deutsches forschungsnetz

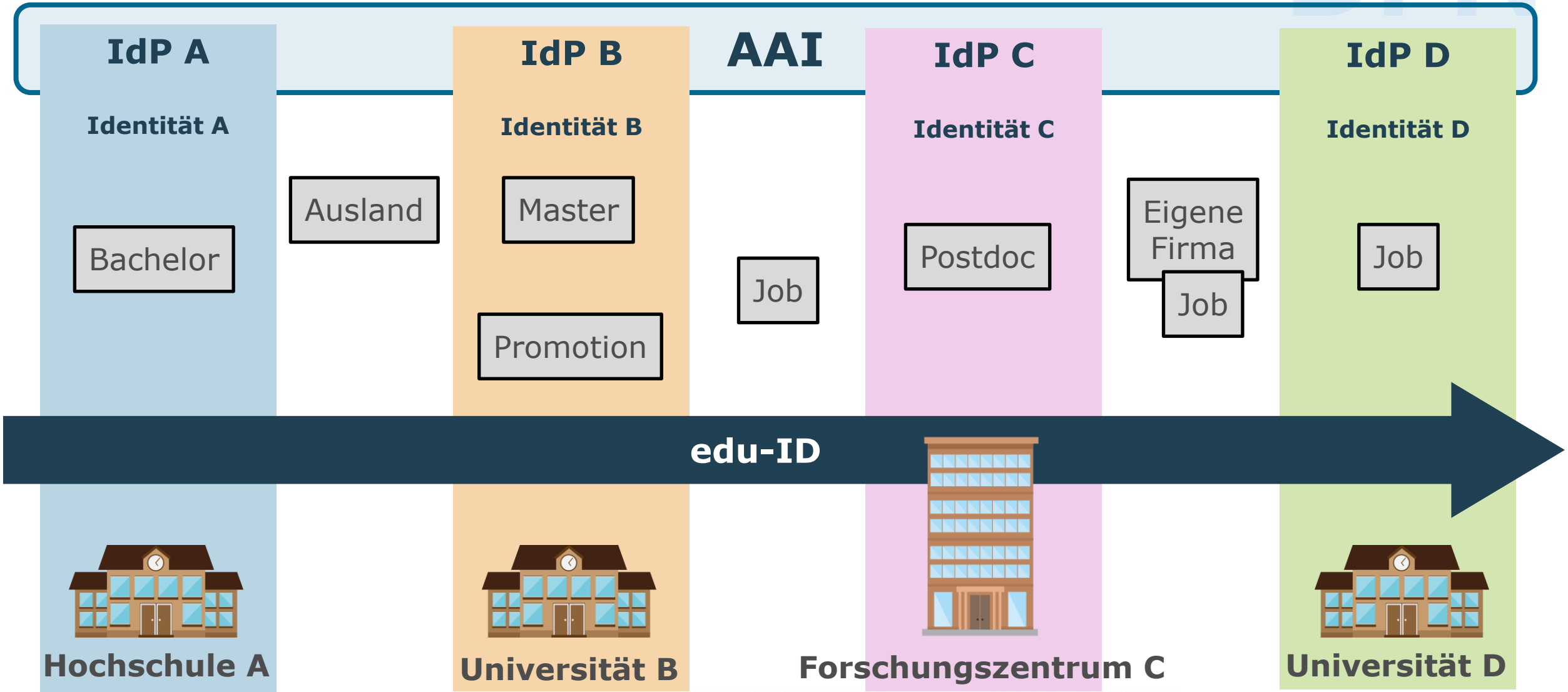
Update edu-ID

79. DFN-Betriebstagung | 17. Oktober 2023

Jürgen Brauckmann, DFN-CERT

Wolfgang Pempe, DFN-Verein

Eine lebenslange digitale Identität



edu-ID: User-centric Identity

- Identität unabhängig von der jeweiligen Heimateinrichtung
- Selbstregistrierung, Bereitstellung der Nutzerdaten
  - Validierung durch edu-ID System bzw. Übernahme aus verlässlichen Systemen
  - Registrierung eines zweiten Faktors
  - Zuordnung zu Verlässlichkeitsklassen (Levels of Assurance) je nach Art/Qualität der Validierung
- Lebenslang gültig
- **Aktive Kontrolle** der Nutzenden über
  - Verknüpfung mit anderen Accounts/Identitäten (Account Linking, ggf. Attribut-Aggregation)
  - Übertragung von Daten an Dienste (Attributfreigabe)
  - Löschung des Accounts

edu-ID Systeme international

- SWITCH edu-ID

  (Nationallizenzen → Speicherdienste → Bibliotheksplattformen…)

- eduid.se – SUNET

  (Onboarding → …)

- eduID.nl – SURF

  (Roadmap: Leistungsnachweise → Student Mobility → …)

