DFN
Deutsches Forschungsnetz

Grundlagen

AAI, Web-SSO, Metadaten und Föderationen

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DFN-AAI IdP-Workshop,
24./25. Juni 2015, HS Amberg-Weiden

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

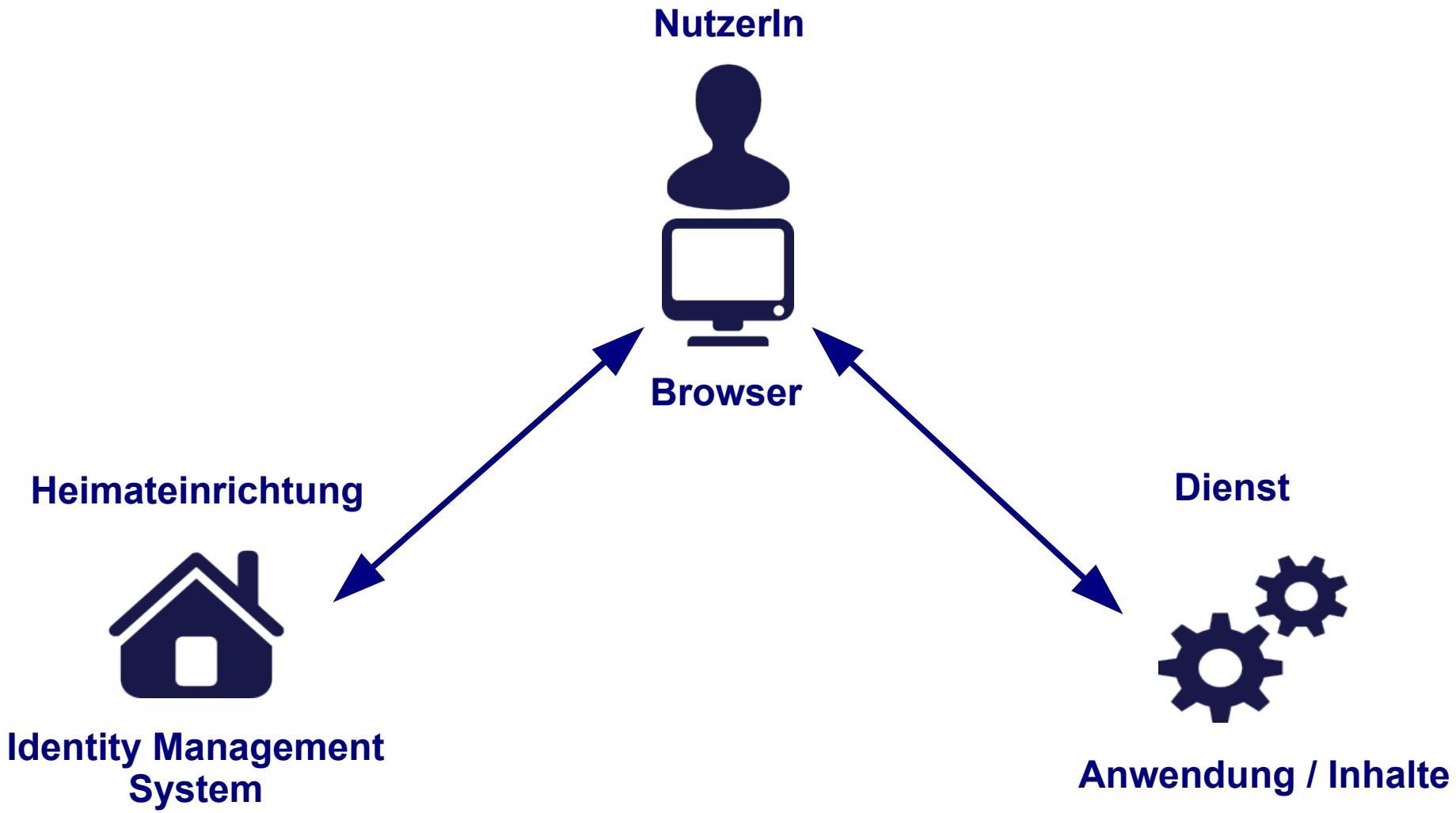
Welche Arten von Diensten?

