deutsches forschungsnetz

# ID-Management im Bildungsbereich

2. Themenfeldkonferenz Bildung | 30. März 2022

Wolfgang Pempe (pempe@dfn.de)

# Überblick

- Föderierte Identitäten in akademischen Föderationen
  - Heimateinrichtungen als Identitätsquelle
- Föderierte Identitäten im Schulbereich, föderales Identitätsmanagement
  - Bundesland als Identitätsquelle
- Konzept edu-ID, Anknüpfungspunkte OZG und SSI
  - Aggregation/Weiterleitung aus unterschiedlichen Identitäts- und Datenquellen

# Grundlagen:

# Föderierte Identitäten, Web-SSO

# Dienstspezifische Identitäten

User Id: `lmuster`
Passwd: ••••••

**Online Shop XY**

User Id: `ludmilla.muster@gmx.de`
Passwd: ••••••

**Datenbankanbieter YZ**

User Id: `lm1970`
Passwd: ••••••

**Verlag WX**

# Föderierte Identität

User Id: `lmuster`
Passwd: ••••••

**Heimateinrichtung**

**Online Shop XY**

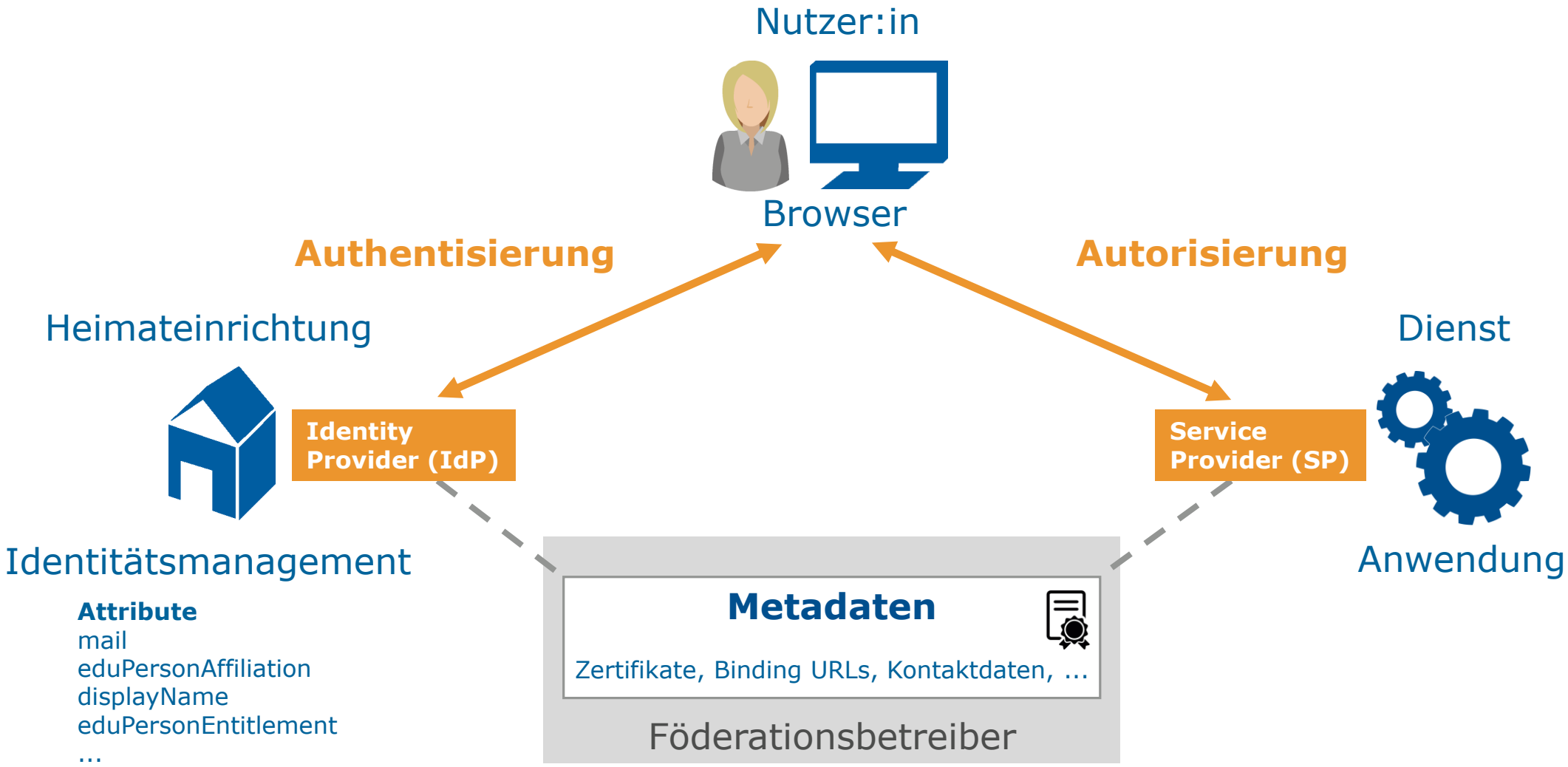
**Datenbankanbieter YZ**

**Verlag WX**

# Begriffsbestimmung

- AAI = **A**uthentication and **A**uthorization **I**nfrastructure
  - Bildet den technischen und organisatorischen Rahmen für föderiertes Identitätsmanagement
- Föderiertes Identitätsmanagement
  - Austausch von Identitätsdaten über Dienst- und Organisationsgrenzen hinweg
  - Vermeidung von dienstspezifischen Identitäten und Username/Password
  - erfordert eine Identitätsquelle als führendes System
- AAI ermöglicht **S**ingle **S**ign-**O**n (SSO)
  - einmal anmelden für mehrere Dienste, für die man zugriffsberechtigt ist
  - üblicherweise auf Web-Anwendungen beschränkt, Erweiterungen jedoch möglich

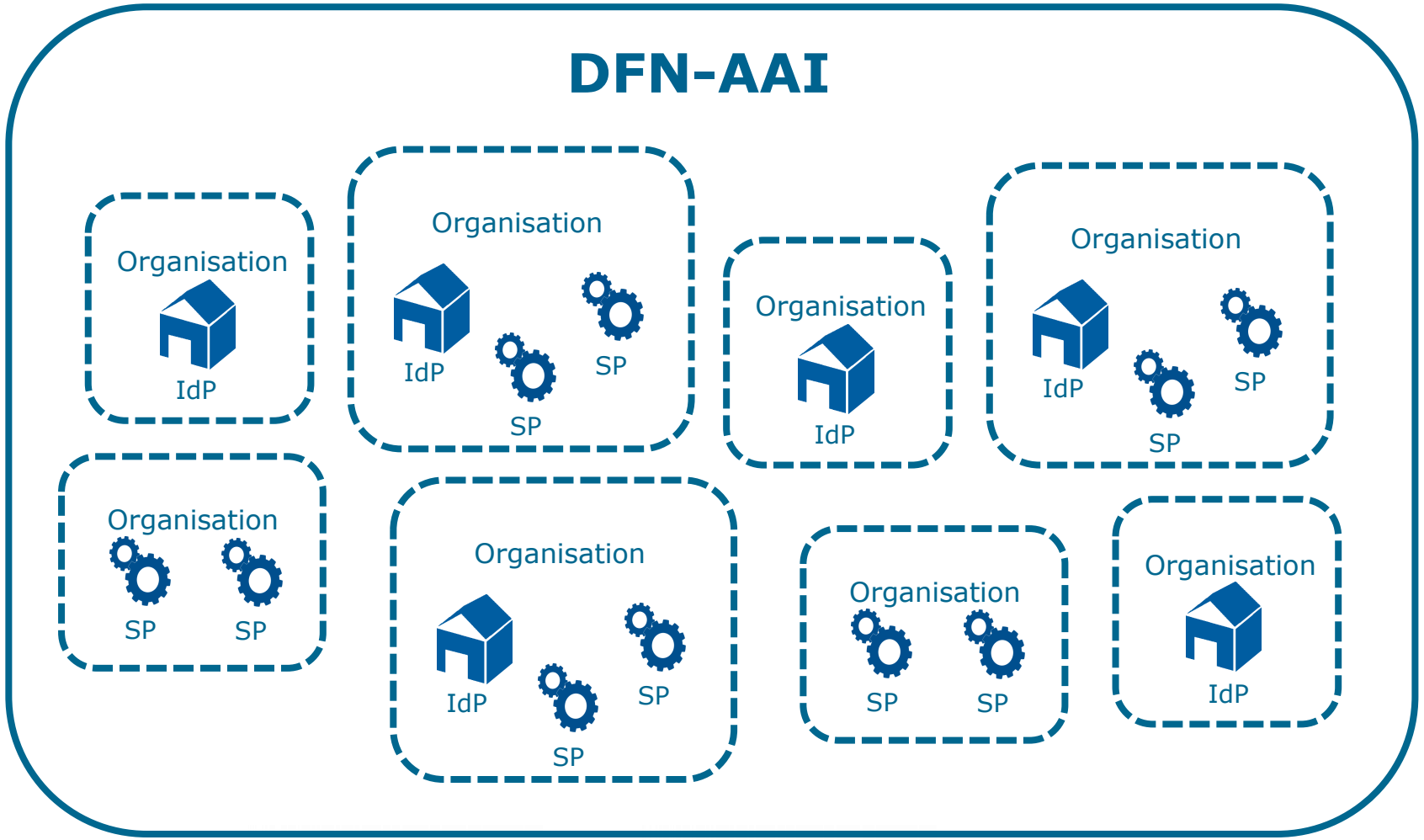
# Wie funktioniert eine Föderation?



