Attribute Authorities

in der DFN-AAI

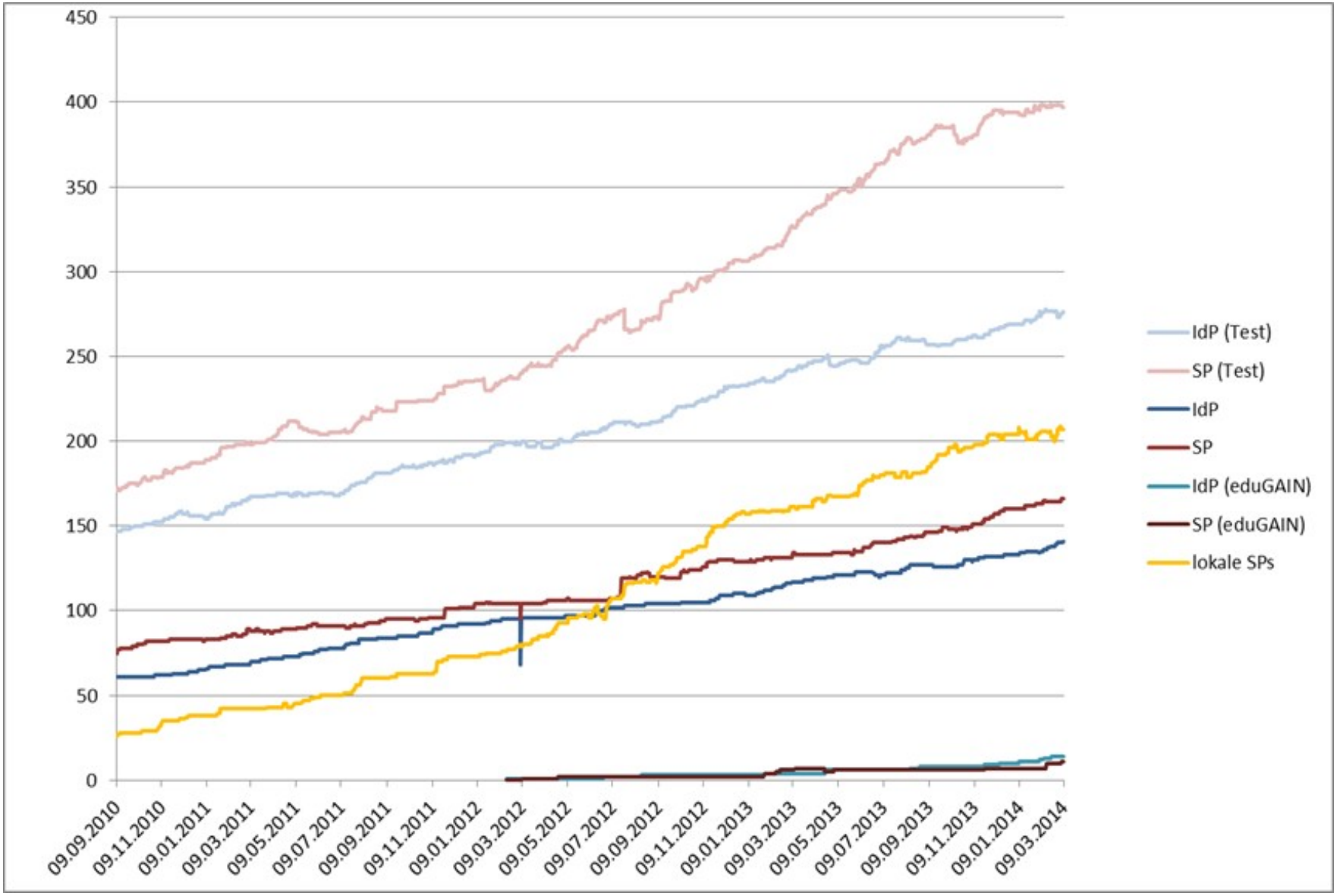
Wolfgang Pempe, DFN-Verein
pempe@dfn.de

60. DFN-Betriebstagung,
11./12. März 2014, Berlin

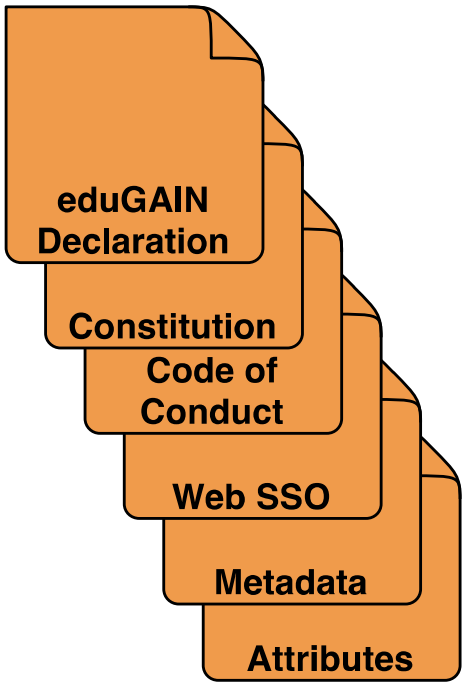
Überblick

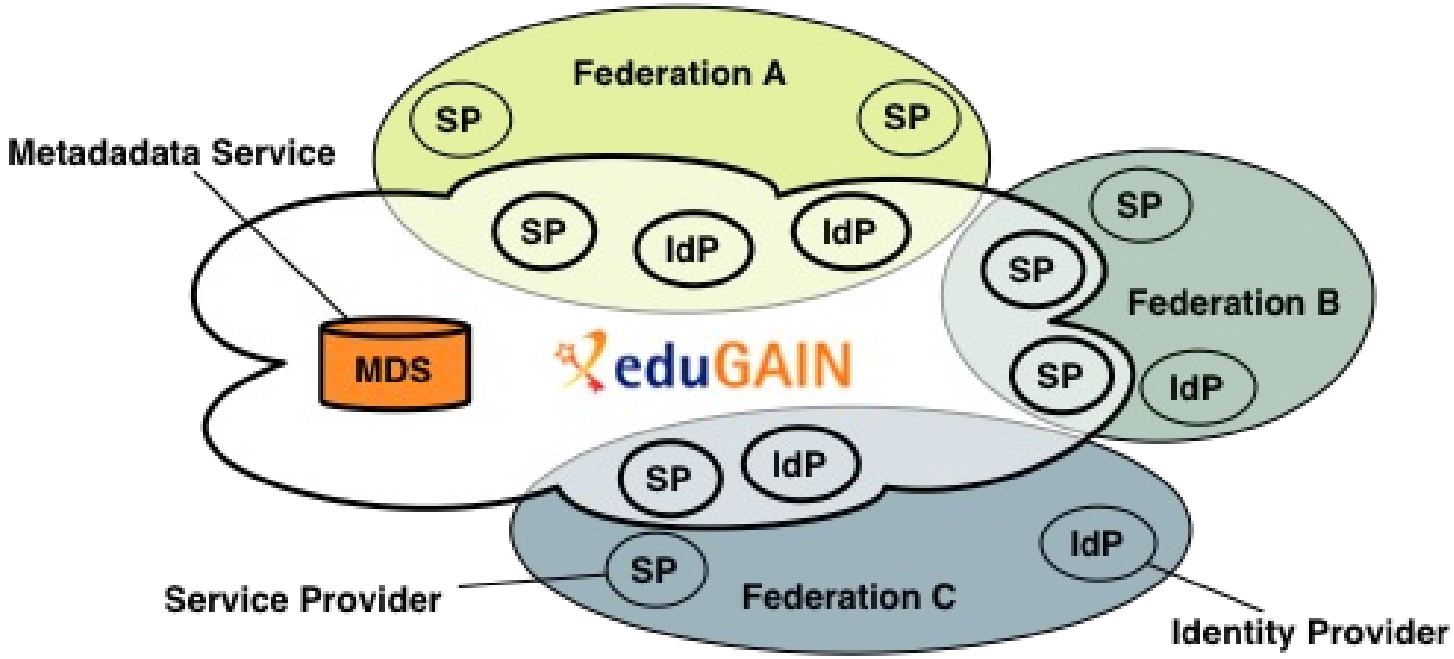
