deutsches forschungsnetz

edu-ID – aktueller Stand und nächste Schritte

ZKI Arbeitsgruppe edu-ID | Uni Bamberg, 26.-28. Nov. 2019

Wolfgang Pempe (pempe@dfn.de)

Föderierte Identität …

User Id: `lmuster`
Passwd: ••••••

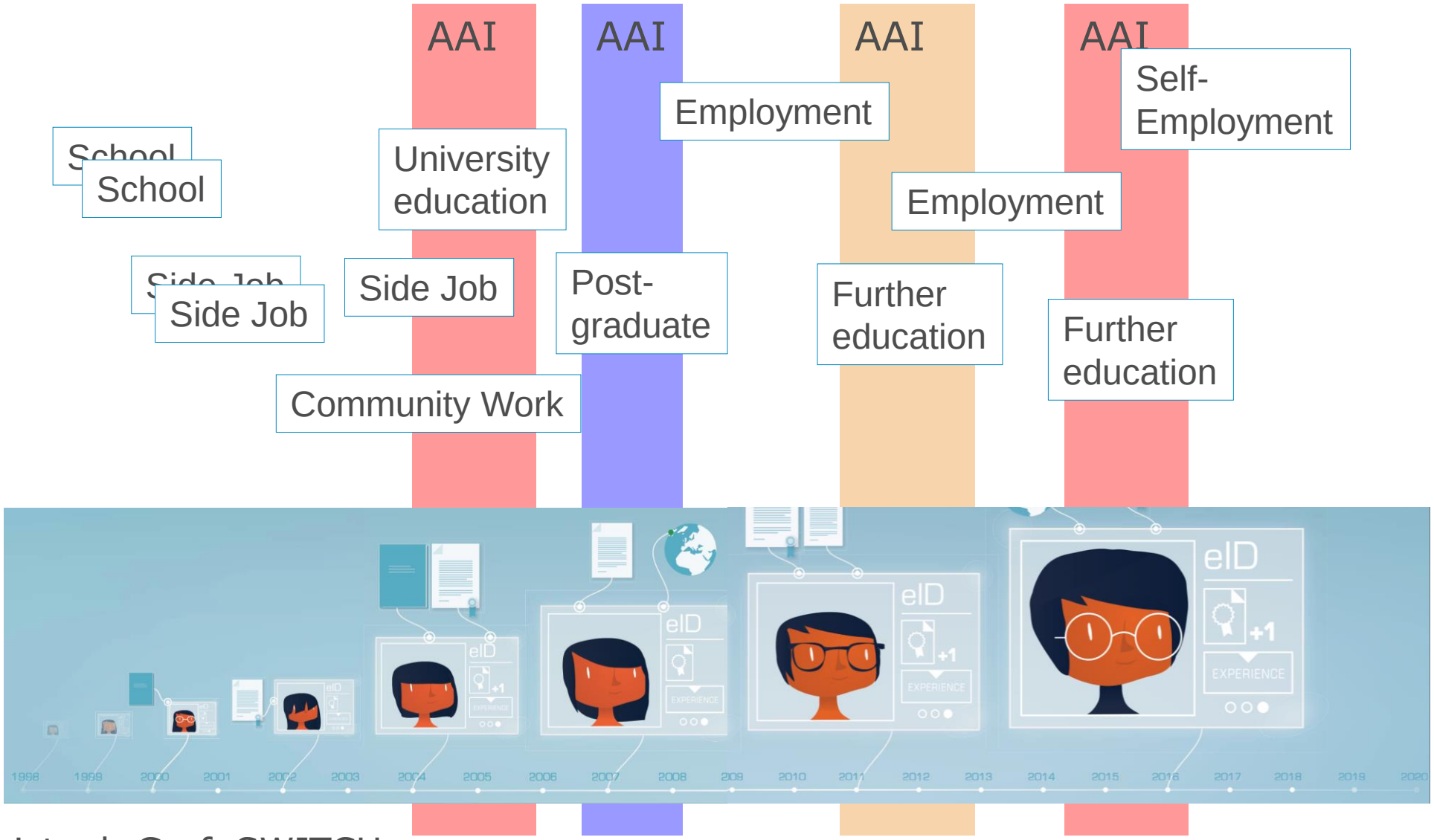
Universität Musterstadt

Online Shop XY

Datenbankanbieter YZ

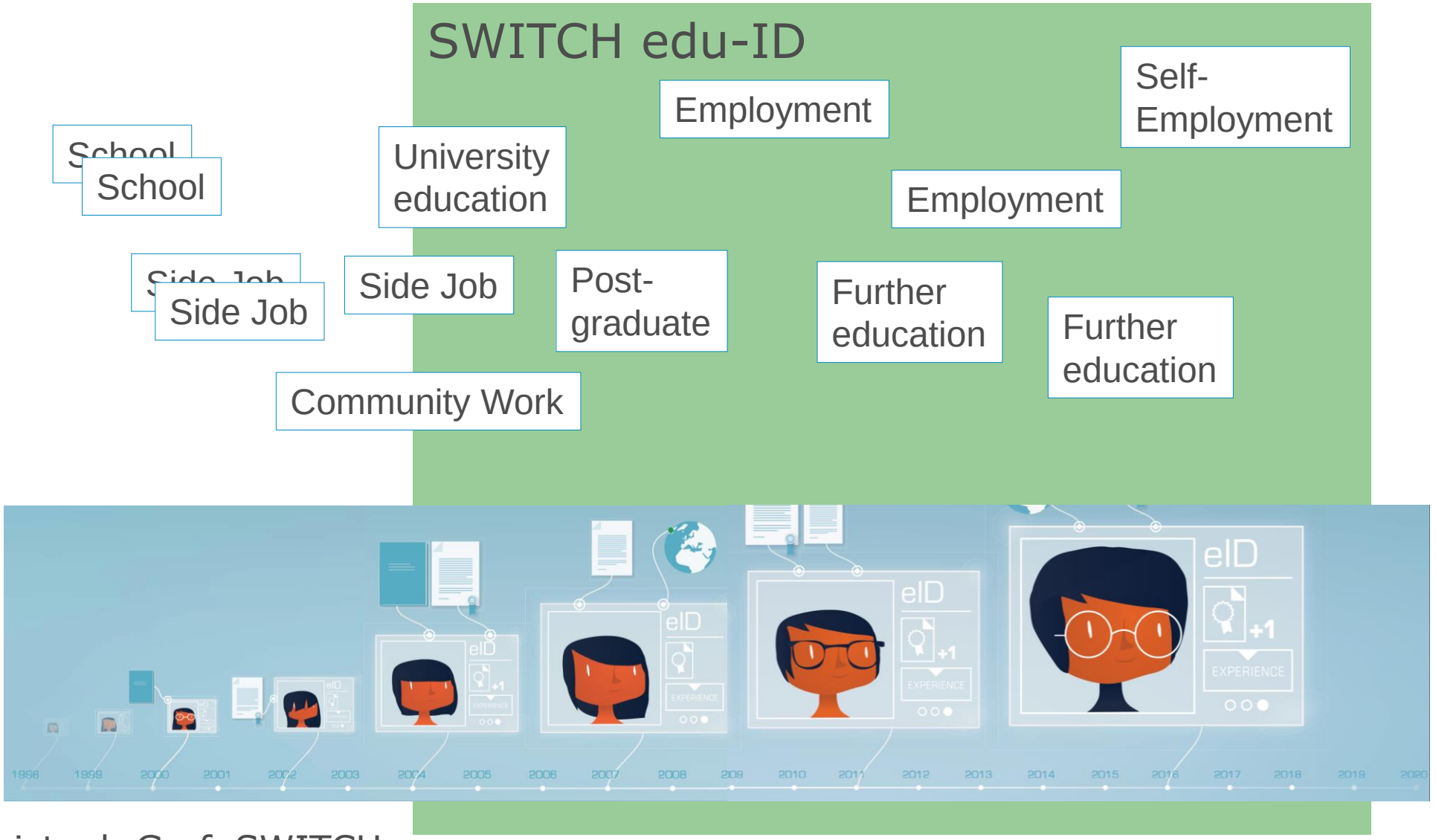
Verlag WX

… immer wieder neu …



Quelle: Christoph Graf, SWITCH

edu-ID als lebenslange akademische Identität



Quelle: Christoph Graf, SWITCH

Was ist eine edu-ID?

- Eine lebenslange, „user-centric“ digitale Identität für Forschung und Bildung
  - Account wird von Nutzer*in selbst eingerichtet
  - Nutzer*in ist für Pflege der Kernattribute verantwortlich
  - Weitergabe von Attributen ist unter der alleinigen Kontrolle der Nutzer*innen (edu-ID IdP)
- Unabhängig von der jeweiligen Heimateinrichtung
- Unterschiedliche Ausprägungen in verschiedenen Föderationen
