Dokumentation: <https://doku.tid.dfn.de/de:aai:eduid:start>

Wie funktioniert das? Proxy-Ansatz

- edu-ID-System agiert zur Föderation / eduGAIN hin als Service-Provider
- ... und zu nachgelagerten Diensten und Infrastrukturen als Identity-Provider
- edu-ID-Account kann mit beliebig vielen Heimat-IdPs verknüpft werden
- Heimat-IdP als Authentifizierungsquelle, Attribute werden vom edu-ID-Proxy weitergeleitet
- ... und um einen permanenten (edu-ID-)Identifier ergänzt



Wie lässt sich das Konzept nutzen?

- ▶ Unterbrechungsfreie Nutzung von Diensten bzw. Zugriff auf Ressourcen, deren Nutzungsberechtigung nicht an die aktuelle Zugehörigkeit zu einer bestimmten Einrichtung geknüpft ist (Speicherdienste, Nationallizenzen, Leistungsnachweise, ...)
- ▶ Erleichterung des Managements virtueller Organisationen durch Forschungsprojekte und –Infrastrukturen (User Mobility, Account Linking, Rechte, Rollen)
- ▶ Identity Provider für Nutzende ohne Heimat-IdP
 - ▶ Gast-IdPs für sog. Homeless Users und Citizen Scientists werden obsolet

Was hat das mit IDM.nrw und NFDI-AAI zu tun?

- ▶ Interoperabilität

- ▶ Voraussetzung sind einheitliche (und weitgehend kompatible) Attribut-Profile für IDM.nrw und die NFDI-AAI
- ▶ Das edu-ID-System unterstützt dies aufgrund seiner Proxy-Funktion (Aggregation, Filter, Normalisierung)

- ▶ Researcher Mobility

- ▶ Das edu-ID-System liefert zusätzlich einen global eindeutigen, lebenslang gültigen Identifier für registrierte Nutzende – unabhängig von der aktuellen Heimateinrichtung

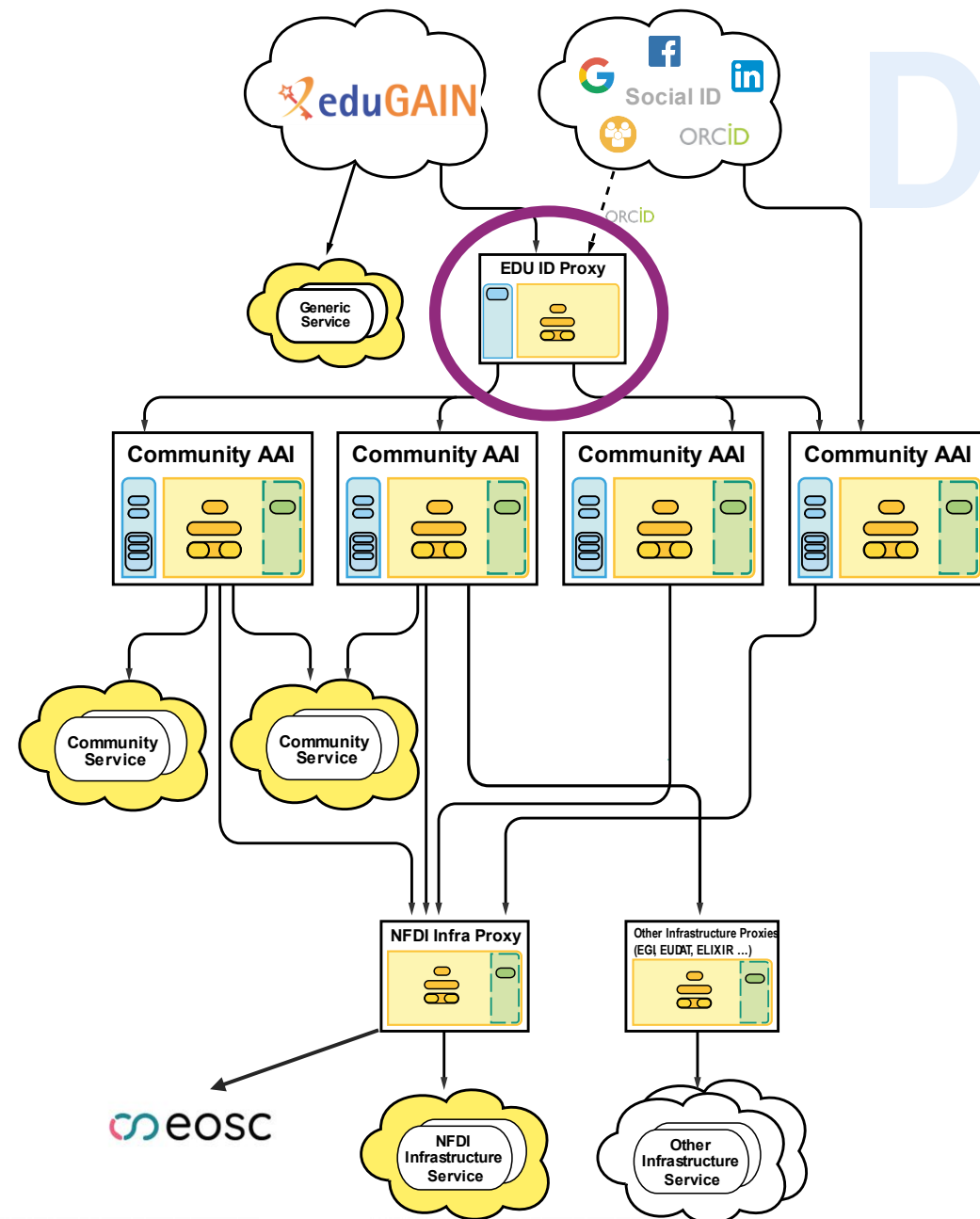
- ▶ Nutzende ohne Zugang zu einem Identity Provider?

