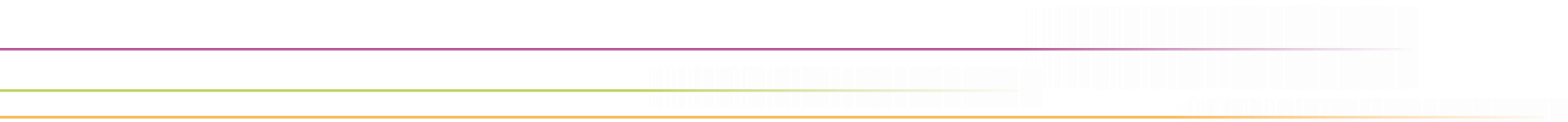


deutsches forschungsnetz

DEN





DFN edu-ID

Die lebenslange Identität für Forschung und Lehre

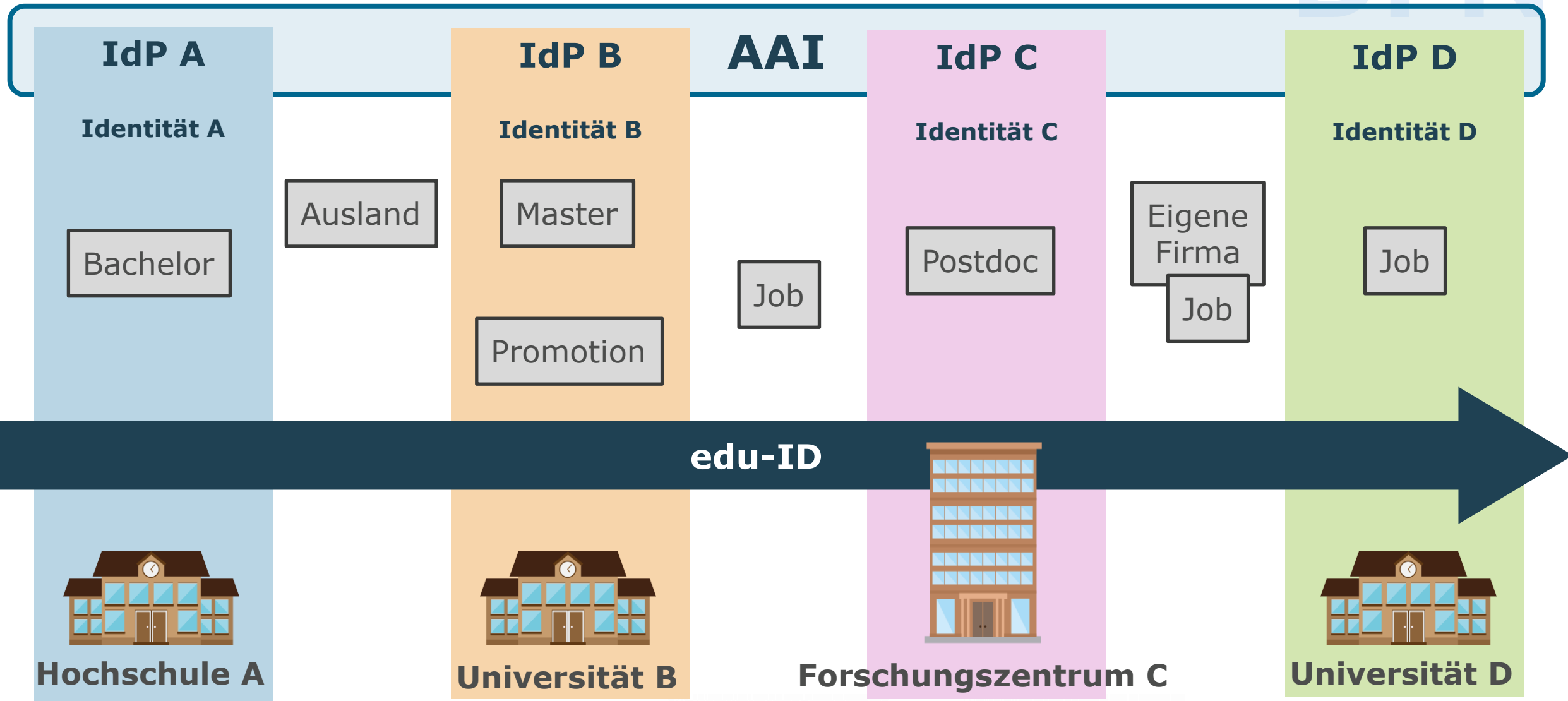
Herbsttreffen der Länder-IdM-Initiativen | 9./10. Oktober 2024

Wolfgang Pempe (pempe@dfn.de)



Eine lebensbegleitende digitale Identität ...