  - SUNET eduID.se (Schweden): primär für Immatrikulation
  - SWITCH edu-ID (Schweiz): Zentrale digitale Identität für den akademischen Sektor, Umbau des Föderationsmodells: *ein* zentraler edu-ID IdP

edu-ID: User-centric Identity

- Selbstregistrierung, Bereitstellung der Nutzerdaten (Validierung erfolgt ggf. separat)
  - E-Mail-Adresse(n), ggf. Mobilfunknummer
  - Vor- und Zuname, Anschrift
  - Geburtsdatum
- Kontrolle der Weitergabe der Daten (Attributfreigabe)
- Aktualisierung, Löschung
- **Daten werden ggf. angereichert durch Attribute aus anderen Quellen, insbes. den IDMs der jeweiligen Heimateinrichtungen**

ZKI-Arbeitsgruppe edu-ID

- **Workshop zur Anforderungsanalyse an einen edu-ID Dienst, Berlin, 2./3. Juli**
- 23 Teilnehmende (Hochschulen, Bibliotheken, KIT, DFN-CERT, ACOnet, [SWITCH])
- Use Cases aus den Bereichen: Studium+Lehre, Forschung, Verwaltung, Sonstige anhand einiger Leitfragen
- Aus den Use Cases werden Anforderungen an einen edu-ID Dienst abgeleitet (läuft):
  - technisch
  - organisatorisch (Prozesse, Rollen, …)
  - juristisch (Datenschutz, Policies, Verträge)

Ergebnisse des Juli-Workshops (1)

- https://doku.tid.dfn.de/de:aai:eduid:eduid_intern:zusammenfassung_ws_juli2019
- „Wiedererkennen“ von Usern (Forschende, Studierende, Lehrbeauftragte,…)
  - Onboarding (insbes. Immatrikulationsprozesse), Offboarding, temp. Accounts
  - Unterbrechungsfreier Zugriff auf Ressourcen (z.B. Forschungsdaten)
  - Kooperationen
- Account Linking, Aggregation von Attributen aus unterschiedlichen Datenquellen
  - (Student) Mobility
  - Virtuelle Organisationen, Forschungsinfrastrukturen,
  - Container für einrichtungsunabhängige Attribute und IDs, z.B. ORCID
- Lokale (ggf. kurzlebige) Accounts sowie Gast-IdPs werden in vielen Fällen obsolet

Ergebnisse des Juli-Workshops (2)

