deutsches forschungsnetz

# Aktueller Stand edu-ID Konzept

73. DFN-Betriebstagung | 15. September 2020

Wolfgang Pempe (pempe@dfn.de)

# Föderierte Identität …

User Id: `lmuster`
Passwd: ••••••

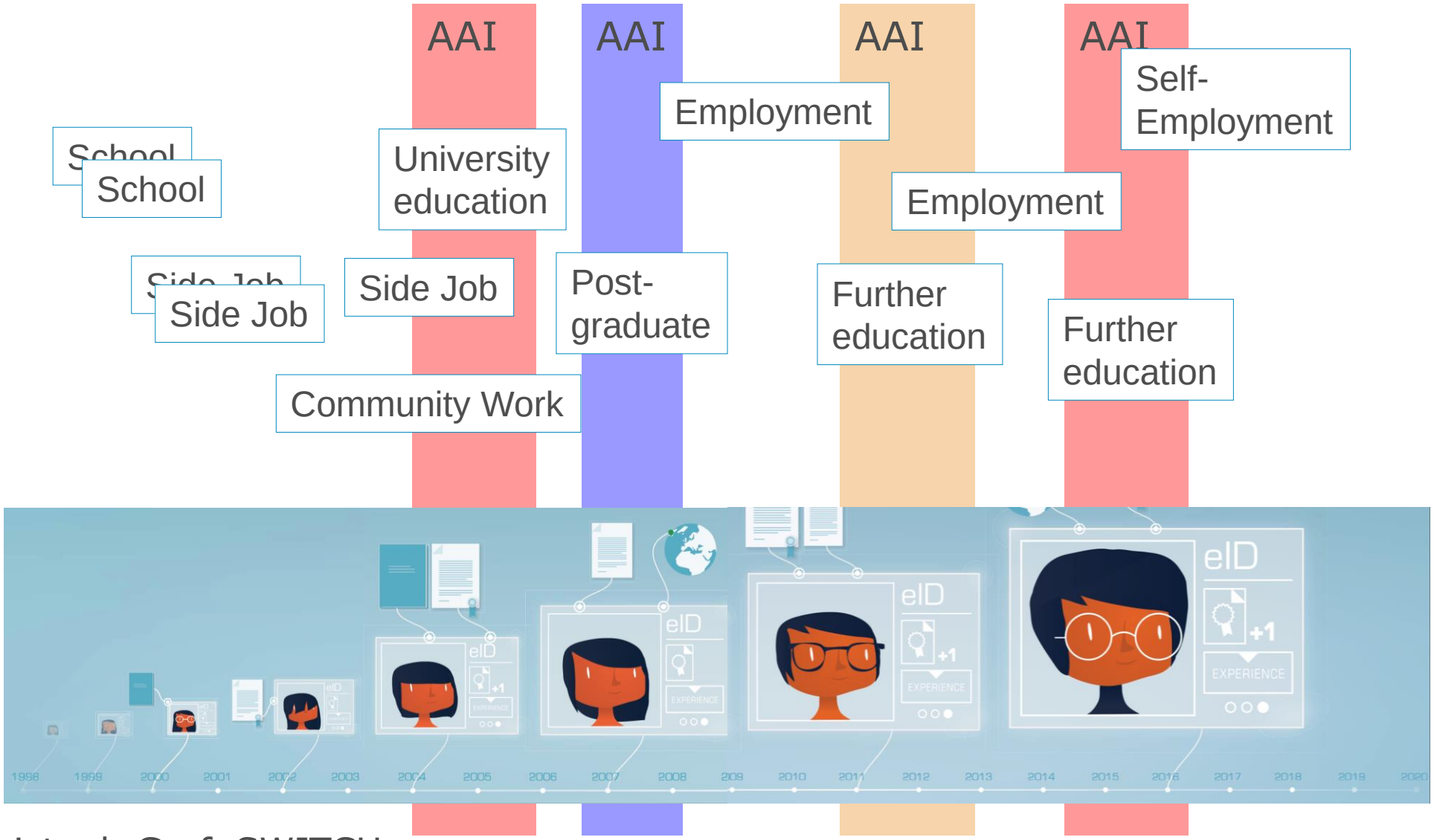
**Universität Musterstadt**

**Online Shop XY**

**Datenbankanbieter YZ**

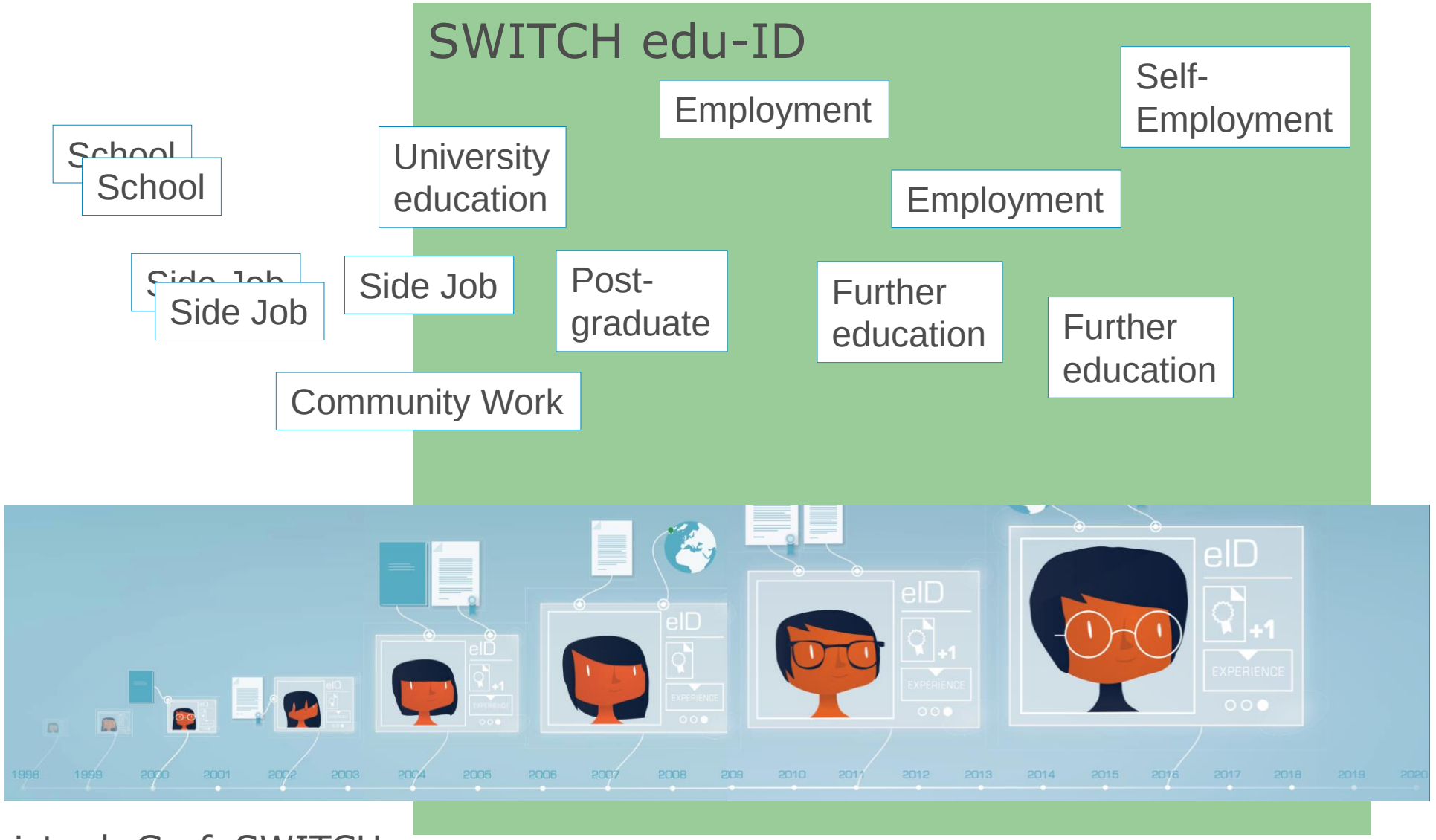
**Verlag WX**

# … immer wieder neu …




**Quelle:** Christoph Graf, SWITCH

# edu-ID als lebenslange akademische Identität

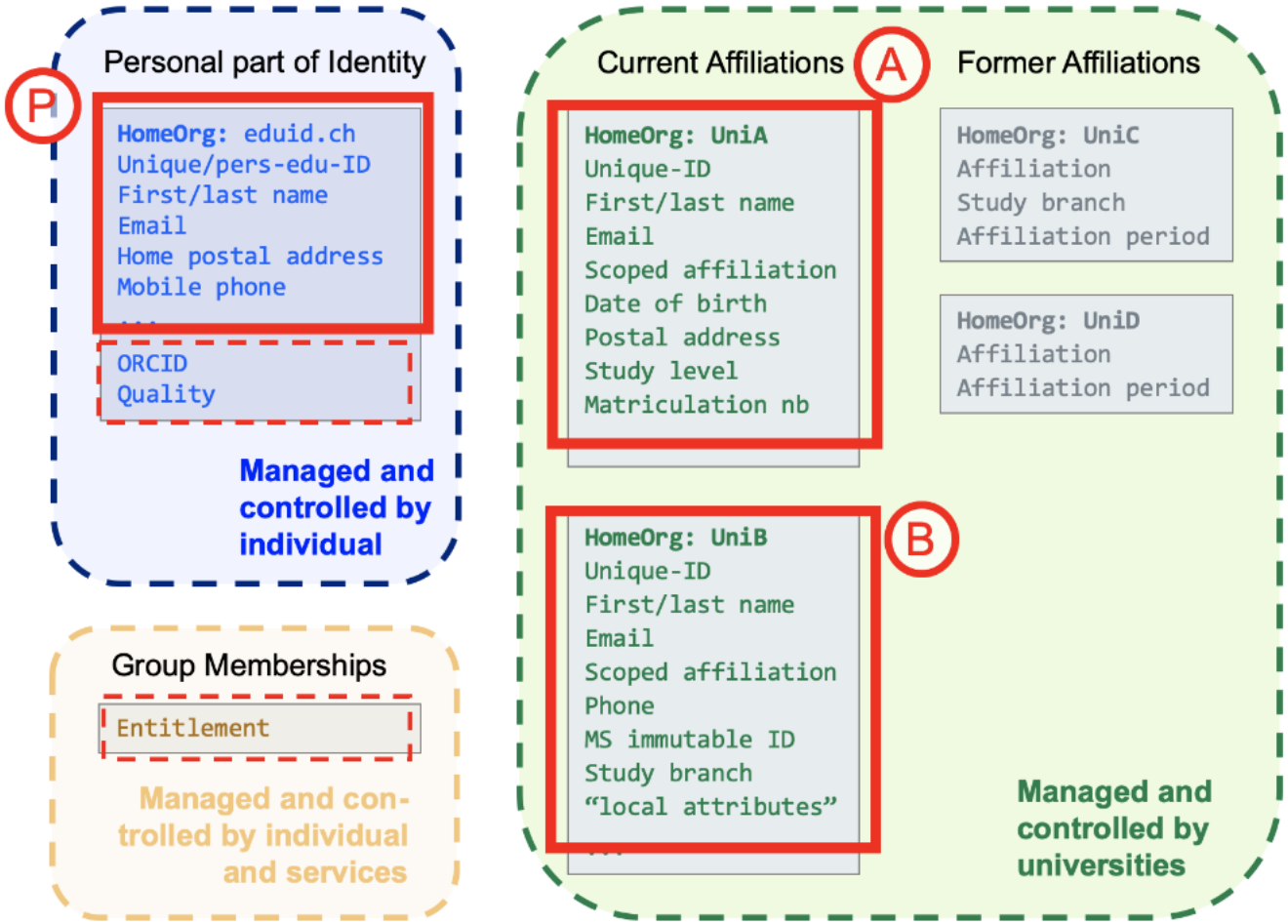



**Quelle:** Christoph Graf, SWITCH

# edu-ID: User-centric Identity

- Identität unabhängig von der jeweiligen Heimateinrichtung
- Selbstregistrierung, Bereitstellung der Nutzerdaten (Validierung ggf. separat)
- Lebenslang gültig
- Aktive Kontrolle über
  - Übertragung von Daten an Dienste (Attributfreigabe)
  - Verknüpfung mit anderen Accounts/Identitäten
