deutsches forschungsnetz

DFN-AAI

HÜF-NRW 08.008 Treffen der IT-Verantwortlichen und IT-Mitarbeiter*innen der Kunst- und Musikhochschulen | 13. November 2019

Wolfgang Pempe (pempe@dfn.de)

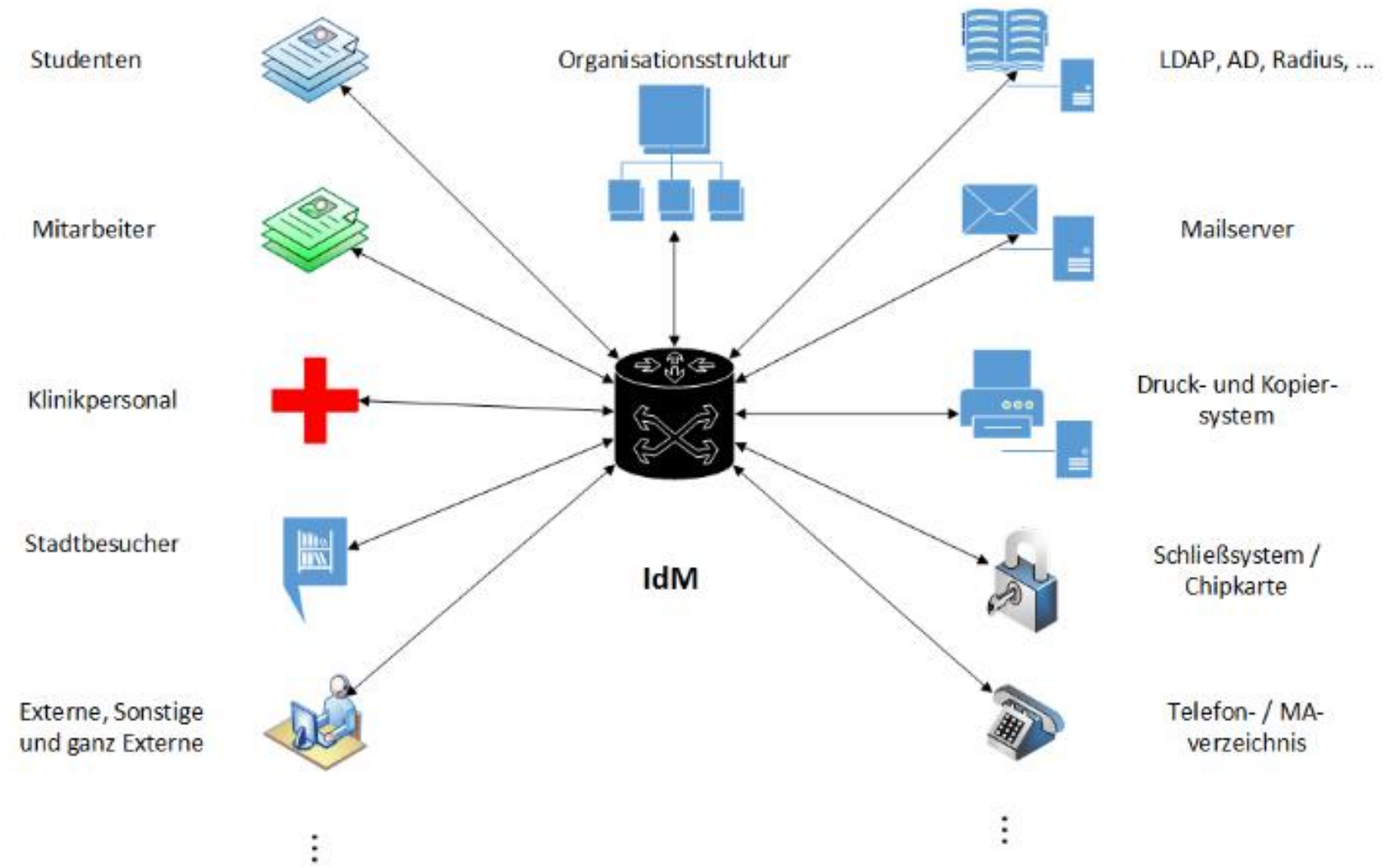
Identity Management (IdM)

Ohne IdM kein föderiertes IdM

Identity Management umfasst mehr als nur die Speicherung von Nutzerdaten

- Organisatorische und technische Prozesse
  - Onboarding, Aufnahme in Beschäftigten- oder Studierendenverhältnis
  - Rollen- und Rechtemanagement
  - Offboarding, Deprovisionierung von Nutzer*innen
- Weitere Aspekte
  - Datenschutz
  - Betriebs- und Informationssicherheit
- Best Practice: führendes System, aus dem z.B. LDAP/AD provisioniert werden