- Zentraler IdP ermöglicht Proxy-Szenarien: Vermeidung von Tenant-SPs, erfordert aber zentrales Lizenzmanagement
- Anforderungen an Datenqualität/Verlässlichkeit
  - Information für SPs, welches Attribut wie verifiziert wurde bzw. welcher Verlässlichkeitsklasse (LoA) es entspricht
  - Dubletten-Erkennung und –Zusammenführung
  - Deprovisionierung
- Schwerpunkt des Identitätsmanagement an den Heimateinrichtungen verlagert sich in Richtung Rechte- und Rollen-Management(?)
  - Onboarding bereits existierender Identitäten
  - Zuordnung zu Gruppen und/oder Rollen

Workshop-Themen (1)

- Wiki: https://doku.tid.dfn.de/de:aai:eduid:eduid_intern:start
  (dort auch Pad verlinkt)
- Bericht von der MyAcademicID Conference
- Neue Use Cases?
  - Seitens der „neuen“ Teilnehmenden?
  - Feedback aus dem AK IT der Leibniz-Gemeinschaft (Wolfgang)
  - Sonstige?

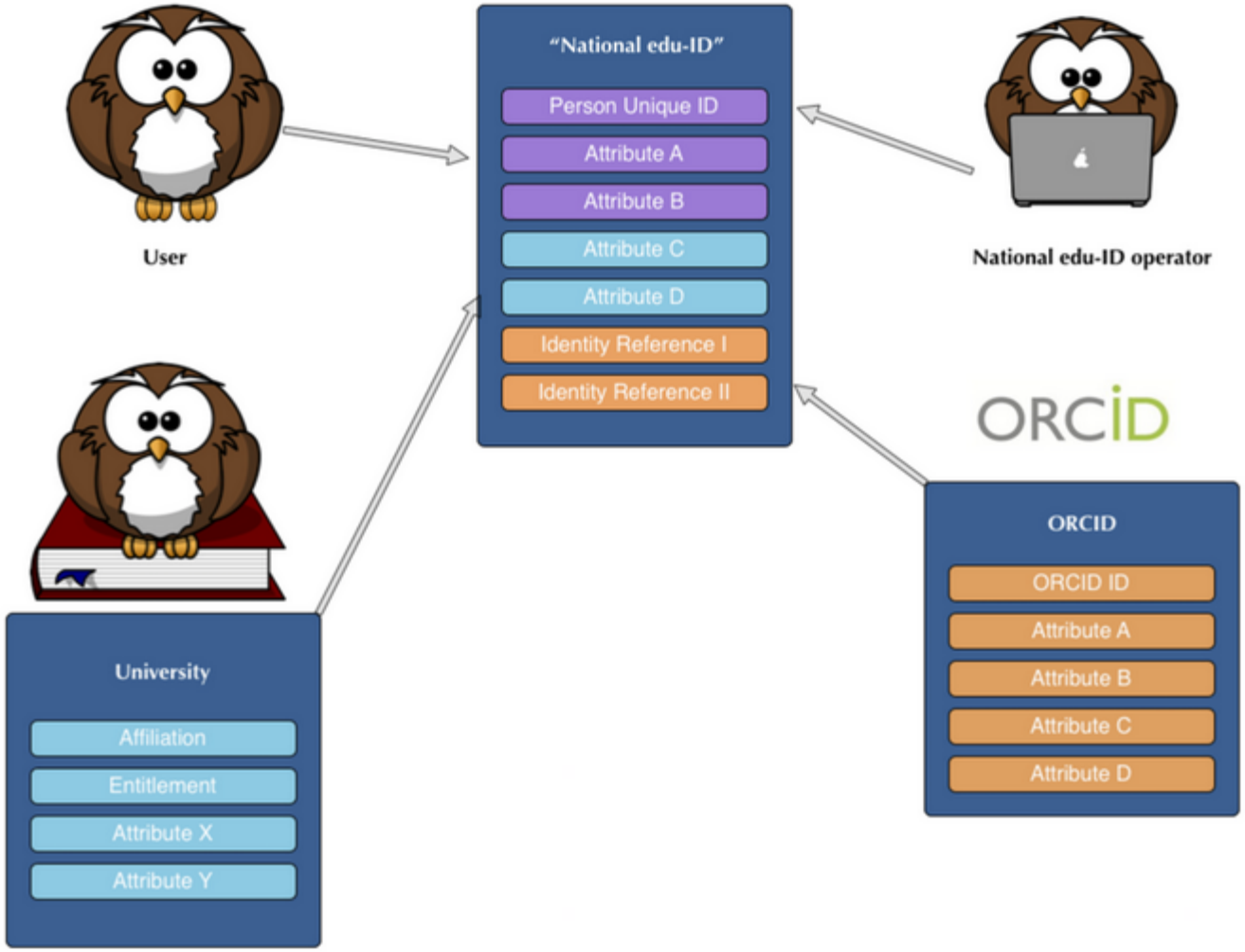
Workshop-Themen (2)

