Grundlagen

AAI, Web-SSO, Metadaten und Föderationen

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

Workshop: DFN-AAI Authentifizierung Hessenbox

15./16. November 2017, HS Darmstadt

Einführung
und
Überblick

Begriffsbestimmung (1)

- **„Shibboleth“** ist eigentlich eine Software …
  (Bezeichnung geht zurück auf Bibel: Richter 12,5-6)
- … wird aber häufig synonym für **SAML**-basiertes **Web-SSO** verwendet
- **SAML** = **S**ecurity **A**ssertion **M**arkup **L**anguage
- **Web-SSO** = Web **S**ingle **S**ign-**O**n
  - Einmal anmelden für 1..n Dienste, für die man zugriffsberechtigt ist
  - Keine dienstspezifischen Credentials, da Login nur bei der Heimatorganisation stattfindet
- Diese Mechanismen und Standards kommen innerhalb einer **AAI** zum Tragen

Begriffsbestimmung (2)

- **AAI** =
  Authentication and **A**uthorization **I**nfrastructure
- Eine AAI kann lokal oder auch Einrichtungs-übergreifend betrieben werden
- Im letztgenannten Fall bedarf es einer *zentralen Instanz*, die als AAI-Betreiber die Einhaltung der technischen und rechtlichen Rahmenbedingungen sicherstellt und auf diese Weise ein Vetrauensverhältnis etabliert
- Dies ist in der Regel eine sog. **Identity Federation**, bzw. einfach „**Föderation**“
- Eine solche Föderation ist z.B. die **DFN-AAI**

Worum geht es in der (DFN-)AAI?

- Zugriff auf **Dienste** via
  - Web-SSO
  - (Non-Web-SSO)
- Technisch: **Metadaten**
- Organisatorisch: **Vertrauen**
- **Zusammenarbeit** lokal, aber v.a. auch über Einrichtungs- und ggf. Föderations-Grenzen hinweg
- Datenschutz bzw. **Datensparsamkeit**: Nutzername + Passwort werden nicht an Dienste übertragen (u.a.m.)

Welche Arten von Diensten?

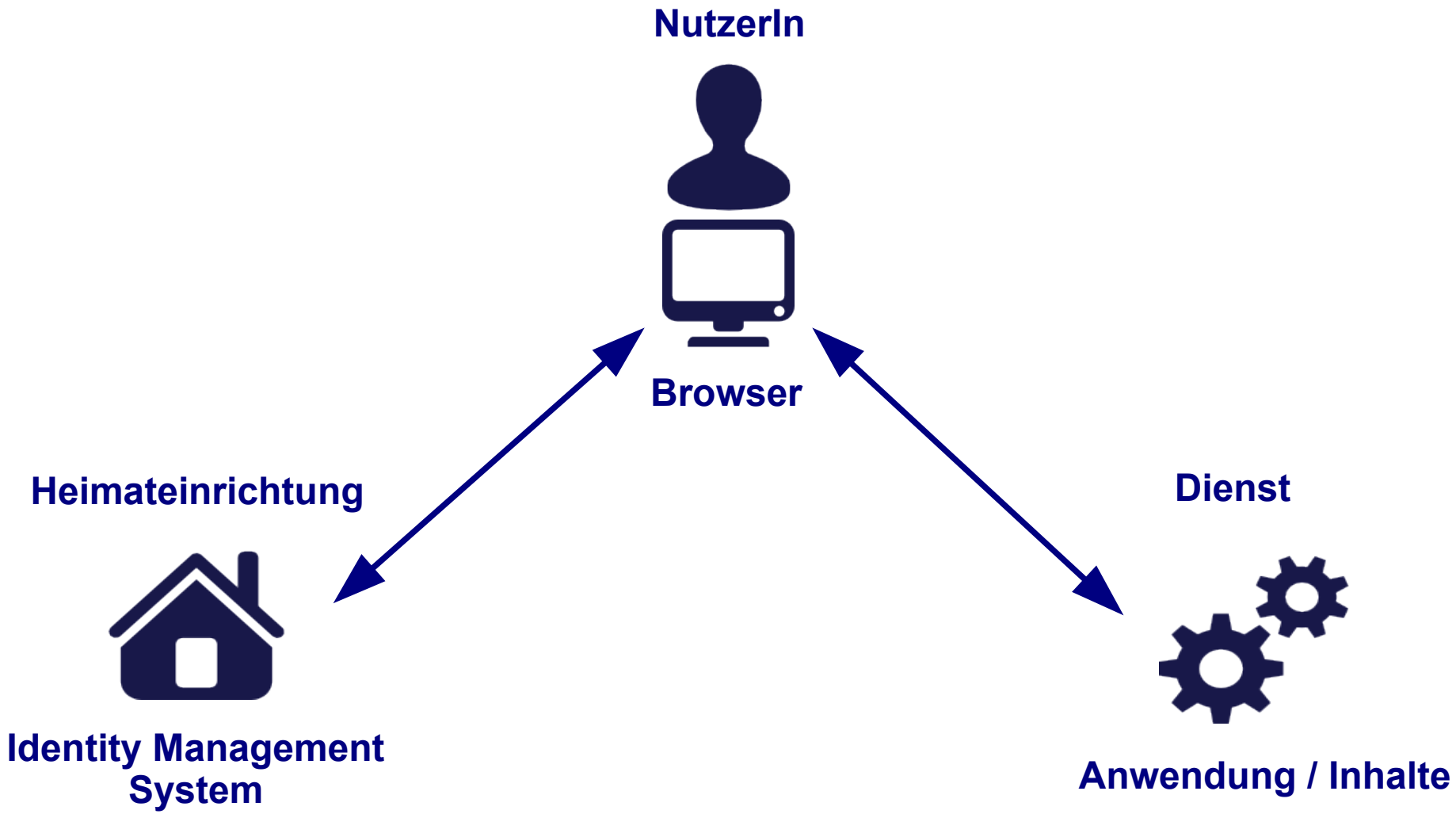
Zielgruppe: Angehörige von Bildungs- und Forschungseinrichtungen

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

siehe auch https://www.aai.dfn.de/verzeichnis/ und https://wiki.aai.dfn.de/de:access_services („Dienste nutzen“)