- Aktuelle Zahlen
  - DFN-AAI
  - Interfederation / eduGAIN
- Attribute Authorities
- Ausblick

DFN-AAI – registrierte Provider



Was ist eduGAIN?

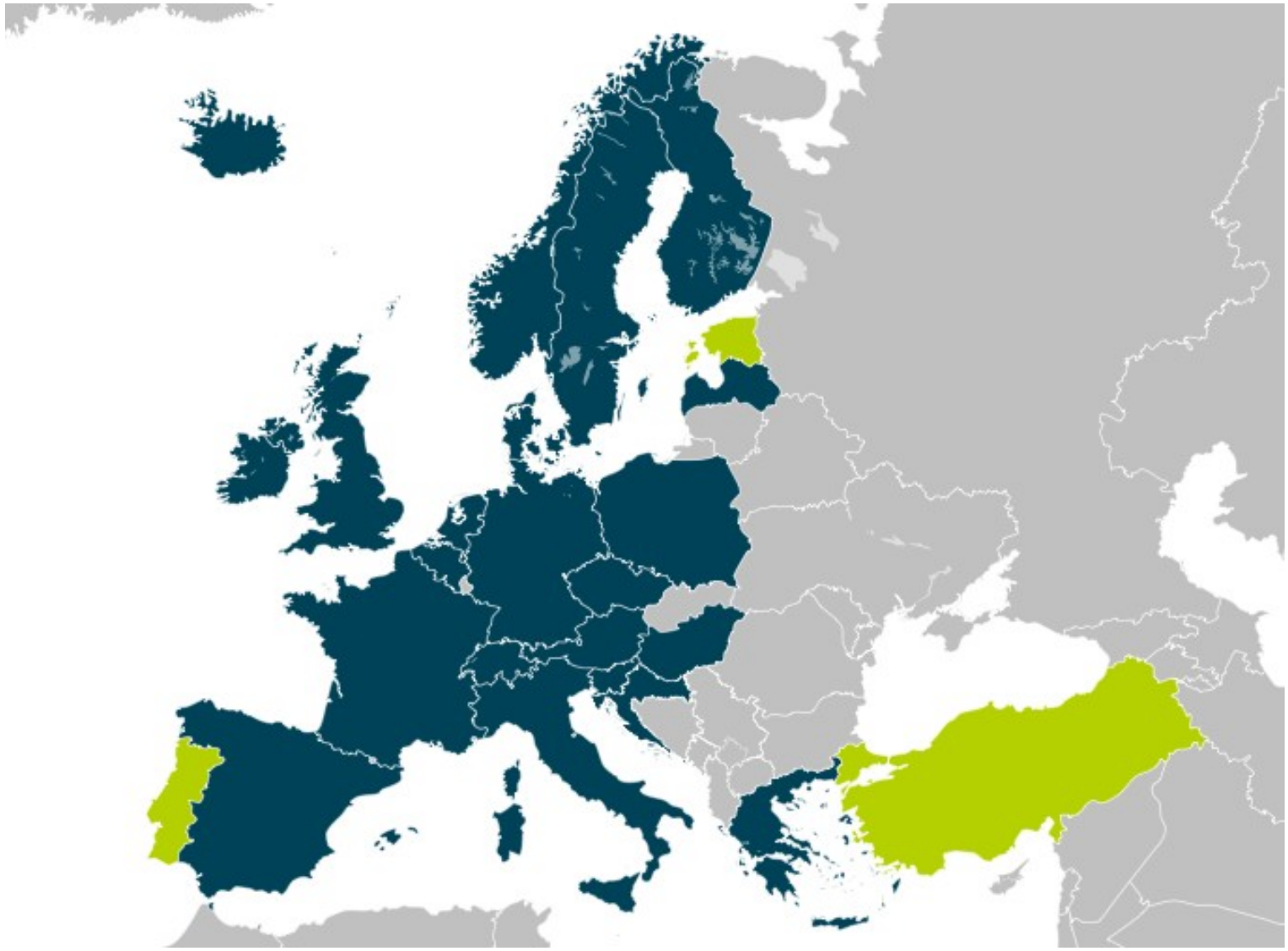




Quelle: Lukas Hämmerle (SWITCH)

