deutsches forschungsnetz

Service Provider Proxy mit Shibboleth

71. DFN-Betriebstagung | 24. September 2019

Wolfgang Pempe

Begriffsbestimmung

- Was ist ein Proxy? (bzw. Proxy Server)
- Wikipedia (https://en.wikipedia.org/wiki/Proxy_server)
- „In computer networks, a **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request **as a way to simplify and control its complexity**. Proxies were invented to add structure and encapsulation to distributed systems.”

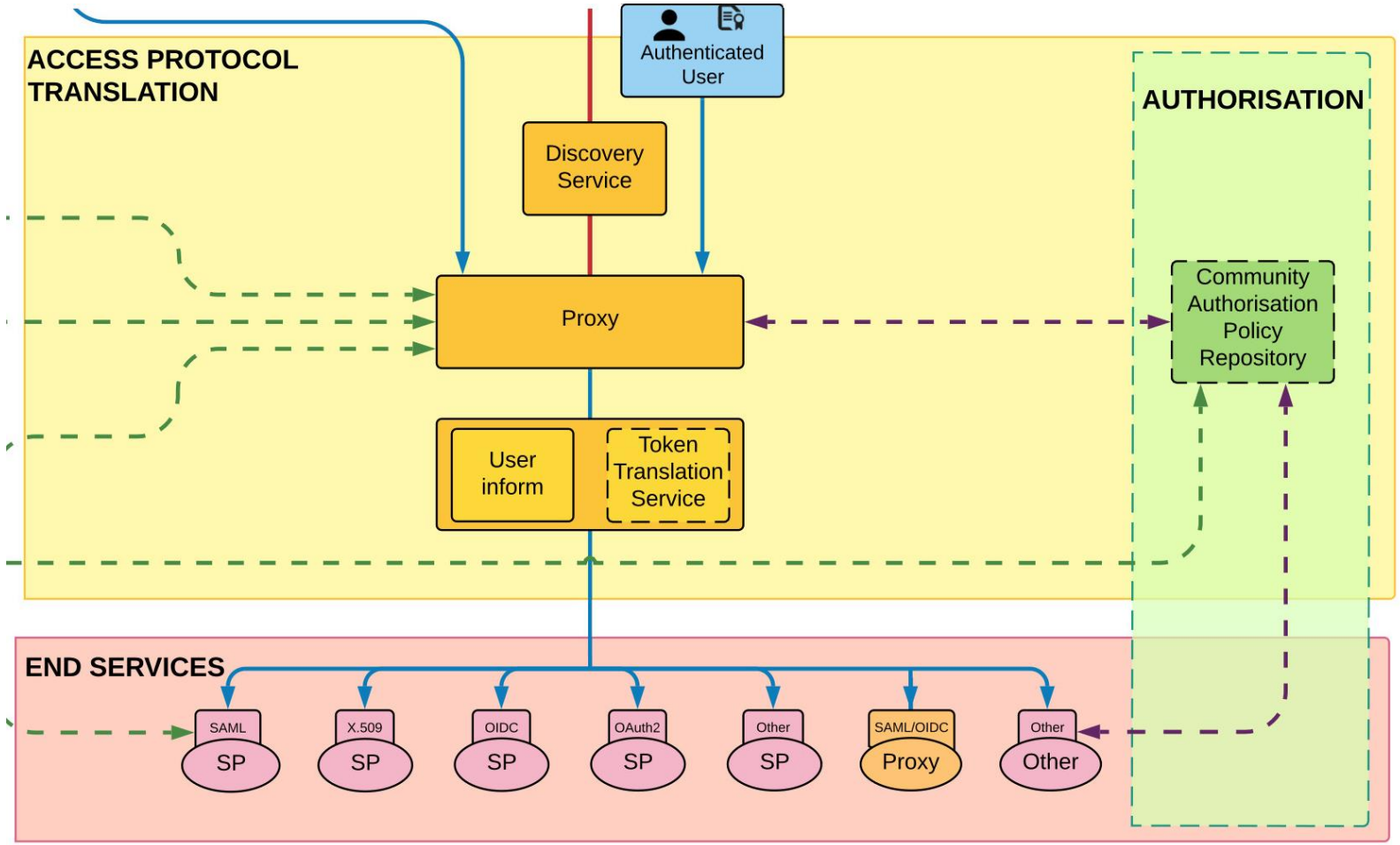
Es geht also um Vereinfachung…

Anwendungsszenarien im Bereich AAI

- **Übersetzung** zwischen unterschiedlichen Protokollen (siehe Vortrag DAASI)
- **Stellvertreter** für einen oder mehrere Identity Provider und/oder Service Provider
- Ein AAI-Proxy ist stets **doppelgesichtig**: jeweils eine IdP- und eine SP-Komponente