- ▶ edu-ID-System kann als zentraler Gast-IdP genutzt werden

NFDI-AAI

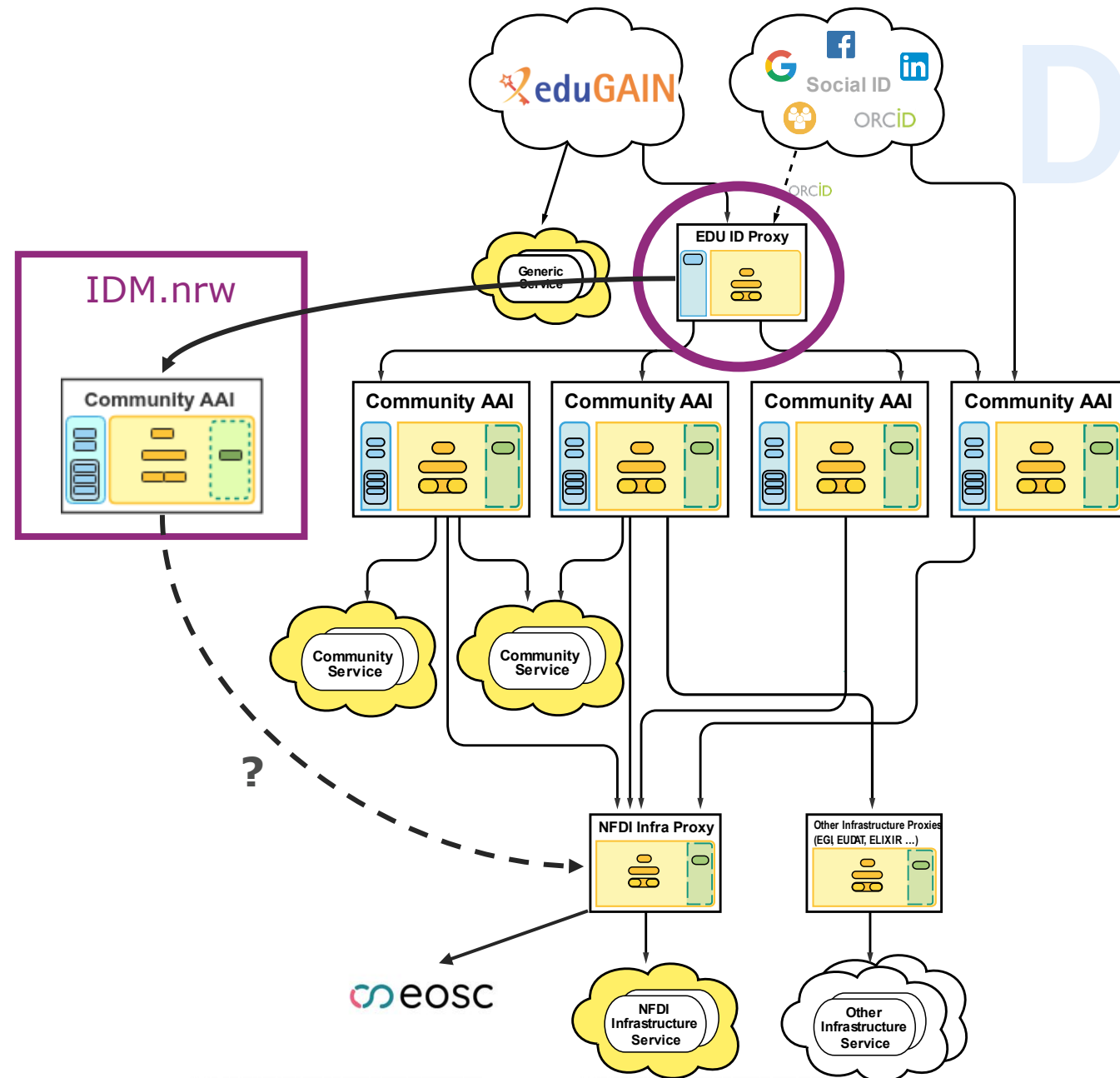
- ▶ edu-ID Proxy als Komponente der NFDI-AAI
 - ▶ Permanente, unveränderliche digitale Identität über von edu-ID abgeleitete subject-id
 - ▶ Aggregation/Verlinkung von Daten aus unterschiedlichen Quellen wie Heimat-IdP und ORCID
 - ▶ Zentraler Homeless-/Gast-IdP