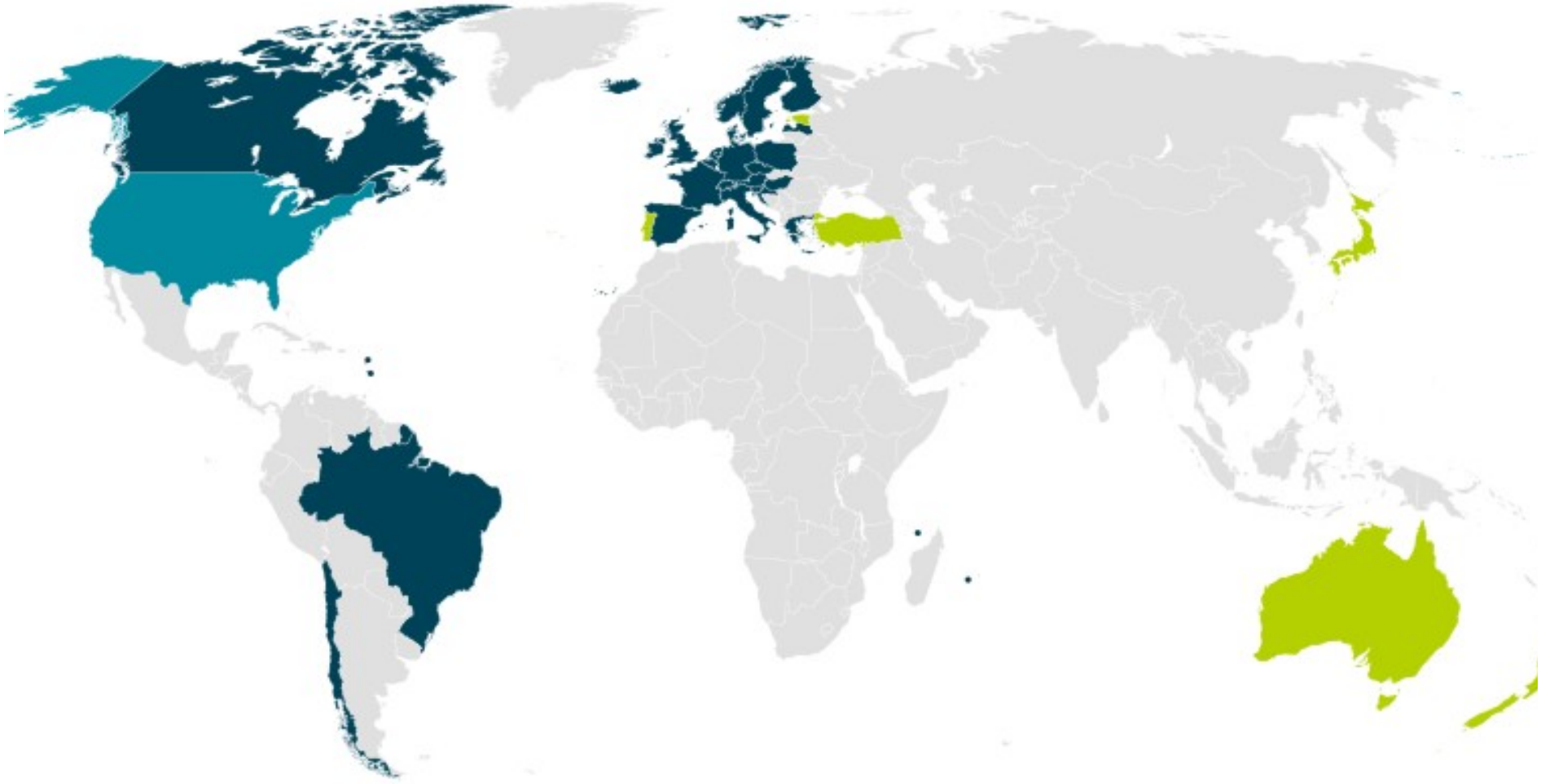
- eduGAIN provides policy framework and standards to build trust
- SPs and IdPs of participating federations should opt-in for eduGAIN
- MDS fetches, aggregates and republishes metadata
- **Beteiligung DFN: GÉANT3plus, SA5 Task5, ”Enabling Users”**

eduGAIN – Europa



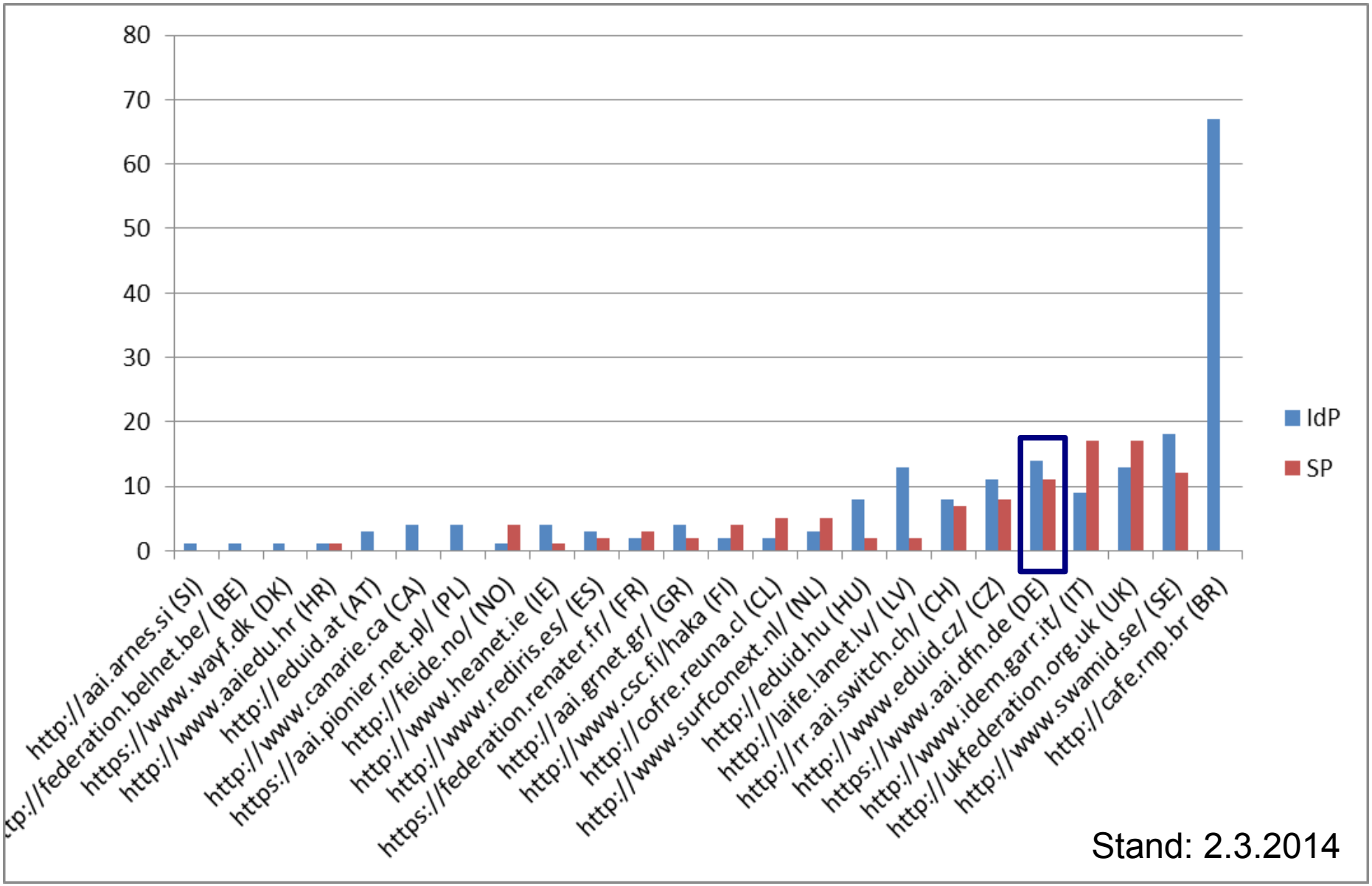
Quelle: Brook Schofield (TERENA)