# Beispiel DFN-AAI

- **Föderationsbetreiber**
  DFN-Verein
- **Vertrauen**
  Verträge mit allen Teilnehmern, Policies, Levels of Assurance
- **Technik**
  Metadatenverwaltung und –Signierung

Aktuell ca. 360 teilnehmende Einrichtungen und 700 Dienste (zzgl. ~1300 lokale SP)



DFN

# Föderales Identitätsmanagement:

# VIDIS

# Das edu-ID Konzept

# Föderierte Identität …

User Id: `lmuster`
Passwd: ••••••

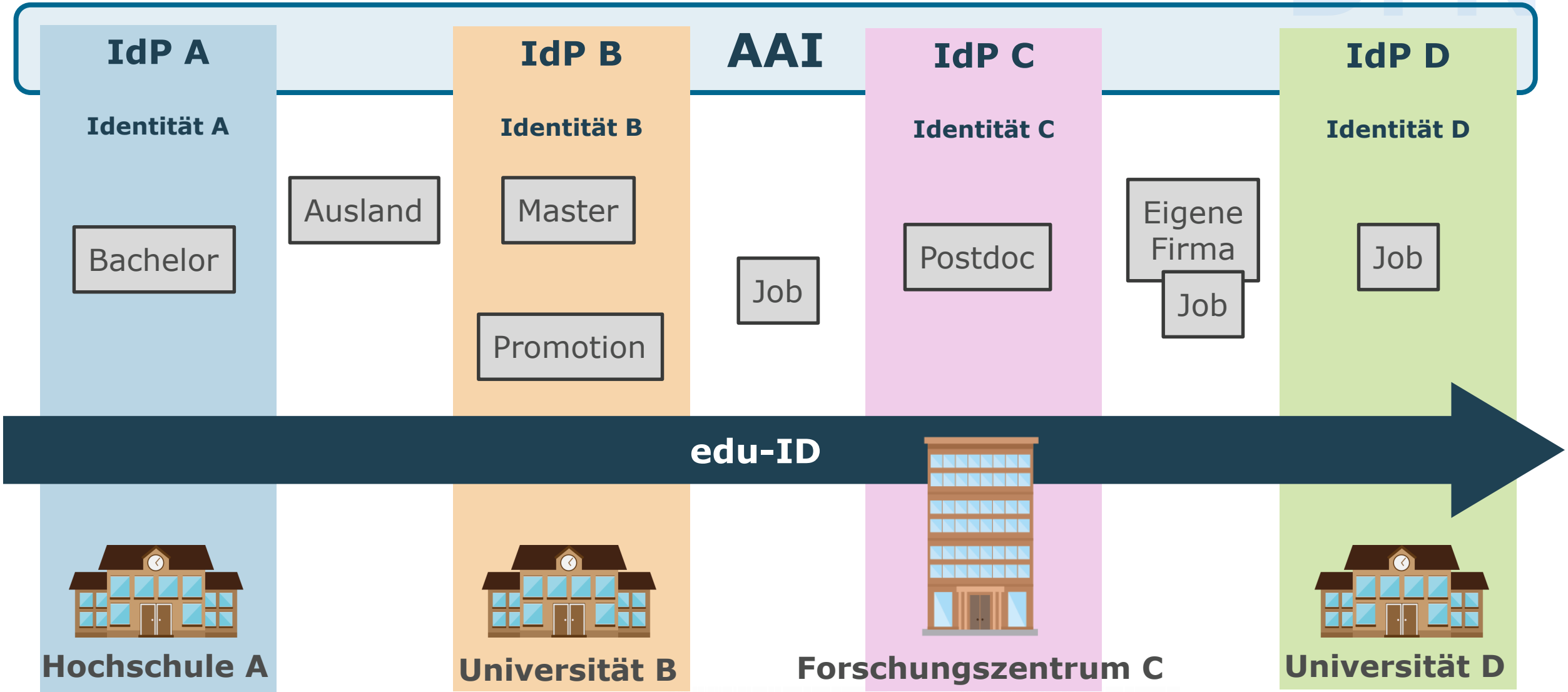
**Universität Musterstadt**

**Online Shop XY**

**Datenbankanbieter YZ**

**Verlag WX**

# … immer wieder neu?



# 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

# 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

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

# edu-ID Use Cases

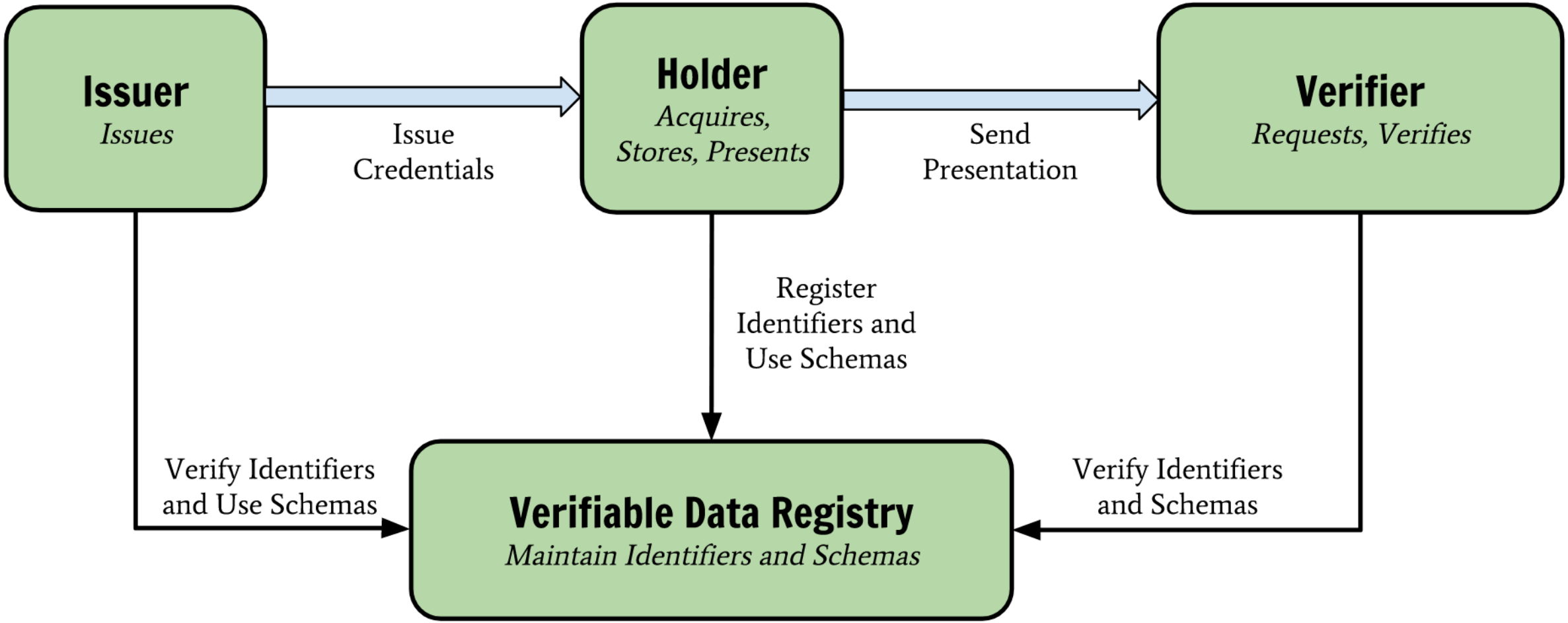
- https://doku.tid.dfn.de/de:aai:eduid:usecases
- Vier Bereiche:
  - UC 1 Student Life Cycle
  - UC 2 Lehre
  - UC 3 Forschung
  - UC 4 Verwaltung
- Use Cases u.a. als Basis für
  - Definition der als essentiell bewerteten Attribute („Kernattribute“)
  - Anforderungen an Verlässlichkeit der Nutzerdaten/Attribute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

# Bezug zum OZG – Gedankenspiele

- Insbes. die Use Cases zum Student Life Cycle (UC 1.x) korrespondieren mit im OZG-Umsetzungskatalog aufgeführten Leistungen zur Lebenslage Studium
- OZG § 3, Abs. 2: Zugriff auf Leistungen über Servicekonto Bund/Land
- Schnittstelle(n) Servicekonten – edu-ID Accounts?
  - Relevant für 7 von 24 Use Cases
  - Würde Nutzbarkeit der Servicekonten indirekt auf weitere edu-ID Use Cases erweitern
  - Voraussetzung(?): Einstufung edu-ID in Vertrauensniveau „substantiell" durch BSI – ist nur unter hohem Aufwand zu erreichen
  - Bringt direkte Interaktion mit Servicekonto echten Mehrwert gegenüber eID-Schnittstelle zum edu-ID System via Ausweis App / Kartenleser und eID-Server?