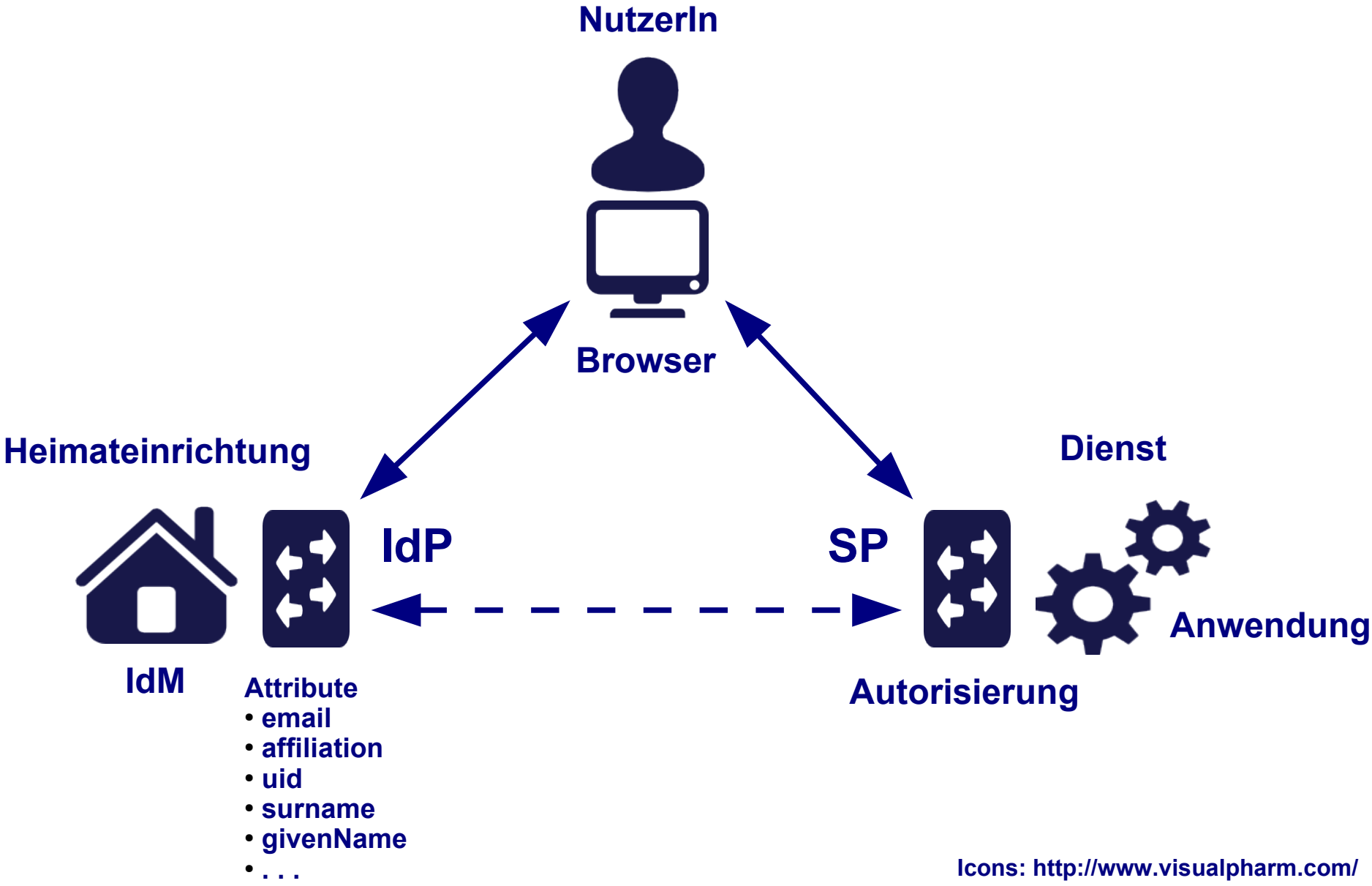
Dienste und Nutzergruppen

Web-SSO = Dreiecksbeziehung



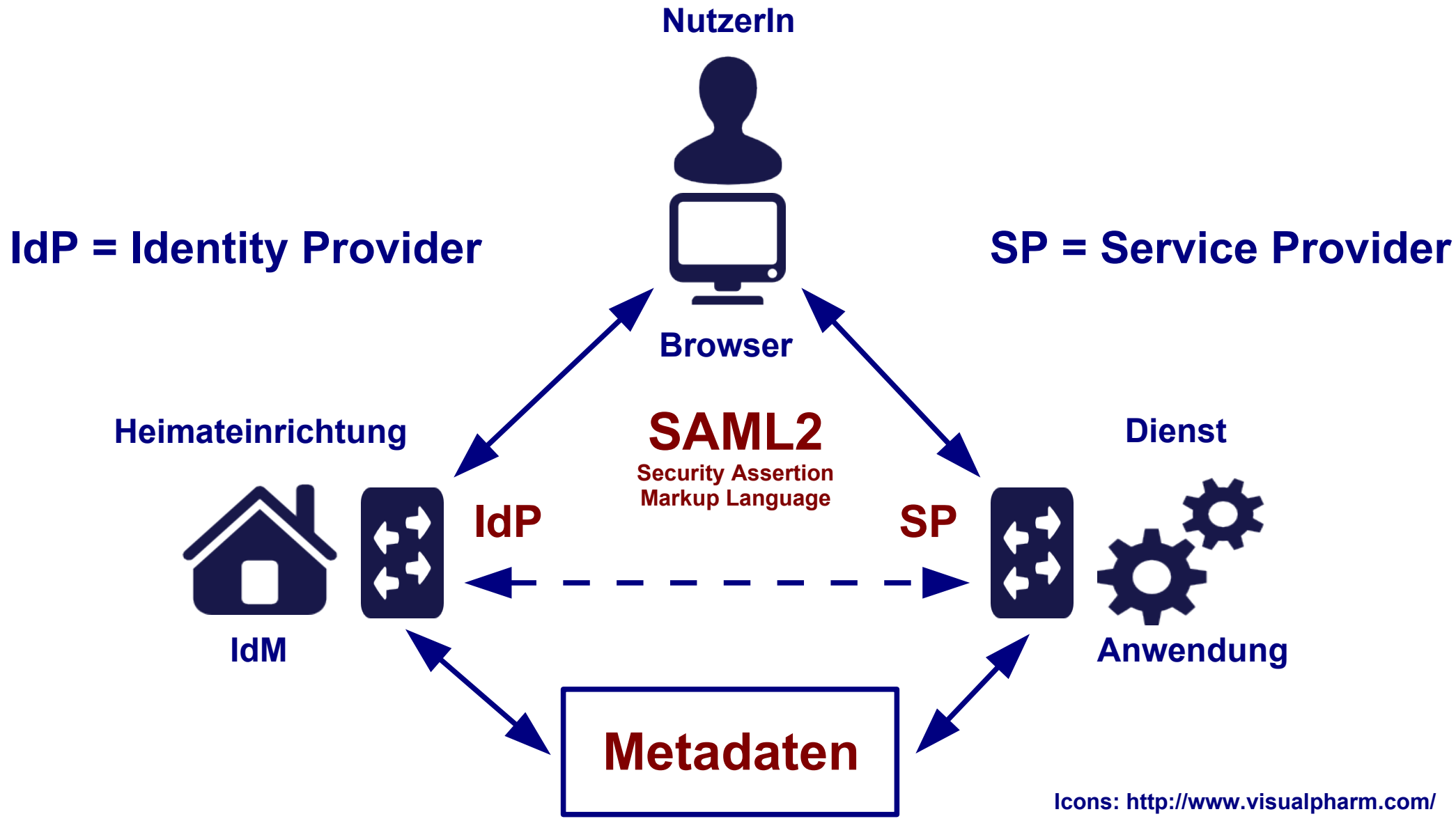
Icons: http://www.visualpharm.com/

Dreiecksbeziehung im Detail



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

Lingua franca: SAML(2)