eduGAIN – weltweit



Quelle: Brook Schofield (TERENA)

eduGAIN – Beteiligung



eduGAIN in Zahlen

- April 2011: Official start of eduGAIN
- Now: 24 Federations (+5 **since October 2013** = 5 months)
- New: Ireland, Austria, Poland, Chile, Slovenia
- 6 federations joining (= policy signed but some information/technical adaptations missing)
- Current Entities: 200 (+57 = + 40%) IdPs, 104 (+31 = +42%) SPs
- Note: One IdP can stand for dozens of organisations depending on federation architecture (hub-and-spoke federations = 1 SP + 1 IdP)
- Whole (academic) SAML landscape:
- 46 (+3) Federations, 2463 (+73) IdPs, 5101 (+447) SPs
- Numbers from http://www.terena.org/~schofield/servicecatalogue/
- Not all of them need to be interfederated, e.g. many internal SPs

(copy + paste from Lukas Hämmerle, SWITCH)

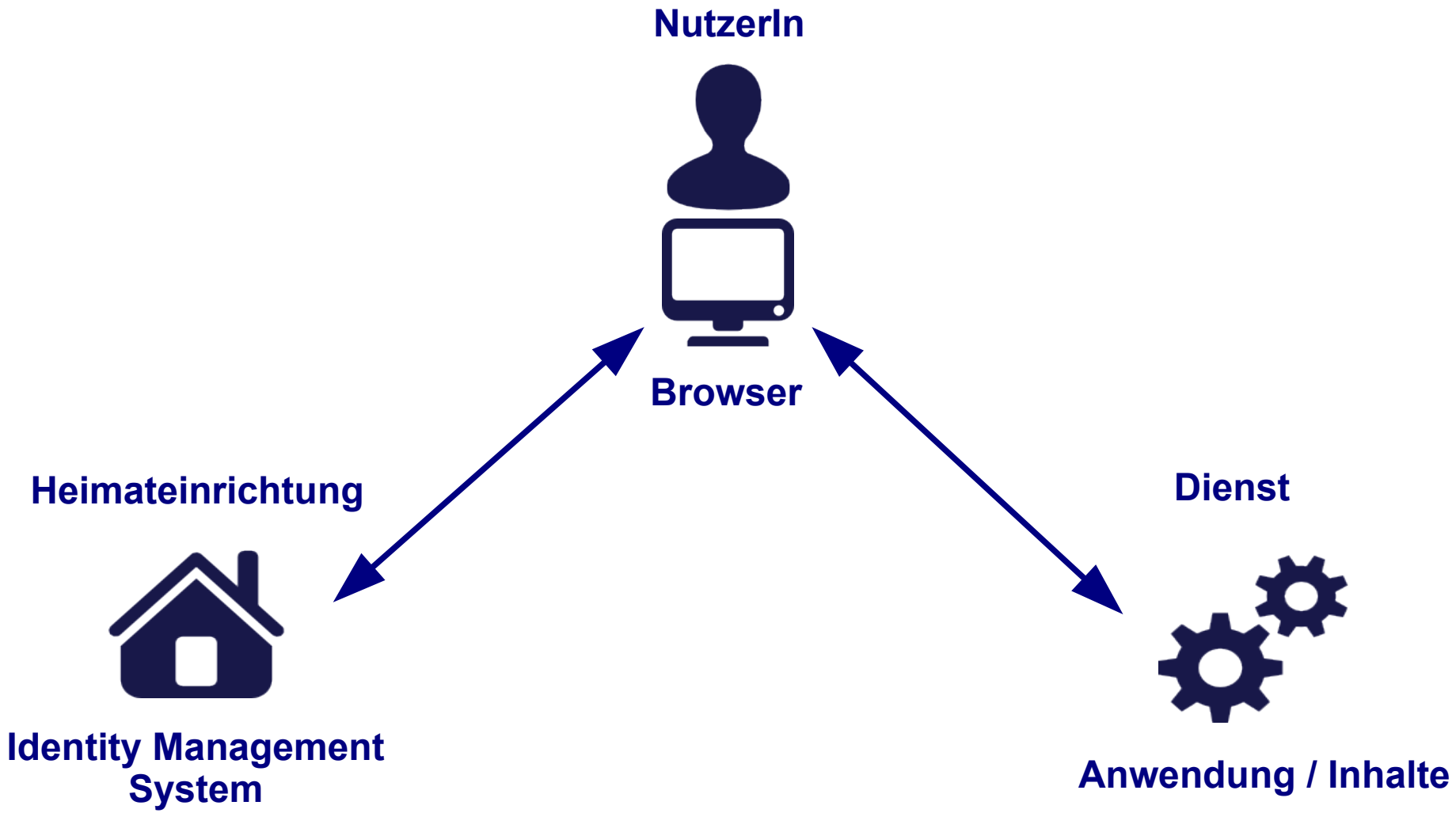
und jetzt ...

