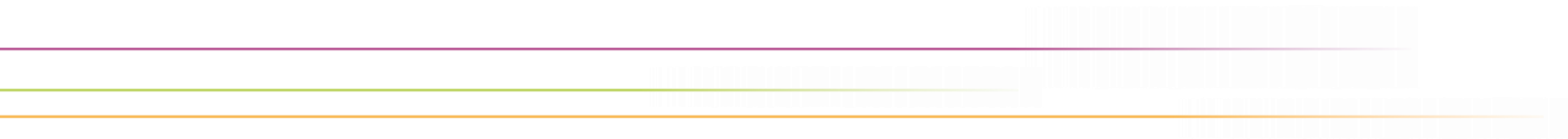


deutsches forschungsnetz



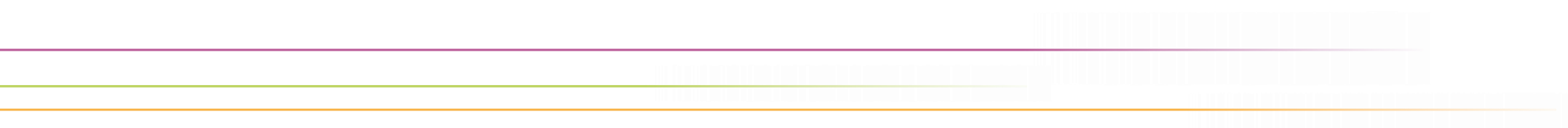


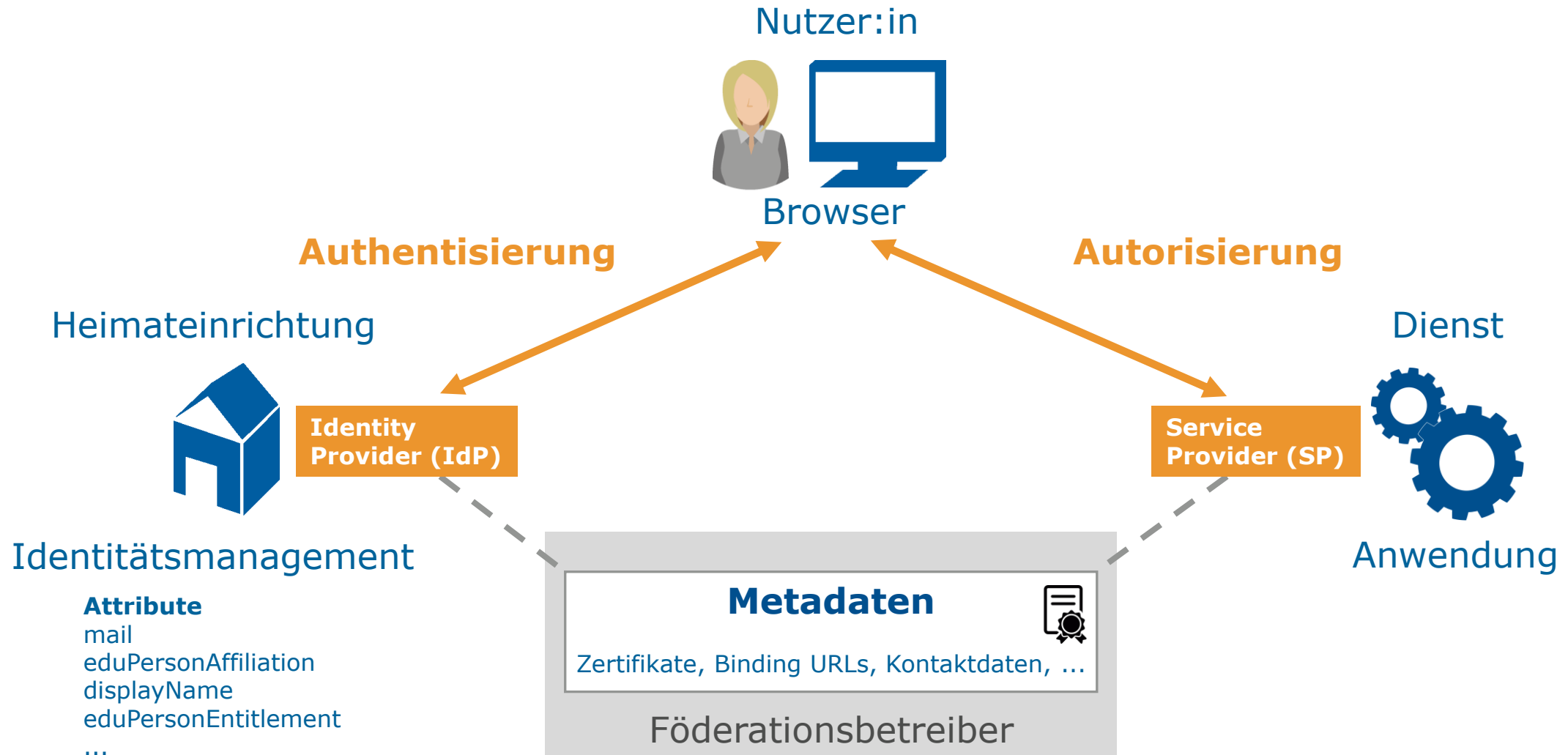
DFN edu-ID

Die lebenslange Identität für Forschung und Lehre

HÜF-Tagung: 08.008 Treffen der IT-Verantwortlichen und der IT-Mitarbeiter:innen der Kunst- und Musikhochschulen | 2./3. Juni 2025

Wolfgang Pempe (pempe@dfn.de)