Identity Management System



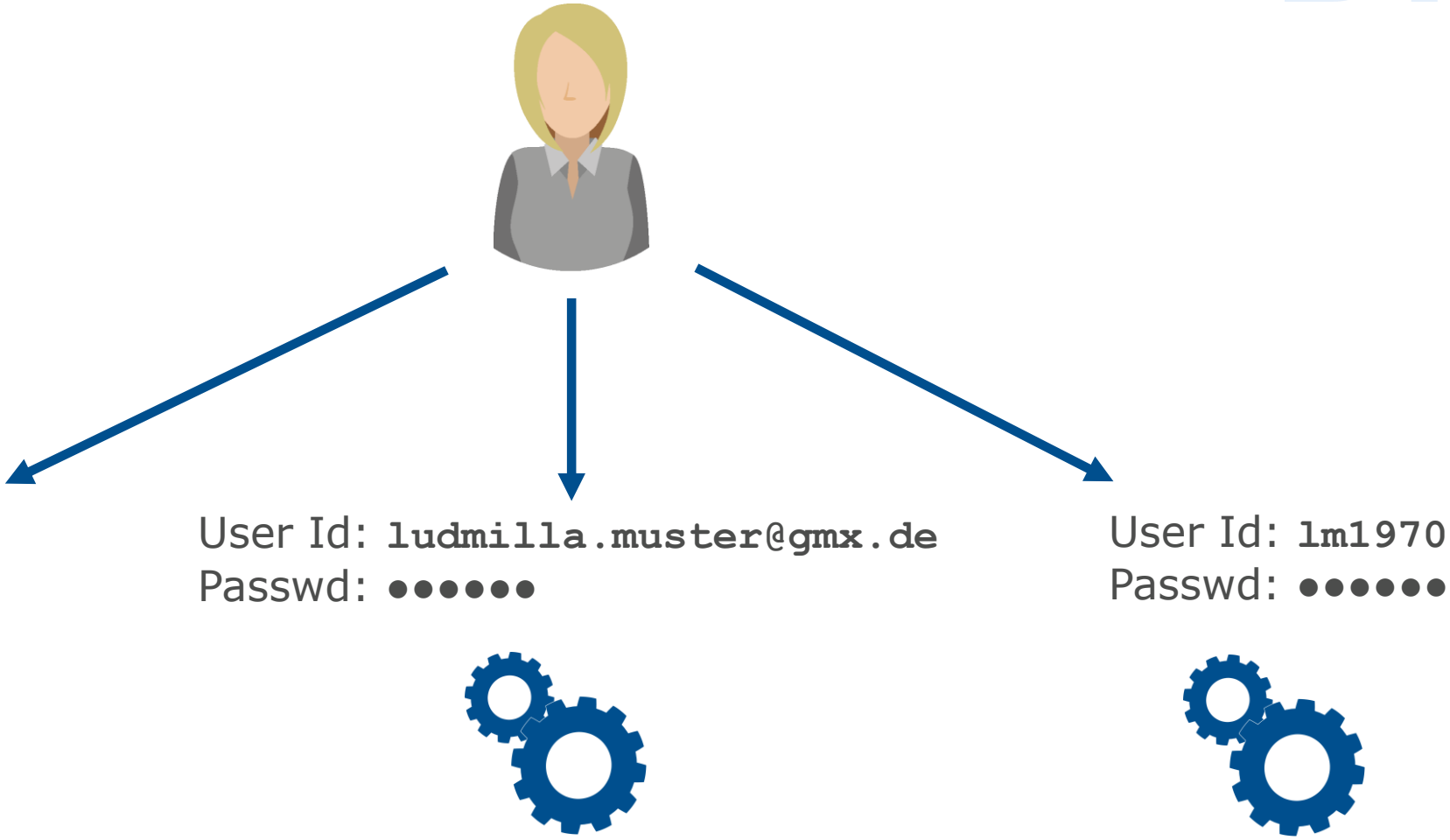
Quelle: Thorsten Michels (Uni Kaiserslautern)
Identity Management und Shibboleth: Ein Überblick