DFN Deutsches Forschungsnetz

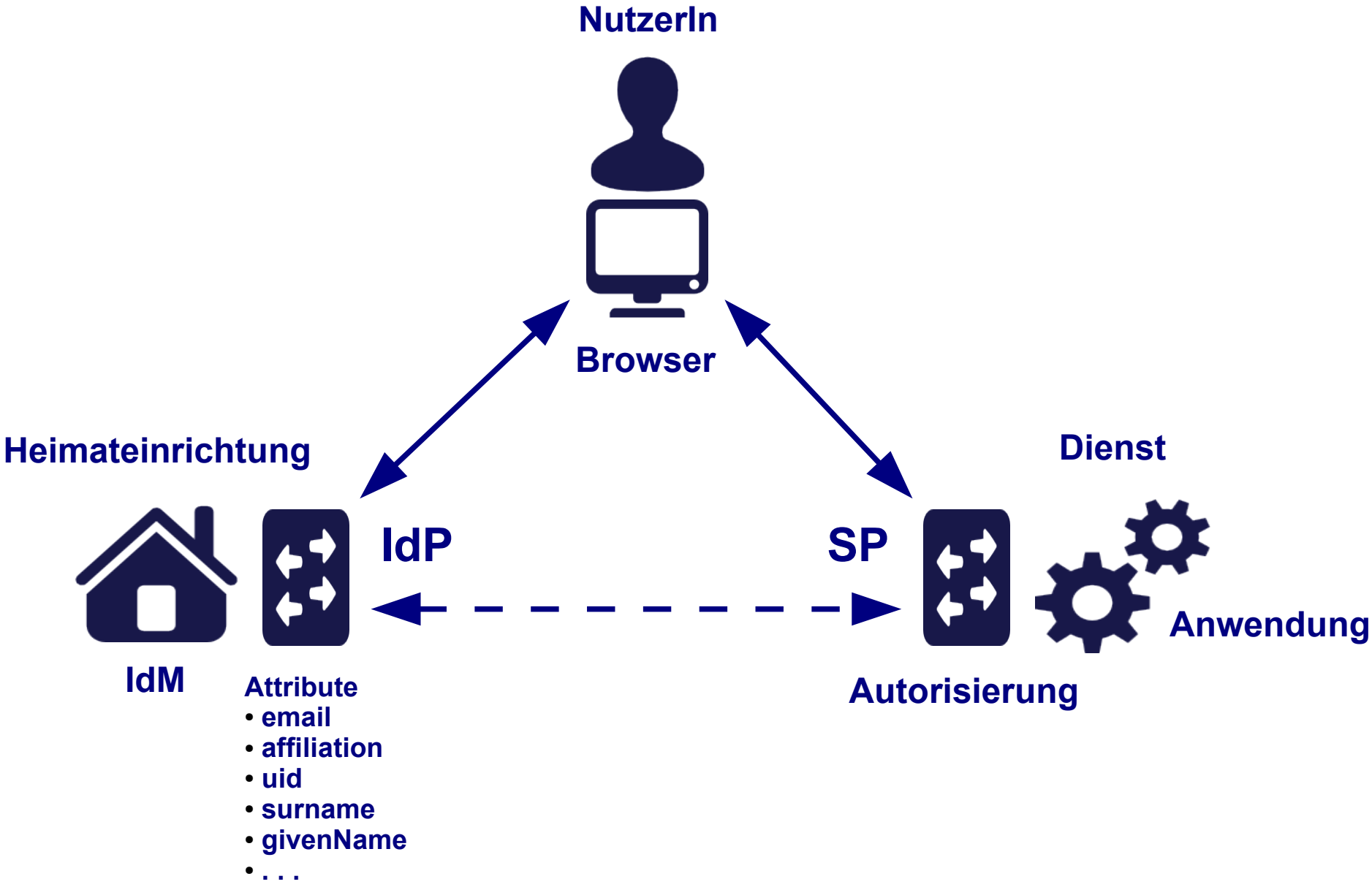
Attribute

Authorities

Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail



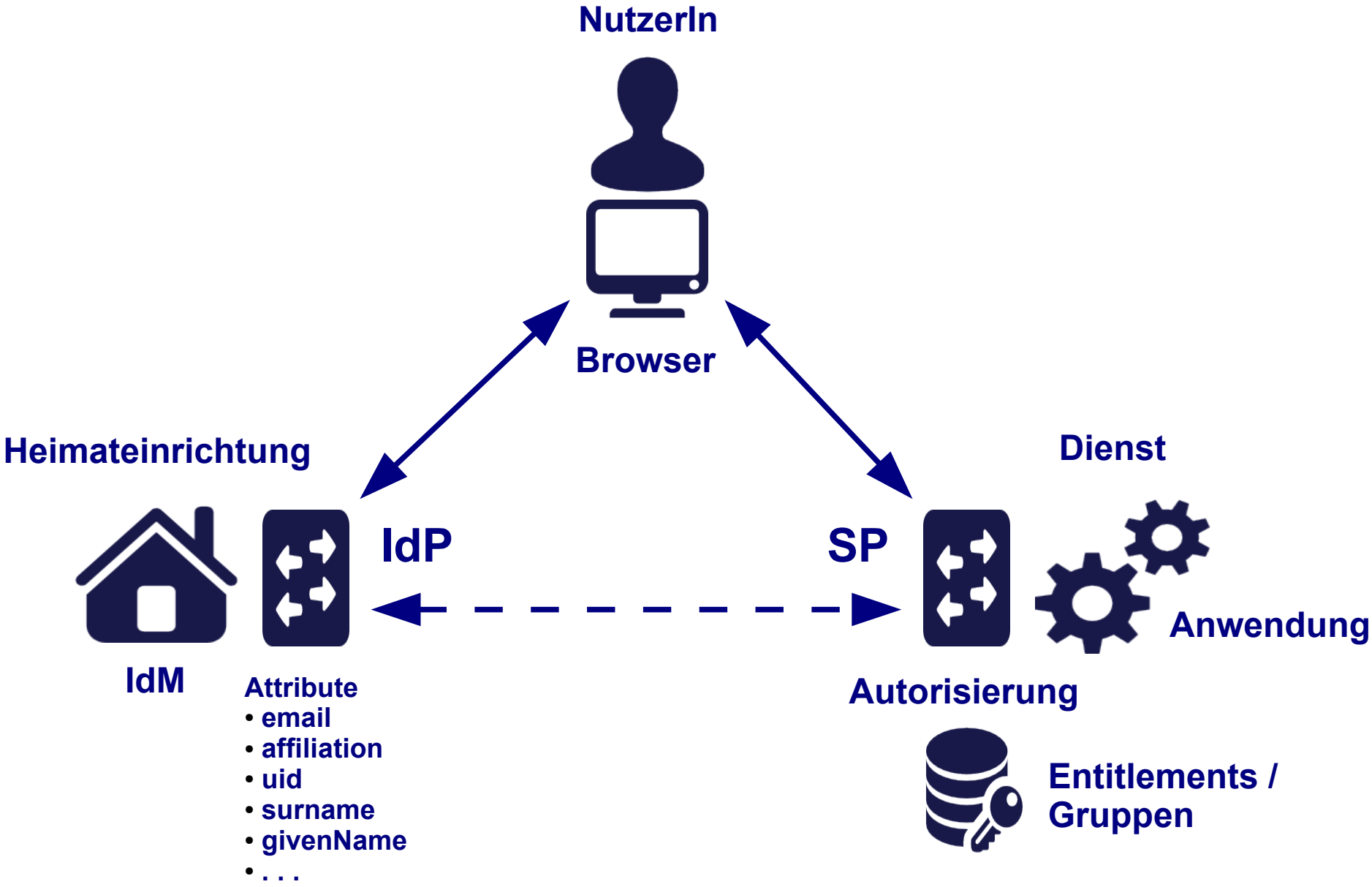
Icons: http://www.visualpharm.com/

Attribute und Autorisierung

- **Problem:**
  - Heimateinrichtungen pflegen im IdM standardmäßig nur Angaben wie eMail-Adresse, Vor- und