Zielgruppe: Angehörige von Bildungs- und Forschungseinrichtungen

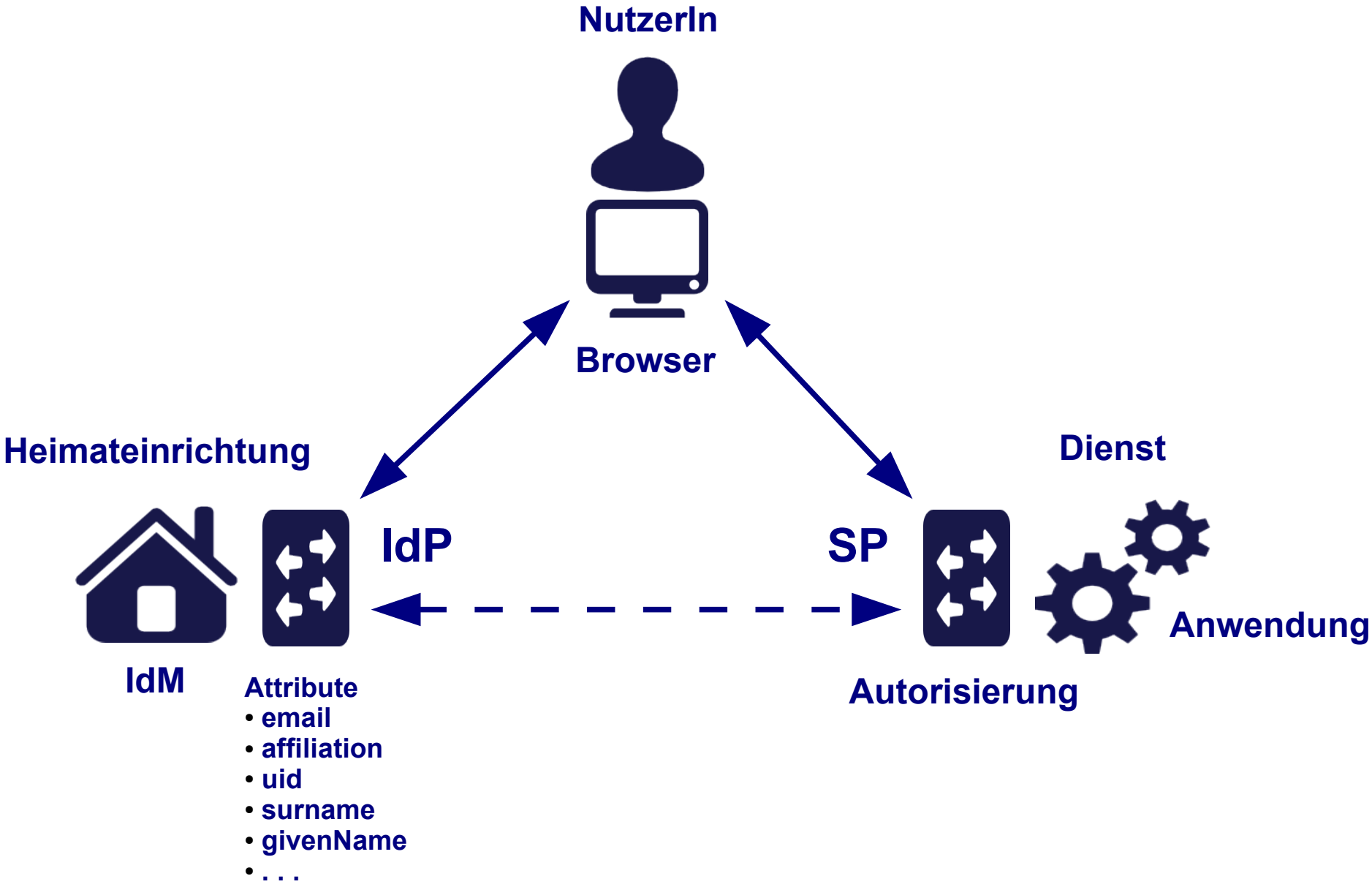
- Verlage und Bibliotheken – Content Provider (Springer, Elsevier, Nationallizenzen, ...)
- Verteilung lizenzierter Software (Microsoft Dreamspark)
- Hochschulinterne Dienste
- e-Learning-Plattformen
- Forschungsprojekte und -infrastrukturen
- Sync & Share Dienste (z.B. Gigamove)
- Webkonferenzen u.a.m.