- Gelegentliche Koordinationstreffen

ZKI Arbeitsgruppe edu-ID

- 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
  - Anforderungsanalyse, Architektur, Levels of Assurance, …
- Konsultationen mit DFN-CERT und SWITCH (betreibt bereits edu-ID System)
- Dokumentation im Wiki: https://doku.tid.dfn.de/de:aai:eduid:start

edu-ID Use Cases

- https://doku.tid.dfn.de/de:aai:eduid:usecases
- Vier Bereiche:
  - UC 1 Student Life Cycle
  - UC 2 Lehre
  - UC 3 Forschung
  - UC 4 Verwaltung
- Use Cases u.a. als Basis für
  - Definition der als essentiell bewerteten Attribute („Kernattribute“)
  - Anforderungen an Verlässlichkeit der Nutzerdaten/Attribute
  - Anforderungen an die Architektur eines edu-ID Systems, die sich möglichst nahtlos in die bestehende Föderation der DFN-AAI einfügt

Stand der Dinge

- 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
  - Kurze Zusammenfassung unter https://www.dfn.de/eine-fuer-alle-die-edu-id/

- Auf Basis des technischen Konzepts: Entwicklung der Proof of Concept-Implementierung beim DFN-CERT → mittlerweile abgeschlossen

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 für Nutzende

- Unterbrechungsfreier Zugriff auf bestimmte Ressourcen
  - Bibliotheksinhalte: Fachinformationsdienste, Nationallizenzen
  - Forschungsdatenrespositorien
  - Leistungsnachweise
  - …
- Keine Supportanfragen bei Ressourcenanbietern im Falle eines Wechsels der Heimateinrichtung
- Lebenslanges Lernen
  - Bspw. Digitale Vernetzungsinfrastruktur Bildung (BMBF)
- edu-ID-System als Switchboard für digitale Identitäten (Account Linking)

Vorteile für Ressourcenanbieter

… und Forschungscommunities

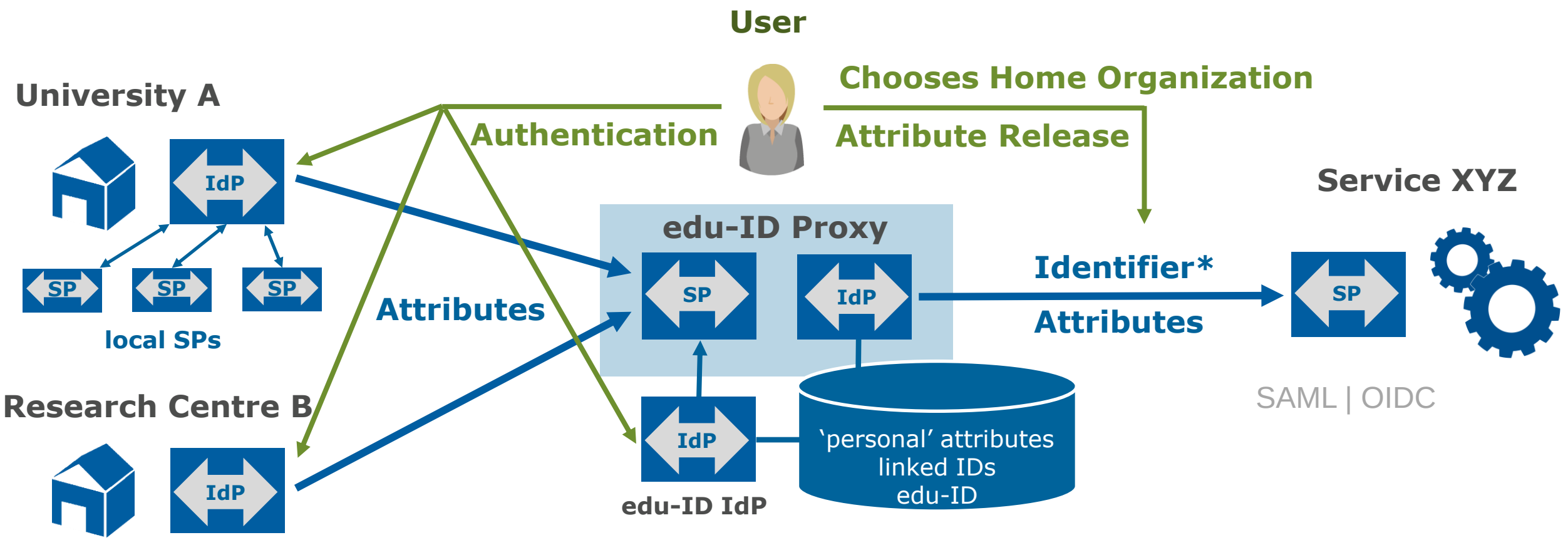
- „Researcher Mobility“ kein Problem mehr, Account Linking bei Wechsel der Heimateinrichtung entfällt
- Notwendigkeit, einen eigenen IdP für „Homeless User“ zu betreiben, entfällt
- Erleichterungen beim Management Virtueller Organisationen