NB: Entwicklungen des Basisdienstes IAM4NFDI und edu-ID werden bis auf weiteres grundsätzlich unabhängig voneinander vorangetrieben



IDM.nrw

- ▶ edu-ID liefert permanente, unveränderliche digitale Identität, adressiert „Researcher Mobility“, ermöglicht Account-Linking
- ▶ Garantiert einheitliches Attributprofil
- ▶ Gast-IdP
- ▶ IDM.nrw potentiell Teil des NFDI-/EOSC-Ökosystems



DFN



Aktueller Stand Pilotphase DFN edu-ID



- ▶ Systemumgebung für den zukünftigen Produktivbetrieb
 - ▶ Georedundanz und hohe Verfügbarkeit
 - ▶ Einzelne Komponenten bereits georedundant, Konzept für „große Lösung“ liegt vor
 - ▶ Benötigte Hardware mittlerweile vorhanden
- ▶ Weitere und komplexere Anwendungsfälle mit ausgewählten Partnern
 - ▶ Studienvorbereitung und Onboarding
 - ▶ Lebenslanges Forschen und Lernen
 - ▶ Einheitlicher Login für Forschungsinfrastrukturen
 - ▶ Sicherheitsaspekte, Incident Response, Pentest für Herbst beauftragt

Kooperationen Pilotphase

- ▶ Staatsbibliothek zu Berlin (bereits PoC), GBV / VZG (Nationallizenzen)
- ▶ TU Dortmund mit weiteren Partnern
 - ▶ Moodle: Studienvorbereitung, Gast-User, u.a.m.
- ▶ NFDI Basisdienst IAM
 - ▶ edu-ID als zentrale Login-Komponente der NFDI-AAI
- ▶ Helmholtz ID
 - ▶ edu-ID als zentrale Login-Komponente für Nutzende außerhalb der Helmholtz-Gemeinschaft
- ▶ IDM.nrw
 - ▶ edu-ID als zentrale Login-Komponente für den im Aufbau befindlichen NRW-Proxy
- ▶ ZKI
 - ▶ Gast-Zugang zu ZKI-Systemen (Wiki, Convera, ...)