# Themenfeld OZG und SSI

# SSI – Prinzip der Verifiable Credentials




Quelle: https://www.w3.org/TR/vc-data-model/

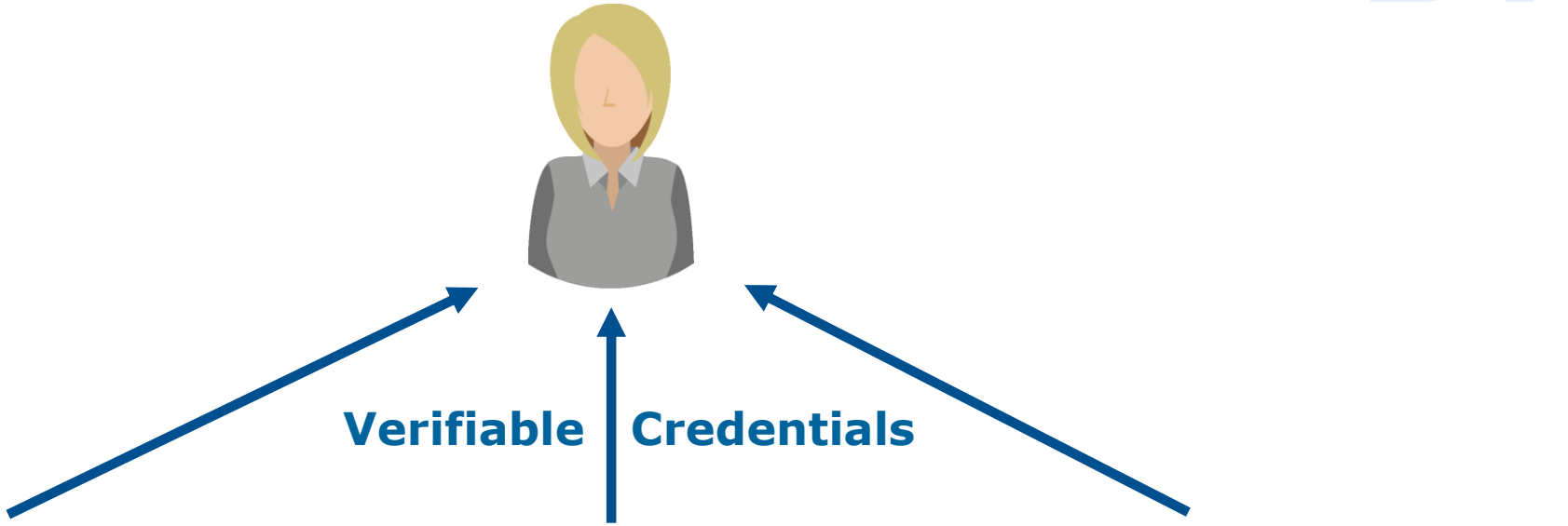
# OZG und SSI

- Self-Sovereign Identity (SSI) wird von EU, Politik und Privatwirtschaft massiv gefördert („eIDAS 2.0“)

  → Wallet als Container für Identitätsdaten und Nachweise

- Anwendbarkeit auf OZG-Use Cases?
  - Konkrete Möglichkeit, das Once-only Prinzip umzusetzen
  - … bzw. Reifegrad Stufe 4 seitens Servicekonten (Föderierung) obsolet zu machen
- Abruf von Leistungs- und sonstigen Nachweisen
  - Irgendwie muss ein Nachweis auch in ein Wallet gelangen…
  - Eine lebenslang gültige, global eindeutige ID könnte hilfreich sein – bPK? edu-ID?