- Fortlaufend: Fragen an SWITCH sammeln → Pad
  - VC am Mittwoch ab 15:30
  - Zuvor Fragen gemeinsam strukturieren
- Vertiefende Diskussion zu **Account Linking** und **Attribut-Aggregation**
  - Verlässlichkeit von aggregierten IDs und Attributen
  - Welche neuen/zusätzlichen Attribute werden benötigt?
    → Die diesbezüglichen Erweiterungen von SWITCH durchsehen
  - Provisionierung bestimmter aggregierter Daten an Heimat-IdPs?

Workshop-Themen (3)

- Gemeinsam die bisherigen Anforderungen sichten: https://doku.tid.dfn.de/de:aai:eduid:eduid_intern:zusammenfassung_ws_juli2019
  - … und priorisieren (was muss?, was kann?
  - … und ergänzen – insbesondere die juristischen
- Diskussion Betriebsmodell bzw. Architektur
  - Zentral vs. dezentral, zukünftige Rolle der Heimat-IdPs, lokale Dienste
- Weitere Themen?
  - …

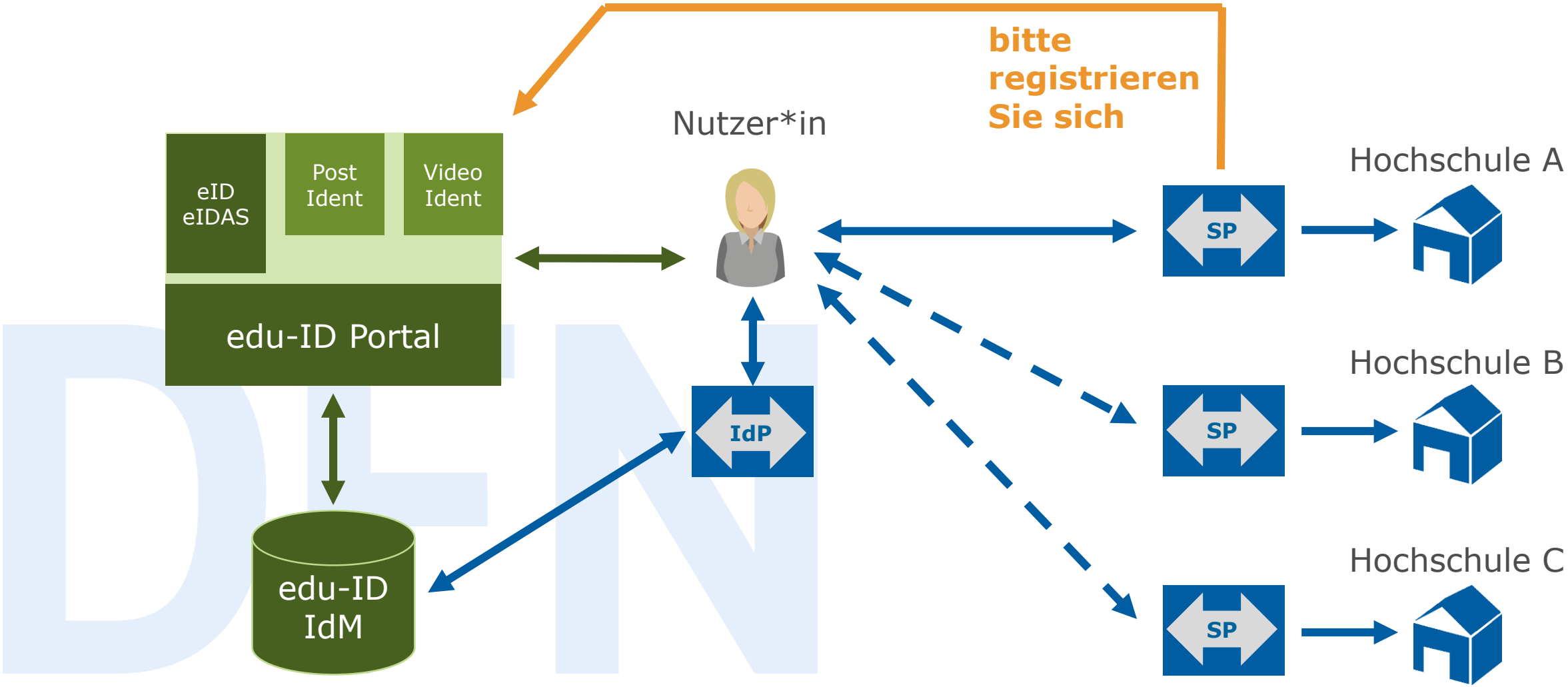
Attribut-Aggregation und Account Linking