Vielen Dank! Gibt es Fragen/Kommentare?



► Kontakt

► Wolfgang Pempe

Teamleiter DFN-AAI

E-Mail: pempe@dfn.de

Telefon: +49 30 884299-308

Anschrift:

DFN-Verein, Geschäftsstelle

Alexanderplatz 1

10178 Berlin



Referenzen

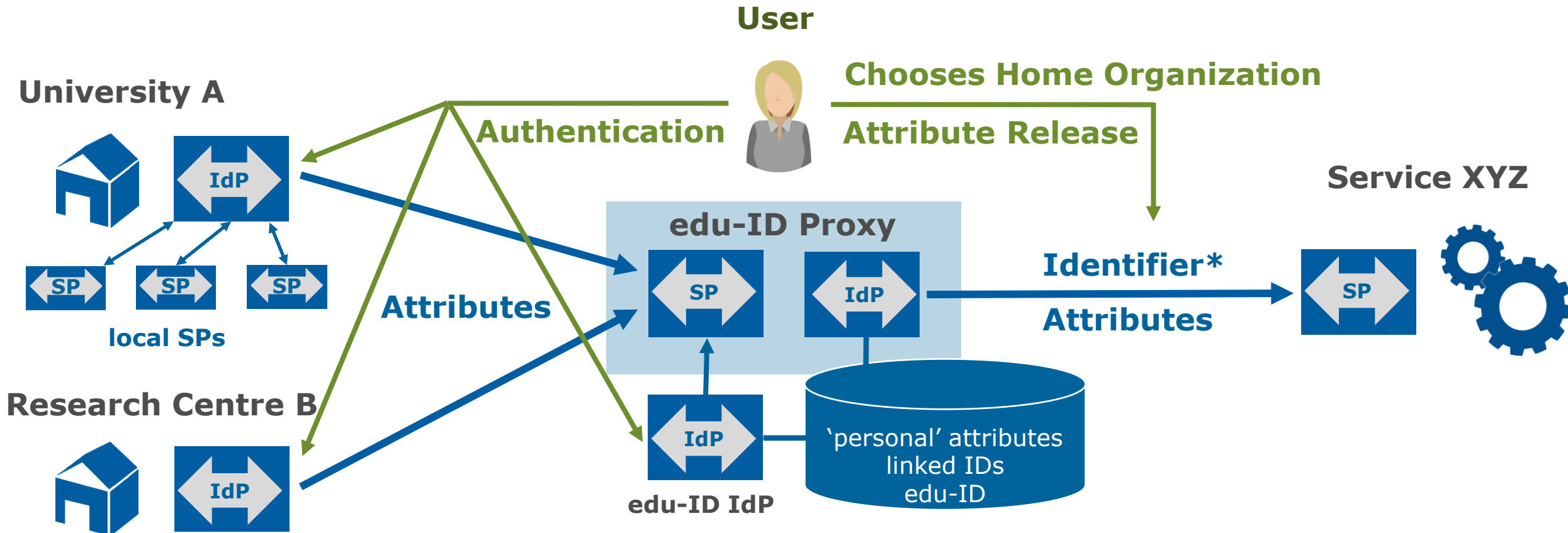
- ▶ AARC-G045: AARC Blueprint Architecture 2019
<https://doi.org/10.5281/zenodo.3672785>
- ▶ AARC-G080: AARC Blueprint Architecture 2025 (Work in Progress)
<https://docs.google.com/document/d/1R86JBLSWWAav5hj30z4nmrpInq2BG2eHU3MOF8yrdaU/edit>
- ▶ DFN edu-ID: <https://doku.tid.dfn.de/de:aai:eduid:start>
- ▶ Projekt IAM4NFDI: <https://base4nfdi.de/projects/iam4nfdi>
 - ▶ Dokumentation NFDI-AAI: <https://doc.nfdi-aai.de>

