Grundlagen

AAI, Web-SSO, Metadaten und Föderationen

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DFN-AAI IdP-Workshop,
7. Juli 2016, TU Kaiserslautern

Was ist DFN-AAI?

DFN
Deutsches Forschungsnetz

AAI

Authentifizierung
Autorisierung
Infrastruktur

Worum geht es?

- Web-basiertes Single Sign-on (Web-SSO)
  - Einmal anmelden für 1..n Dienste, für die man zugriffsberechtigt ist
  - Keine dienstspezifischen Credentials, da Login nur bei der Heimatorganisation stattfindet
- (Non-web SSO)
- Metadaten (SAML, was sonst)
- Vertrauen
- Zusammenarbeit lokal, aber v.a. auch über Einrichtungs- und ggf. Föderations-Grenzen hinweg

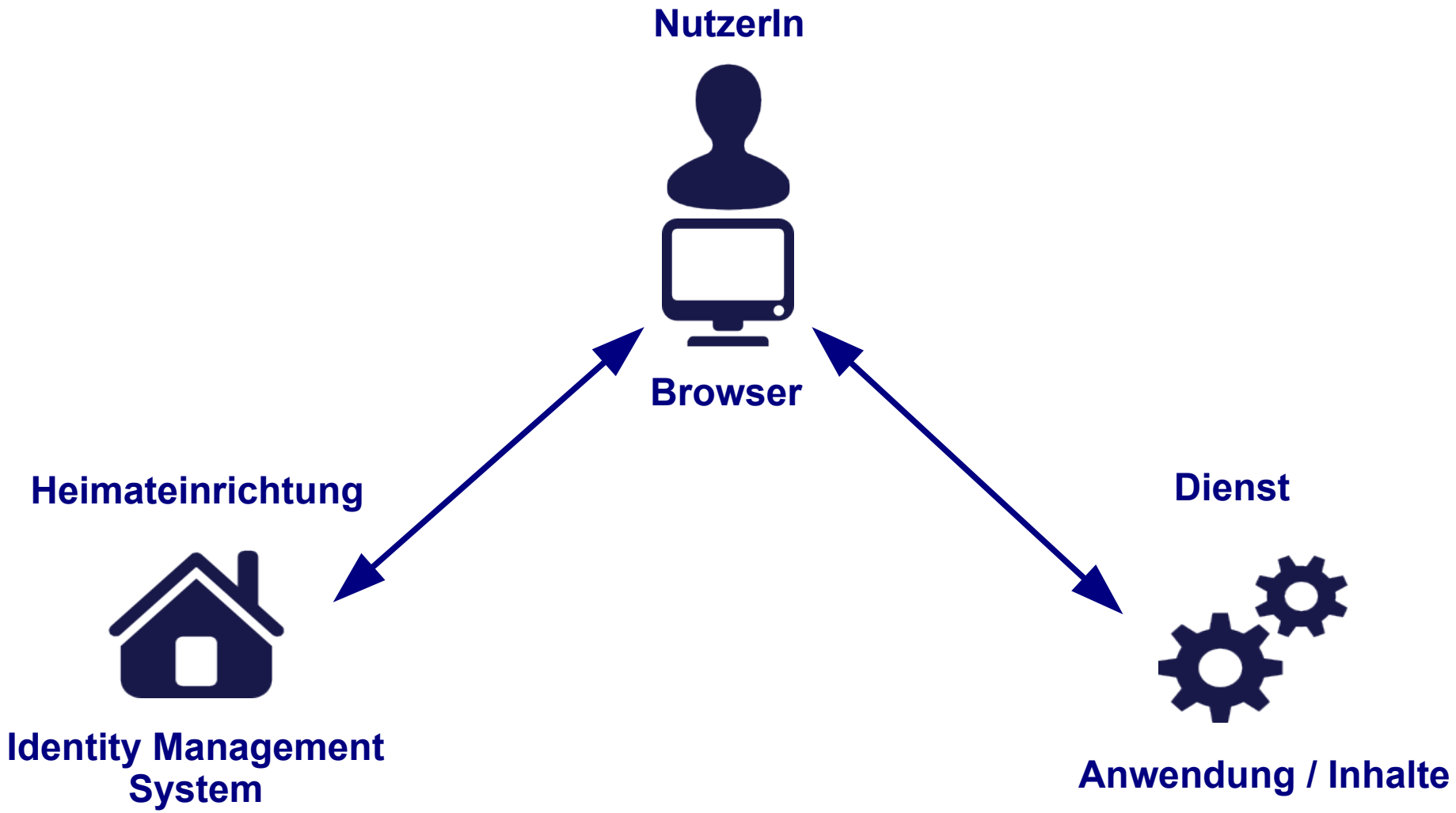
Welche Arten von Diensten?

Zielgruppe: Angehörige von Bildungs- und Forschungseinrichtungen

- Verlage und Bibliotheken – Content Provider (Springer, Elsevier, Nationallizenzen, ...)
- Verteilung lizenzierter Software (Microsoft Dreamspark)
- Hochschulinterne Dienste
- e-Learning-Plattformen
- Forschungsprojekte und -infrastrukturen
- Sync & Share Dienste (z.B. Gigamove)
- Landesdienste
- Webkonferenzen u.a.m.