# ~~Dienst~~Issuer-spezifische Identitäten?




User Id: `lmuster`
Passwd: ••••••

User Id: `ludmilla.muster@gmx.de`
Passwd: ••••••

User Id: `lm1970`
Passwd: ••••••

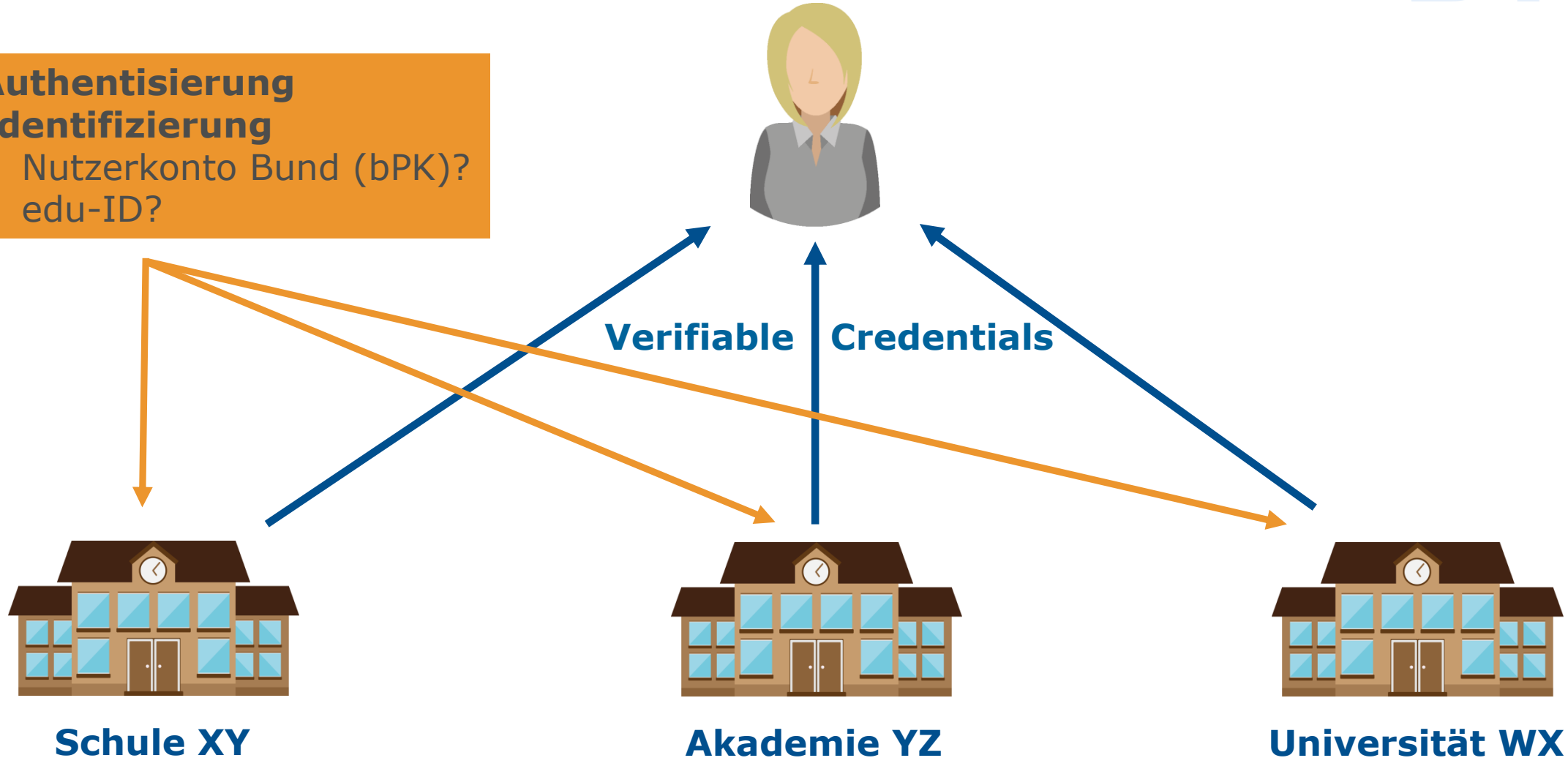
**Schule XY**

**Akademie YZ**

**Universität WX**

# ~~Dienst~~Issuer-spezifische Identitäten?