Zuname, Status/Affiliation (StudentIn, MitarbeiterIn etc.)
  - Nur in Ausnahmefällen Dienst- oder Projekt-spezifische Berechtigungen (Entitlements, Gruppenzugehörigkeit)
  - . . . schon gar nicht für externe Dienste (die das mitunter auch gar nicht wünschen!)

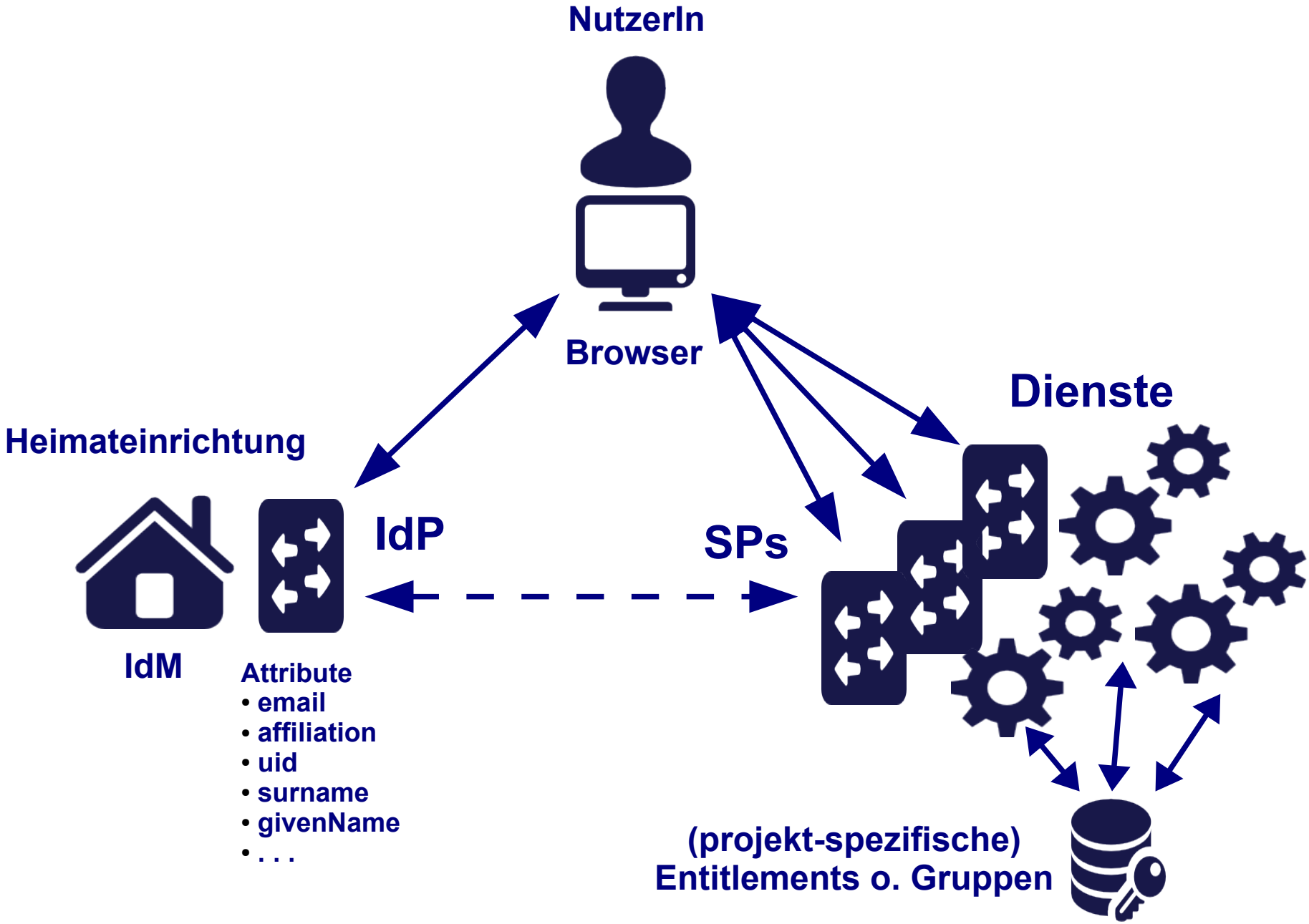
→ Rechtemangement muss beim Dienst selber erfolgen