DFN

Backup

Architektur: edu-ID System als Proxy

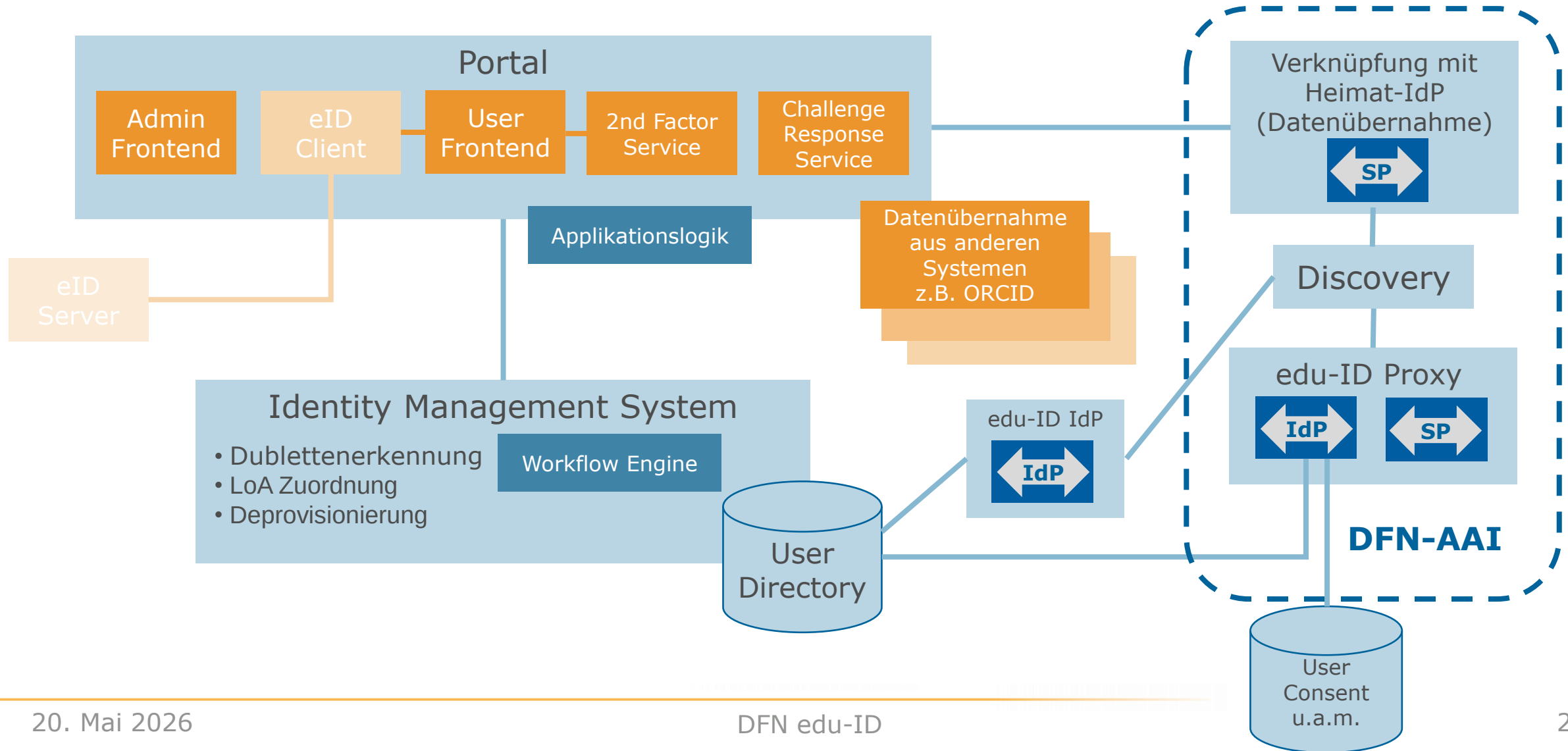
Für "Homeless Users" ist der edu-ID IdP auch Authentifizierungsquelle