Quelle: Wikipedia

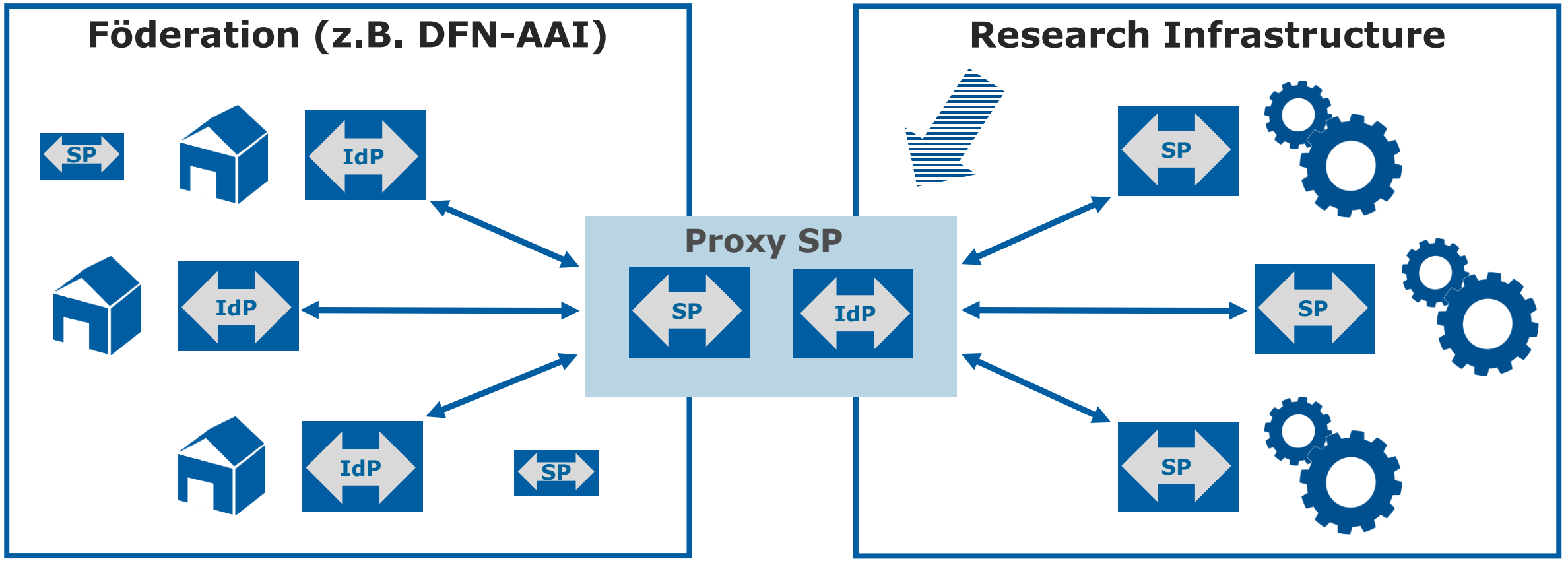
Beispiel: AARC Blueprint Architecture (BPA)