**Authentisierung**
**Identifizierung**
- Nutzerkonto Bund (bPK)?
- edu-ID?



# Vielen Dank! Fragen? Kommentare?

- Kontakt
  - Wolfgang Pempe, Leiter DFN-AAI

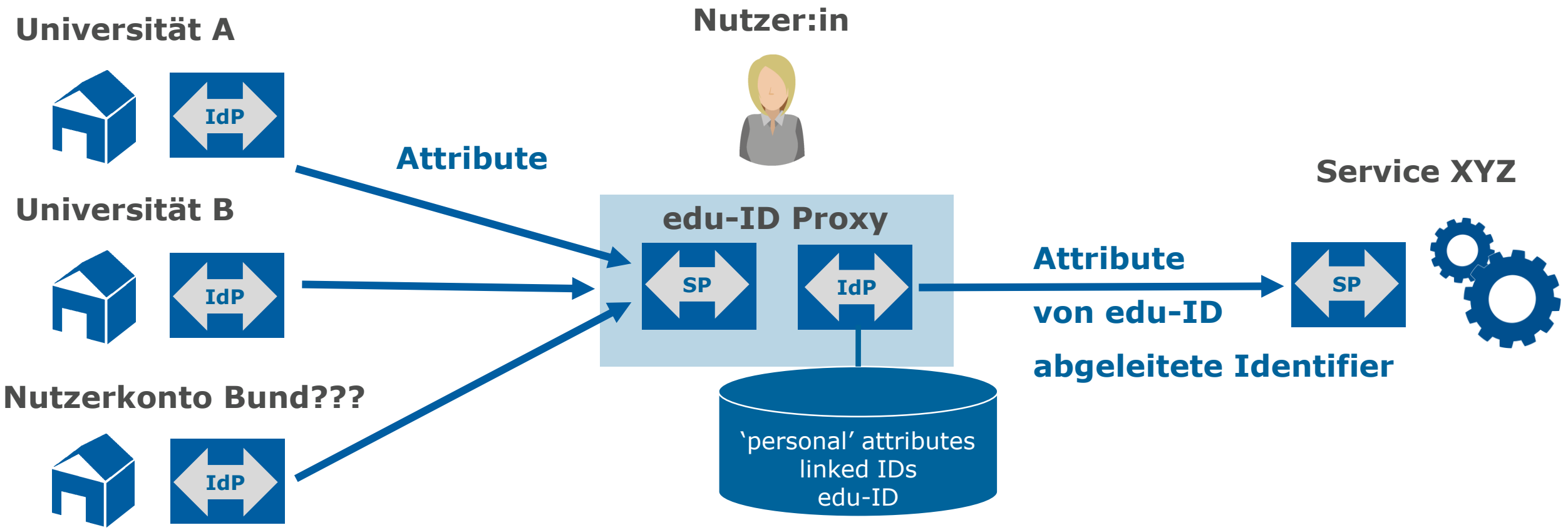
E-Mail: pempe@dfn.de
Tel.: +49-30-884299-308
Fax: +49-30-884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz 1
D-10178 Berlin