Vorteile für Heimateinrichtungen

- Vereinfachte Attributfreigabe
  - Eine Attribute Filter Policy für sämtliche – auch zukünftige – an das edu-ID-System angeschlossene Dienste und Ressourcen
- Bereitstellung von Leistungsnachweisen erfordert keine langfristige Speicherung von Identitäten im eigenen IdM
  - Verknüpfung von Ressourcen mit von edu-ID abgeleiteten Identifier reicht aus
- Validierte, vertrauenswürdige digitale Identitäten bei Onboarding-Szenarien

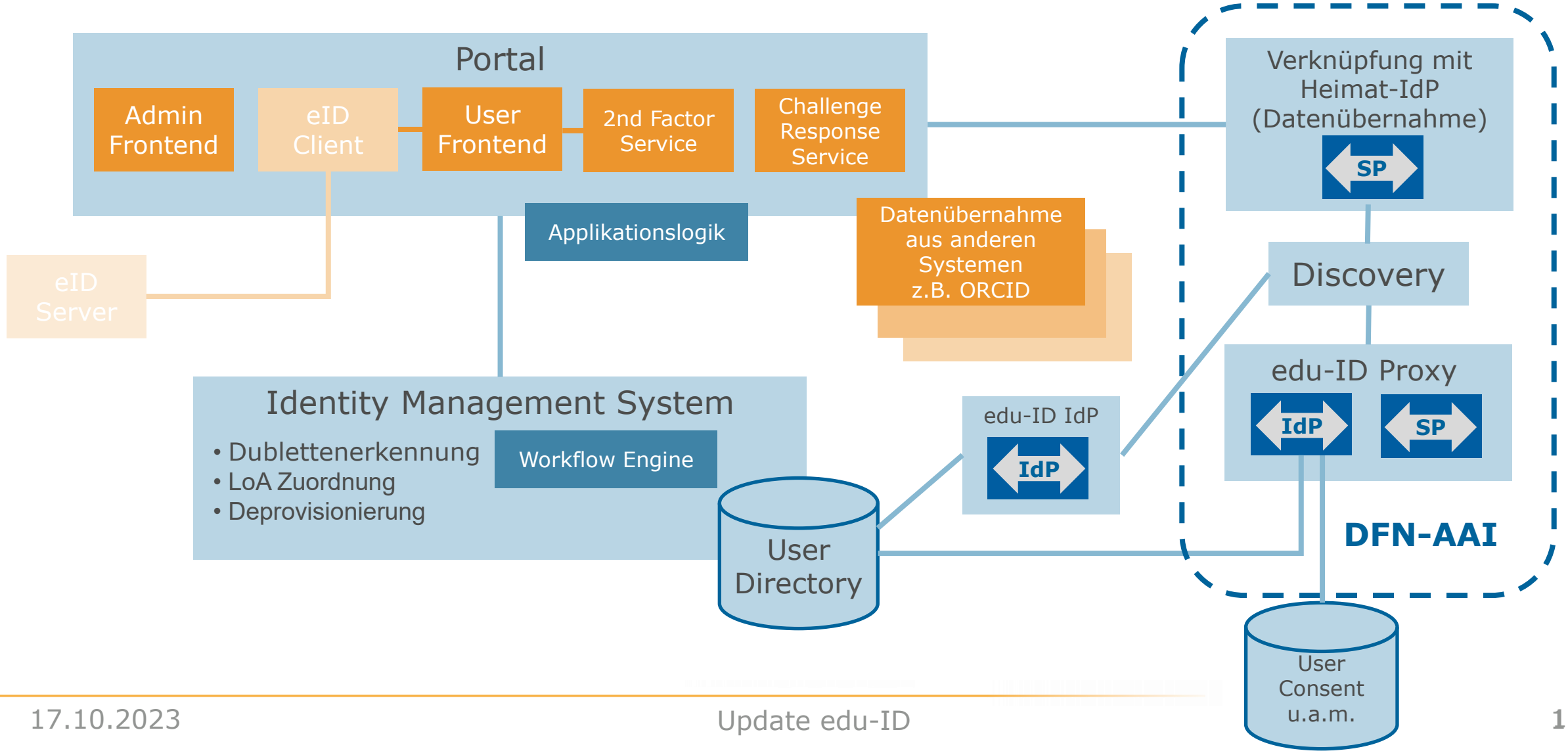
Architektur: edu-ID System als Proxy

Für “Homeless Users” ist der edu-ID IdP auch Authentifizierungsquelle