Beispiel DFN-AAI

- **Föderationsbetreiber**

DFN-Verein

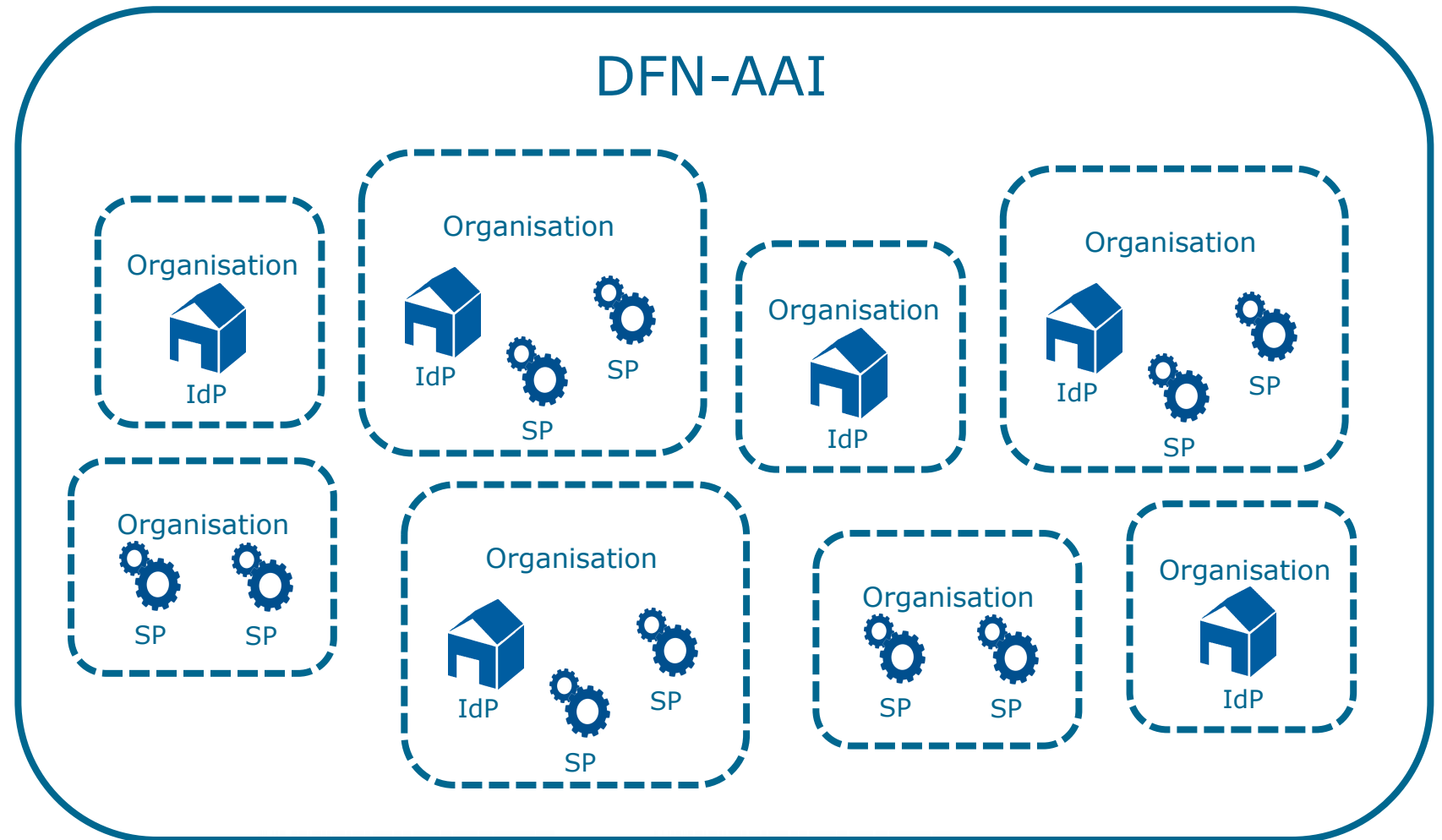
- **Vertrauen**

Verträge mit allen
Teilnehmern, Policies,
Levels of Assurance

- **Technik**

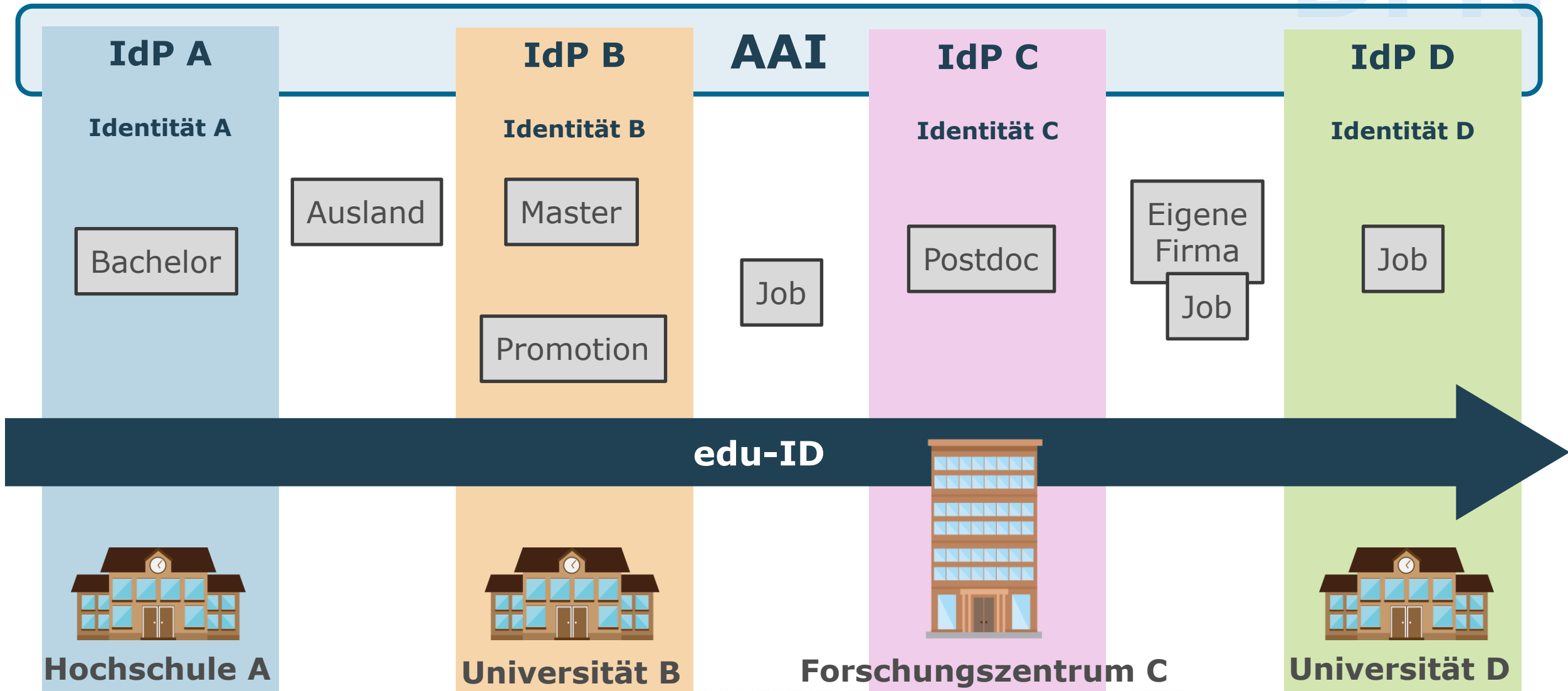
Metadatenverwaltung
und -Signierung

Aktuell ca. 420 teilnehmende
Einrichtungen und 970 Dienste
(zzgl. ~1960 lokale SP)



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: Heimateinrichtung, ORCID, MyAccessID (zukünftig evtl. auch bundID)
- ▶ **Dokumentation:** <https://doku.tid.dfn.de/de:aai:eduid:start>