(Ausschnitt) Quelle: https://aarc-project.eu/architecture/

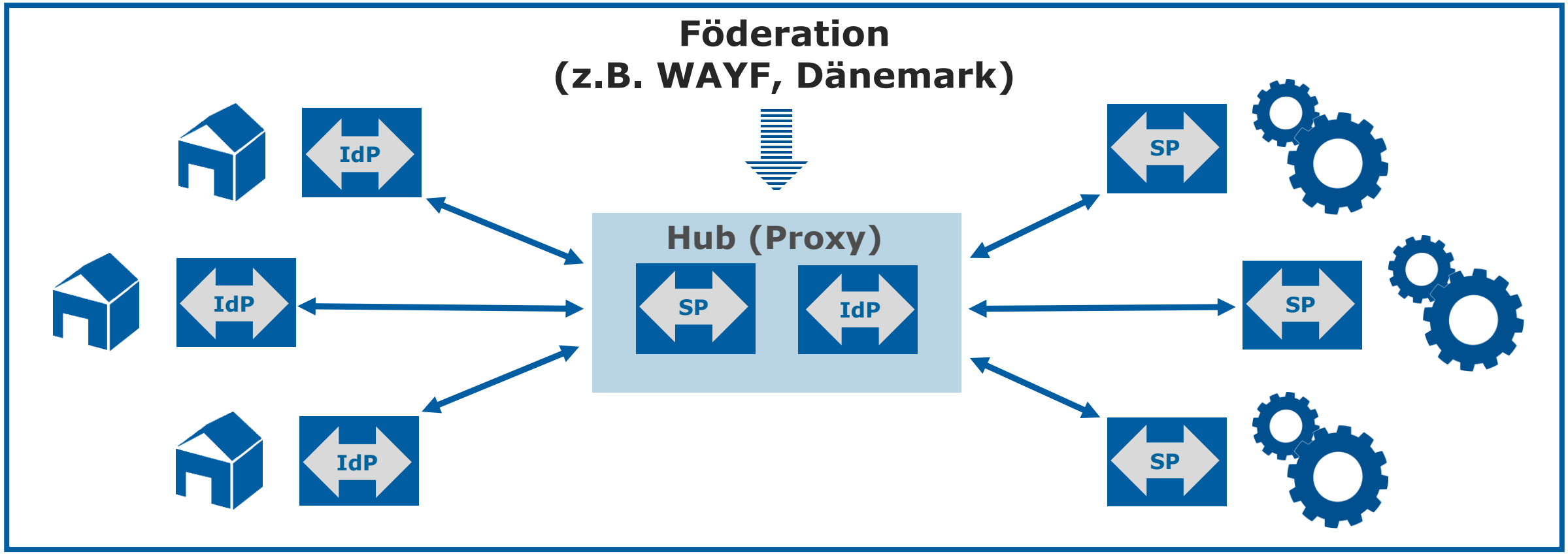
BPA aus Föderationssicht

stellvertretend für alle Konstrukte dieser Art…



Beispiel Hub-and-Spoke Föderation

Zentraler IdP-SP Proxy (Hub)

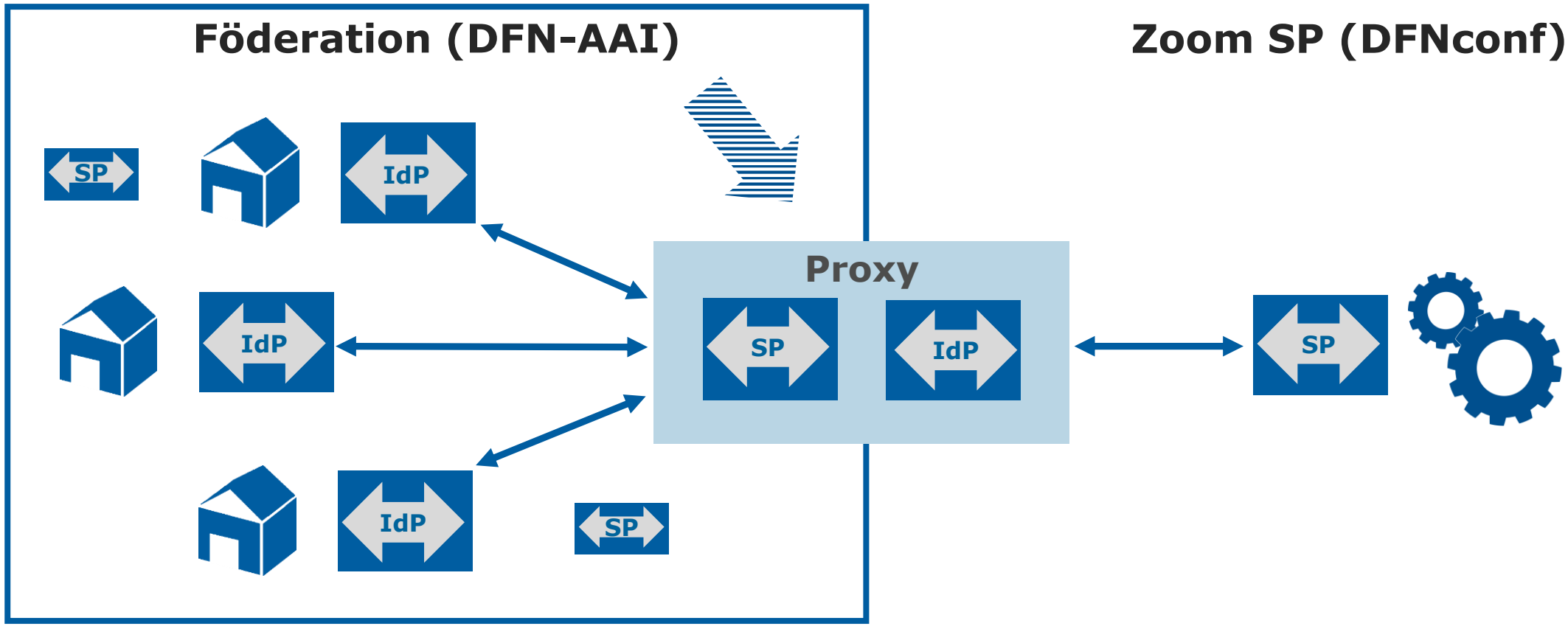


Cloud-basierte Service Provider: Tenant SPs

- Aktueller Trend bei vielen Anbietern: pro Lizenznehmer/Einrichtung wird anhand manuell eingepflegter IdP-Metadaten ein Cloud-basierter SP konfiguriert : „Tenant SP“, der dann direkt mit dem jeweiligen IdP verdrahtet werden muss (außerhalb der Föderation) → Wartung problematisch
- Beispiele: Adobe, LinkedIn Learning (ehemals lynda.com), JobTeaser, Zoom, u.a.m.
- DFNconf: Zoom Meetings & Chat als möglicher Bestandteil des Portfolios?
- Lösungsansatz für PoC: Proxy-basierter Zugang, um Tenant-SPs für Teilnehmer zu vermeiden (Voraussetzung: Sammellizenz)