* abgeleitet von edu-ID

Technische Komponenten edu-ID

DFN

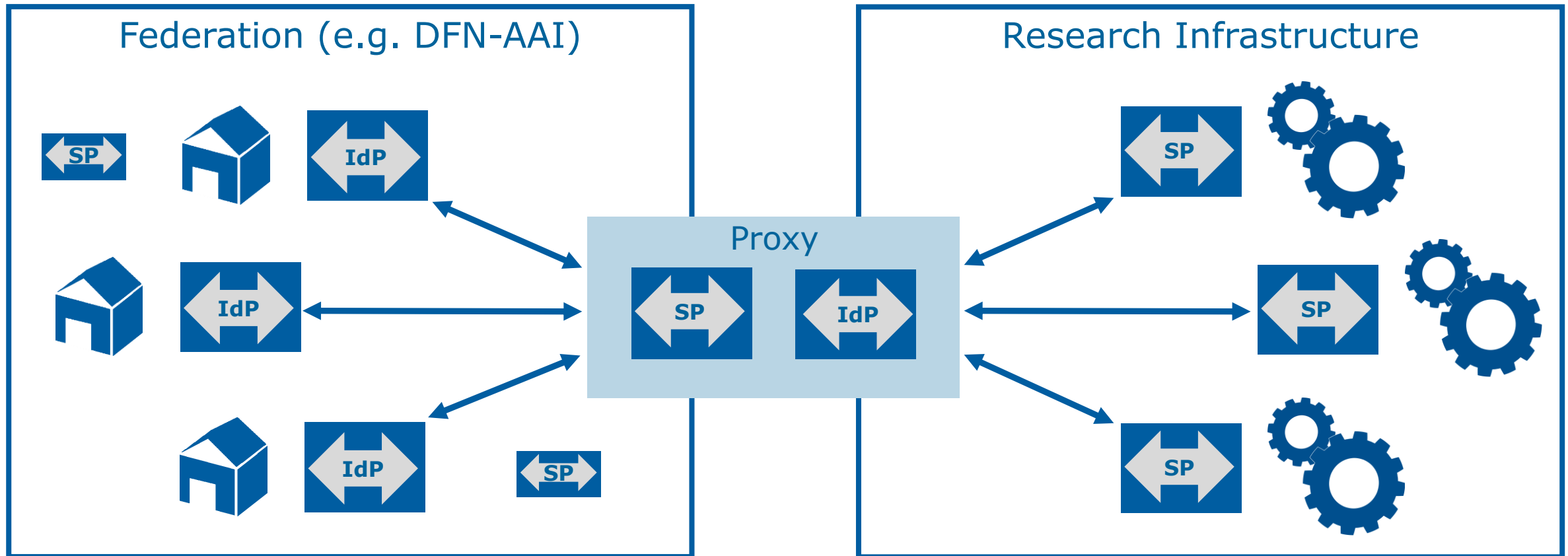


Vorteile edu-ID (Auswahl)