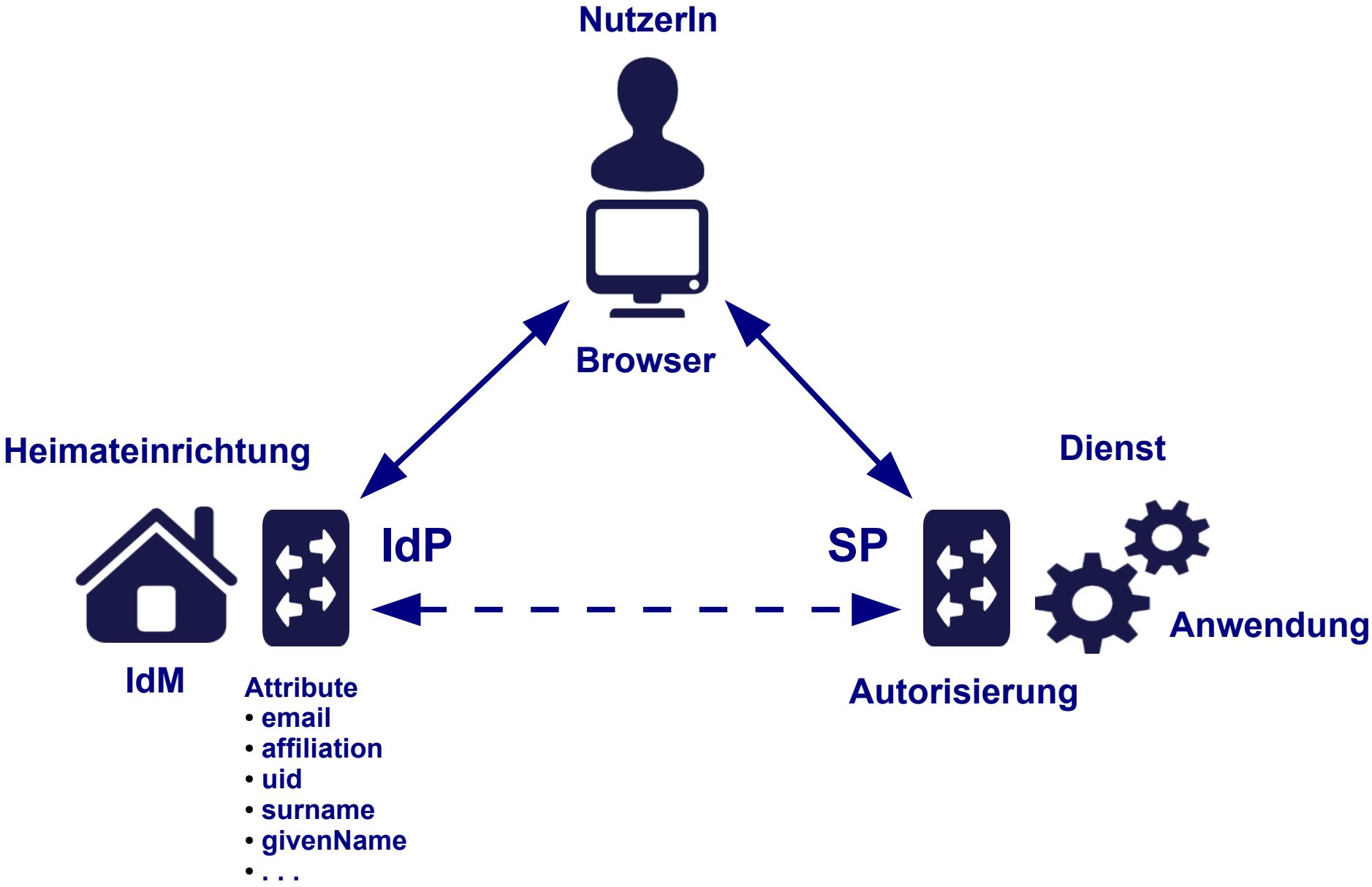
siehe auch https://www.aai.dfn.de/verzeichnis/ und https://www.aai.dfn.de/teilnahme/dienste-nutzen/