DFNconf-Proxy für Zoom Meetings & Chat

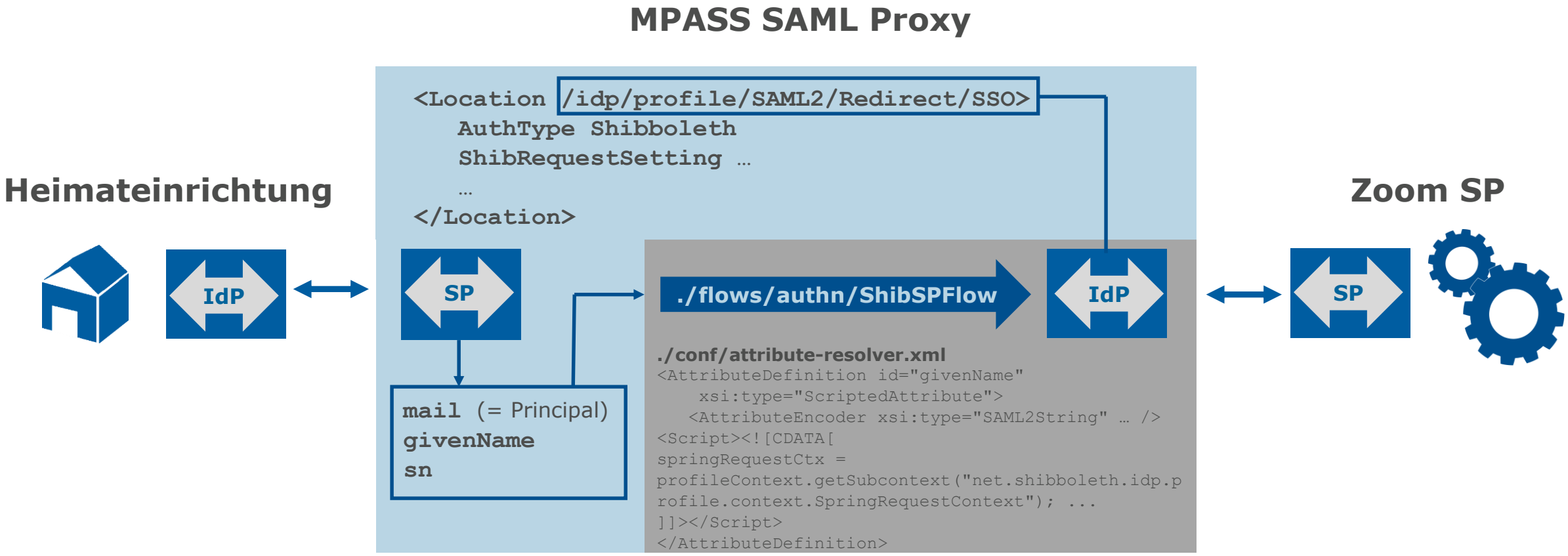
Ein einziger Tenant SP für die gesamte Föderation



Software für AAI-Proxies

- Altbewährt:
  - SimpleSAMLphp
  - ADFS
- Proxy-Konstruktionen mit Shibboleth bislang nicht üblich
- Seit einiger Zeit existiert ein externes Modul, das für Shib IdP 3.x einen Authentication Flow bereitstellt, der Attribute verarbeitet, die ein auf dem selben (virtuellen) Host laufender SP liefert: https://github.com/mpassid/shibboleth-idp-authn-shibsp
- **Mittel der Wahl für Zoom-Proxy**

Funktionsweise des „MPASSid SAML Proxy “



Voraussetzung: selber virtueller Host für SP und IdP

Anmerkungen

- Lösung bereits für diverse Anbieter bei SWITCH im Einsatz (Lizenzmanagement für teilnehmende Einrichtungen)
- Code soll Bestandteil der offiziellen Shib IdP Distribution werden (evtl. v4.x)
- Probleme:
  - Bescheidene Doku
  - Umlaute in Attributwerten – muss derzeit noch in Scripted Attribute Definition abgefangen werden
  - Logout Flow (noch) nicht implementiert
    (→ Redirect auf Logout Handler des Proxy SP)
- Mögliches Thema für Shibboleth Workshop in 2020?

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