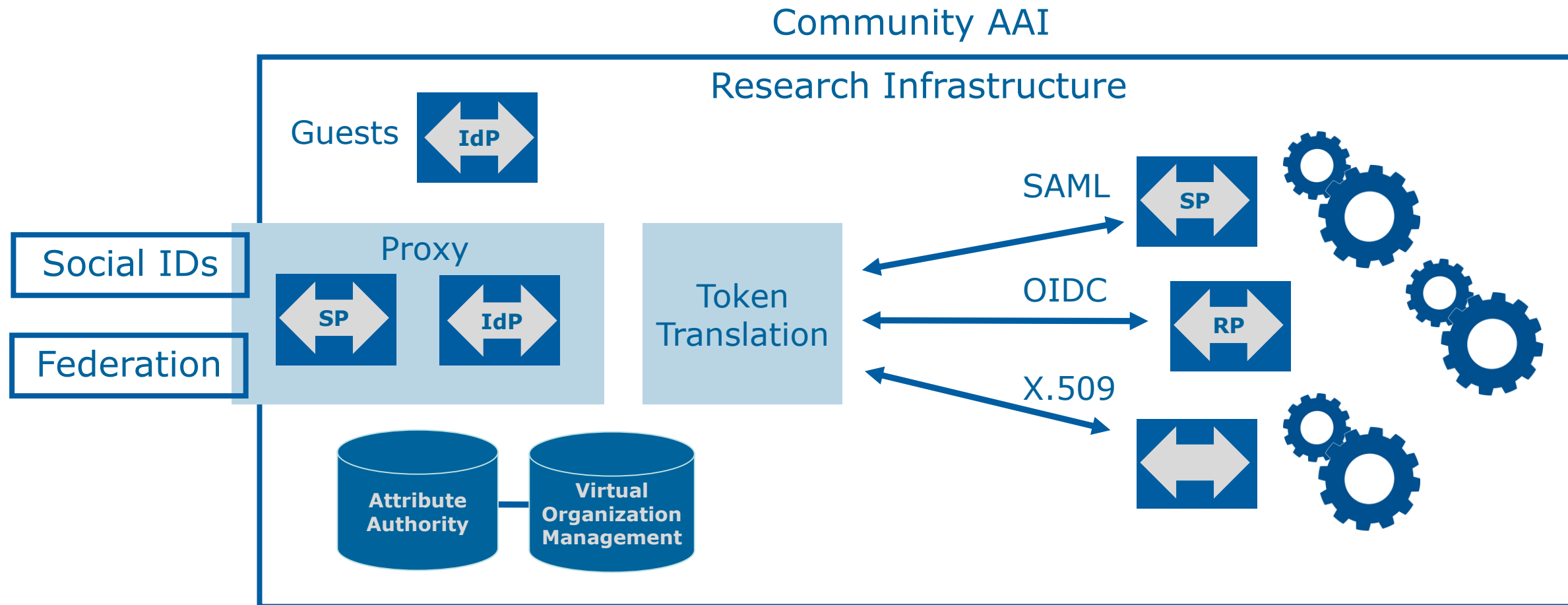
- ▶ Sicht Nutzende
 - ▶ keine Neu-Registrierung bei Ressourcenanbietern nach Wechsel der Heimateinrichtung
 - ▶ edu-ID-System als Switchboard ermöglicht Account Linking zwischen verschiedenen digitalen Identitäten
 - ▶ Lebenslanges Lernen
- ▶ Sicht Ressourcenanbieter und Forschungs-Communities
 - ▶ Wechsel der Heimateinrichtung von Nutzenden erzeugt keinen neuen Verwaltungsaufwand
 - ▶ Notwendigkeit eines eigenen IdP für „Homeless User“ entfällt
 - ▶ Erleichterungen beim Management Virtueller Organisationen
- ▶ Sicht Heimateinrichtungen
 - ▶ Notwendigkeit für Nachhalten „ehemaliger“ Identitäten im eigenen IdM entfällt, z.B. für Abruf von Leistungsnachweisen
 - ▶ Skalierung Attributfreigabe
 - ▶ edu-ID liefert bereits validierte, vertrauenswürdige digitale Identitäten für Onboarding-Szenarien