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

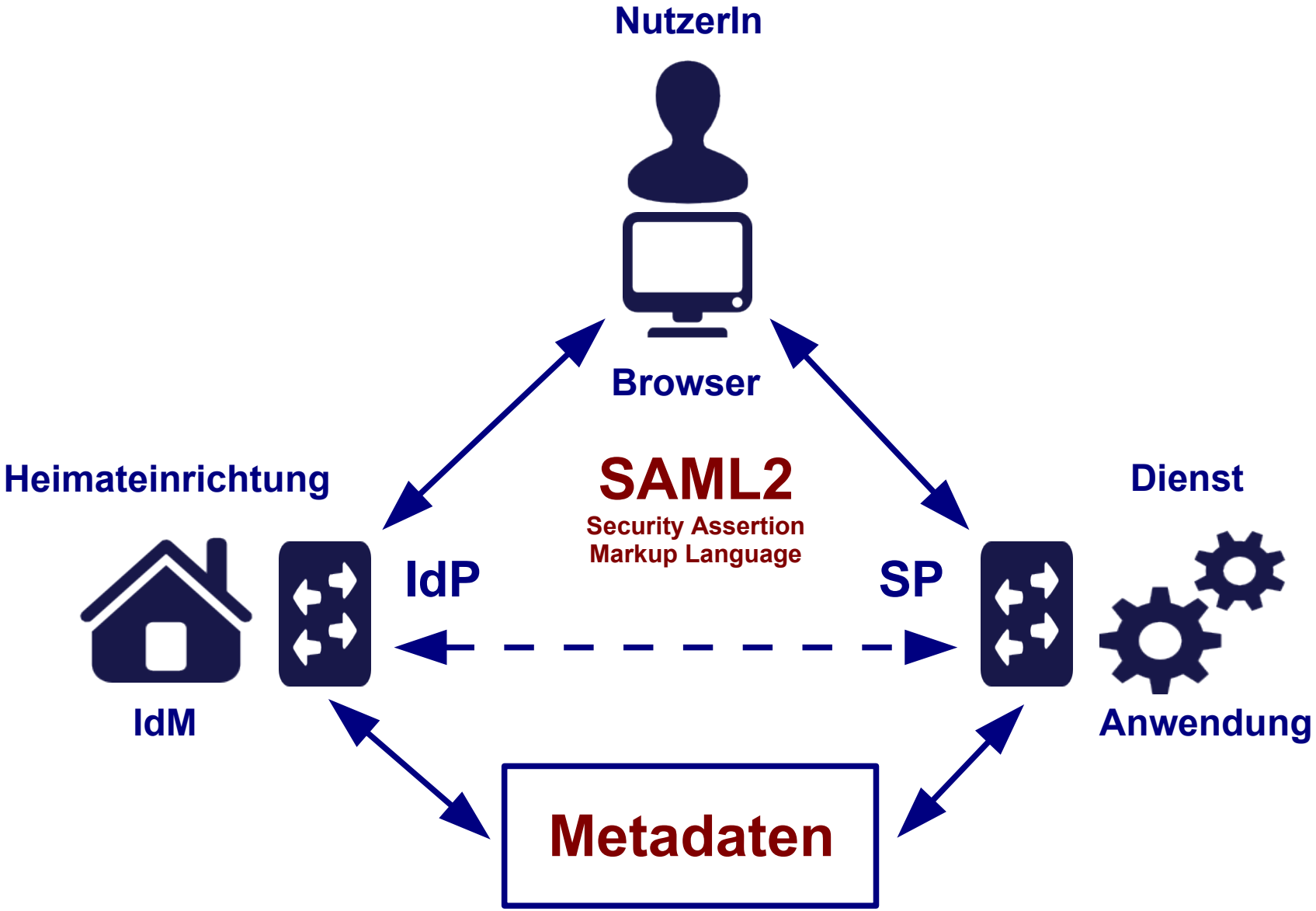
Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail



Lingua franca: SAML(2)



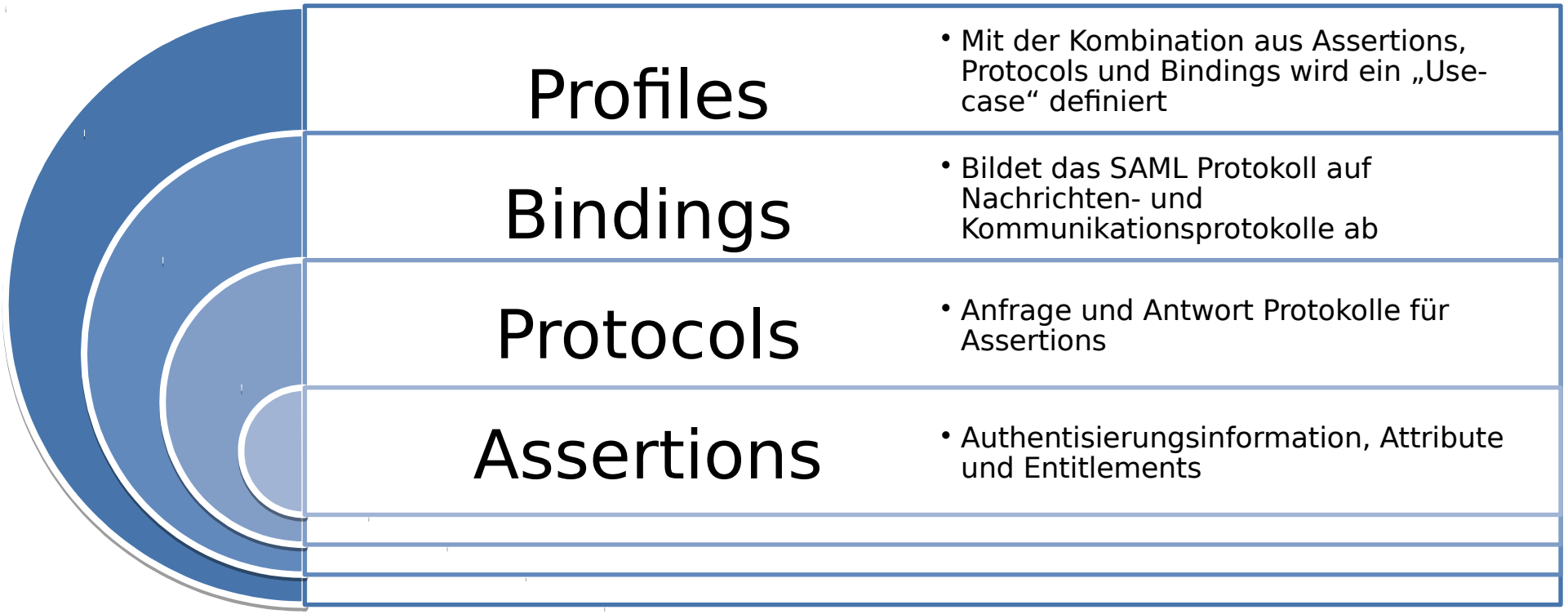
Siehe auch: https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