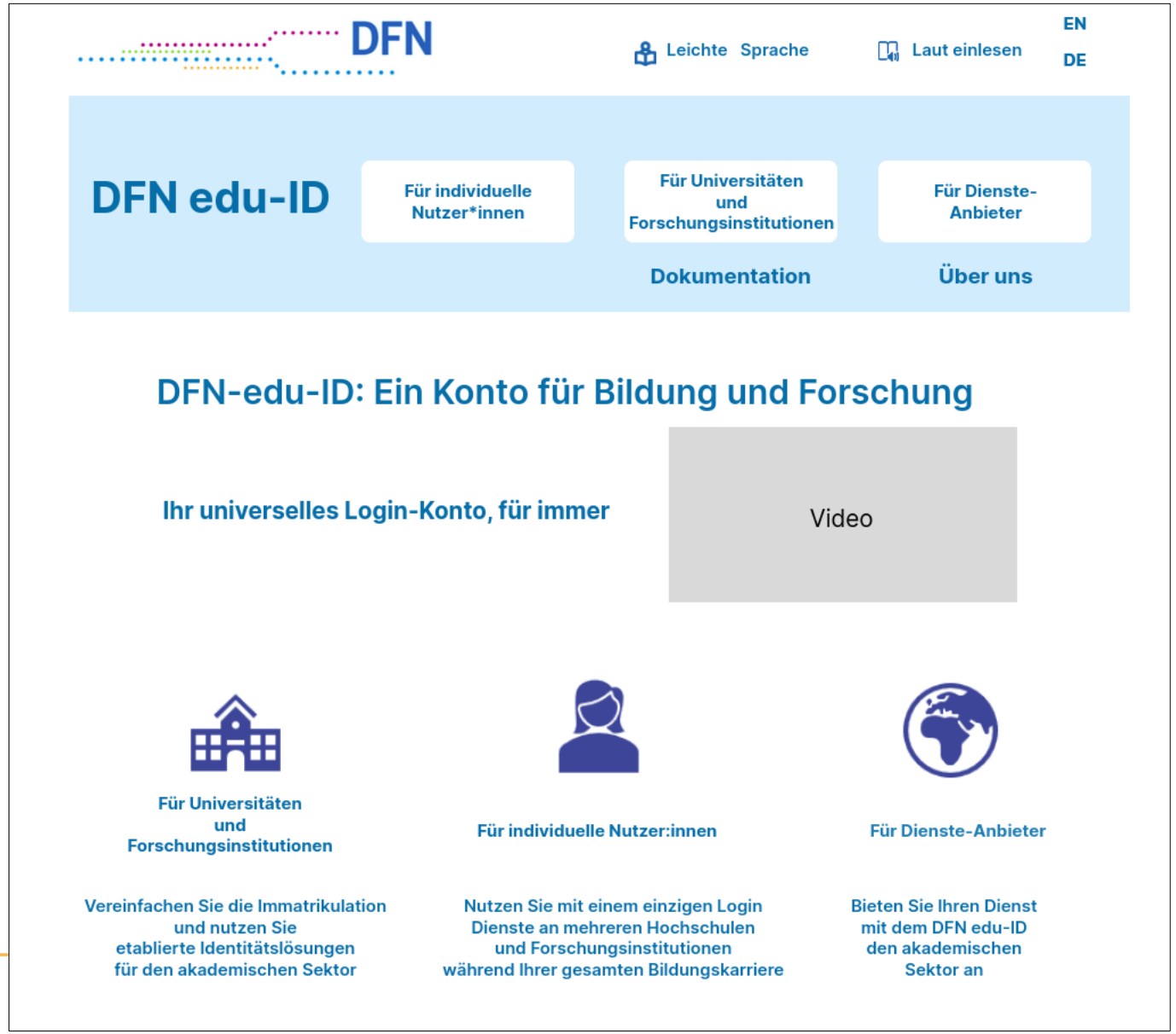


* abgeleitet von edu-ID

Technische Komponenten edu-ID-System

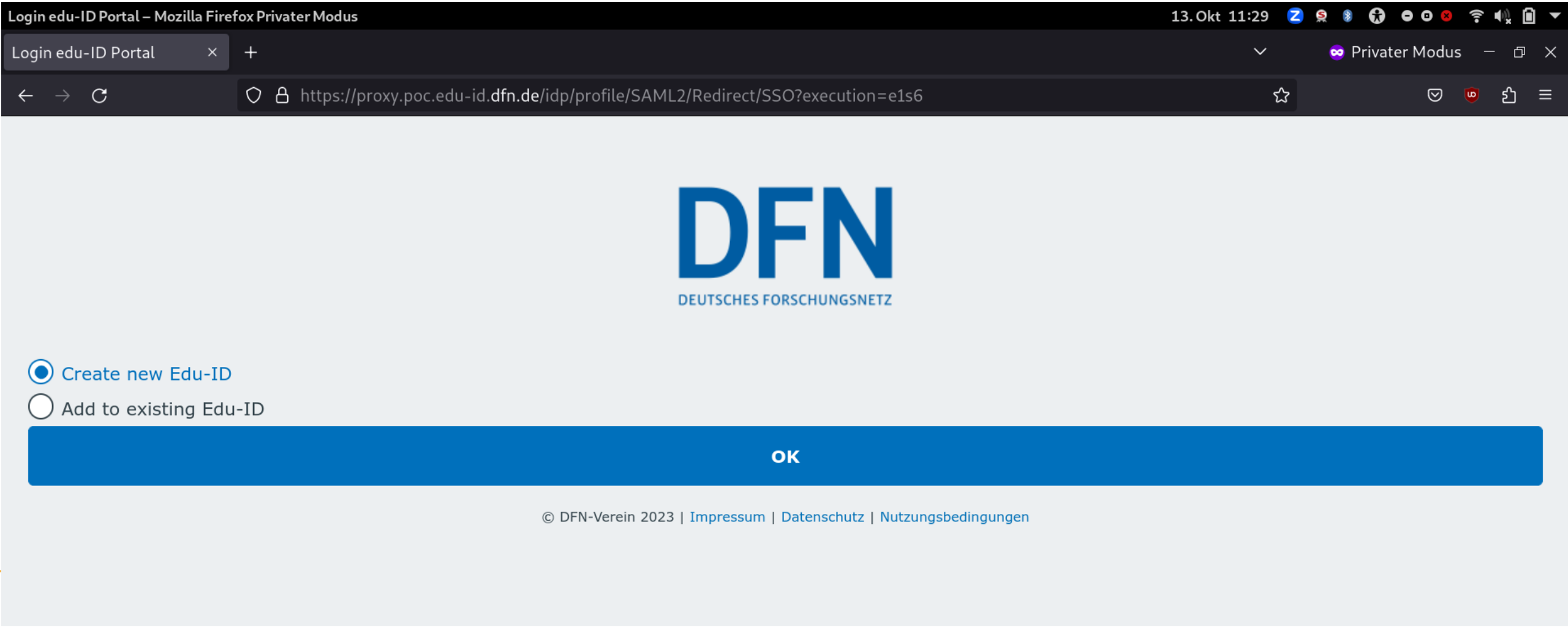


Screenshots PoC



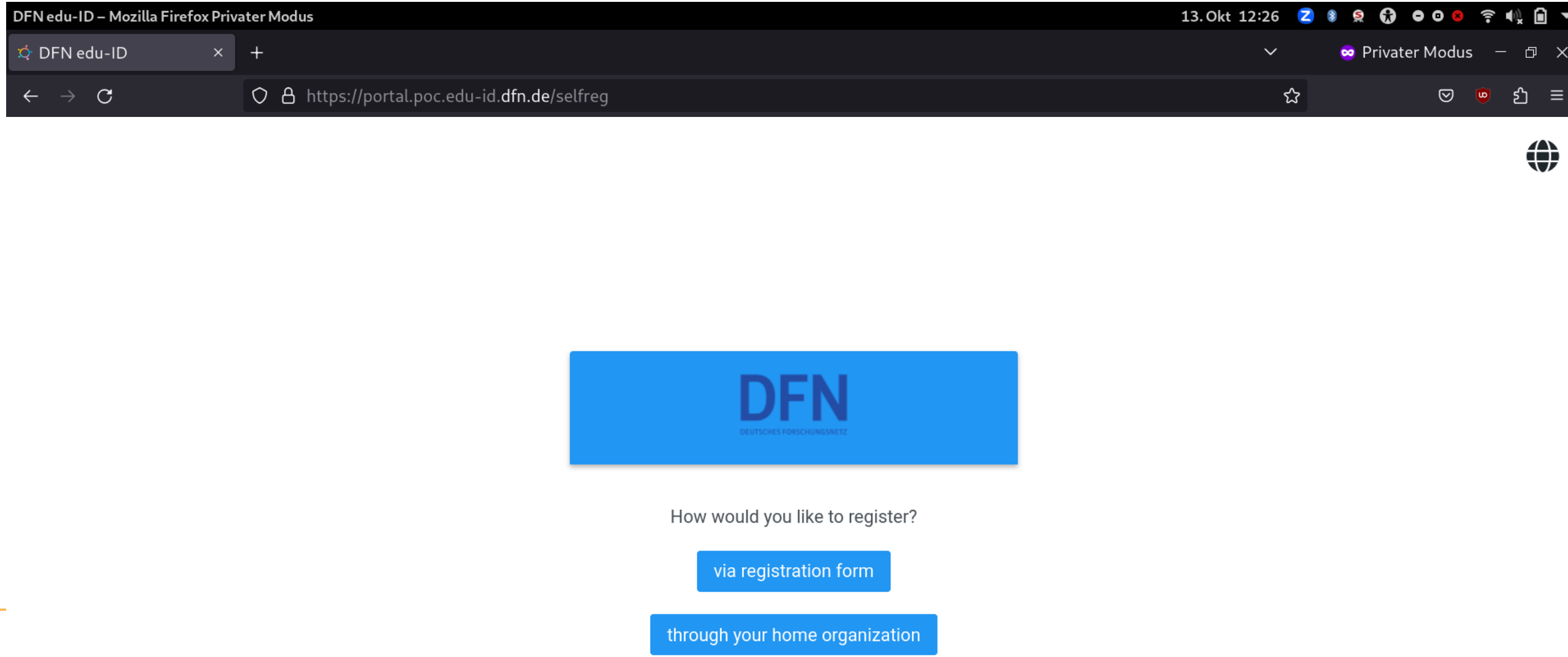
Screenshots PoC

Einstieg für User 1:
Erzeugung einer edu-ID während eines Login an einem teilnehmenden SP