Proxy – a simple Model

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

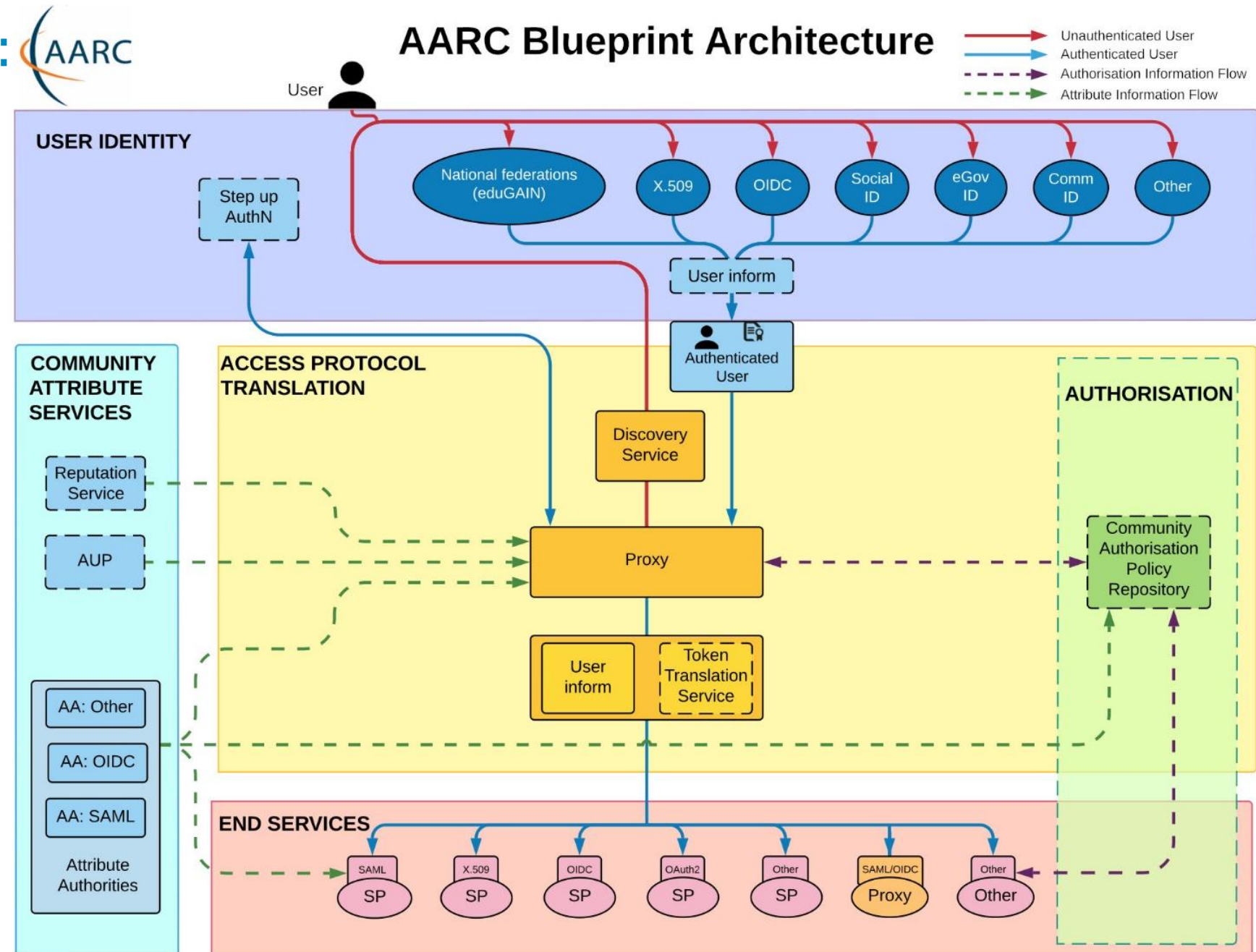


... that can be easily extended



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/>

Attribute

Organisation



eduPersonAffiliation
eduPersonAssurance
eduPersonEntitlement
eduPersonOrcid

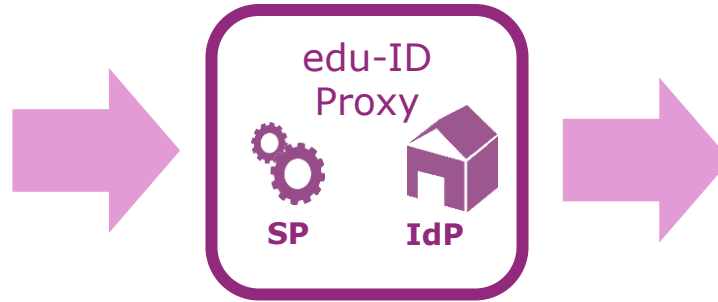
ORCID

mail
displayName
givenName
sn
homePostalAddress
o
pairwise-id

edu-ID



schacHomeOrganization
schacDateOfBirth
schacPlaceOfBirth
schacCountryOfResidence
schacPersonalUniqueCode



eduPersonAffiliation
eduPersonAssurance
eduPersonEntitlement
eduPersonOrcid

mail
displayName
givenName
sn
homePostalAddress
o
pairwise-id*
subject-id*

schacHomeOrganization
schacCountryOfResidence
schacPersonalUniqueCode

SAML

* abgeleitet von edu-ID

DFN

OpenID Connect

edu_person_affiliation
edu_person_assurance / asr
edu_person_entitlement
orcid

email
name
given_name
family_name
home_postal_address
org_name
sub* (pairwise) + iss
sub* (public) + iss

org_domain
schac_country_of_residence
schac_personal_unique_code