- ▶ Im März 2019 aus ZKI Arbeitskreis Identity und Access Management etabliert (ZKI = Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.)
 - ▶ Teilnehmende: Angehörige von Hochschulen, Bibliotheken sowie Forschungseinrichtungen und –Communities, diverse Dienstleister, HIS, SfH
 - ▶ Use Cases → Funktionalität und Reichweite eines möglichen edu-ID Dienstes
 - ▶ Erstellung eines Anforderungsprofils an einen möglichen edu-ID Dienst
- ▶ Fortlaufende Workshops und Videokonferenzen von 2019 bis 2022
 - ▶ Anforderungsanalyse, Architektur, Levels of Assurance, ...
- ▶ Begleitet von DFN-CERT und SWITCH (betreibt bereits seit 2016 ein edu-ID System)
- ▶ Dokumentation im Wiki: <https://doku.tid.dfn.de/de:aai:eduid:start>

Nutzungsszenarien

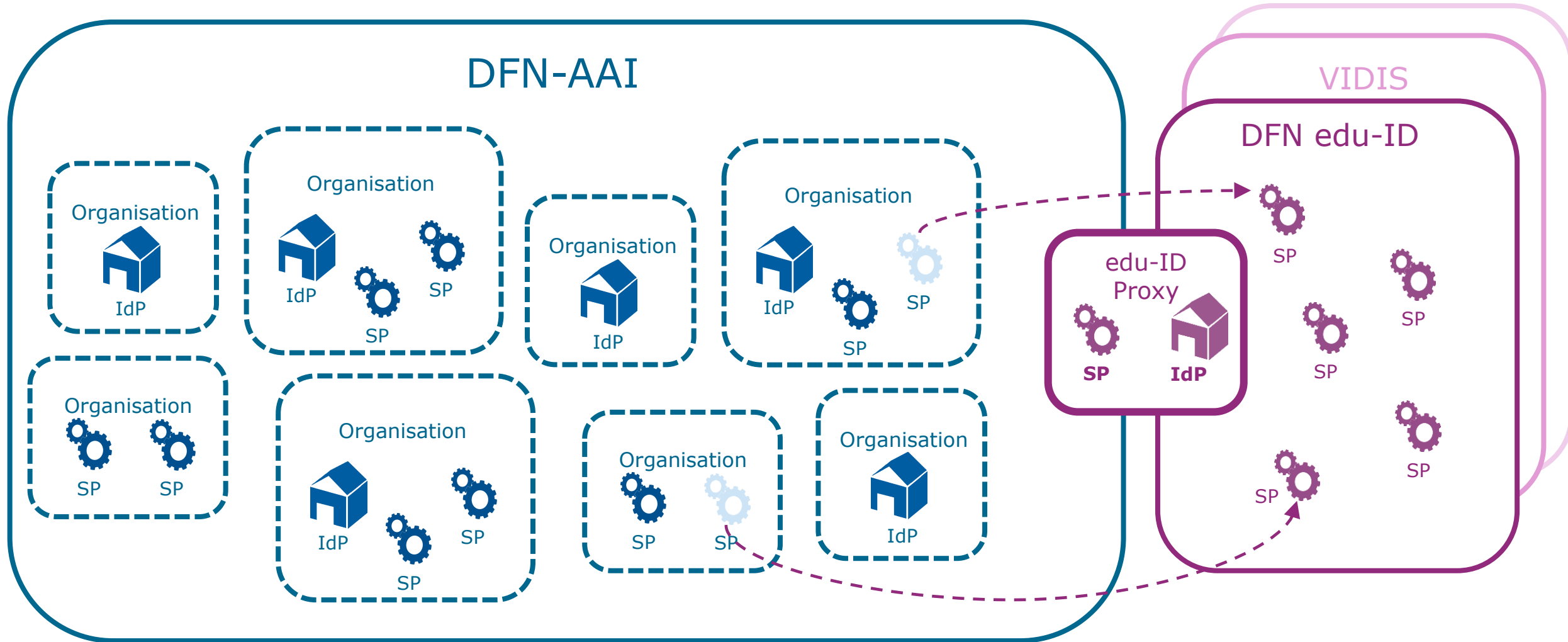
- ▶ Unterbrechungsfreie Nutzung von Diensten bzw. Zugriff auf Ressourcen, deren Nutzungsberechtigung nicht an die aktuelle Zugehörigkeit zu einer bestimmten Einrichtung geknüpft ist (Speicherdienste, Nationallizenzen, Leistungsnachweise, ...)
- ▶ Erleichterung des Managements virtueller Organisationen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