Web-SSO = Dreiecksbeziehung

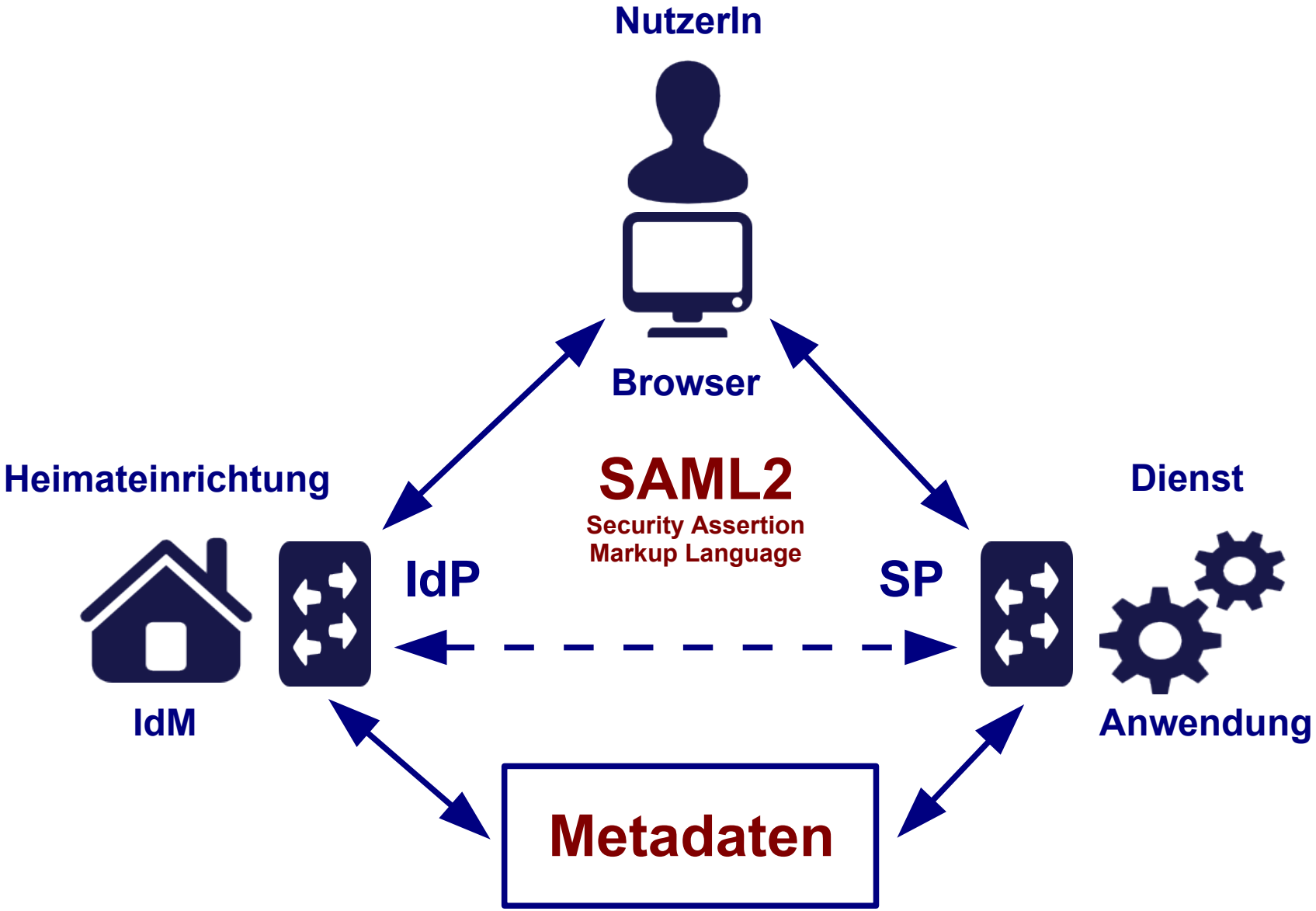


Icons: http://www.visualpharm.com/

Dreiecksbeziehung im Detail



Lingua franca: SAML(2)



Siehe auch: https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

SAML

- Steht für: **S**ecurity **A**ssertion **M**arkup **L**anguage
- XML-Framework (offener Standard bei OASIS), das aus mehreren Spezifikationen besteht
- Die wichtigsten Komponenten:
  - Metadata
  - Assertions + Protocols
  - Bindings
  - Profiles

Siehe https://www.oasis-open.org/standards#samlv2.0
bzw. https://wiki.oasis-open.org/security

Metadaten (1)

- Standardisiertes XML-Format (→ SAML)
- Enthalten alle Informationen, die für eine Kommunikation zwischen den beteiligten Entities (IdPs, SPs, Attribute Authorities) benötigt werden
- Eindeutiger Identifier: entity ID
  - Datentyp: anyURI (z.B. https://idp.dfn.de/idp/shibboleth)
  - Muss nicht auf eine Web-Ressource verweisen (Best Practice: IdP/SP-Metadaten), also auch nicht notwendigerweise dem Hostnamen der jeweiligen Entity entsprechen
  - Allerdings sollte die jeweilige Einrichtung auch die Rechte an der betreffenden Domain besitzen
  - Best Practice: Pro Dienst eine Entity ID (keine Proxies)
- Einführung und Überblick unter

  https://www.oasis-open.org/committees/download.php/51890/SAML%20MD%20simplified%20overview.pdf

Metadaten (2)

Was lässt sich mit (SAML-)Metadaten alles anstellen?

- Föderationen
  - Auf nationaler Ebene (z.B. DFN-AAI)
  - Lokal (Einrichtung)
  - „Virtuelle Subföderationen“ (z.B. auf Länder- oder Projekt-Ebene)
- Interföderation, föderationsübergreifende AAI (z.B. eduGAIN)

Föderation

- Das **technische** Rückgrat einer Föderation stellen die Metadaten dar:
  Nur wenn auf beiden Seiten (IdP, SP) die Metadaten des jeweiligen Kommunikationspartners bekannt sind (und ihnen vertraut wird), funktioniert die Kommunikation!
- Der DFN als Föderationsbetreiber schafft das notwendige **Vertrauensverhältnis:**
  - Verträge mit allen Teilnehmern
  - Metadatenverwaltung
  - Zertifikatsüberpüfung und -überwachung
  - **Signierte Metadaten**

Föderation(en) + Metadaten in der DFN-AAI

- Organisatorisch handelt es sich bei der DFN-AAI um **eine** Identity Federation, die **mehrere** Metadatensätze verwaltet und zur Verfügung stellt:

Föderationen

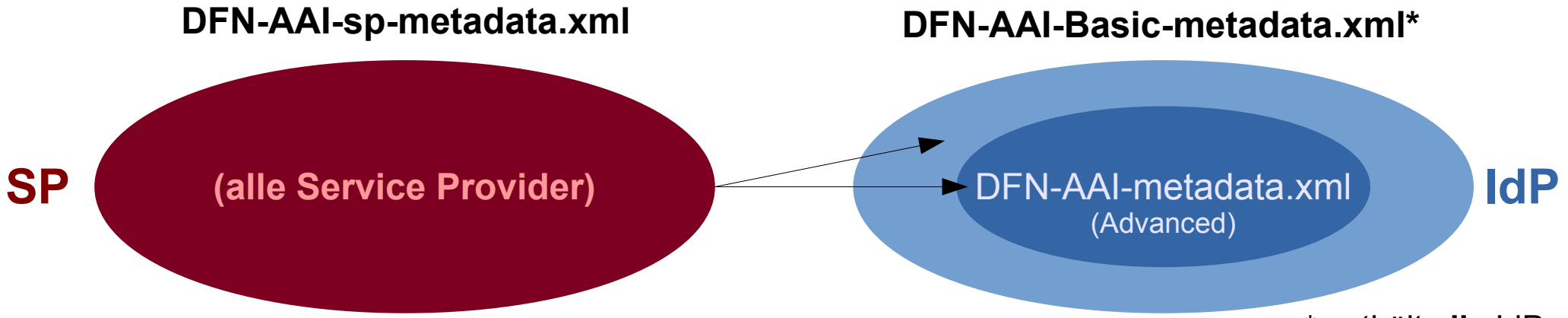
Typ	Aktivierung	Name	Status	Kommentar
Produktion: DFN-AAI	◉	DFN-AAI	zugelassen	
	○	DFN-AAI-Basic		
	○	keine		
	☐	lokale Metadaten		
Produktion: Interföderation	☐	eduGAIN		
Test	☑	DFN-AAI-Test	zugelassen	

schreiben | schreiben & zurück | **abbrechen**

Metadaten in der DFN-AAI

- Liste unter https://wiki.aai.dfn.de/de:metadata
- Testföderation: https://www.aai.dfn.de/fileadmin/metadata/DFN-AAI-Test-metadata.xml
- Produktivföderation, nach Verlässlichkeitsklassen, SP- und IdP-spezifisch, siehe https://www.aai.dfn.de/teilnahme/produktionsbetrieb/

Provider-Typ	"Advanced"	"Basic"	"Advanced + Basic"	eduGAIN
Identity Provider (IdP)	DFN-AAI-sp-metadata.xml	DFN-AAI-sp-metadata.xml	--	DFN-AAI-sp-metadata.xml DFN-AAI-eduGAIN+sp-metadata.xml
Service Provider (SP)	DFN-AAI-metadata.xml	--	DFN-AAI-Basic-metadata.xml	DFN-AAI-Basic-metadata.xml DFN-AAI-eduGAIN+idp-metadata.xml



* enthält **alle** IdPs

Lokale Metadaten (= Mini-Föderation)

- Einrichtungs-spezifischer Metadatensatz, in dem interne SPs sowie der jeweilige IdP registriert sind
- Metadaten werden stündlich neu generiert und signiert, bei Bedarf Zugriff nur für bestimmte IP-Bereiche
- Validierung der Metadaten, automatische Zertfikat-Checks
- Lohnt sich vor allem für Einrichtungen mit vielen lokalen SPs (z.B. FU Berlin mit 105 SPs)
- Angebot wird derzeit von 70 Einrichtungen mit insgesamt 536 SPs genutzt
- Doku: https://wiki.aai.dfn.de/de:metadata_local

Konfiguration lokale Metadaten

Konfiguration über Schaltfläche in Vertragsdaten erreichbar:

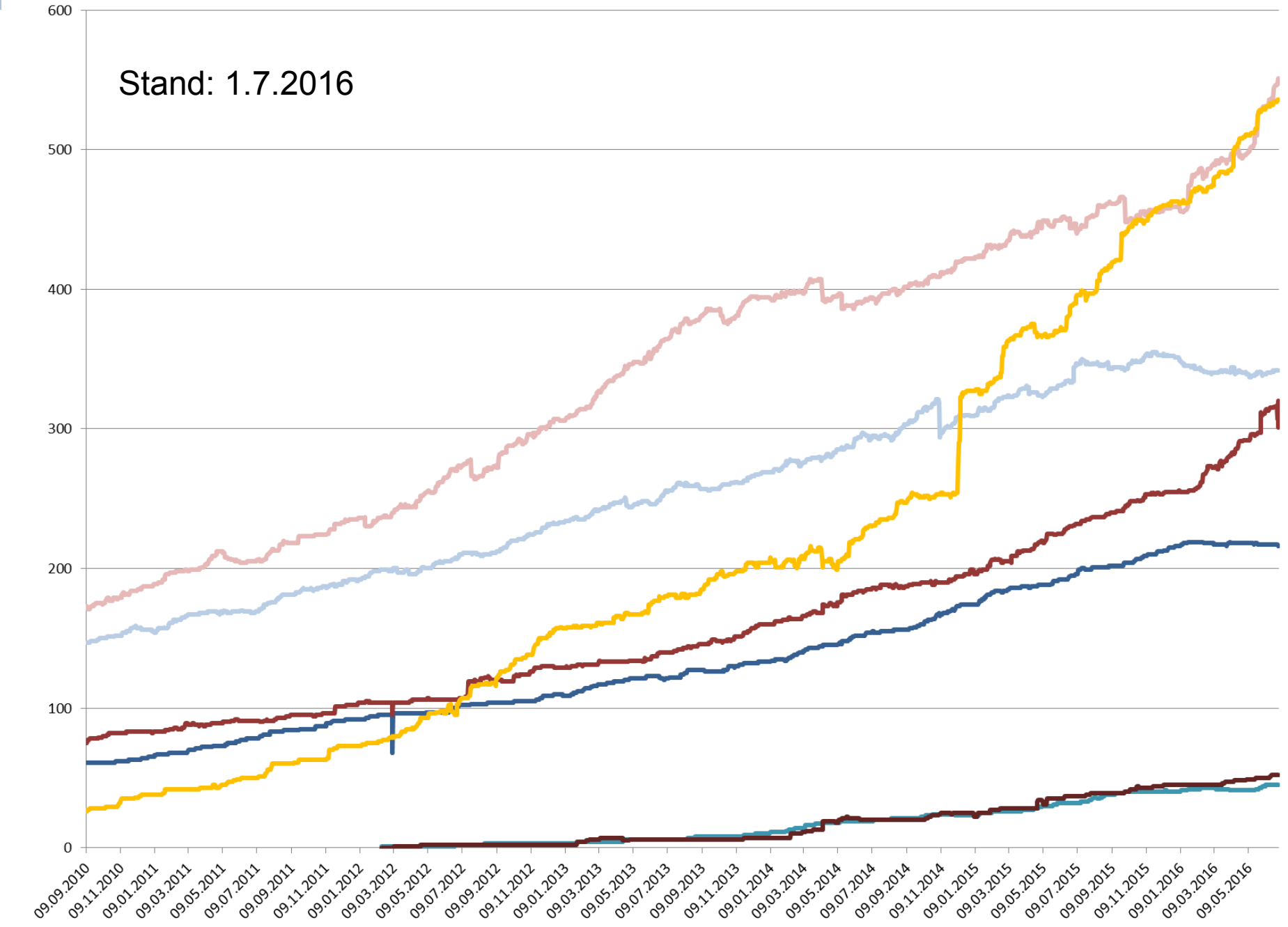
Verlässlichkeitsklasse	lokale Metadaten	
Advanced	aktiviert download	

dann:

Vertragsdaten editieren

Nummer	AAI10
Einrichtung	Verein zur Förderung eines Deutschen Forschungsnetzes, Berlin
Kontakt	Ulrich Kähler, (0 30) 88 42 99-35, kaehler@dfn.de
Verlässlichkeitsklasse	Basic ◉ Advanced
Service Provider	Vertrag vorhanden / Vertragssoption aktiviert
lokale Metadaten	☑ aktivieren
Zugang zu lokalen Metadaten auf IP Bereich(e) beschränken	
schreiben	**abbrechen**