Screenshots PoC

Einstieg für User 2: Unabhängige Erzeugung einer edu-ID



DFN
DEUTSCHES FORSCHUNGSNETZ

Vorname:	Juergen
Name:	Brauckmann
Anzeigename:	Juergen Brauckmann
Benutzername / Primäre E-Mail-Adresse:	
E-Mail-Adresse aus Heimateinrichtung:	brauckmann@dfn-cert.de
Geburtsdatum:	TT . MM . JJJJ
Geburtsort:	
Straße und Hausnummer:	
Ort:	
Land:	Deutschland

Name:	Brauckmann
Anzeigename:	Juergen Brauckmann
Benutzername / Primäre E-Mail-Adresse:	brauckmann@dfn-cert.de
E-Mail-Adresse aus Heimateinrichtung:	brauckmann@dfn-cert.de
Geburtsdatum:	01 . 01 . 1970
Geburtsort:	Pellworm
Straße und Hausnummer:	Moorende 13
Ort:	Pellworm
Land:	Deutschland

☐ Ich habe die Nutzungsbedingungen gelesen und akzeptiert.

☐ Ich habe die DFN edu-ID Datenschutzerklärung gelesen und aktzeptiere diese.

Registrieren

DFN

DEUTSCHES FORSCHUNGSNETZ

Alles in Ordnung Vielen Dank für Ihre Registrierung. Bitte prüfen Sie ihre e-Mails.

DFN
DEUTSCHES FORSCHUNGSNETZ

Neues Passwort

Neues Passwort bestätigen

Passwort festlegen

⊗ Das Passwort muss mindestens 7 Zeichen lang sein.
⊗ Das Passwort muss mindestens einen Kleinbuchstaben enthalten.
⊗ Das Passwort muss mindestens einen Großbuchstaben enthalten.
⊗ Das Passwort muss mindestens eines der folgenden Zeichen enthalten:
^!§$%&/()=?*@#<>|

Zur Anmeldung

DFN

Alles in Ordnung Das Passwort wurde eingerichtet

Zur Anmeldung

DFN edu-ID – Mozilla Firefox Privater Modus

13. Okt 12:18

DFN edu-ID

Privater Modus

https://portal.poc.edu-id.dfn.de/profile

DFN

THEMES | Sprache | Juergen Brauckmann

- Meine Daten
- My Affiliations
- Other Identifiers
- Datenvalidierung über HE
- Passwort ändern
- MFA-Tokens
- Terms of Use
- Verwaltung von Vorauswahlen
- DSGVO-Auskunft
- edu-ID löschen

Benutzerinformationen

Benutzername / Primäre E-Mail-Adresse:	brauckmann@dfn-cert.de
Vorname:	Juergen
Name:	Brauckmann
Anzeigename:	Juergen Brauckmann
E-Mail-Adressen:	brauckmann@dfn-cert.de
Handynummern:	
Geburtsdatum:	01.01.1970
Geburtsort:	Pellworm
Straße und Hausnummer:	Moorende 13
Ort:	Pellworm

Meine Daten
My Affiliations
Other Identifiers
Datenvalidierung über HE
Passwort ändern
MFA-Tokens
Terms of Use
Verwaltung von Vorauswahlen
DSGVO-Auskunft
edu-ID löschen

My Affiliations

+ Add affiliation

DFN-CERT Services GmbH

Löschen

Organization:	DFN-CERT Services GmbH
Affiliation Type:	ho
Aktiv:	true
External ID:	VQPEOYWLXBH6BUE2UBGJZYKGG4X75NTD@dfn-cert.de
Id of IdP:	https://idp-test.dfn-cert.de/idp/shibboleth
Vorname:	Juergen
Name:	Brauckmann
Anzeigename:	Juergen Brauckmann
E-Mail-Adresse:	brauckmann@dfn-cert.de
eduPersonAffiliation:	staff
Home Organization:	dfn-cert.de
eduPersonAssurance:	https://refeds.org/assurance/ID/eppn-unique-reassign-1y
eduPersonEntitlement:	

Meine Daten
My Affiliations
Other Identifiers
Datenvalidierung über HE
Passwort ändern
MFA-Tokens
Terms of Use
Verwaltung von Vorauswahlen
DSGVO-Auskunft
edu-ID löschen

My Other Identifiers

+ Add identifier

orcid

Löschen

Affiliation Type: orcid

External ID: 0000-0002-3806-2210

Meine Daten
My Affiliations
Other Identifiers
Datenvalidierung über HE
Passwort ändern
MFA-Tokens
Terms of Use
Verwaltung von Vorauswahlen
DSGVO-Auskunft
edu-ID löschen