Nutzungsszenarien (Fortsetzung)

- ▶ Vereinheitlichung und Vereinfachung der Verfahren bei Onboarding-Prozessen, z.B. Registrierung, Einstellung, Online-Immatrikulation
 - ▶ Verlässliche digitale Identität bereits vorhanden:
Verifizierung der edu-ID-Nutzerdaten über eIDAS-konforme eID-Systeme
 - ▶ Dublettenvermeidung, Unterstützung beim Aufspüren von Dubletten
 - ▶ Einzelne Use Cases auch als OZG-Leistungen klassifiziert
- ▶ Zusammenführung verschiedener Identitäten bzw. Accounts (Account Linking)
 - ▶ ORCID und andere Identifier (z.B. European Student Identifier)
 - ▶ Nutzerdaten („Affiliations“) aus den Heimateinrichtungen

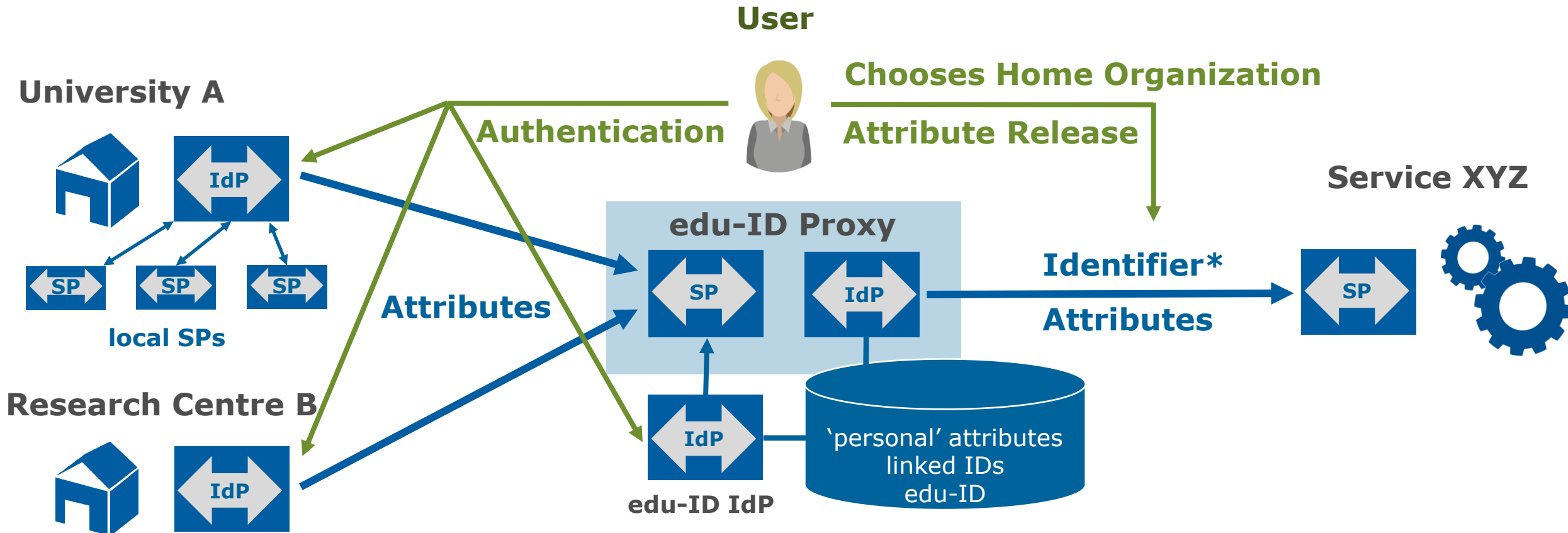
Vorteile edu-ID (Auswahl)