DFN



Das edu-ID-Konzept

- ▶ **Kontinuität:**

Eine lebenslange digitale Identität für den Forschungs- und Bildungssektor

- ▶ **Digitale Souveränität:**

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

- ▶ **Interoperabilität:**

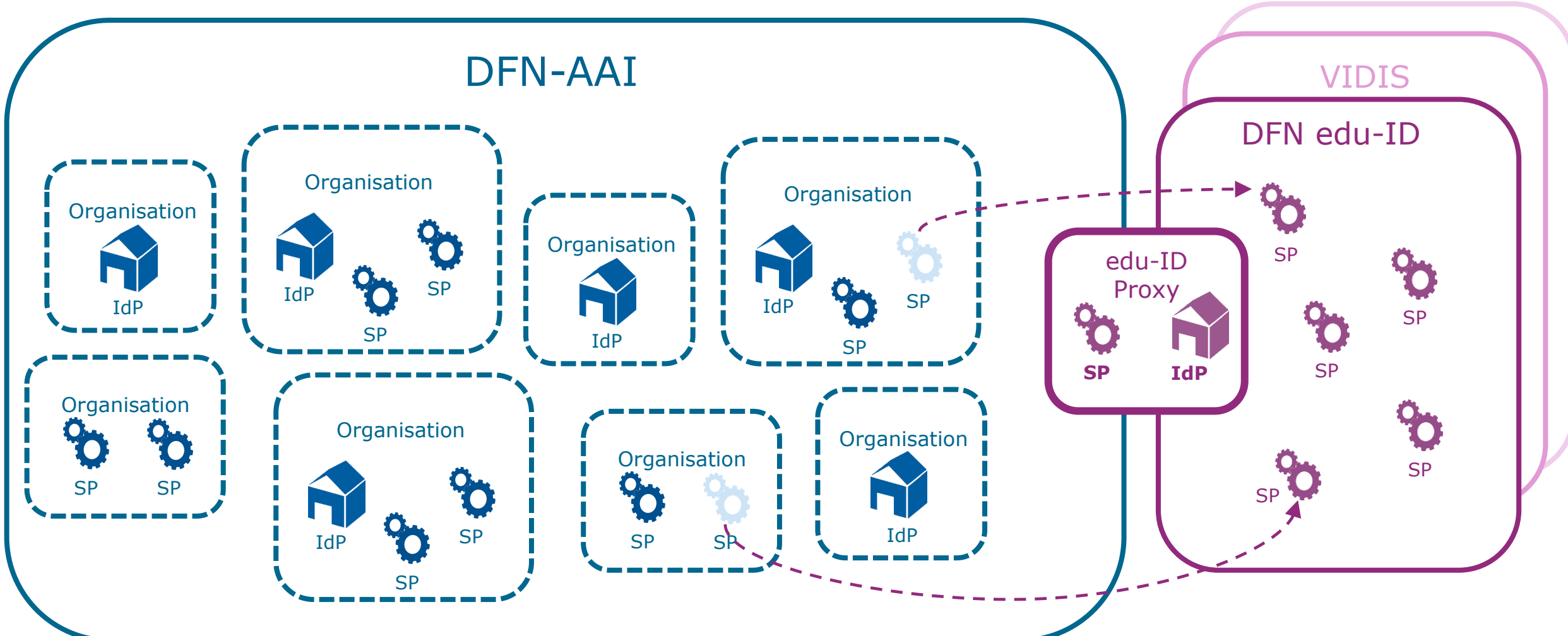
Verknüpfung mit anderen digitalen Identitäten: DFN-AAI, ORCID, MyAccessID
(zukünftig evtl. auch bundID)