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

SAML2

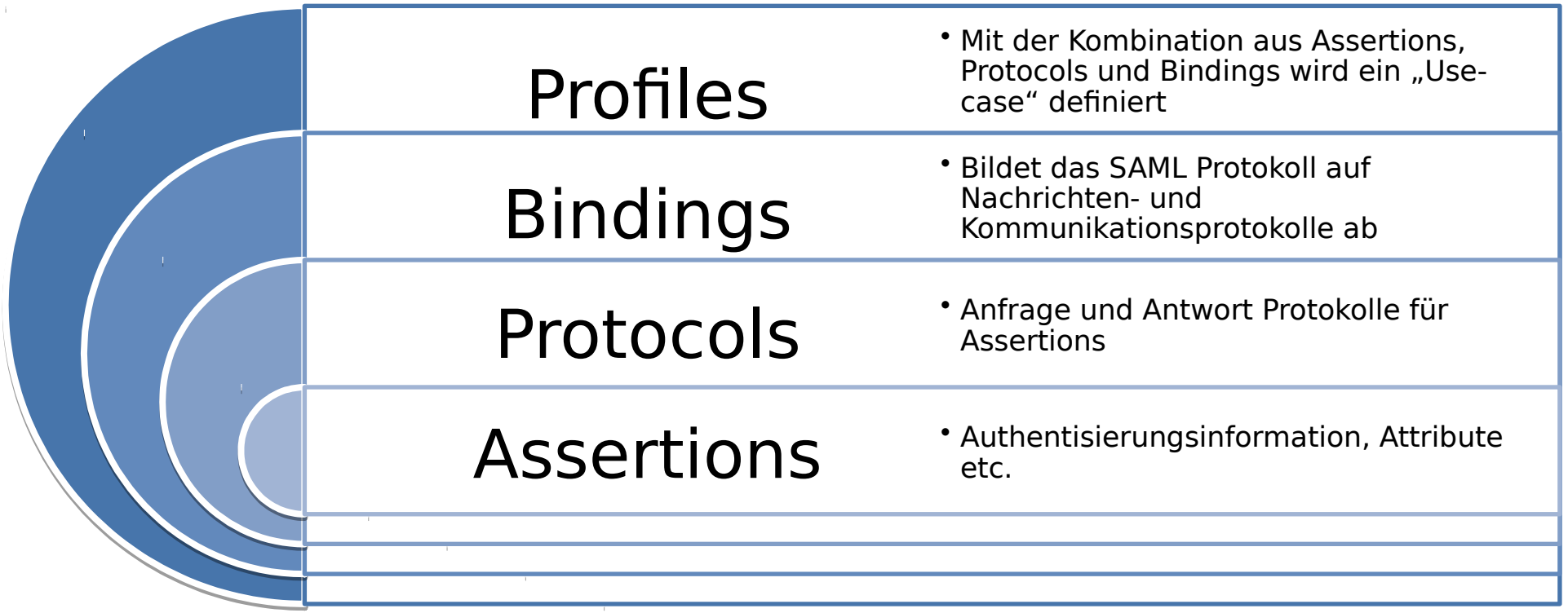
Security Assertion Markup Language

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

SAML Komponenten



Authentication Context

- Definiert Art und Weise der Authentifizierung

Metadata

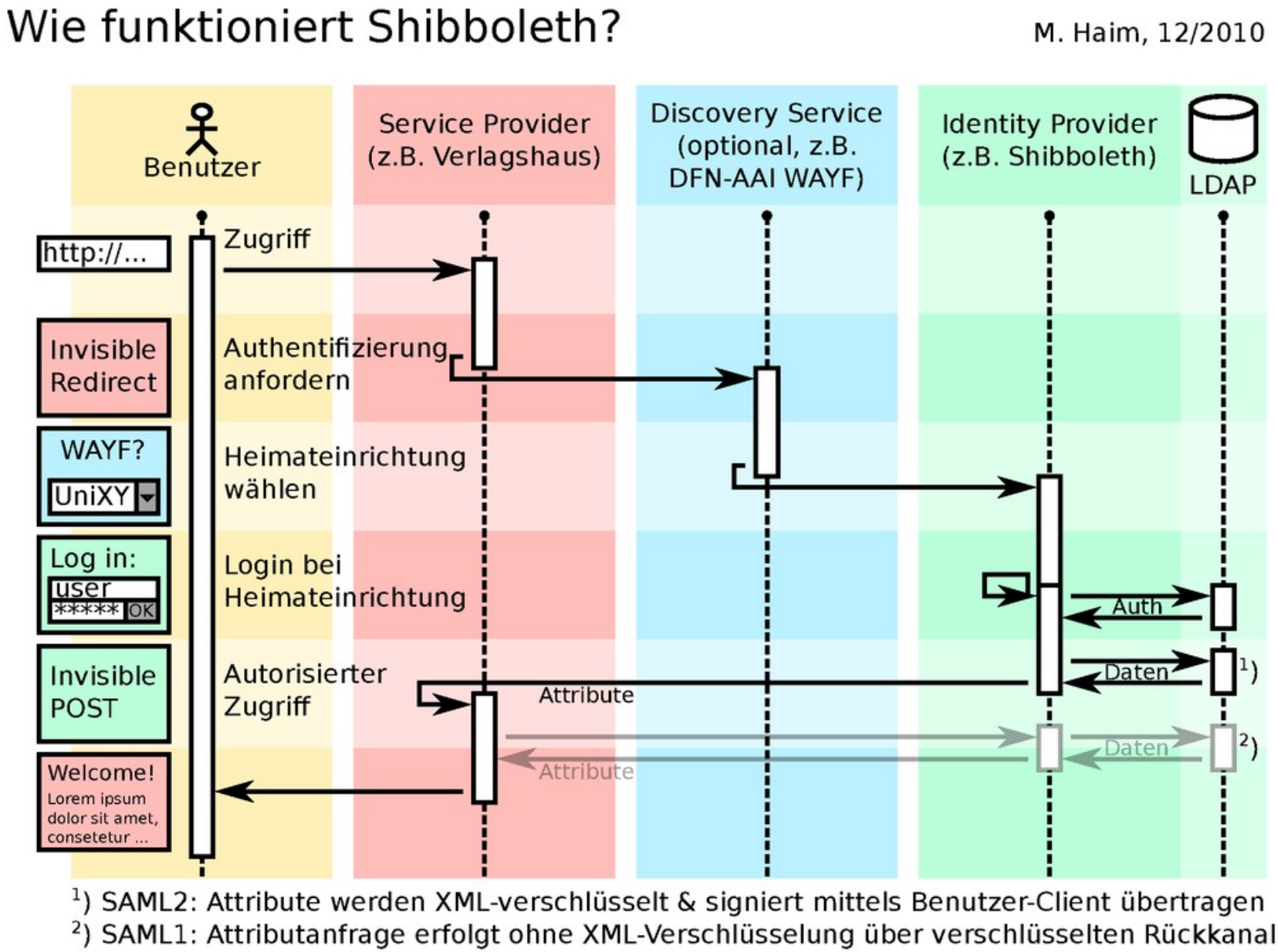
- Konfigurationsdaten für Service- und Identityprovider

Quelle: Michael Simon, KIT

Beispiel für SAML Profile: Web-SSO

- Bietet Single Sign-On für browser-basierte Webapplikationen
- Nutzer(in) mit Browser will auf eine geschützte Resource beim Service Provider (SP) zugreifen
- ... wird an einen Discovery Service weitergeleitet, dort Auswahl der Heimateinrichtung (Zuordnung zu IdP)
- ... wird zum Identity Provider (IdP) weitergeleitet
- ... authentisiert sich am IdP
- ... wird wieder zum Service Provider weitergeleitet
- Dabei kommen (z.B.) folgende Kombinationen zum Einsatz:
  - Protocol: Authentication Request Protocol
  - Binding: HTTP Redirect, HTTP POST, (HTTP Artifact)

Kommunikation im Detail



Quelle: Manuel Haim, Uni Marburg

SAML Metadaten

- 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://sso.h-da.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
- Einführung und Überblick unter

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

Typen von Entities

IdP = Identity Provider

- Liefert Informationen (*Assertions*) über Nutzer an SPs
  - Authentifizierung erfolgreich
  - Attribute (weitere Angaben, dienen der Autorisierung am SP sowie der Identifizierung des Nutzers / der Nutzerin bzw. der Personalisierung des betreffenden Dienstes)

Attribute Authority

- „Abgespeckter IdP“, liefert nur Attribute
- Direkter Zugriff seitens SP anhand einer *Name ID*

SP = Service Provider

- Schützt Ressourcen
- Wertet Assertions aus und reicht Attribute an die dahinterliegende(n) Anwendunge(n) weiter

Metadaten – typunabhängige Elemente

Wurzelelement

`<EntityDescriptor entityID="https://entity-xyz.de">`

Erweiterung gegenüber der ersten Fassung des Standards

`<Extensions>`

Informationen für User Interfaces

`<UIInfo>`

Zertifikate

`<KeyDescriptor>`

Benötigte / unterstützte Name Identifier

`<NameIDFormat>`

Kontaktdaten

`<Organization>`

`<ContactPerson>`

Metadaten – IdP und Attribute Authority

IdP Single Sign-On Descriptor (nur IdP)

```
<IDPSSODescriptor>
```

„Scope“ - Bezeichnung der Heimateinrichtung

```
<saml1md:Scope regexp="false">dfn.de</saml1md:Scope>
```

Bindings für SSO und SLO (Single Log-out)

```
<SingleSignOnService>

<SingleLogoutService>
```

Attribute Authority Descriptor (bei IdP optional)

```
<AttributeAuthorityDescriptor>
```