- ▶ 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



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

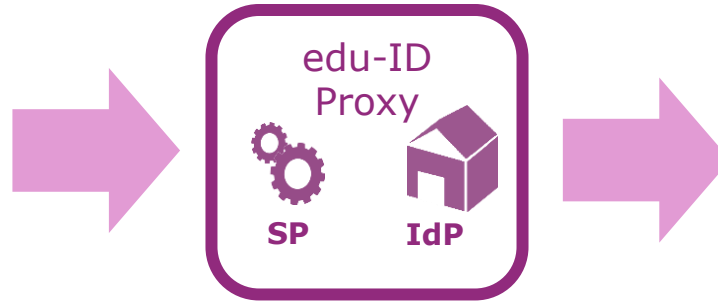
ORCID

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

* 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

Stand der Dinge (Überblick)

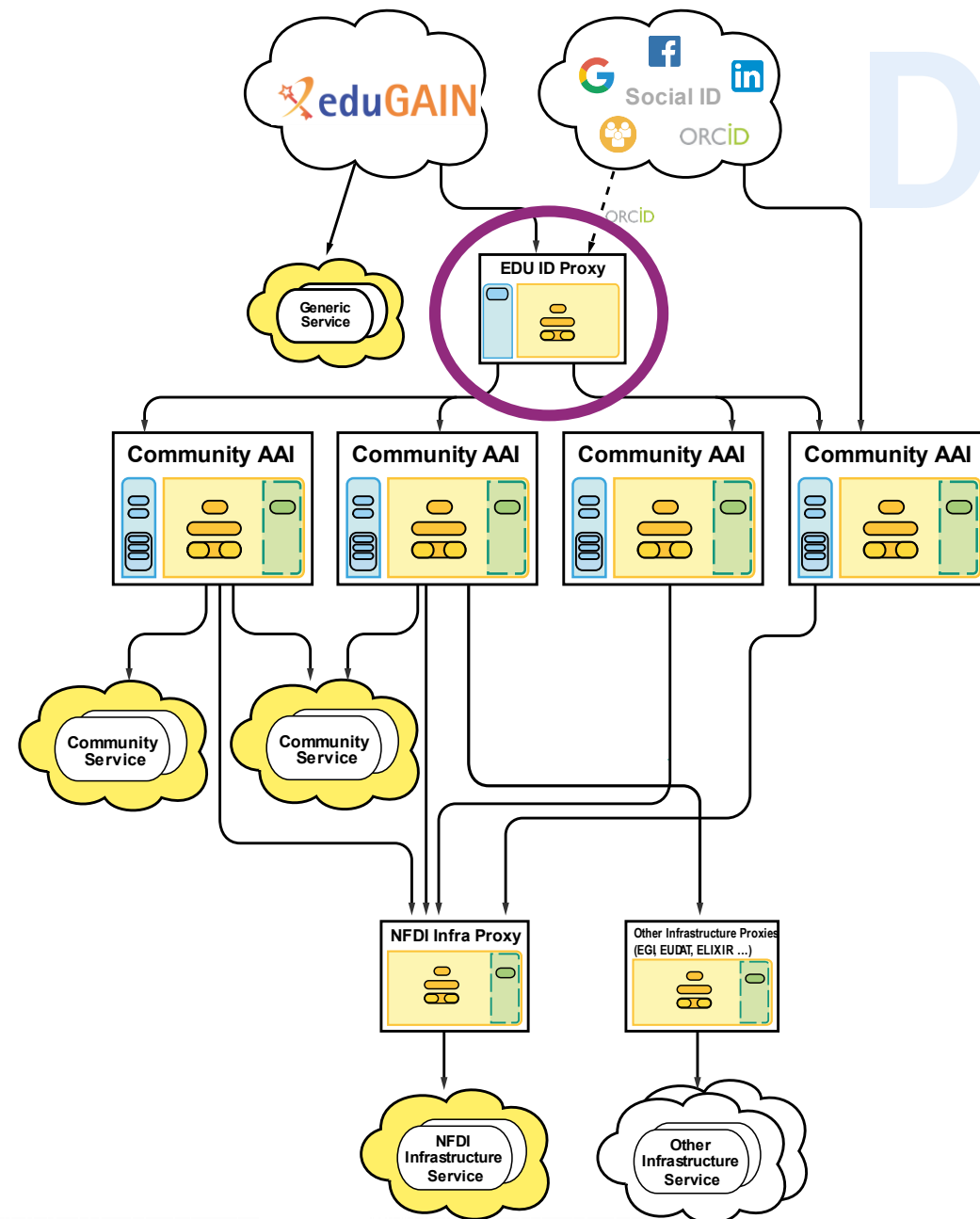
- ▶ Ergebnisse der ZKI Arbeitsgruppe edu-ID Ende 2022 publiziert:
 - ▶ Eine edu-ID für die Wissenschaft in Deutschland – technisches Konzept
<https://doi.org/10.5281/zenodo.7418055>
 - ▶ Whitepaper der ZKI AG edu-ID zur Verortung des Konzepts einer edu-ID in der aktuellen Landschaft digitaler Identitäten in Deutschland und Europa <https://doi.org/10.5281/zenodo.7425176>
- ▶ Technischer Proof of Concept Mitte 2023 bis Ende 2024
 - ▶ 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, ...
 - ▶ Überarbeitung und Ergänzung technisches Konzept
- ▶ Pilotphase kürzlich gestartet (2025)
 - ▶ Weitere Use Cases, Aufbau der zukünftigen Betriebsumgebung, Supportstrukturen, ...