Service-seitiges Rechtemanagement



Icons: http://www.visualpharm.com/

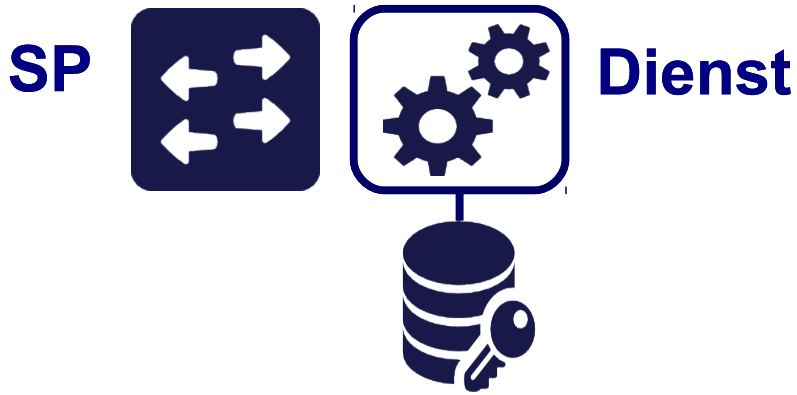
Service-seitiges Rechtemanagement



Icons: http://www.visualpharm.com/

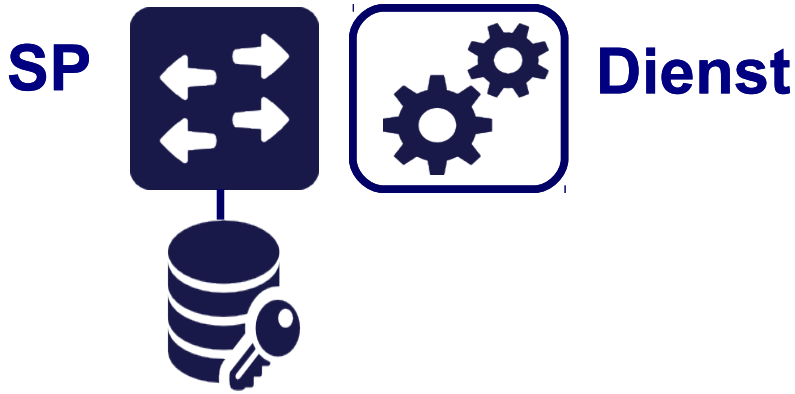
Implementierungs-Varianten

- **Variante 1:**
  angeschlossen an die Anwendung



- **Variante 2:**
  Shibboleth SP: Simple Aggregation Attribute Resolver

  = Attribute Authority



Icons: http://www.visualpharm.com/

Attribute Authority (AA)

AA = IdP mit eingeschränkter Funktionalität

- Metadaten-technisch besteht ein IdP aus zwei Komponenten:
  - IdPSSODescriptor
  - AttributeAuthorityDescriptor
- Es wird nur <AttributeAuthorityDescriptor> benötigt
- Nur AttributeQuery Profile erforderlich, kein SSO
- Attribute Query nur seitens berechtiger SPs
- Identifizierendes Attribut als Direct Principal Connector benötigt (Mapping), z.B. eduPersonPrincipalName

Motivation (1)

Föderierter Zugang zu DFN-Dienst (Wiki)

- Wiki durch Shibboleth SP geschützt
- Kleiner, überschaubarer Nutzerkreis
- Nutzer aus unterschiedlichen Institutionen
- Nicht jede dieser Institutionen mit IdP in DFN-AAI
- Unterschiedliche Rechte/Rollen (Entitlements)
- Diese Attribute sollten **nicht** von der HO verwaltet werden

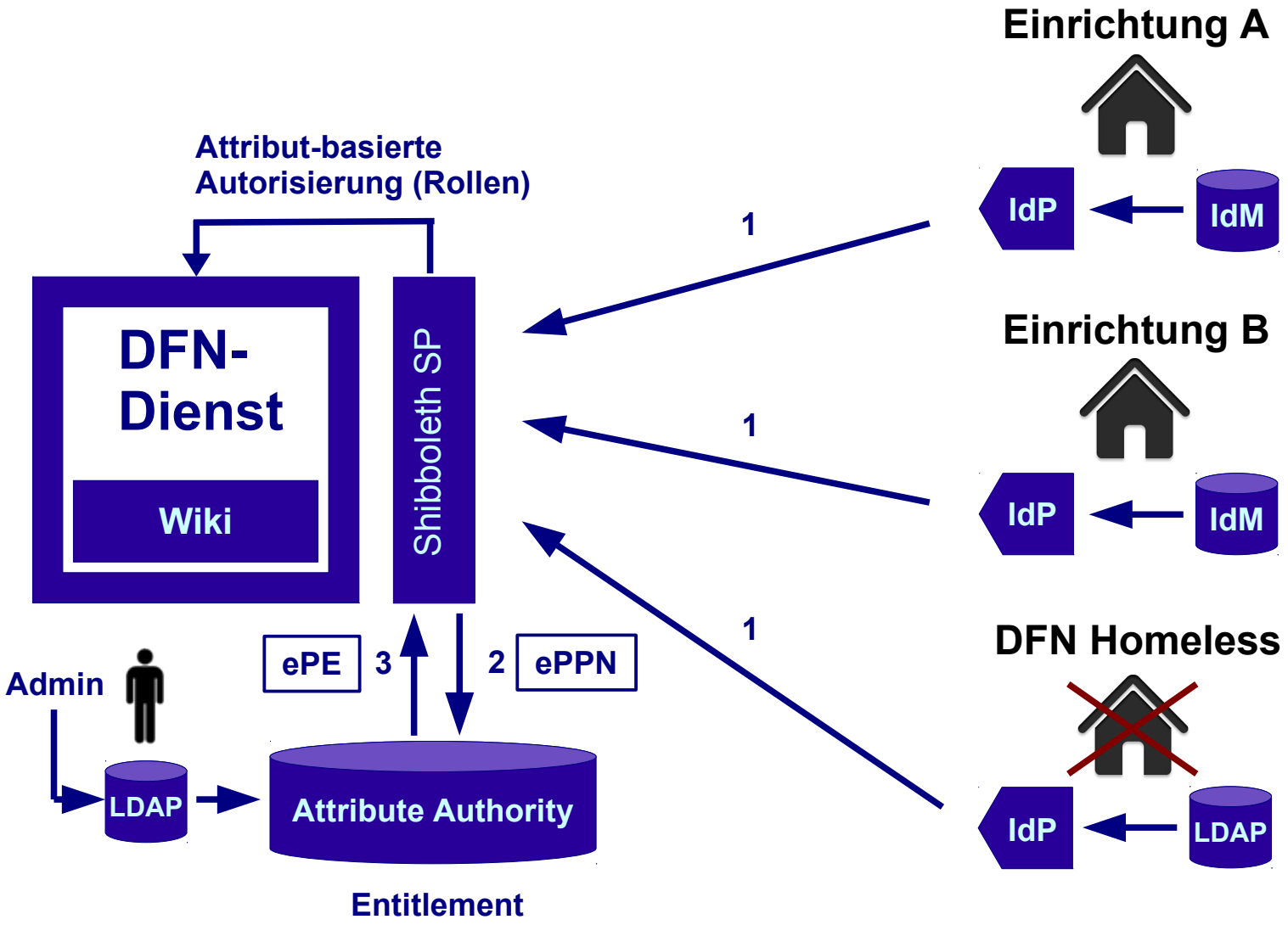
→ Homeless IdP für Nutzer von DFN-Diensten