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

SAML Komponenten



Authentication Context	Metadata
• Definiert Art und Weise der Authentifizierung	• Konfigurationsdaten für Service- und Identityprovider

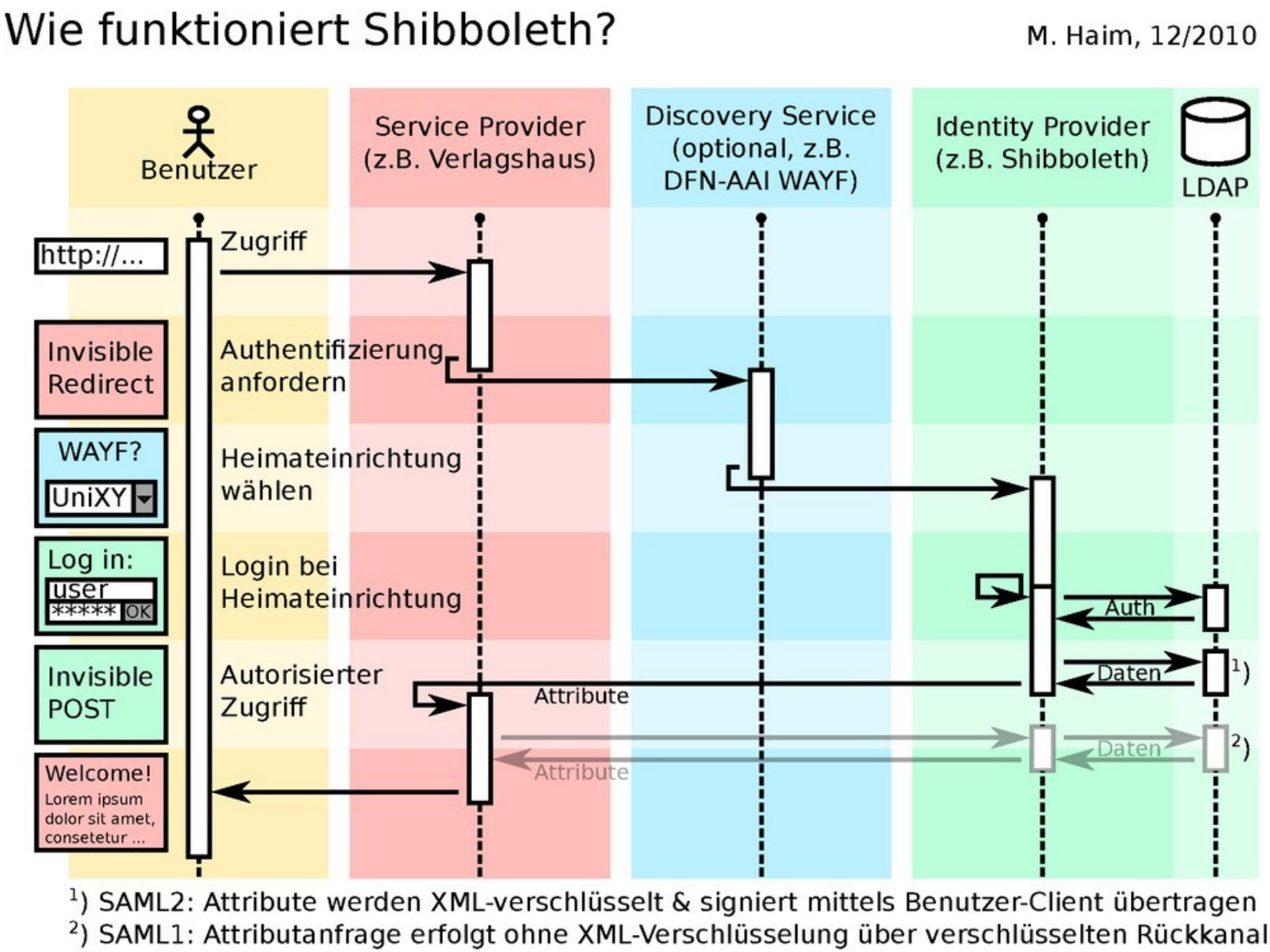
Quelle: Michael Simon, KIT

Beispiel für SAML Profile: Web-SSO

- Bietet Single Sign On für browserbasierende Webapplikationen
- Benutzer mit Browser will auf eine geschützte Resource beim Service Provider zugreifen
- Er wird an einen Discovery Service weitergeleitet, dort wählt er sich seinen IdP
- Er wird zum IdP weitergeleitet
- Der IdP authentisiert ihn
- Er wird wieder zum Service Provider weitergeleitet
- Dabei kommen folgende Kombinationen zum Einsatz:
  - Protocol: Authentication Request Protocol
  - Binding: HTTP Redirect, HTTP POST, HTTP Artifact