Beliebig erweiterbar…

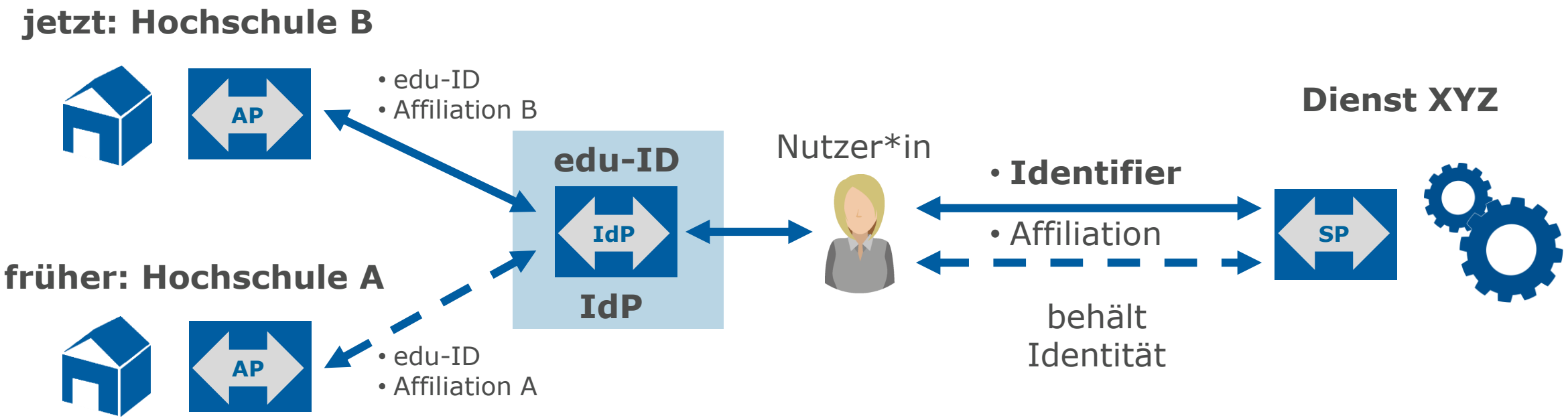
Quelle: GN4-2 JRA3 T3.1B User-centric identity federation: Best Practice for User Centric Federated Identity