Bindings für Attribute Queries (bei IdP optional)

```
<AttributeService>
```

Metadaten – SP

SP Single Sign-On Descriptor

`<SPSSODescriptor>`

Bindings für die Entgegennahme von Assertions

`<AssertionConsumerService>`

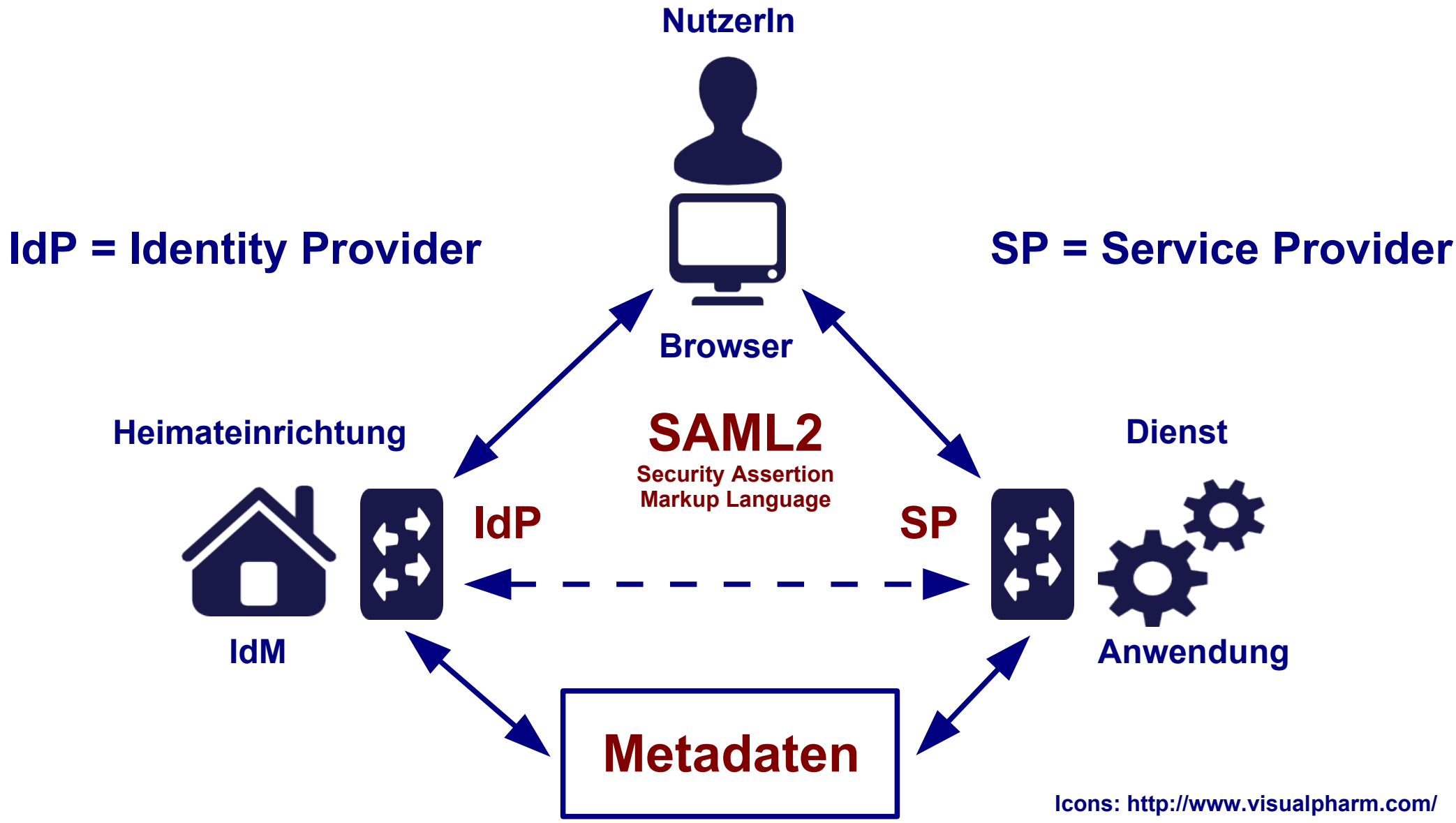
Bindings für SLO (Single Log-out)

`<SingleLogoutService>`

Deklaration der vom SP benötigten Attribute

`<AttributeConsumingService>`

Wir erinnern uns...



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

SAML-Kommunikation zw. SP und IdP/AA

Metadaten

- **IdP**
  (https://sso.h-da.de/idp/shibboleth)
- **Attribute Authority**
  (https://attributes.dfn.de/idp/shibboleth)
- **SP**
  (https://clarin.ids-mannheim.de/shibboleth)
- **Föderationsmetadaten**
  siehe unter
  https://wiki.aai.dfn.de/de:metadata

Metadaten und Föderationen

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)

Föderationen

DFN-AAI

https://www.aai.dfn.de

Föderation

- Das **technische** Rückgrat einer Föderation stellen die Metadaten dar:
  Nur wenn auf beiden Seiten (IdP/AA, 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 zwar um **eine** Identity Federation, die aber **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	

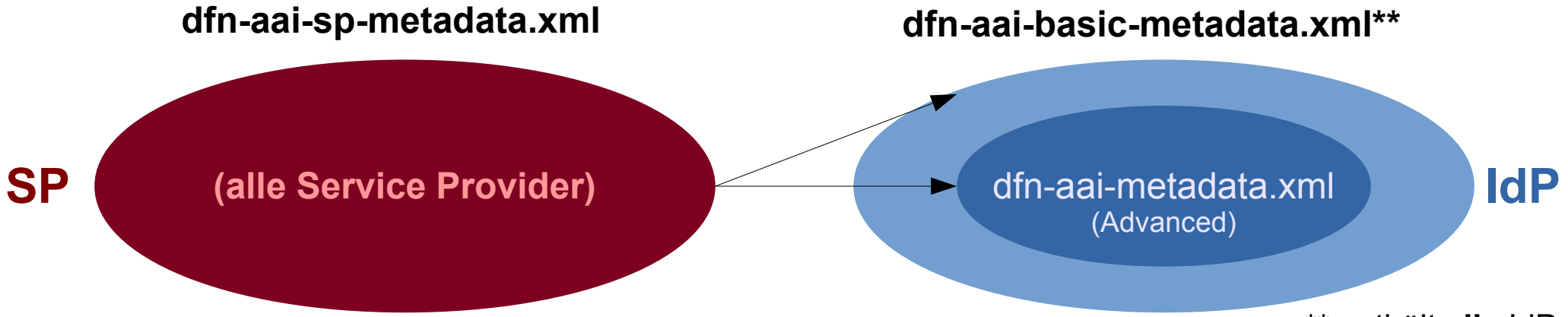
schreiben | schreiben & zurück | abbrechen

Metadaten in der DFN-AAI

- Liste unter https://wiki.aai.dfn.de/de:metadata
- Testföderation
- Produktivföderation, nach Verlässlichkeitsklassen, SP- und IdP-spezifisch, siehe https://wiki.aai.dfn.de/de:production

	IdP / AA	SP
Advanced	`dfn-aai-sp-metadata.xml`	`dfn-aai-metadata.xml`
Basic	`dfn-aai-sp-metadata.xml`	–
Advanced + Basic	–	`dfn-aai-basic-metadata.xml`
eduGAIN	`dfn-aai-edugain+sp-metadata.xml`	`dfn-aai-edugain+idp-metadata.xml`
Lokale Metadaten	`dfn-aai-local-999-metadata.xml*`	`dfn-aai-local-999-metadata.xml*`

* „999“ wird durch einrichtungsspez. Nummer ersetzt



** enthält **alle** IdPs

Exkurs: Klassen der Verlässlichkeit

Klasse	Identifizierung	AuthN	Datenhaltung und Prozesse zur Pflege der Identitäten
Test	...	...	...
Basic	Rückantwort von eindeutiger Adresse (eMail, Tel. Nr., Postanschrift, etc.)	Eindeutige digitale Adresse	Verpflichtung bzgl. Aktualität innerhalb von 3 Monaten
Advanced	pers. Vorsprechen gegenüber Vertrauensinstanz unter Vorlage amtlicher Dokumente (alternativ: Post-Ident, eID/nPA). **Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert**	pers. Account, Nutzername + Passwort bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Verpflichtung bzgl. Aktualität innerhalb von 2 Wochen

Siehe https://wiki.aai.dfn.de/de:degrees_of_reliance

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 über hundert SPs)
- Angebot wird derzeit (10.11.2017) von 95 Einrichtungen mit insgesamt 742 SPs genutzt
- Doku: https://wiki.aai.dfn.de/de:metadata_local

Konfiguration lokale Metadaten

Konfiguration über Schaltfläche in Vertragsdaten erreichbar:

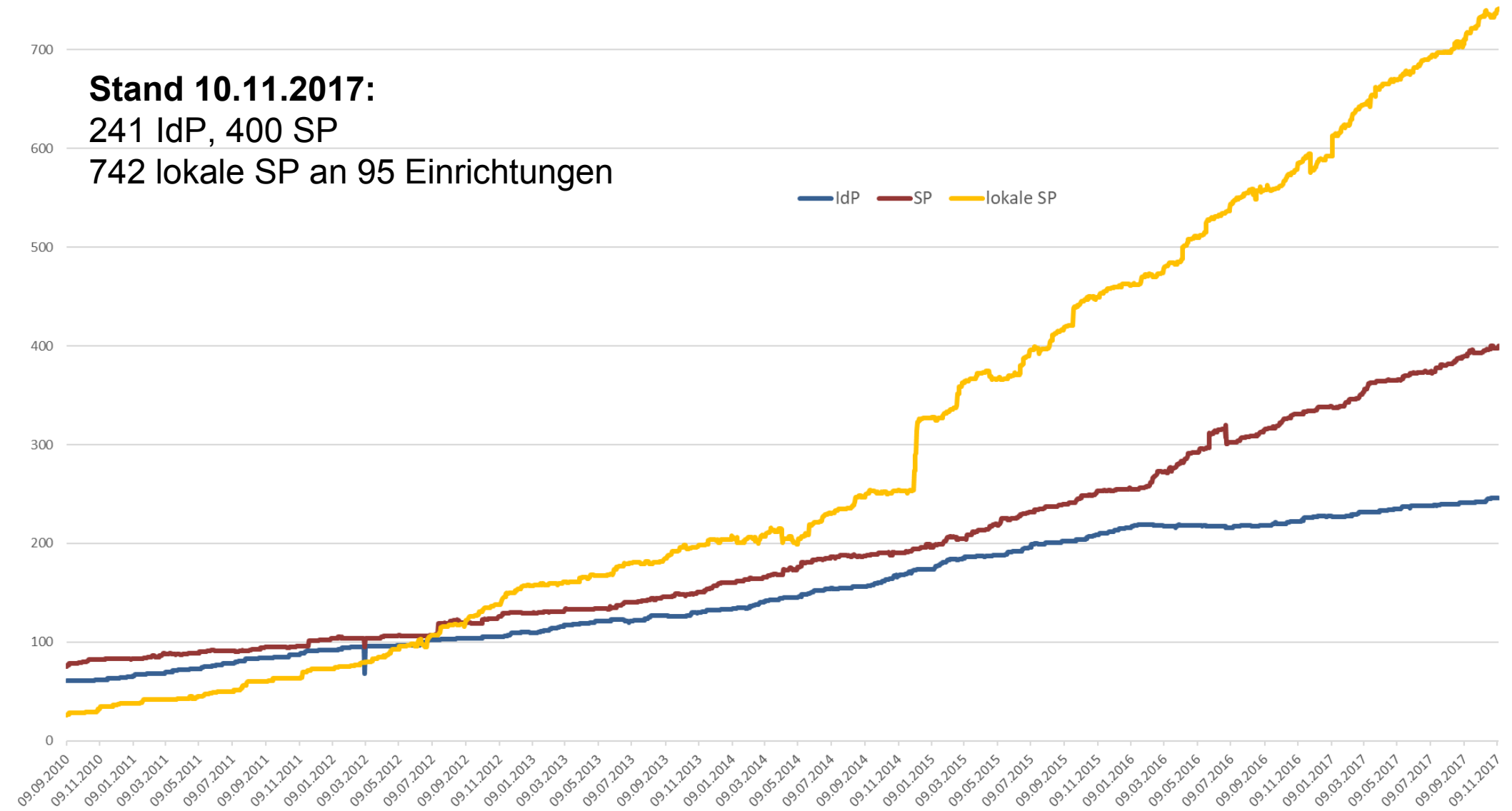
Verlässlichkeitsklasse	lokale Metadaten	
Advanced	aktiviert download	

dann:

Nummer	AAI10
Einrichtung	Verein zur Förderung eines Deutschen Forschungsnetzes, Berlin/Mitte
Kontakt	Heike Kaufmann, (0 30) 88 42 99-3 18, heike.kaufmann@dfn.de
Verlässlichkeitsklasse	Basic ◉ Advanced
Service Provider	Vertrag vorhanden / Vertragssoption aktiviert
lokale Metadaten	☑ aktivieren
Zugang zu lokalen Metadaten auf IP Bereich(e) beschränken (Hinweise zur Syntax)	
schreiben	**zurück zur Übersicht**