Quelle: Michael Simon, KIT

Kommunikation im Detail



Quelle: Manuel Haim, Uni Marburg

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://idp.dfn.de/idp/shibboleth)
  - Muss nicht auf eine Web-Ressource verweisen, 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

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

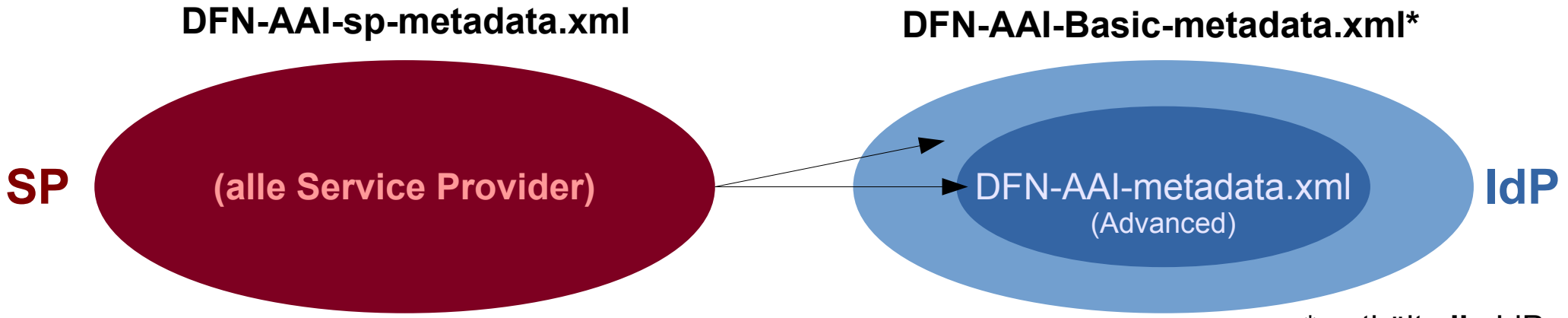
Typ	Aktivierung	Name	Status	Kommentar
Produktion: DFN-AAI	◉	DFN-AAI	zugelassen	
	○	DFN-AAI-Basic		
	○	keine		
	☐	lokale Metadaten		
Produktion: Interföderation	☐	eduGAIN		
Test	☑	DFN-AAI-Test	zugelassen	

schreiben | schreiben & zurück | abbrechen

Metadaten in der DFN-AAI

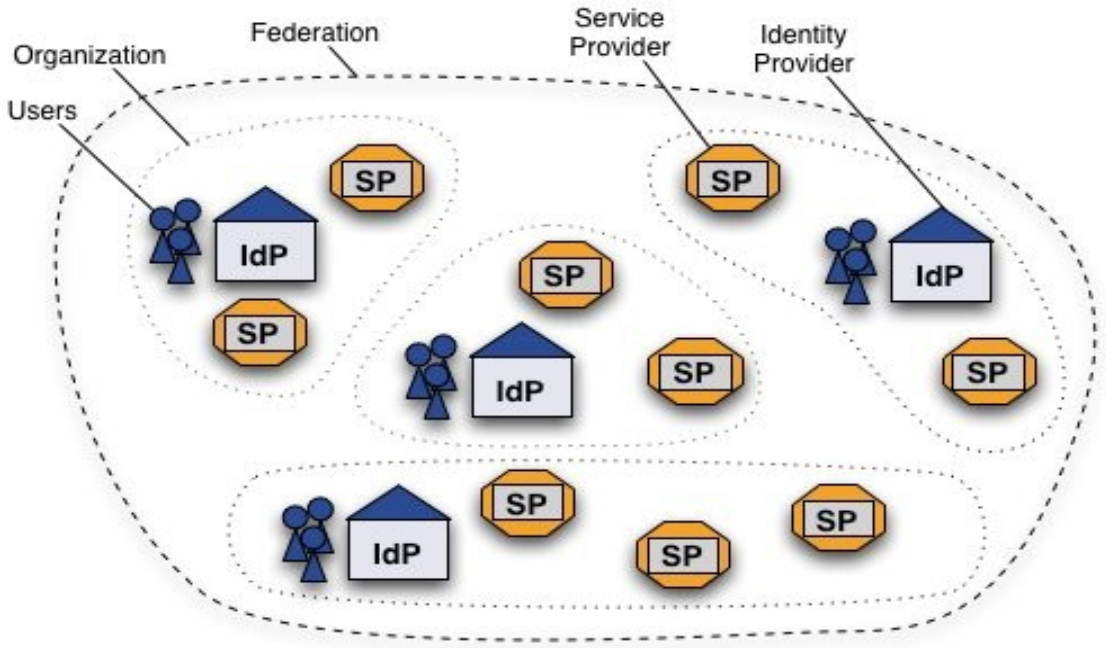
- Liste unter https://www.aai.dfn.de/teilnahme/metadaten/
- Testföderation:
  https://www.aai.dfn.de/fileadmin/metadata/DFN-AAI-Test-metadata.xml
- Produktivföderation, nach Verlässlichkeitsklassen, SP- und IdP-spezifisch, siehe https://www.aai.dfn.de/teilnahme/produktionsbetrieb/

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

Metadaten und Föderation



(Quelle: http://www.switch.ch/aai/about/federation/)

Auf Softwareebene gibt es keine Föderationen, sondern nur Metadaten.
Aber ohne Föderationen gäbe es keine verlässlichen Metadaten!