edu-ID: Registrierung und Immatrikulation



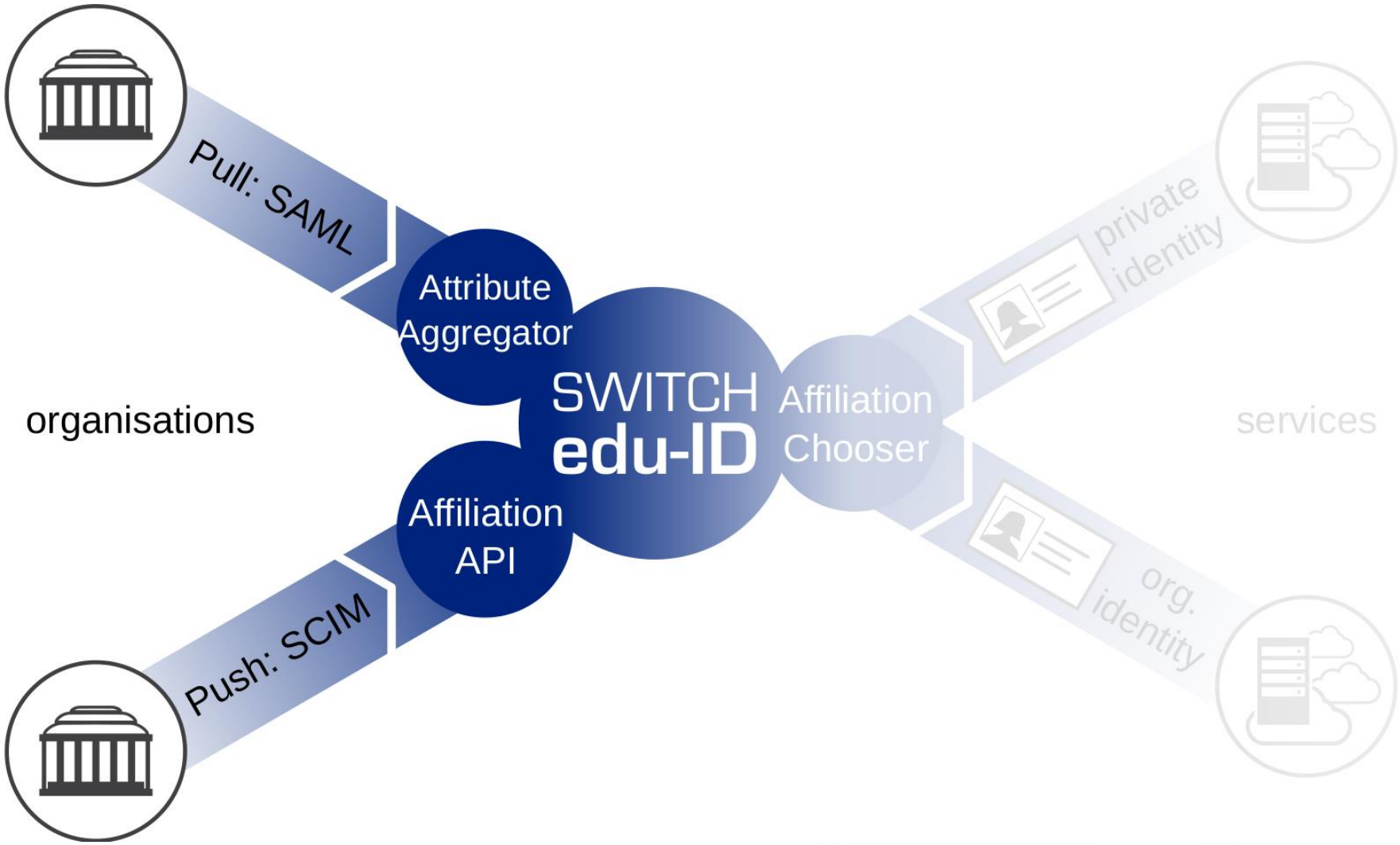
edu-ID und (sonstige) AAI-Dienste

Voraussetzung: edu-ID als Attribut im IdM der Heimateinrichtung



AP = Attribute Provider

Modell SWITCHaai



Quelle: Etienne Dysli Metref (SWITCH)