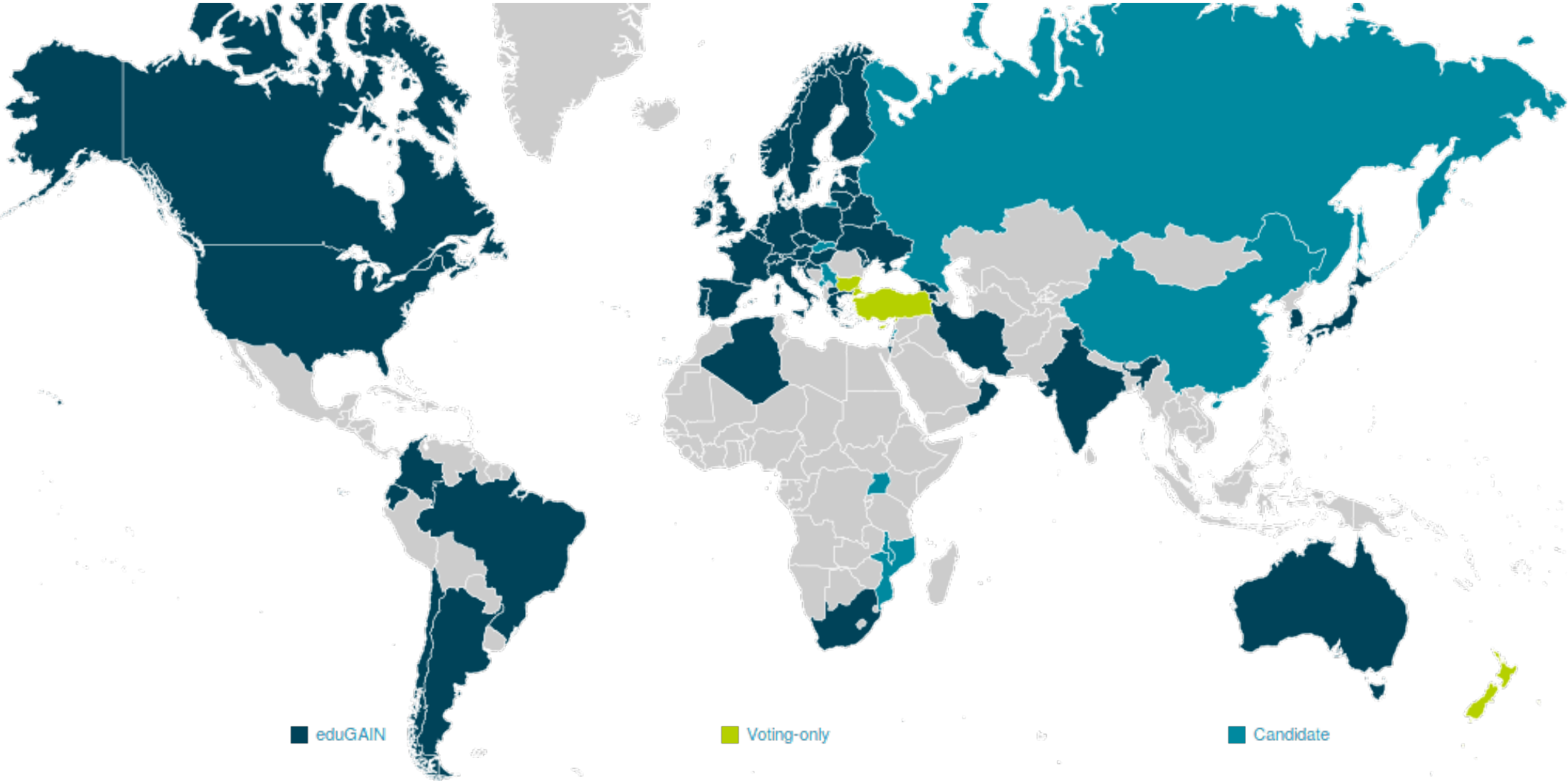
DFN-AAI – registrierte Entities

Stand 10.11.2017:
241 IdP, 400 SP
742 lokale SP an 95 Einrichtungen



Interföderation - eduGAIN

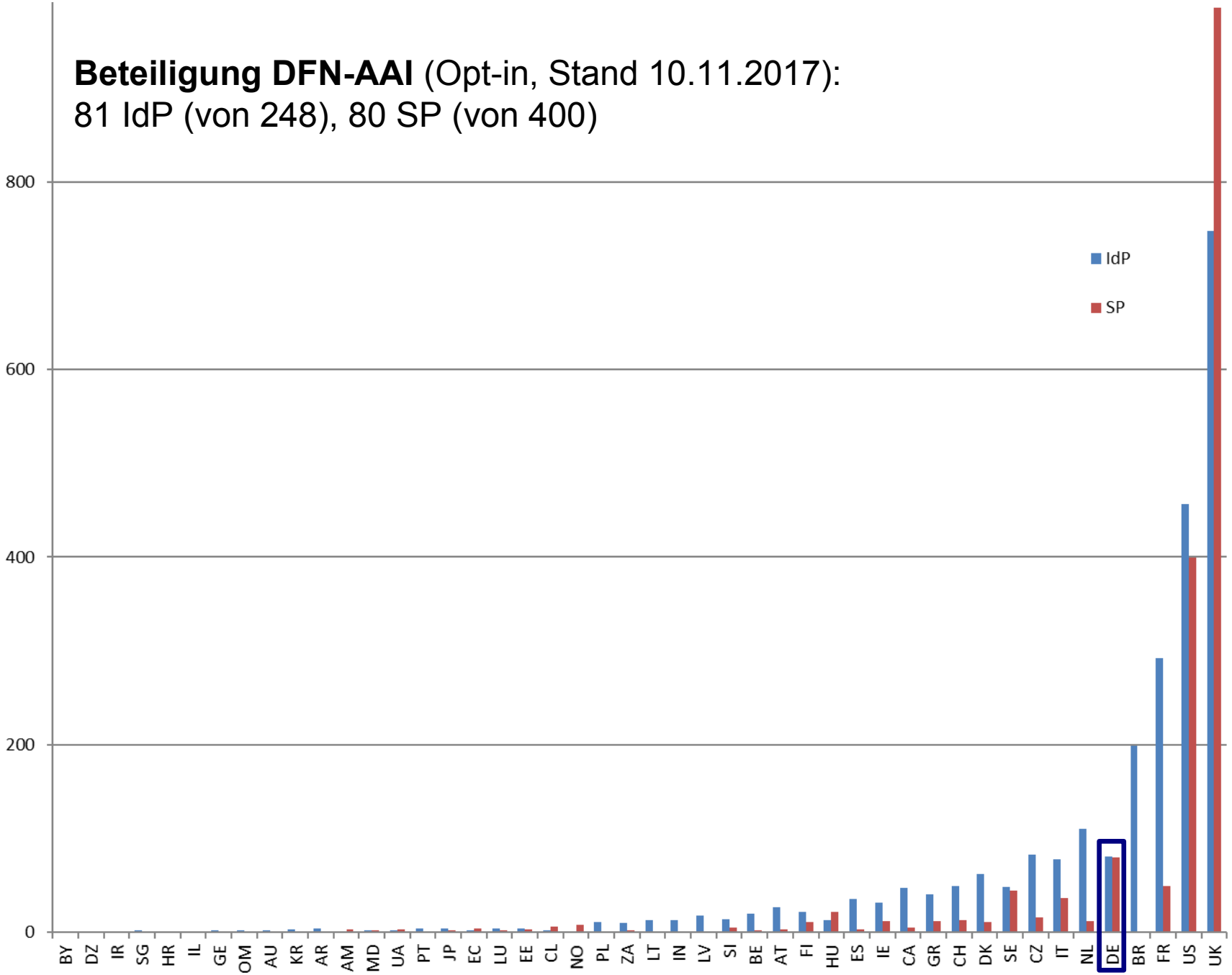
Föderationsübergreifende AAI über eduGAIN



Doku: https://technical.edugain.org/ und https://wiki.aai.dfn.de/de:edugain

eduGAIN - Beteiligung

Beteiligung DFN-AAI (Opt-in, Stand 10.11.2017):
81 IdP (von 248), 80 SP (von 400)



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.)

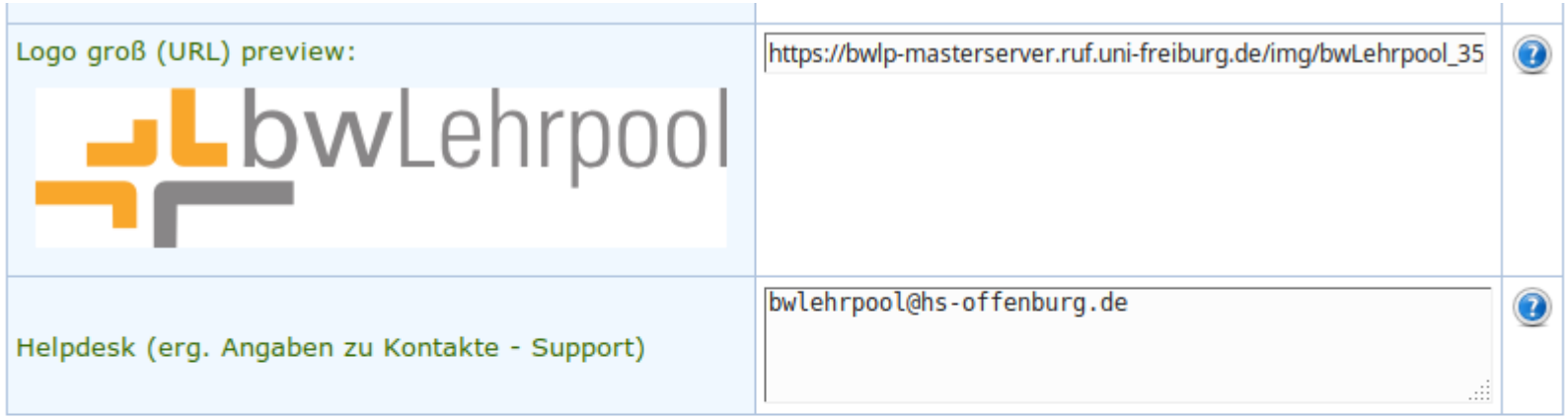
Virtuelle Subföderation (2)

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)
  - Virtuelle Hochschule Bayern (VHB)
- Föderationsseitig schnell implementiert
- Wünsche bitte an hotline@aai.dfn.de richten

Metadatenverwaltung – Front-End



Technische Infrastruktur

Bereits behandelt:

- Metadaten-Management
  - Mandantenfähiges System, das die Pflege der Daten seitens der Teilnehmer ermöglicht
  - Überprüfung und Kontrolle bzgl. Vollständigkeit, Standard-Konformität und Sicherheit (Zertifikate, Binding-URLs nur als https, etc.)
  - Stündliche Generierung und Signierung der Metadaten
- Produktivföderation in (derzeit noch) zwei Verlässlichkeitsklassen, „Advanced“ und „Basic“
- Testföderation inkl. Test-IdPs und -SPs
- Lokale Metadaten für einrichtungsinterne Dienste (inkl. .htaccess zum Schutz vor fremdem Zugriff)

Sonstige Dienste und Leistungen

- Discovery Service (”WAYF”)
  - Stündlich neu aus den jew. Metadatensätzen generiert
  - DFN-AAI (”Advanced”)
  - DFN-AAI-Basic
  - DFN-AAI-Basic+eduGAIN
  - DFN-AAI-Test
  - projektspezifische DS' anhand Whitelist
- Testumgebung
  - Testföderation, Test-IdPs und -SPs
- DFN-AAI Wiki: https://wiki.aai.dfn.de, wird unter Beteiligung der Community gepflegt und erweitert
- Mailinglisten: https://www.aai.dfn.de/mailinglisten/
- Support: hotline@aai.dfn.de
- Workshops, Schulungen (1x jährlich und auf Anfrage)