(Bernd Oberknapp, UB Freiburg, http://aar.vascoda.de/doc/praesentation/workshop-2006-10-10/AAR_20061010_Metadaten.pdf)

Spezialfall lokale Metadaten

- 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 Zertfikatsüberprüfung
- Lohnt sich vor allem für Einrichtungen mit vielen lokalen SPs (z.B. FU Berlin mit 88 SPs)
- Angebot wird derzeit von 58 Einrichtungen mit insgesamt 380 SPs genutzt

Konfiguration lokale Metadaten

Konfiguration über Schaltfläche in Vertragsdaten erreichbar:

Verlässlichkeitsklasse	lokale Metadaten	
Advanced	aktiviert download	

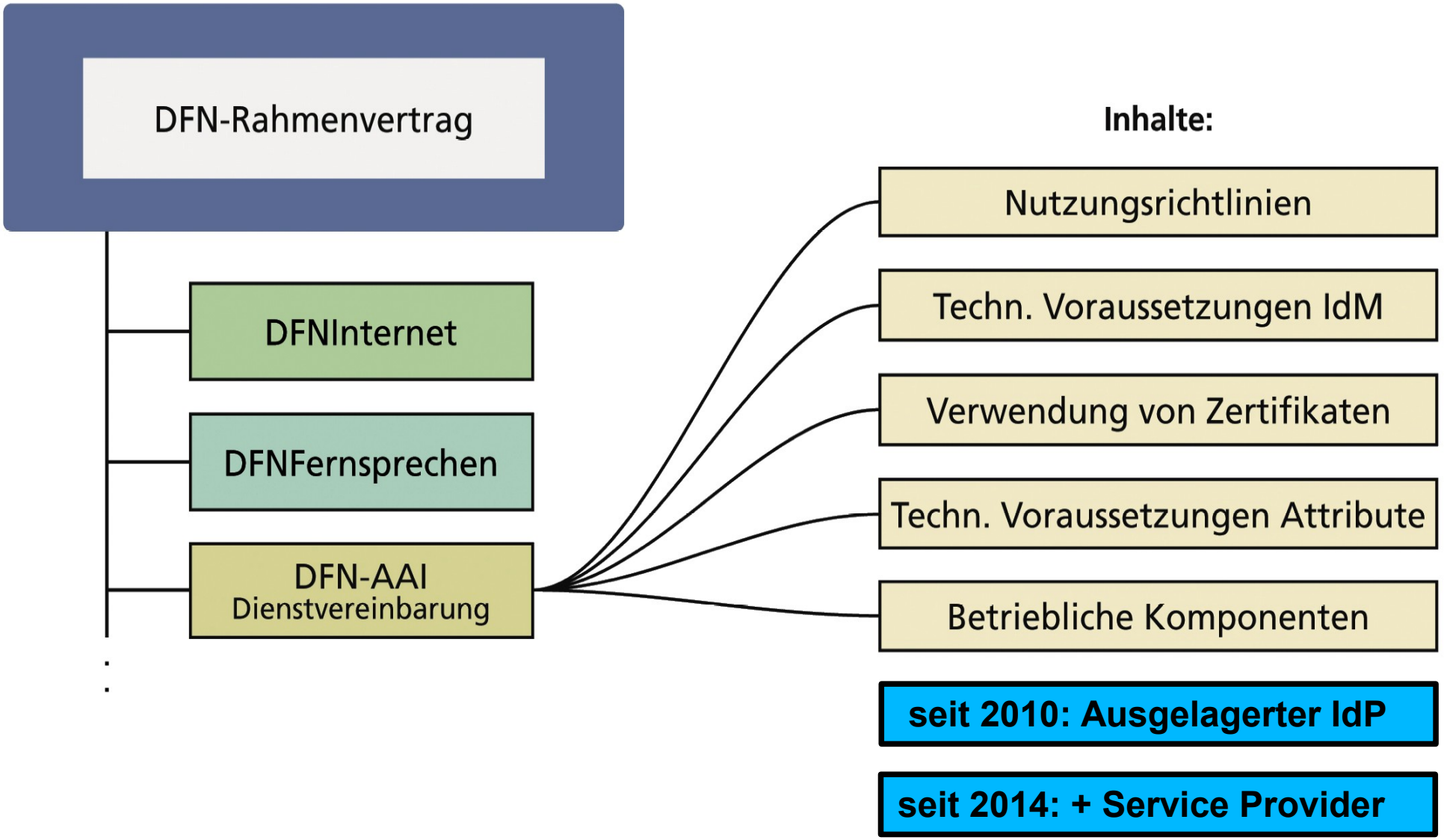
dann:

Vertragsdaten editieren

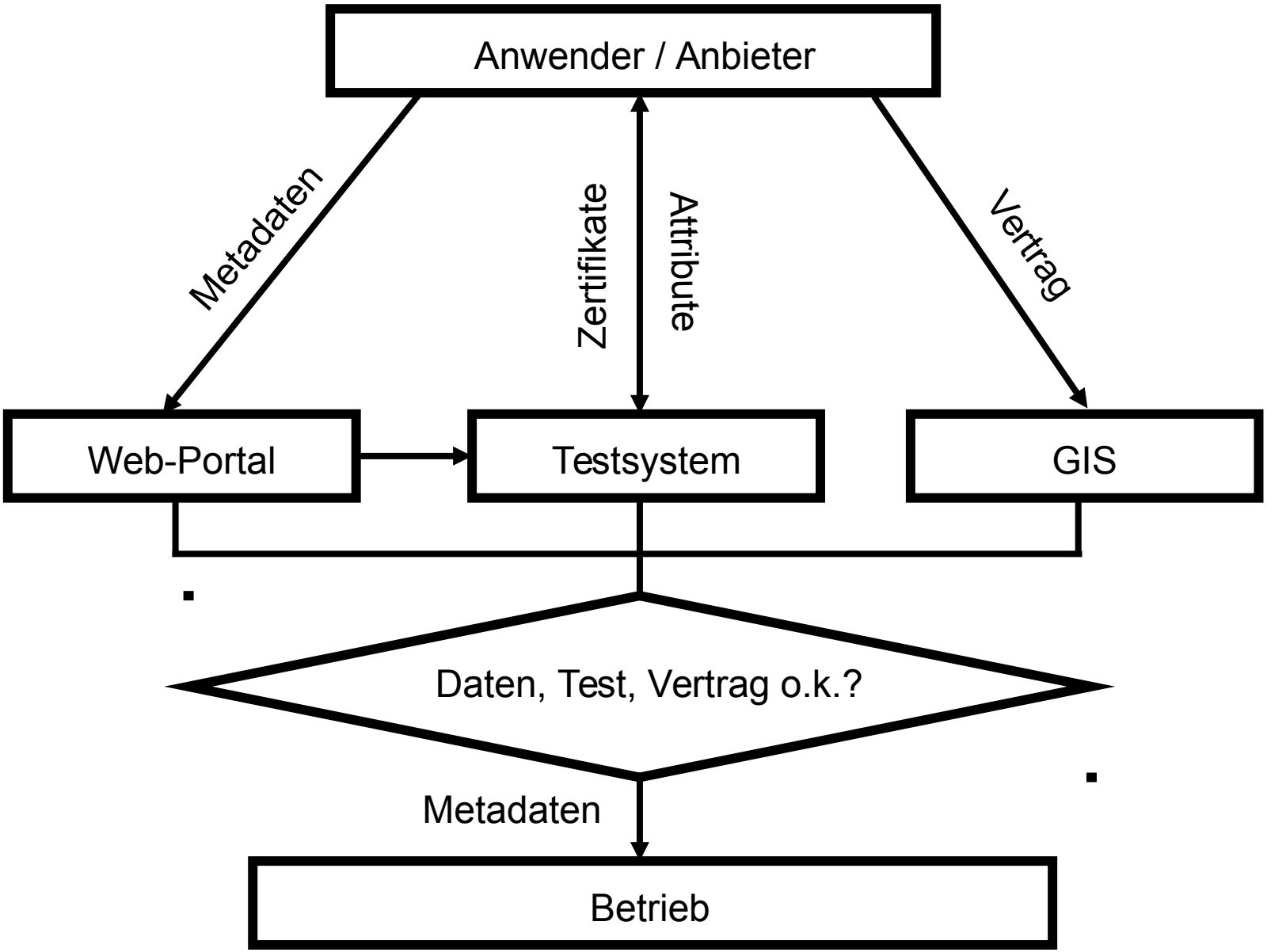
Nummer	AAI10
Einrichtung	Verein zur Förderung eines Deutschen Forschungsnetzes, Berlin
Kontakt	Ulrich Kähler, (0 30) 88 42 99-35, kaehler@dfn.de
Verlässlichkeitsklasse	Basic ◉ Advanced
Service Provider	Vertrag vorhanden / Vertragssoption aktiviert
lokale Metadaten	☑ aktivieren
Zugang zu lokalen Metadaten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