Ausblick: Kooperationen Pilotphase

- ▶ Staatsbibliothek zu Berlin (bereits PoC), GBV / VZG (Nationallizenzen)
- ▶ OpenMoodle TU Dortmund
- ▶ NFDI Basisdienst IAM -> edu-ID als Komponente der NFDI-AAI
- ▶ ZKI (bereits PoC)
- ▶ KIT
- ▶ Helmholtz AAI
- ▶ IDM.nrw, Git.nrw
- ▶ MyAccessID -> EuroHPC, European Open Science Cloud (EOSC)
- ▶ Noch offen: VIDIS, 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

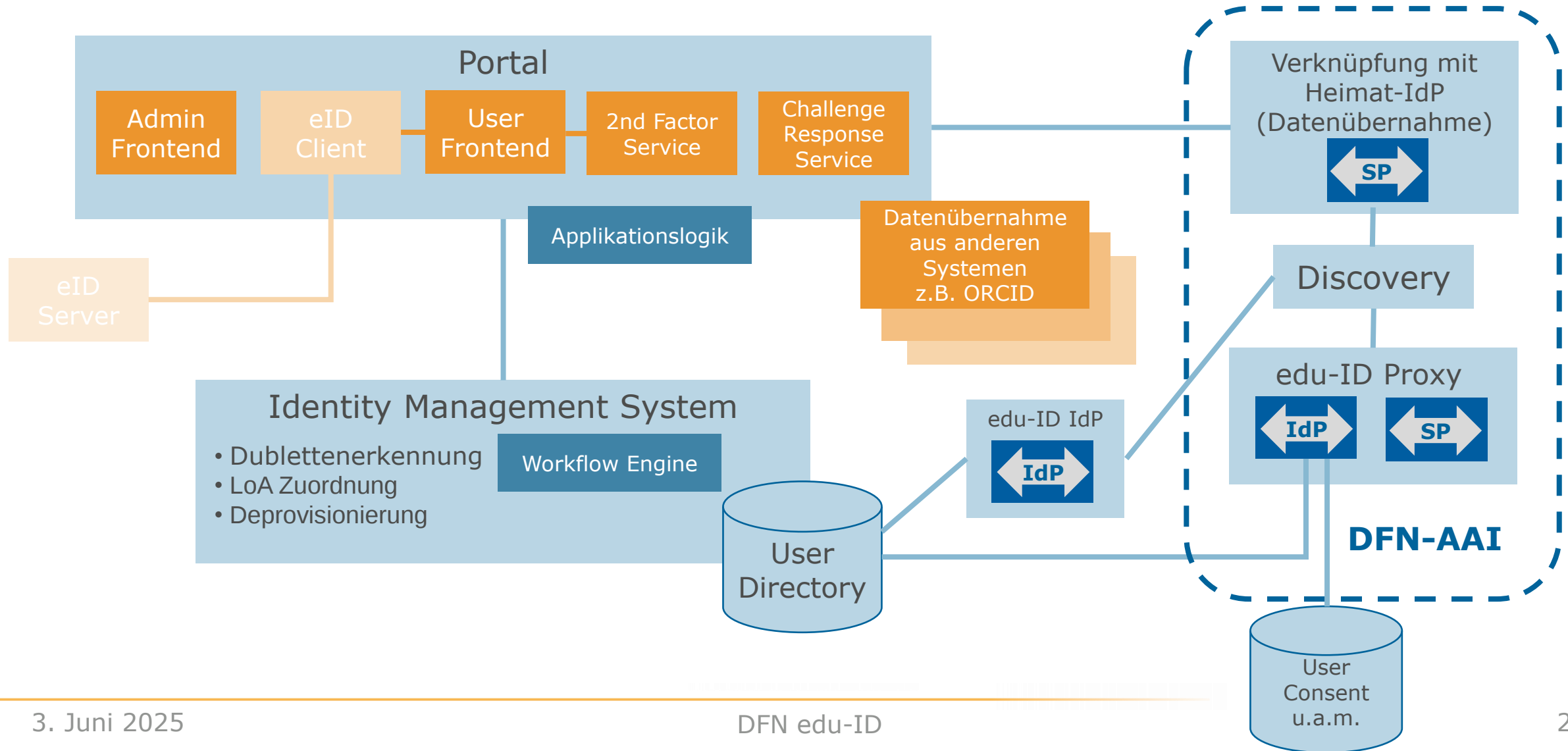
- ▶ Nahtlose Integration in DFN-AAI
 - ▶ Einmal verknüpft mit dem edu-ID-Account, bleibt der Identity-Provider (IdP) der Heimateinrichtung weiterhin Authentifizierungsquelle
 - ▶ Heimat-IdP bleibt auch Attributquelle, diese werden in Echtzeit vom edu-ID-System durchgereicht
 - ▶ edu-ID-System ergänzt 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*

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

Technische Komponenten edu-ID

DFN



Rollout in der Fläche (1)

- ▶ Zielgruppen vor allem
 - ▶ Endnutzer:innen
 - ▶ Forschungscommunities