DFN-AAI – registrierte Entities



produktiv

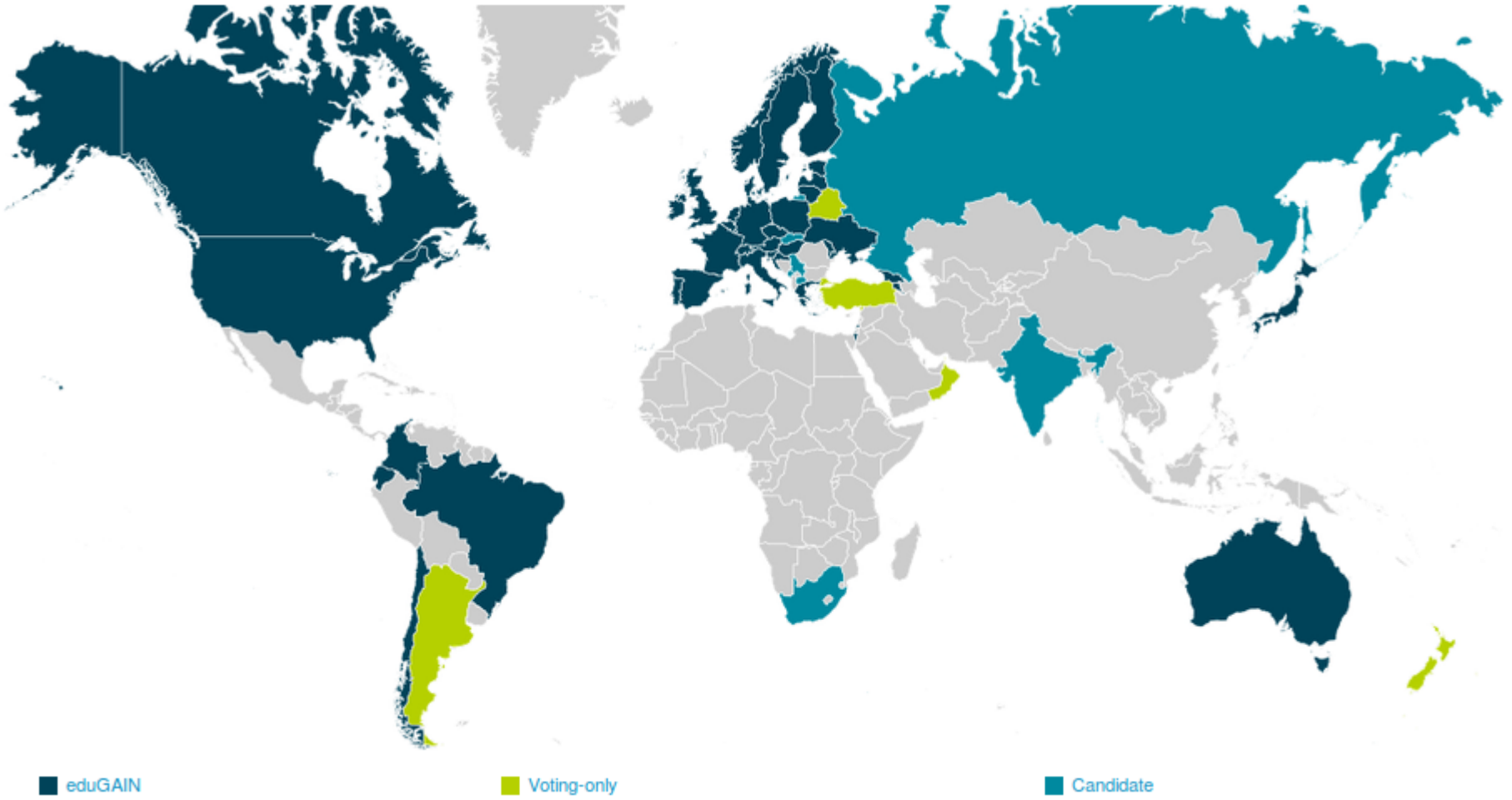
IdP: 216

SP: 301

lokale SPs: 536

Interföderation - eduGAIN

Föderationsübergreifende AAI (Interfederation)



Doku: https://technical.edugain.org/ und https://wiki.edugain.org sowie https://www.aai.dfn.de/teilnahme/interfederation/

Virtuelle Subföderation (1)

- Wird **nicht** über eigenen Metadatensatz modelliert
- Stattdessen kommt ein spezielles Entity Attribut zum Einsatz, eine sog. Entity Category, die in den IdP-/SP-Metadaten gesetzt wird
- Diese Entity Category erlaubt IdP- und SP-seitiges Filtern:
  - SP: Positivauswahl teilnehmender IdPs/Einrichtungen
  - IdP: Erleichterte Attributfreigabe, eine Regel für alle Projekt-SPs
- Vergabe wird anhand projektspezifischer Whitelist in der Metadatenverwaltung kontrolliert
- Einsatzgebiet: Landesprojekte (u.a.m.)

Virtuelle Subföderation (2)

DFN Deutsches Forschungsnetz

Beispiel:
Projektspezifische Entity Category für bwIDM

```
<EntityDescriptor entityID="https://bwidm.scc.kit.edu/sp">
   <Extensions>
      <mdattr:EntityAttributes>
        <saml:Attribute Name="http://macedir.org/entity-category"
           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
          <saml:AttributeValue>http://aai.dfn.de/category/bwidm-member</saml:AttributeValue>
        </saml:Attribute>
      </mdattr:EntityAttributes>
   </Extensions>
```

- Weitere Anwendungsfälle:
  - Niedersachsen (ndsIDM, produktiv)
  - Sachsen (saxID, in Vorbereitung)
- Föderationsseitig schnell implementiert
- Wünsche bitte an hotline@aai.dfn.de richten

Metadatenverwaltung – Front-End

Logo klein (URL) preview:	https://bwlp-masterserver.ruf.uni-freiburg.de/img/bwLehrpool_16
Logo groß (URL) preview:	https://bwlp-masterserver.ruf.uni-freiburg.de/img/bwLehrpool_35
Helpdesk (erg. Angaben zu Kontakte - Support)	bwlehrpool@hs-offenburg.de