Validate my Data via Home Organization

	Identity	Affiliation	Action
Vorname	Juergen	Juergen	will be verified
Name	Brauckmann	Brauckmann	will be verified
E-Mail-Adresse	brauckmann@dfn-cert.de	brauckmann@dfn-cert.de	

Speichern

Meine Daten
My Affiliations
Other Identifiers
Datenvalidierung über HE
Passwort ändern
MFA-Tokens
Terms of Use
Verwaltung von Vorauswahlen
DSGVO-Auskunft
edu-ID löschen

Terms of Use

Current Terms of Use

Version 0.1 Activated on 14.09.2023

Version 0.1 vom 18.8.2023

Mit der Erstellung oder der Nutzung Ihres DFN edu-ID-Kontos erklären Sie sich mit folgenden Bedingungen einverstanden.

Bitte nehmen Sie sich die Zeit, um diese Nutzungsbedingungen sorgfältig zu lesen bevor Sie den Dienst nutzen. Die aktuell gültige Version der Nutzungsbedingungen für den Dienst DFN edu-ID ist jederzeit unter https://portal.poc.edu-id.dfn.de/tou.html abrufbar.

Kurzüberblick:

- Die DFN edu-ID dient als eine lebenslange digitale Identität für den Bereich Forschung und Bildung, um Sie eindeutig identifizieren zu können und Ihnen langfristigen Zugang zu bestimmten Diensten in der DFN-AAI und daran angeschlossenen Infrastrukturen zu ermöglichen.
- Jede natürliche Person kann für sich selbst ein DFN edu-ID-Konto erstellen.
- Sie dürfen nur ein einziges DFN edu-ID-Konto haben! Sie sind verpflichtet, Duplikate zu vermeiden und zu beseitigen.
- Alle Daten welche Sie bei der Erstellung des Kontos oder bei nachträglichen Änderungen und Ergänzungen angeben, müssen wahrheitsgetreu sein. Nur so kann der Dienst mit einem akzeptablen Qualitätsniveau erbracht werden. Bewusst falsch eingegebene Daten können zur Löschung des Kontos führen.
- Schützen Sie Ihre Zugangsdaten (z.B. Ihr Passwort), denn Sie sind verantwortlich für die Aktivitäten welche im Zusammenhang mit Ihrem DFN edu-ID-Konto ausgeführt werden.
- Ihr DFN edu-ID-Konto gehört Ihnen und bleibt auch dann aktiv, wenn Sie eine Organisation verlassen, die im Rahmen der DFN-AAI an das edu-ID-Portal

Schritte zum Regelbetrieb

Proof of Concept | **Pilotphase** | **Regelbetrieb**

Q 4/2023 | Q 1/2024 | Q 2/2024 | Q 3/2024 | Q 4/2024

- Initiale Use Cases
- User Journeys
- UX-Tests
- Anpassen + nachbessern

- Mit ausgewählten Partnern
- Weitere Use Cases
- Voller Funktionsumfang
- Skalierbarkeit?
- Anpassen + nachbessern

Parallel dazu:

Betriebskonzept, datenschutzrechtliche Bewertung, Nutzungsbedingungen, Supportmodell

Nächste Schritte

- Erste Use Cases aus dem Bibliotheksbereich mit Staatsbibliothek zu Berlin
  - Validierung des technischen Konzepts
  - User Experience – Probanden aus unterschiedlichen Nutzendengruppen
  - FAQs + Dokumentation für unterschiedliche Zielgruppen entwickeln
- TODO:
  - Anbindung BundID: Validierung von Identitäten
    - Hohe LoAs für ‘Homeless Users‘, Support für Onboarding-Szenarien
  - Policies, Verträge
  - Datenschutzrechtliche Bewertung
  - Planung der Pilotphase

Initiale Use Cases (1)