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

- ▶ Nahtlose Integration in DFN-AAI
 - ▶ Einmal verknüpft mit dem edu-ID-Account, bleibt der Identity-Provider (IdP) der Heimateinrichtung weiterhin Authentifizierungsquelle
 - ▶ Heimat-IdP bleibt auch Attributquelle, diese werden in Echtzeit vom edu-ID-System durchgereicht
 - ▶ edu-ID-System ergänzt Attribute um einen lebenslang gültigen, global eindeutigen Identifikator
 - ▶ ... und ggf. auch Attribute aus weiteren, mit dem System verknüpften Identitäten, z.B. ORCiD oder MyAccessID
- ▶ edu-ID-System als Brücke
 - ▶ Aufgrund der Proxy-Architektur als Verbindung zu weiteren Vertrauensgefügen nutzbar: z.B. Schulföderation VIDIS, meinbildungsraum.de, EOSC-AAI, ...
 - ▶ Unterstützung der gängigen SSO-Standards: SAML, OpenID Connect
- ▶ edu-ID-IdP als allgemeiner Heimat-IdP bzw. *IdP of last resort*

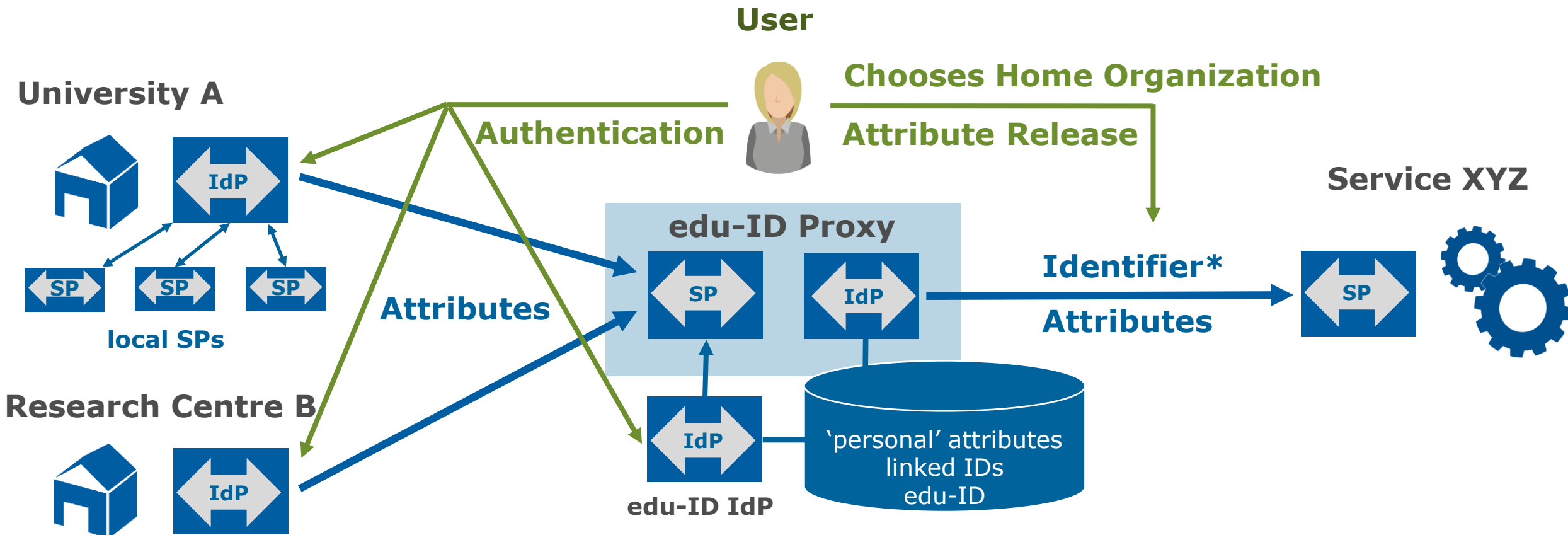
edu-ID und DFN-AAI

DFN



Architektur: edu-ID System als Proxy

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



* abgeleitet von edu-ID

Attribute

Organisation



eduPersonAffiliation
eduPersonAssurance
eduPersonEntitlement
eduPersonOrcid

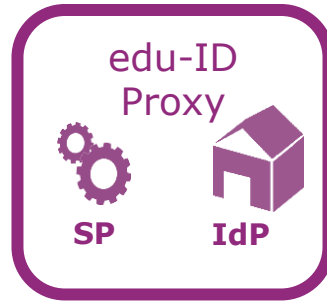
ORCID

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

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