  - Aktualisierung, Löschung
- Daten werden ggf. angereichert durch Attribute und Identitäten aus anderen Quellen, insbesondere den Heimateinrichtungen

# Datenmodell (SWITCH edu-ID)




Quelle: https://www.switch.ch/edu-id/services/attributes/classic-model/

# ZKI Arbeitsgruppe

- ZKI Arbeitsgruppe (seit März 2019)
  - an der sich Angehörige von Hochschulen, Bibliotheken sowie Forschungseinrichtungen und -Communities beteiligen
  - 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 SWITCHaai (fortlaufend)
- Aktueller Stand der Arbeiten im Wiki:
  https://doku.tid.dfn.de/de:aai:eduid:start

# Warum eine edu-ID? Zentrale Use Cases

1. Vereinheitlichung und Vereinfachung der Verfahren bei Onboarding-Prozessen, z.B. Registrierung, Einstellung, Online-Immatrikulation (↔ OZG Umsetzung?)
   - Verlässliche digitale Identität bereits vorhanden
2. Langlebige digitale ID, die nicht an eine Organisationseinheit gebunden ist
   - Unterbrechungsfreie Nutzung von Diensten, deren Nutzungsberechtigung nicht an die aktuelle Zugehörigkeit zu einer bestimmten Einrichtung geknüpft ist (Speicherdienste, Nationallizenzen, Leistungsnachweise, …)
   - Account-Linking, Verknüpfung mit anderen Identitäten, z.B. ORCID
   - Erleichterungen beim Management virtueller Organisationen durch Forschungsprojekte und –Infrastrukturen (Rechte, Rollen, Gruppenmitgliedschaften)
3. Zentraler Identity Provider
   - Gast-IdPs für sog. Homeless Users und Citizen Scientists werden obsolet

# edu-ID Systeme international

- SWITCH edu-ID

  (Nationallizenzen → Speicherdienste → Bibliothekslattformen…)

- eduid.se – SUNET

  (Onboarding)

- eduID.nl – SURF

  (Roadmap: Leistungsnachweise → Student Mobility → …)

- Schrittweise Einführung bestimmter Features als Modell für die (DFN) edu-ID?