Entity-Kategorien

http://aai.dfn.de/category/bwidm-member

Neuer Wert

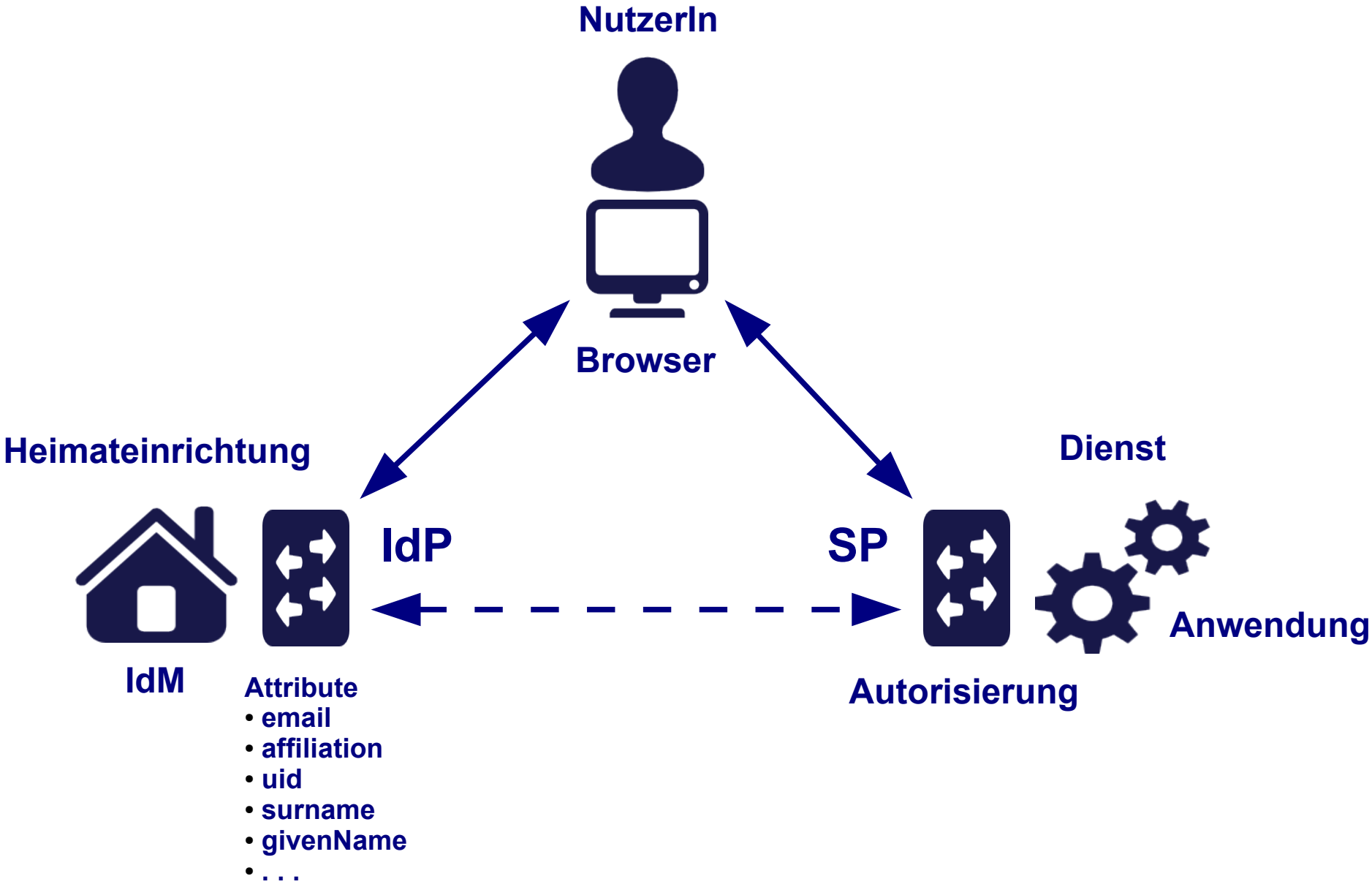
☐ **REFEDS Research & Scholarship (R&S) Entity-Kategorie beantragen:**

The REFEDS Research and Scholarship (R&S) Entity Category is applicable to Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management as an essential component. This Entity Category should not be used for access to licensed content such as e-journals.