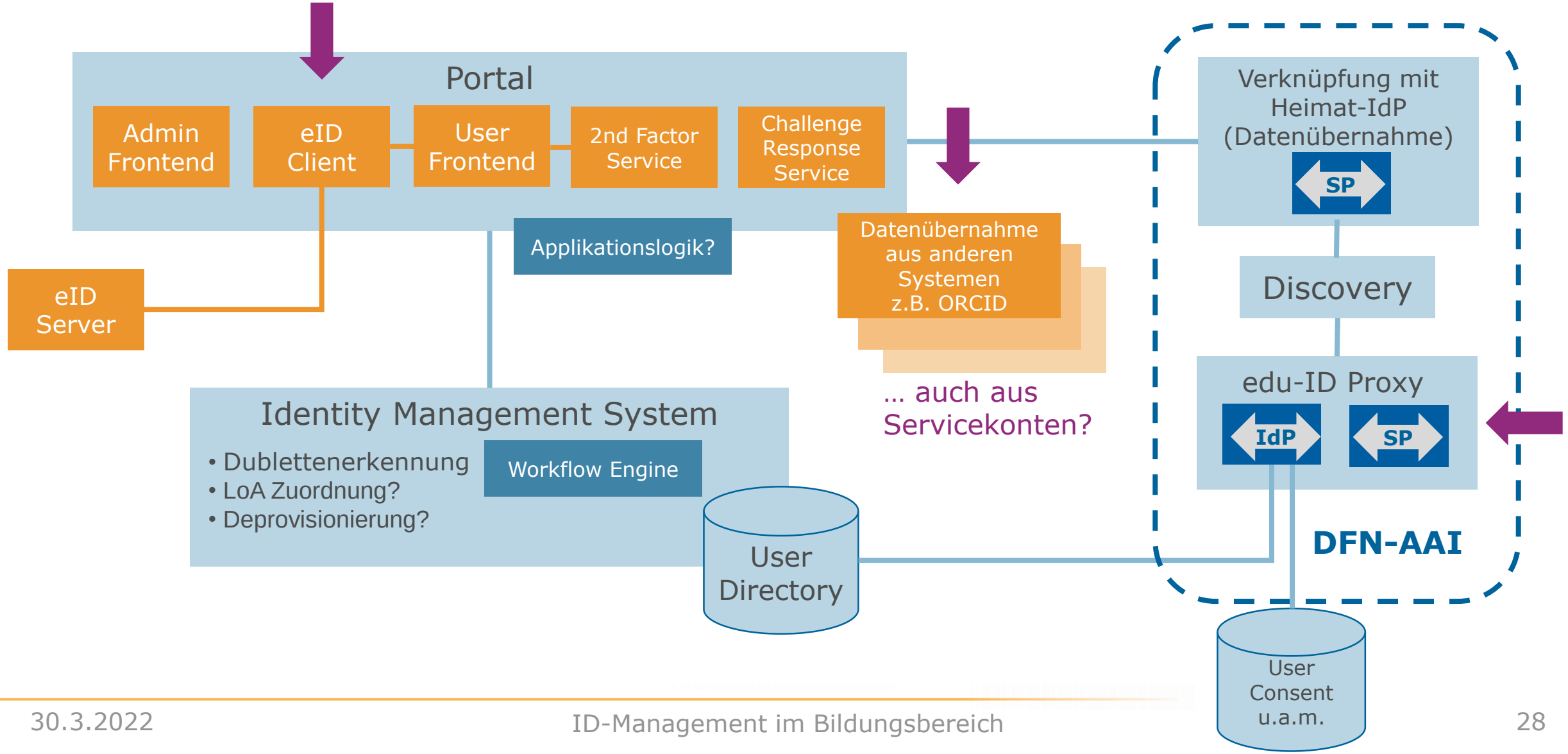
# Backup-Folien

# edu-ID System als Proxy

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



# Technische Komponenten edu-ID System



# edu-ID Use Cases (1)

- UC 1 Student Lifecycle
  - ~~UC 1.1 Studienplatzbewerbung (Onboarding)~~
  - ~~UC 1.2 Immatrikulation (Onboarding)~~
  - ~~UC 1.3 Abschlussarbeit / Staatsexamen~~ (Zuordnung Leistungsnachweise)
  - ~~UC 1.4 Referendariat (Zugriff auf Ressourcen)~~
  - ~~UC 1.5 (Bewerbung) Promotion (Onboarding)~~
  - ~~UC 1.6 Hochschul-Externe (Onboarding)~~
- UC 2 Lehre
  - UC 2.1 Nutzung von Lernmanagementsystemen (Zugriff auf Ressourcen)
  - UC 2.2 Temporäre Konten für Mitarbeitende anderer Institutionen (Onboarding etc.)
  - UC 2.4 Hochschulübergreifende Weiterbildungsveranstaltungen (Onboarding etc.)
  - UC 2.5 Lehrerbildung (Onboarding etc.)

# edu-ID Use Cases (2)

- UC 3 Forschung
  - UC 3.1 Zugang zu Publikationsservern (Zugriff auf Ressourcen)
  - UC 3.2 Forschungsdatenmanagement und Verknüpfung von Identitäten und Publikationen (Zugriff auf Ressourcen, Account-Linking)
  - UC 3.3 Verbindung zu anderen Identifikatoren / Ids (Account-Linking)
  - UC 3.4 Kollaborative Dokumenterstellung (Zugriff auf Ressourcen)
  - UC 3.5 Researcher Mobility (Onboarding)
  - UC 3.6 Zugriff auf Nationallizenzen (Zugriff auf Ressourcen)
  - UC 3.7 Services von nationalen Bibliotheken / Informationseinrichtungen (Zugriff auf Ressourcen, Gast-Identitäten)
  - UC 3.8 Zugriff auf zentrale Ressourcen
  - UC 3.9 Management virtueller Organisationen (Zugriff auf Ressourcen, Gast-Identitäten)
  - UC 3.10 Homeless Nutzer*innen (Gast-Identitäten)

# edu-ID Use Cases (3)

- UC 4 Verwaltung
  - UC 4.1 Mitgliedschaften in universitären Gremien (Onboarding)
  - UC 4.2 Personalgewinnung (Onboarding)
  - ~~UC 4.3 Bewerbungen auf Studiengänge → UC 1.1 und 1.2~~
  - UC 4.4 Unterstützung der Dublettenerkennung