```

* abgeleitet von edu-ID

Stand der Dinge (Überblick)

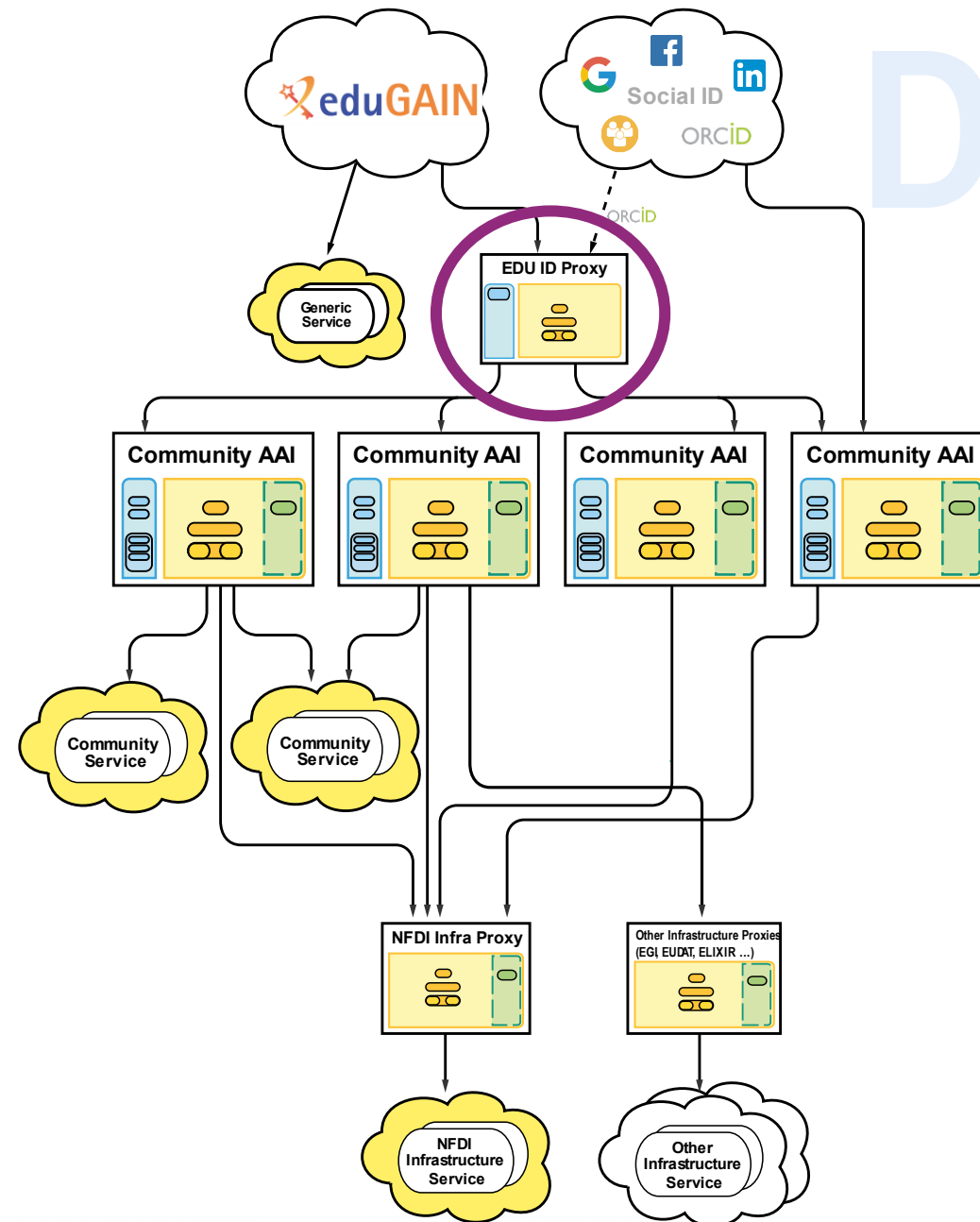
- ▶ Konzept im Rahmen einer ZKI-Arbeitsgruppe entwickelt, Ergebnisse Ende 2022 publiziert:
 - ▶ Eine edu-ID für die Wissenschaft in Deutschland – technisches Konzept
<https://doi.org/10.5281/zenodo.7418055>
 - ▶ Whitepaper der ZKI AG edu-ID zur Verortung des Konzepts einer edu-ID in der aktuellen Landschaft digitaler Identitäten in Deutschland und Europa <https://doi.org/10.5281/zenodo.7425176>
- ▶ Technischer Proof of Concept seit Mitte 2023
 - ▶ Implementierung beim DFN-CERT, auf Basis des o.g. technischen Konzepts
 - ▶ Validierung technisches Konzept, User Experience, Datenschutz, Nutzungsbedingungen
 - ▶ Wichtigster Partner: Staatsbibliothek zu Berlin mit Fachinformationsdienst CrossAsia
 - ▶ Berechtigungsmanagement, Migrationsstrategien, ...
 - ▶ Geplant: Überarbeitung und Ergänzung technisches Konzept
- ▶ Pilotphase voraussichtlich ab Dezember 2024
 - ▶ Weitere Use Cases, Aufbau der zukünftigen Betriebsumgebung

Ausblick: Kooperationen Pilotphase

- ▶ Staatsbibliothek zu Berlin (bereits PoC), GBV / VZG (Nationallizenzen)
- ▶ NFDI Basisdienst IAM -> edu-ID als Komponente der NFDI-AAI
- ▶ ZKI (bereits PoC)
- ▶ KIT
- ▶ Helmholtz AAI
- ▶ IDM.nrw, Git.nrw
- ▶ MyAccessID -> EuroHPC