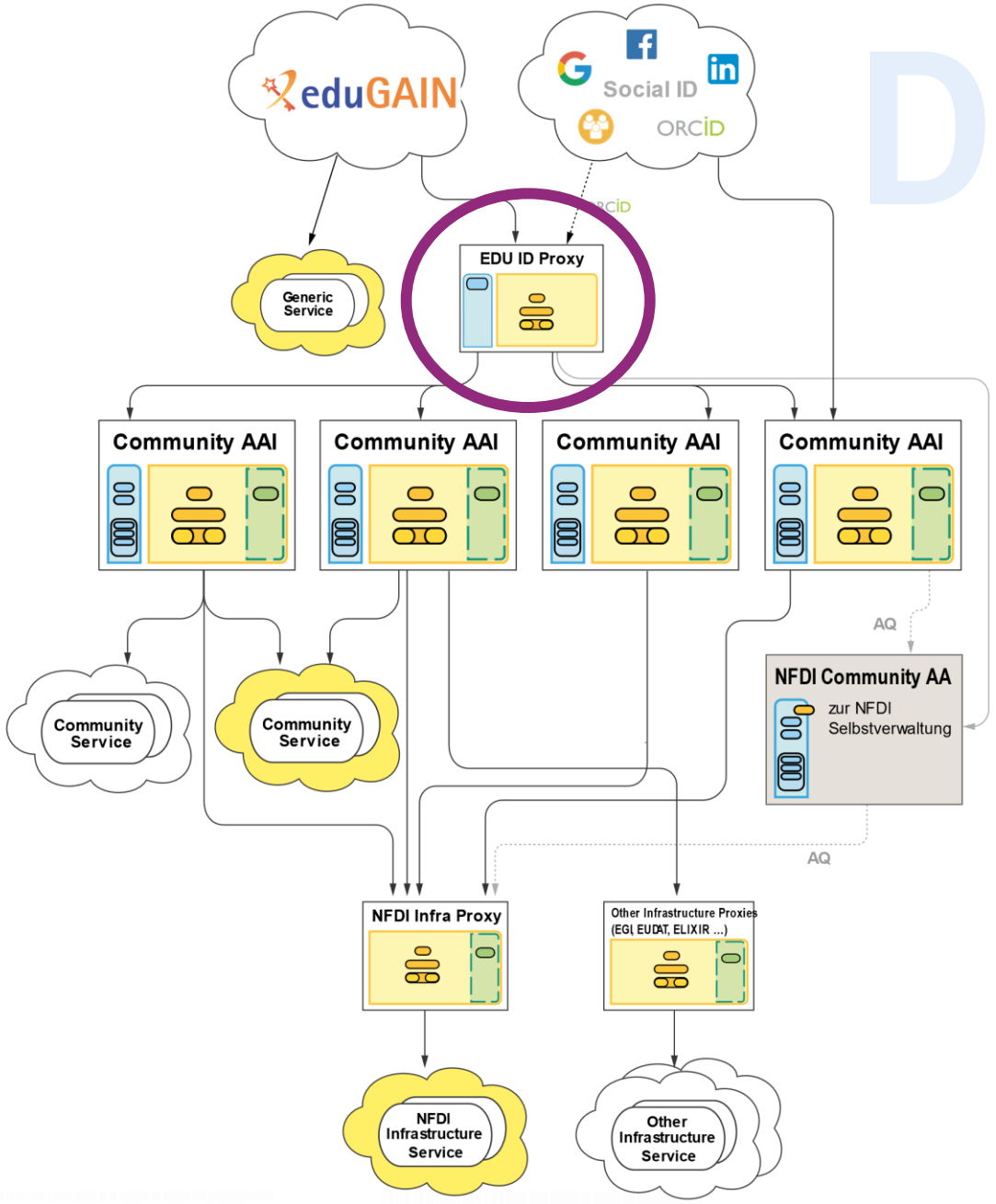
- Geplant: Verwendung der edu-ID für Nationallizenzen, Staatsbibliotheken, Zugriff auf zentrale Ressourcen und „Homeless Users“
  - Use Cases 3.6, 3.7, 3.8 und 3.10 aus https://doku.tid.dfn.de/de:aai:eduid:usecases
- Use Case Nationallizenzen (3.6) zurückgestellt, da Meldeadresse nicht verlässlich verfügbar, hierfür fehlt Anbindung an BundID bzw. eID-Server (unklar, ob alle Heimat-IdPs `schacCountryOfResidence` liefern können)
- Zugriff auf zentrale Ressourcen (3.8): Fachinformationsdienst (FID) Asien, Staatsbibliothek zu Berlin
  - Unter anderem Anwendungsfall User Migration

Initiale Use Cases (2)

- Aufgrund der Proxy-Funktionalität eignet sich das edu-ID-System als Brücke zu anderen Authentifizierungs- und Autorisierungs-Infrastrukturen
- Geplante Kooperationen
  - Schulföderation VIDIS
    Lehramtsstudierende aus der DFN-AAI sollen Zugriff auf ausgewählte Lernplattformen erhalten
    → Prototypische Anbindung für Unis in Mecklenburg-Vorpommern
  - Vernetzungsinfrastruktur Digitale Bildung (a.k.a. Nationale Bildungsplattform)
    Prototypische Schnittstelle DFN-AAI, um Use Cases der universitären Bildung zu ermöglichen
    → Teilnahme an „Closed Beta“

Initiale Use Cases (3)

- 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



Vielen Dank! Haben Sie noch Fragen?

- Kontakt
  - Jürgen Brauckmann

    Teamleiter DFN-PKI
    E-Mail: brauckmann@dfn-cert.de
    Telefon: +49 40 808077-580

    Anschrift:
    DFN-CERT Services GmbH
    Nagelsweg 41
    20097 Hamburg

- Kontakt
  - Wolfgang Pempe

    Teamleiter DFN-AAI
    E-Mail: pempe@dfn.de
    Telefon: +49 30 884299-380

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz 1
    10178 Berlin