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

Informationsquellen

- edu-ID

  https://doku.tid.dfn.de/de:aai:eduid

- SWITCH edu-ID:

  https://www.switch.ch/edu-id/

  https://projects.switch.ch/eduid/about/swiss-edu-id-vs.-switchaai/

Backup-Folien

Nächste und übernächste Schritte

- Fragen der Machbarkeit sollten vorerst noch ausgeblendet werden
- Generell: taugt SWITCH edu-ID als Modell für einen DFN edu-ID Dienst?
- Spätere Iteration(en): Betriebs- und Informationssicherheit, Datenschutz, Betriebskonzept, Kostenmodell, …
- Sobald Prozesse sowie Details zu Datenspeicherung und –transfer definiert sind, kann mit der juristischen Bewertung begonnen werden

Nächste und übernächste Schritte

- **Anforderungsprofil** aus den im Workshop gesammelten Szenarien ableiten
- Ausgehend vom Anforderungsprofil ergeben sich weitergehende Fragen:
  - Integrationstiefe (→ Hub & Spoke Modell?)
  - Grundsätzlich: Machbarkeit?
    - Technisch
    - Organisatorisch und finanziell
    - Juristische Rahmenbedingungen
  - Betriebsmodell?
    - Organisatorisch (wer macht was) und technisch (und wie)
  - Kostenmodell?
    - Welche Kosten fallen an? Wer würde welche Kosten tragen?

Vorteile (1)

- Endnutzer*innen
  - **Eine** digitale akademische Identität (perspektivisch)
  - Mobilität
  - Nahtlose Nutzung bestimmter Dienste
  - Einrichtungsübergreifende Kooperation
- Dienstanbieter
  - Sicherheit, dass Identifier (abgeleitet von edu-ID) nicht neu vergeben werden oder sich durch IdP-seitige Modifikationen plötzlich ändern
  - Einheitliche (hohe) Sicherheitsstandards und LoAs
  - Keine dienstlokalen Accounts für Homeless Users

Vorteile (2)

- Heimateinrichtungen
  - Hochschulen: Einheitliche Schnittstelle für Online-Immatrikulation
  - Identity Vetting geschieht zentral
  - Keine/weniger SP-spezifische Attribut-Konfigurationen
  - Lokale / einrichtungsspezifische Dienste können leichter zentralisiert werden
- Virtuelle Organisationen, Forschungsinfrastrukturen
  - Account Linking, keine VO-spezifische ID erforderlich(?)
  - Kein Guest IdP erforderlich, in Verbindung z.B. mit eduTEAMS (Instanz von DFN gestellt?) keine Eigenentwicklung für VO-Management erforderlich
- Föderationen
  - Zentraler IdP: Einführung neuer Protokolle/Technologien (z.B. OIDC) erleichtert

Warum eine edu-ID?

1. Vereinheitlichung und Vereinfachung der Verfahren zur Online-Immatrikulation
   - Verlässliche digitale Identität bereits vorhanden
   - Zentraler Identity Provider
2. Langlebige digitale ID, die nicht an eine Organisationseinheit gebunden ist
   - Unterbrechungsfreie Nutzung von Diensten, deren Nutzungsberechtigung nicht an die Zugehörigkeit zu einer **ganz bestimmten** Einrichtung geknüpft ist (Speicherdienste, Nationallizenzen, LMS, …)
   - Gast-IdPs für sog. Homeless Users und Citizen Scientists werden obsolet
   - Erleichterungen beim Management virtueller Organisationen durch Forschungsprojekte und –Infrastrukturen (Attribute Authorities u.a.m.)