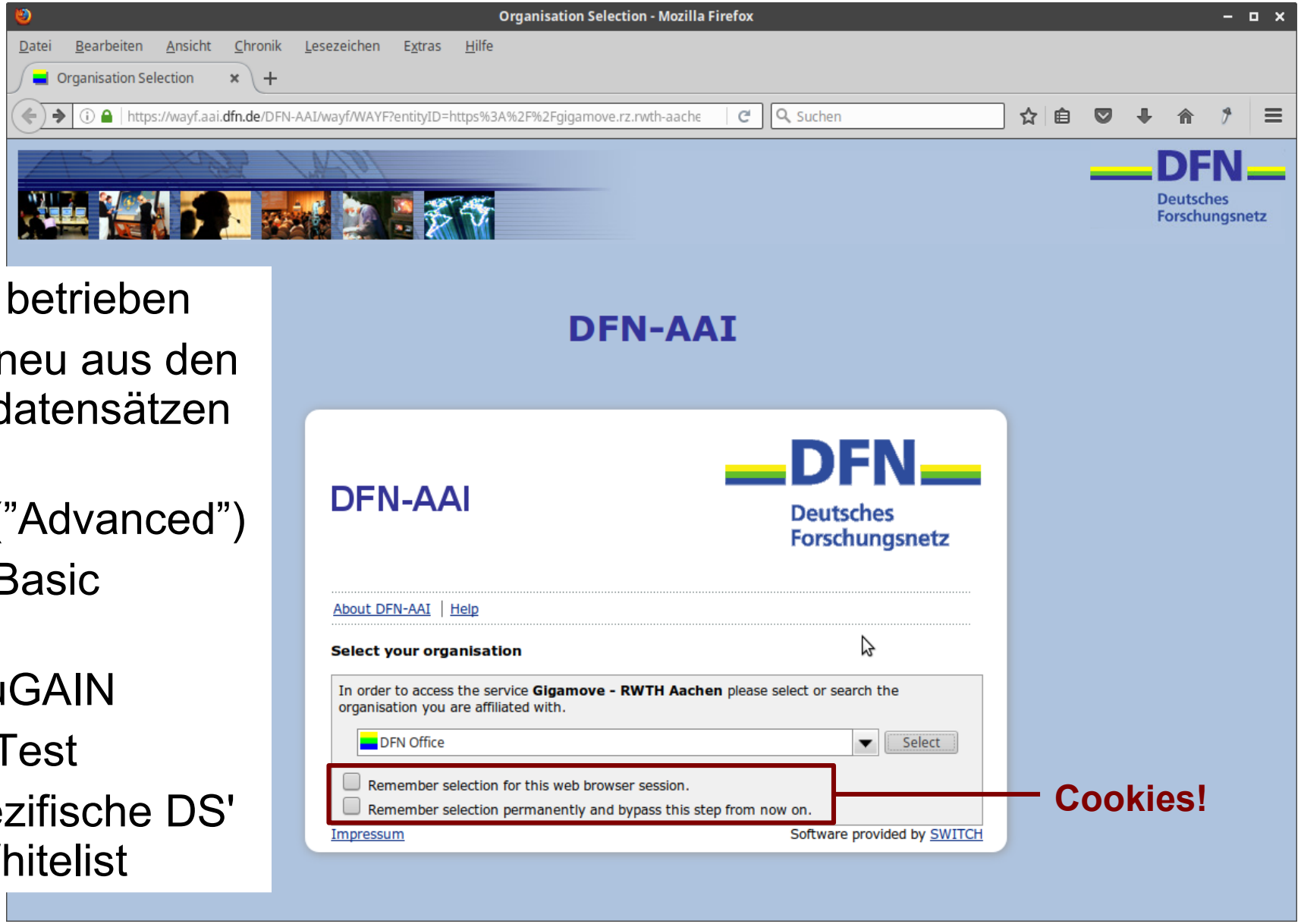
Discovery

Discovery Service

- Auch bekannt als WAYF,
  „**W**here **A**re **Y**ou **F**rom“
- Dient der Browser-gestützten Einrichtungsauswahl für den/die Endnutzer(in)
- Stellt Verbindung zwischen SP und IdP her
- Varianten:
  - Zentraler Discovery Service
    (z.B. von Föderation betrieben)
  - Emdedded Discovery Service (am SP)
  - WAYFless URLs
- DFN-AAI Wiki: https://wiki.aai.dfn.de/de:discovery

Beispiel zentraler Discovery Service

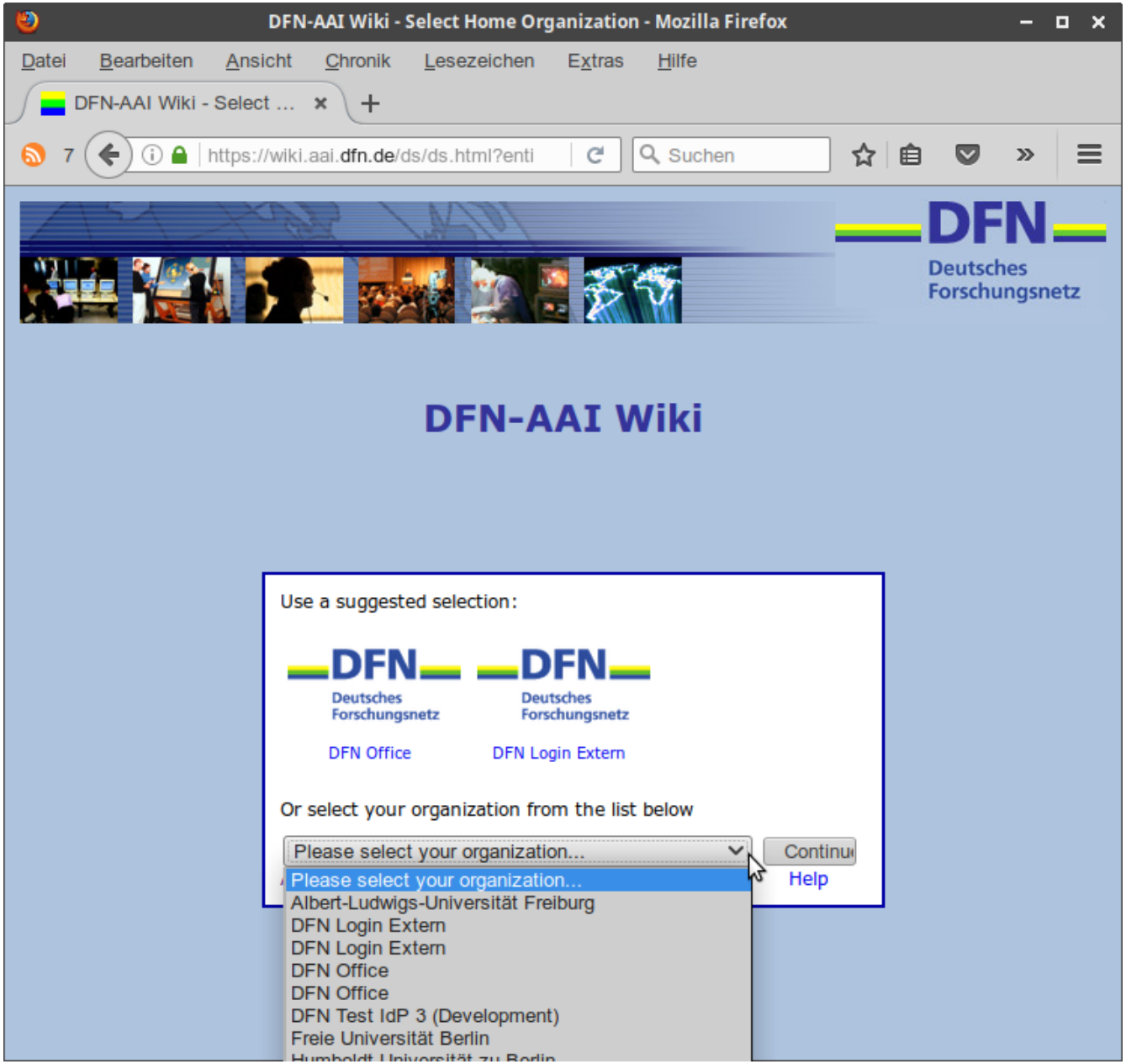
- Vom DFN betrieben
- Stündlich neu aus den jew. Metadatensätzen generiert
- DFN-AAI (”Advanced”)
- DFN-AAI-Basic
- DFN-AAI-Basic+eduGAIN
- DFN-AAI-Test
- projektspezifische DS' anhand Whitelist



Embedded Discovery Service

- Nutzerfreundlich, da nur IdPs gelistet, die tatsächlich für den Dienst relevant sind
- Wird lokal am SP anhand der eingelesenen Metadaten konfiguriert
- Üblicherweise JavaScript Anwendung
- Filterfunktion: Listet nur die IdPs, die für den jeweiligen SP bzw. Dienst relevant sind
- Beispiele
  - SWITCH EDS
    https://www.switch.ch/aai/guides/discovery/embedded-wayf/
  - Shibboleth EDS
    https://wiki.aai.dfn.de/de:shibeds
- Best Practice Empfehlungen: NISO ESPRESSO, REFEDS Discovery Guide; aktuell: RA21 Initiative

Embedded Discovery Service (2)



WAYFless URLs

- URL, der beim betreffenden SP direkt einen *Authentication Request* zu einem bestimmten IdP auslöst
- IdP und SP sind hart verdrahtet
- Sehr nutzerfreundlich, da Einrichtungsauswahl entfällt
- Muss angepasst werden, wenn sich der betreffende URL des SP ändert!
- Wird nicht von allen SPs unterstützt
- Beispiel:
  https://wiki.aai.dfn.de/Shibboleth.sso/Login?entityID=https://idp.dfn.de/idp/shibboleth
- Siehe auch unter
  https://wiki.aai.dfn.de/de:shibwayfless