 - ▶ Dienstanbieter (NB: nicht für jeden Dienst relevant)
- ▶ Heimateinrichtungen als IdP-Betreiber müssen „einfach nur mitmachen“
 - ▶ Einmalige Konfiguration einer Attribute Filter Policy
 - ▶ Unterstützung von Attribute Queries seitens des edu-ID-Systems
 - ▶ Doku unter <https://doku.tid.dfn.de/de:aai:eduid:idpconfig>

Rollout in der Fläche (2)

- ▶ Größere Einrichtungen und Bibliotheken finden sich oft in einer Doppelrolle, d.h. auch als Dienstanbieter
 - ▶ Staatsbibliothek zu Berlin, KIT, ...
 - ▶ Voraussichtlich wenig Überzeugungsarbeit erforderlich, wenn dann hinsichtlich der Datenschutzaspekte (wie üblich)
- ▶ Forschungseinrichtungen voraussichtlich ebenfalls interessiert, zumindest die Helmholtz-Gemeinschaft hat großes Interesse (s.o., Kooperationen)
- ▶ Kleinere Hochschulen: eher abhängig von relevanten Diensten
 - ▶ Landesinitiativen (bwIDM, IDM.nrw, HVB,...) motivieren, auf edu-ID zu setzen?
 - ▶ Onboarding-Szenarien, wenn edu-ID-Identitäten verlässlich sind? (→ bundID)