- ▶ Interessensbekundungen seitens DATEV, Stiftung für Hochschulzulassung, Uni Bonn u.a.m.
- ▶ Noch offen: VIDIS (Finanzierung), meinbildungsraum.de (neuer Projektträger)

NFDI-AAI

- ▶ edu-ID Proxy als (optionale) 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
- ▶ Entwicklungen des Basisdienstes IAM4NFDI und edu-ID werden bis auf weiteres grundsätzlich unabhängig voneinander vorangetrieben



Vielen Dank! Gibt es Fragen/Kommentare?

DFN

► Kontakt

► Wolfgang Pempe

Teamleiter DFN-AAI

E-Mail: pempe@dfn.de

Telefon: +49 30 884299-308

Anschrift:

DFN-Verein, Geschäftsstelle

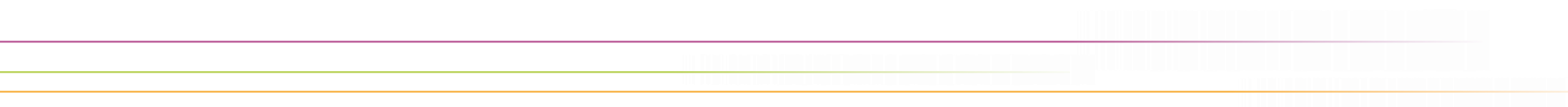
Alexanderplatz 1

10178 Berlin



DFN

Backup



Bibliotheken als Early Adopters

- ▶ Erster Use Case (PoC) aus dem Bibliotheksbereich mit Staatsbibliothek zu Berlin: Fachinformationsdienst „CrossAsia“
- ▶ Wissenschaftliche Bibliotheken mit überregionalem Versorgungsauftrag benötigen
 1. Einheitliches Web-basiertes Single Sign-on, auch für User ohne Heimat-IdP
 2. Stabile, unveränderliche Identifikatoren für das Zugriffs-Management
 3. Verlässliche Personendaten (Name, Meldeadresse) -> Nationallizenzen
- ▶ Punkte 1 und 2 bereits durch edu-ID-System abgedeckt
- ▶ Punkt 3 aktuell ggf. über Verknüpfung mit Heimat-IdP
-> Anbindung bundID wird angestrebt