Sonstiges

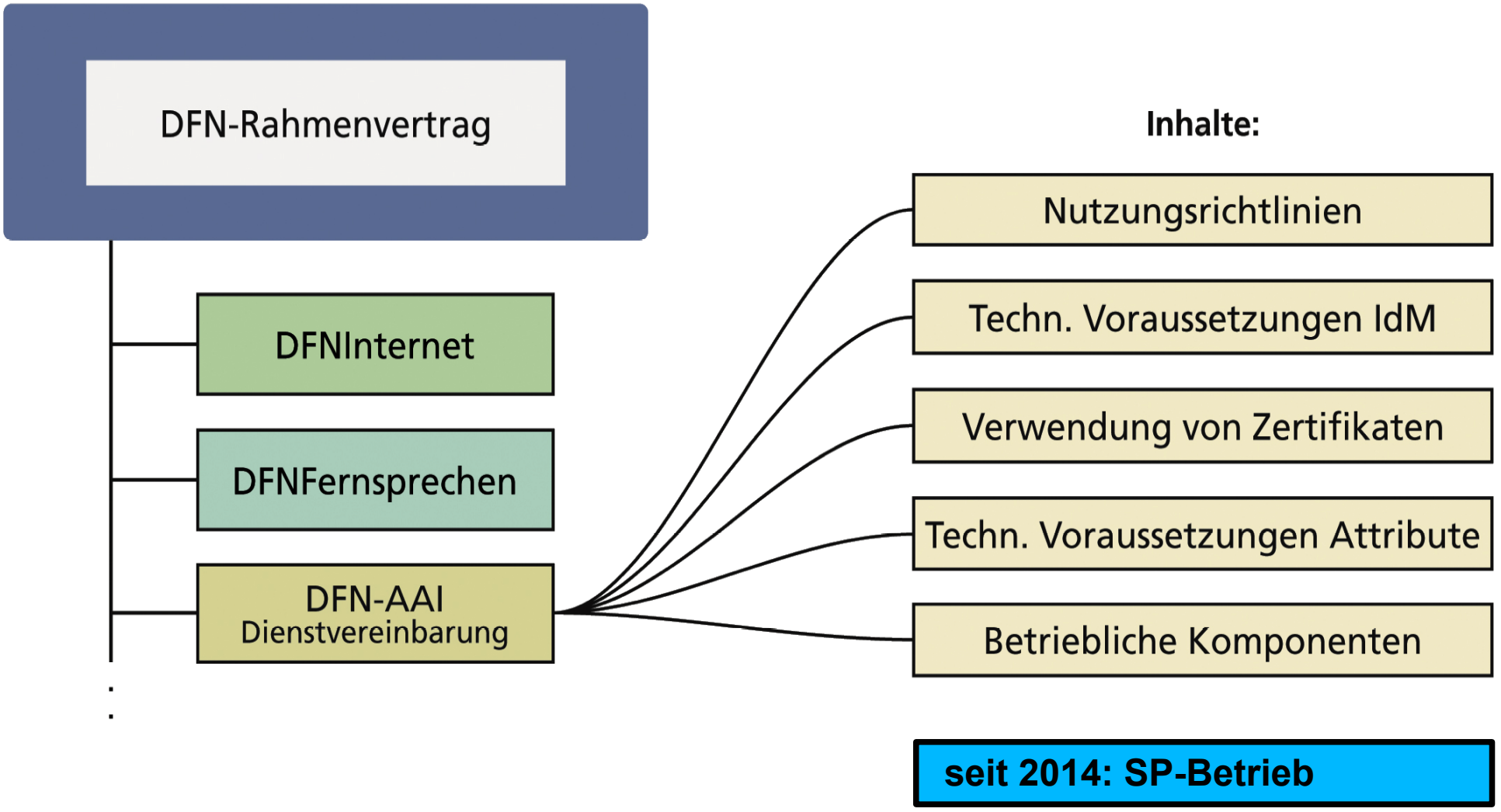
Planungen für die nähere Zukunft

- **Verlässlichkeitsklassen / Levels of Assurance** nicht mehr nur über verschiedene Metadatensätze modellieren, sondern über Attribute (eduPersonAssurance) und Authentication Context Classes
  - Übernahme des REFEDS Assurance Framework
    https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework
  - Ermöglicht LoAs per Identität / Login-Vorgang
- **Unterstützung für OpenID Connect**
  http://openid.net/connect/
  - Proof of Concept Implementierung der *OpenID Connect Federation* Spezifikation für die DFN-AAI
  - Testbed für Shibboleth IdP OIDC-Implementierung
  - Überlegungen zum Einsatz von Bridging Elementen SAML2 ↔ OIDC innerhalb der DFN-AAI

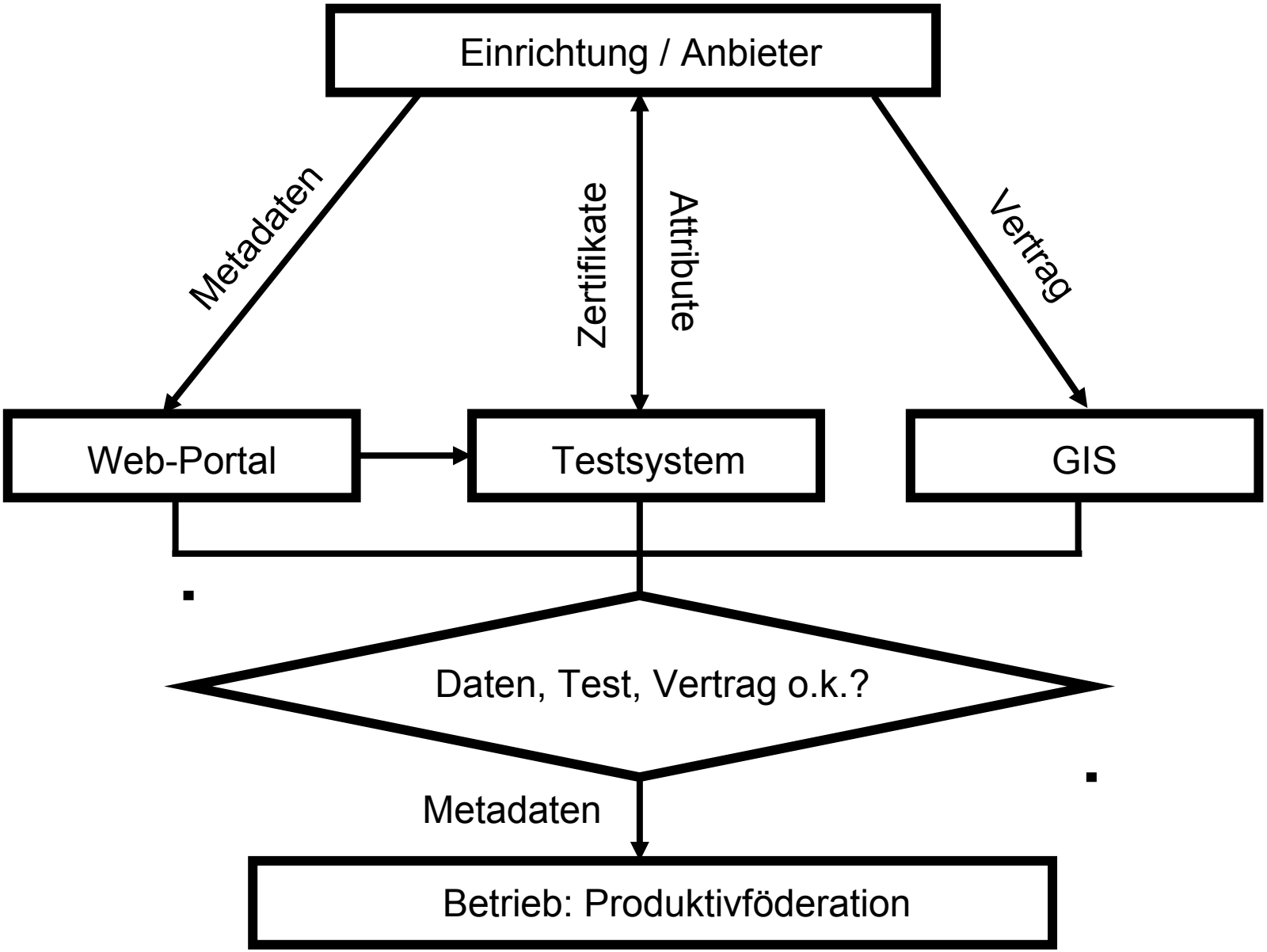
Teilnahme

- Die wichtigsten Schritte sind im DFN-AAI Wiki unter https://wiki.aai.dfn.de/de:join dokumentiert
- Teilnahme:
  - Rahmenvertrag (falls noch nicht vorhanden)
  - Dienstvereinbarung für DFN-AAI, deckt auch Betrieb von SPs ab
- Kosten:
  - Entgelt ist im Entgelt für DFNInternet enthalten, vgl. https://www.dfn.de/dienstleistungen/dfninternet/entgelte/ (ab Kategorie Portanschluss I02)

Vertragsgestaltung / -abschluss



Aufnahme in Produktivföderation



Informationsquellen

- DFN-AAI Wiki
  https://wiki.aai.dfn.de
  Änderungsfeed: https://wiki.aai.dfn.de/feed.php
- Materialien aus anderen Veranstaltungen (Betriebstagungen, Workshops, etc.)
  https://www.aai.dfn.de/aktuelles/archiv/
- Shibboleth Wiki:
  https://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

E-Mail: aai@dfn.de

Tel.: +49 30 884299-9124