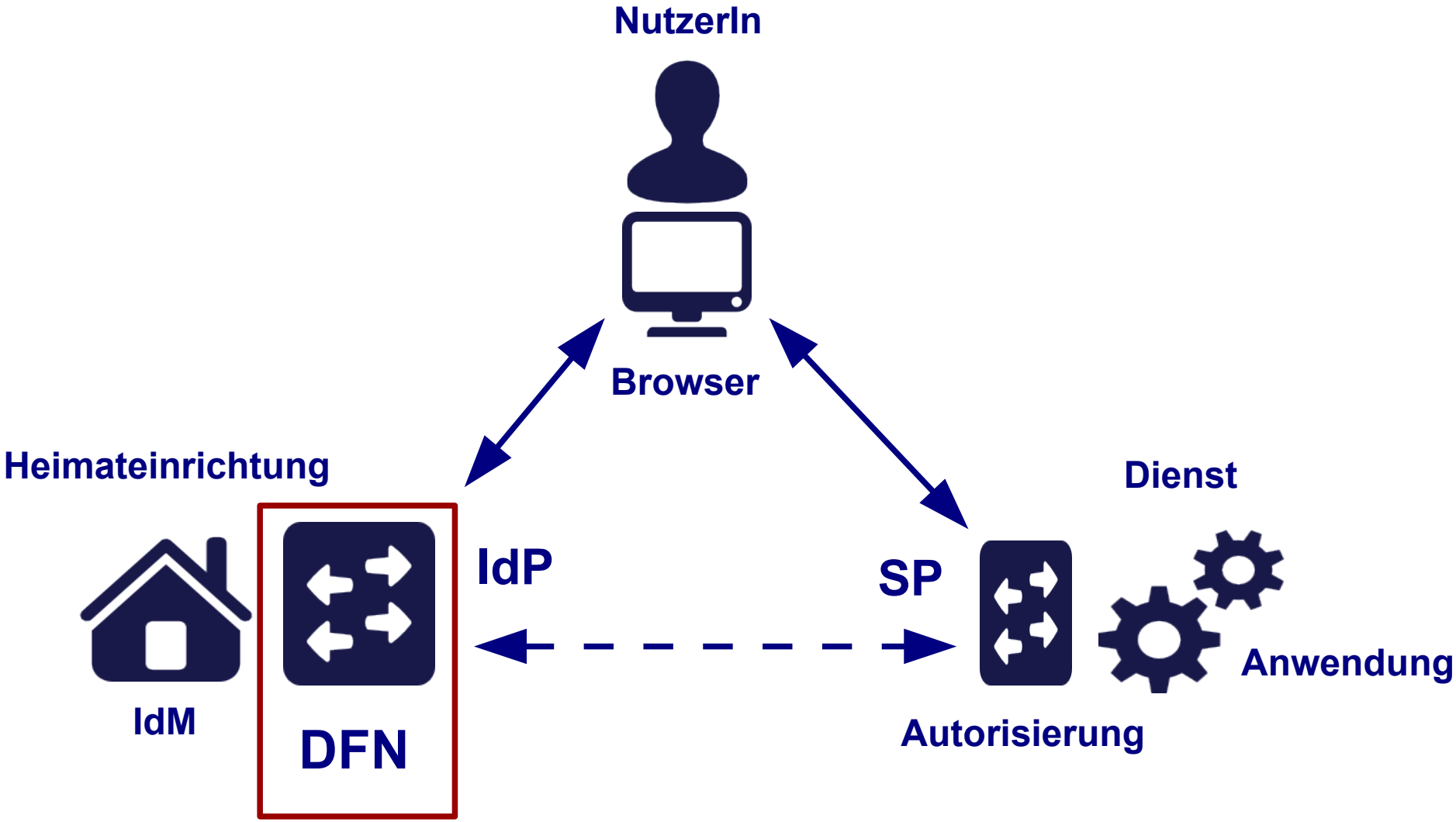
Ausgelagerter IdP

https://www.aai.dfn.de/der-dienst/ausgelagerter-idp/

Wir erinnern uns ...



IdP-Hosting seitens des DFN



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

Der Dienst

- Dienst des DFN-Vereins seit Sommer 2010
  (aktuell 26 im Produktivbetrieb, 1 weiterer im Aufbau)
- Vertraglich über DFN-AAI Dienstvereinbarung abgedeckt
- DFN-Verein konfiguriert den IdP in Rücksprache mit Anwender
- DFN-Verein stellt mit Anwender die Anbindung an dessen IdM bzw. Nutzerverzeichnis her
- Auf Wunsch Übertragung der Logfiles
- Wartung, Betrieb, Updates durch DFN-Verein
- **Obacht!** Verarbeitung personenbezogener Daten seitens des DFN-Vereins
- Vorteil für Anwender / Heimateinrichtung:

  Kein Shibboleth-Know-How erforderlich

Datenschutz und -verarbeitung

- Der DFN-Verein verarbeitet personenbezogene Daten
  - User ID und Passwort
  - Zugriff auf IdM / Nutzerverzeichnis(se)
  - Log Files (je nach Debug Level)
  - MySQL-DB für User Consent
  - MySQL-DB für Persistent ID (optional)
- Dienstvereinbarung DFN-AAI:

  “Zum Zwecke der Nutzung des DFN-Shibboleth-IdP übermittelt der Teilnehmer dem DFN-Verein in der Regel auch personenbezogene Daten der Nutzer zum Zwecke der automatisierten Verarbeitung und weiteren Übermittlung an Anbieter. Der Teilnehmer gewährleistet insoweit die rechtliche Zulässigkeit, in der Regel wird hierzu die Einwilligung der Nutzer benötigt.”
- Nutzungsbestimmungen müssen dementsprechend formuliert werden → User Consent (vormals uApprove)

Terms of Use

DFN-AAI

Nutzungsbedingungen für den Identity Provider der Universität Bayreuth

Version 1.0 in der Fassung vom 27.01.2014

1. Der Identity Provider (IdP) der Universität Bayreuth dient der Authentifizierung und Autorisierung der Mitarbeiterinnen und Mitarbeiter der Universität Bayreuth gegenüber Dienstanbietern, sogenannten Service Providern (SP), im Rahmen der DFN-AAI. Die Authentifizierungs- und Autorisierungs-Infrastruktur DFN-AAI wird vom DFN-Verein (Verein zur Förderung eines Deutschen Forschungsnetzes e.V.) verwaltet. Die DFN-AAI sorgt für das notwendige Vertrauensverhältnis zwischen Einrichtungen und Anbietern in der DFN-AAI.

   Der IdP der Universität Bayreuth wird vom DFN-Verein im Auftrag der Universität Bayreuth betrieben und sorgt für den Austausch von Benutzerinformationen der Angehörigen der Universität Bayreuth und den Dienstanbietern in der DFN-AAI.

   Die Universität Bayreuth behält sich vor, diese Bestimmungen ohne vorherige Ankündigung zu ändern oder zu ergänzen.

2. Um den Dienst des IdP in der DFN-AAI nutzen zu können benötigen Sie eine gültige Benutzerkennung im Identity Management (IDM) der Universität Bayreuth.

Informationsquellen

- DFN-AAI Wiki
  https://wiki.aai.dfn.de/de:start
  Änderungsfeed
  https://wiki.aai.dfn.de/feed.php
- Materialien aus anderen Veranstaltungen (BT, Workshops)
  https://www.aai.dfn.de/aktuelles/archiv/
- Shibboleth Wiki
  http://wiki.shibboleth.net/
- Online-Doku SWITCHaai
  https://www.switch.ch/aai/guides/

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