# Architektur

- Hybrid-Modell (edu-ID IdP und Heimat-IdPs nebeneinander)
- edu-ID System erfüllt mehrere Rollen:
  - IdP: für Homeless Users, insbesondere in Onboarding-Szenarien
  - Proxy-SP: Heimat-IdP als Authentifizierungsquelle → eine User Session (SSO) (Use Case „Wiedererkennen“, Unterbrechungsfreie Nutzung von Diensten)
  - Attribut- und Identitäts-Aggregator (hier noch offene Punkte)
- Von edu-ID abgeleitete Identifier:
  - (targeted) pairwise-id, fallweise auch (unique) subject-id
  - Werden vom edu-ID System generiert
- https://doku.tid.dfn.de/de:aai:eduid:architektur

# Themen für die weitere Arbeit

- Levels of Assurance spezifizieren (kontrolliertes Vokabular, Profile?)
- Welche Identifier-Systeme sollten mit einem edu-ID Account verknüpft werden können? (ORCID etc.)
- Deprovisionierung
- Dubletten-Erkennung, Vermeiden von Mehrfachanmeldungen
- Registrierung eines zweiten Faktors
- Technische Umsetzung, Identity-Management-System für edu-ID Dienst
- Rechtliche Fragen, Datenschutz, Betriebs- und Kostenmodell
- u.a.m.

# Vielen Dank! Fragen? Kommentare?

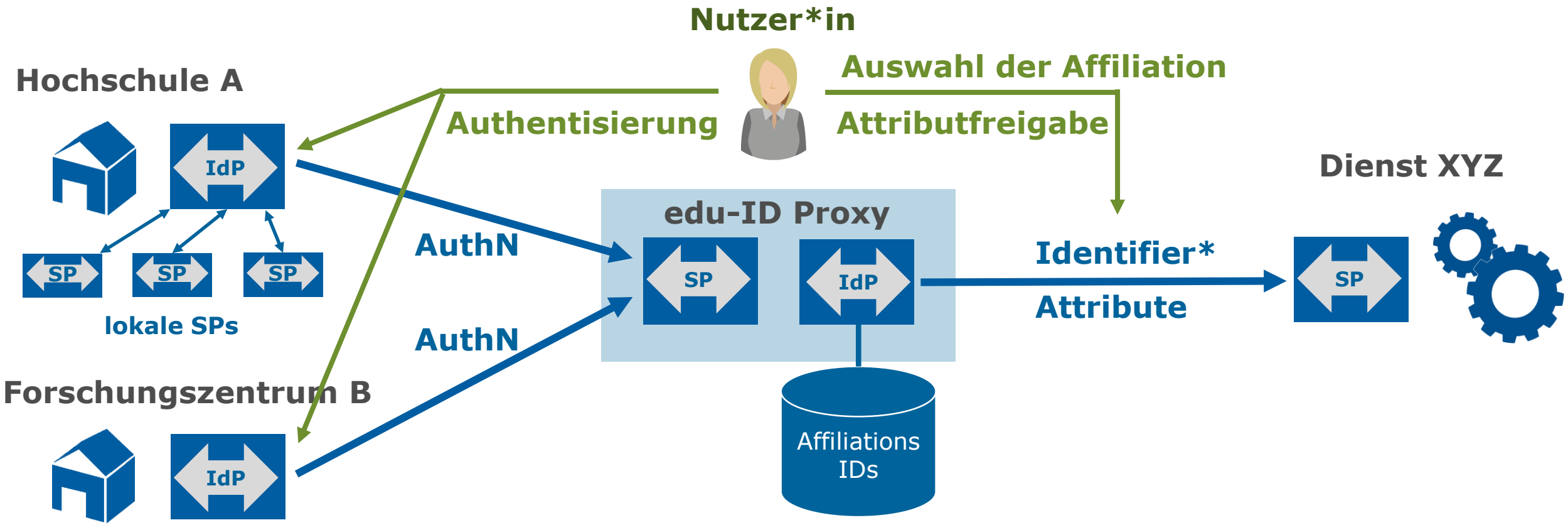
- Kontakt
  - Wolfgang Pempe

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

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

# edu-ID-System als Proxy

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




* abgeleitet von edu-ID