→ **Attribute Authority für dienstspezifische Entitlements**

Motivation (2)

- Eigenbedarf
  - Collab Wiki
    - Nutzer aus verschiedenen Einrichtungen
    - Teilweise ohne eigenen IdP
  - Mailsupport Portal
    - Konfigurationsverwaltung
    - Delegation von Zugriffsrechten
- Forschungsprojekte
  - DARIAH (z.B.)
    - Partner über Europa verteilt
    - Zentrale Gruppenverwaltung

Umsetzung – Überblick



Umsetzung – Metadatenverwaltung

Attribute Authority als eigener Typ

https://testidp2.aai.dfn.de/idp/shibboleth				XML				
https://testidp3-dev.aai.dfn.de/idp/shibboleth				XML				
neuen IdP anlegen								

Attribute Authority-Liste

EntityID	DFN-AAI	DFN-AAI-Basic	eduGAIN	DFN-AAI-Test	lokale Metadaten			
https://attributes.dfn.de/idp/shibboleth	XML				XML			
neue Attribute Authority anlegen								

SP-Liste

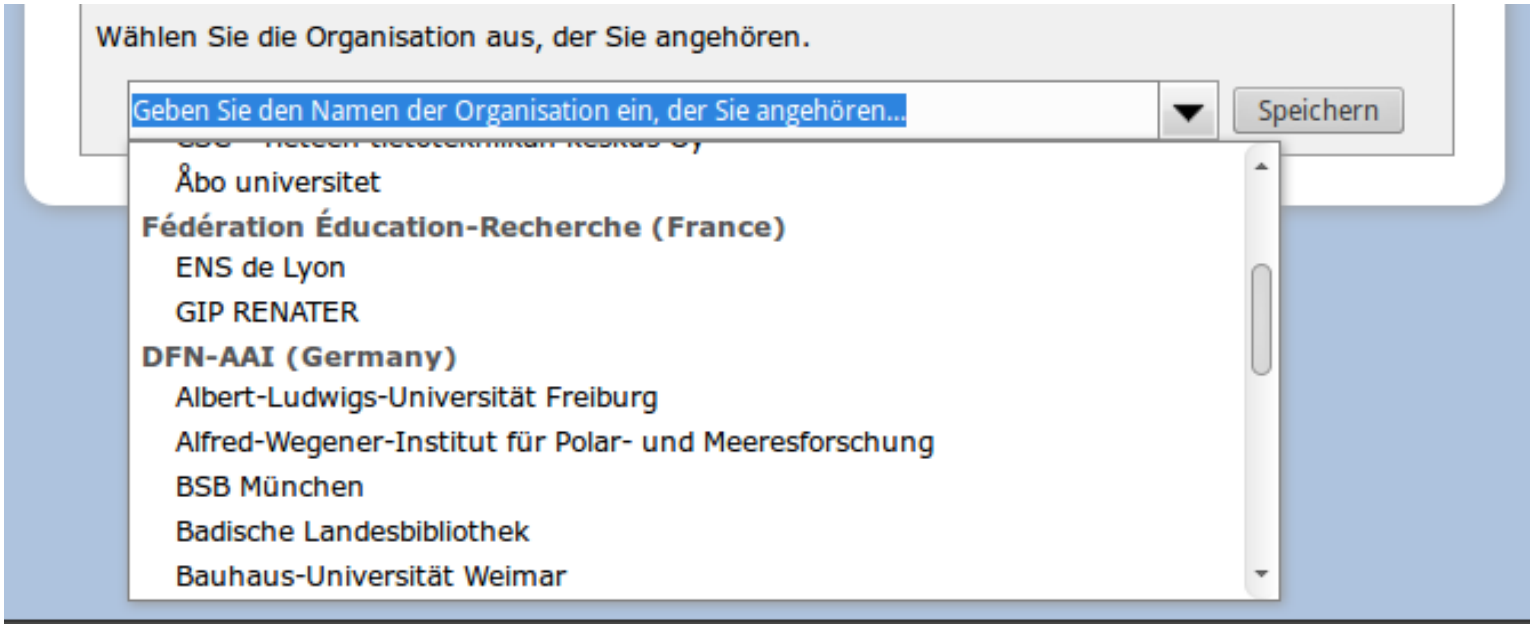
EntityID	DFN-AAI	DFN-AAI-Basic	eduGAIN	DFN-AAI-Test	lokale Metadaten			
https://abstimmung.dfn.de/				XML	XML			

Policy:

- Dienstvereinbarung DFN-AAI erforderlich (IdP-Vertrag)
- Automatische Freischaltung für DFN-AAI-Basic

Vorteile

- Metadaten-technisch saubere Lösung
- DFN-Policy: Nur ein produktiver IdP pro Einrichtung
  → aber mehrere Attribute Authorities
- WAYF-Generierung
  → nur Entities mit IdPSSODescriptor



Screenshot: https://wayf.aai.dfn.de/DFN-AAI-eduGAIN/wayf = DFN-AAI (alle) + eduGAIN

Ausblick

Tools für Rechtemanagement und Gruppenverwaltung

- SWITCHaai: SWITCH Toolbox (zentraler Dienst)
  https://www.switch.ch/toolbox/
- GÉANT3plus:
  - JRA3 Task 1 ”Attributes and Groups in the cross instituion environment”
    http://www.terena.org/activities/tf-emc2/meetings/26/GN3p-JRA3-T1-tfemc2-feb2014-Zurich.pdf
  - Open Call Project: HEXAA
    http://www.geant.net/opencall/Authentication/Pages/Home.aspx#HEXAA
- CESNET: PERUN - User and Resource Management System for Virtual Organizations/Research Communities
  http://perun.cesnet.cz/web/

Vielen Dank für Ihre Aufmerksamkeit!

Ideen? Fragen? Anmerkungen?

Kontakt

Portal: https://www.aai.dfn.de

EMail: hotline@aai.dfn.de

Tel.: +49 711 63314 215