Dienstvereinbarung DFN-AAI

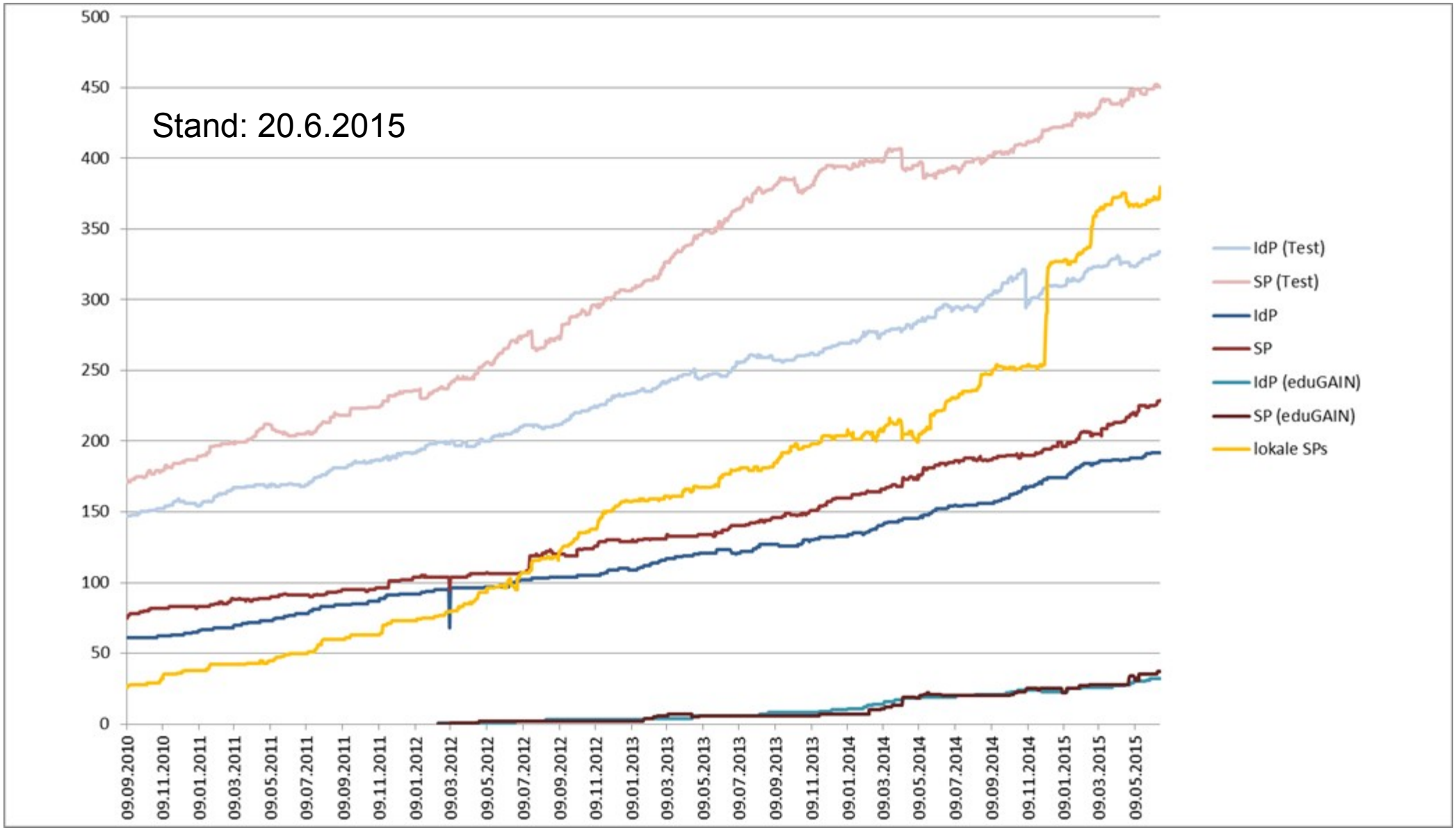
= Vertrag für Heimateinrichtungen (IdPs)



Aufnahme in Produktivföderation



DFN-AAI – registrierte Provider

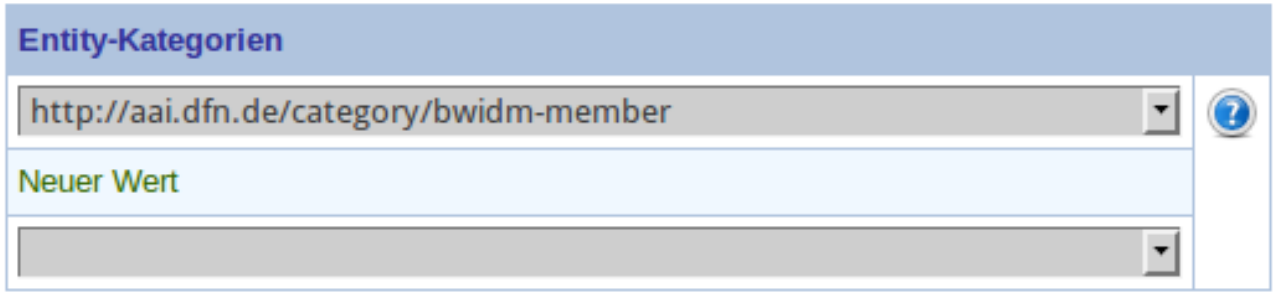


Technische Infrastruktur (1)

- 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 zwei Verlässlichkeitsklassen, „Advanced“ und „Basic“ (jew. eigener Metadatensatz)
- Testföderation inkl. Test-IdPs und -SPs
- Lokale Metadaten für einrichtungsinterne Dienste (inkl. .htaccess zum Schutz vor fremdem Zugriff)

Technische Infrastruktur (2)

- 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
- Hosting ausgelagerter IdPs
- Unterstützung von Entity Attributen, z.B. für virtuelle Subföderationen (Vergabe anhand projektspezifischer Whitelist)



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