Föderiertes Identity Management, AAI und Web-SSO,

Begriffsbestimmung

- **AAI** = **A**uthentication and **A**uthorization **I**nfrastructure
- AAI bildet den technischen und organisatorischen Rahmen für föderiertes Identity Management
- **Föderiertes Identity Management:**
  - Austausch von Identitätsdaten über Dienst- und Organisationsgrenzen hinweg
  - Keine dienstspezifischen Identitäten
  - Eine Identitätsquelle als führendes System
- Voraussetzung für (Web-)SSO, (Web) **S**ingle **S**ign-**O**n
  - Einmal anmelden für 1..n Dienste, für die man zugriffsberechtigt ist

Dienstspezifische Identitäten



Föderierte Identität

User Id: `lmuster`
Passwd: ••••••

Heimateinrichtung

Online Shop XY

Datenbankanbieter YZ

Verlag WX

Föderation

- Eine AAI kann lokal oder auch einrichtungsübergreifend 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 Vertrauensverhältnis 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.)

Dienste und Nutzergruppen

2007 → heute

„Content Provider" (Verlage, Datenbanken) – Springer, Elsevier, etc.

Verteilung lizenzierter Software – Kivuto, Bildung365, etc.

E-Learning – Moodle, Bildungsportal Sachsen, VHB, etc.

Speicher-, Kommunikationsdienste – Gigamove, DFNconf …

Landesdienste – bwIDM, SaxID, sciebo, hessenbox, …

E-Research – CLARIN, DARIAH, ELIXIR …

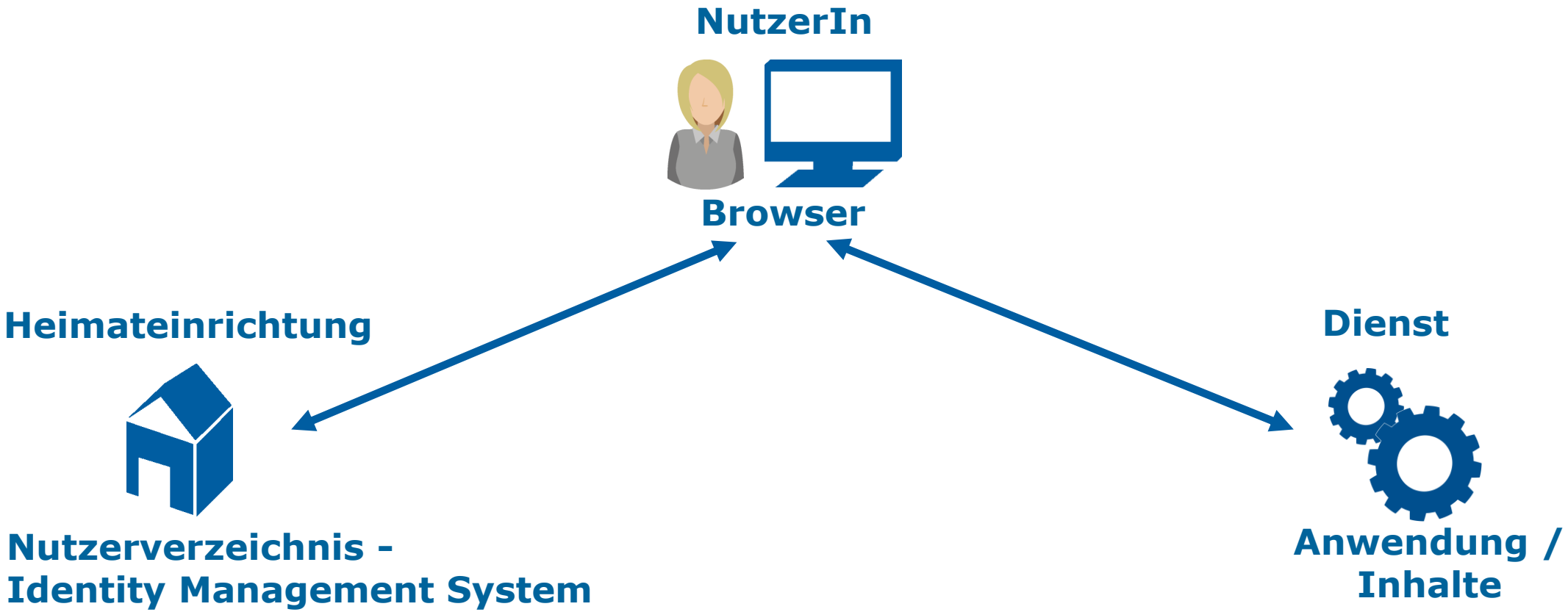
Internat. Forschungscommunities (→ eduGAIN)

Bibliotheksnutzer*Innen

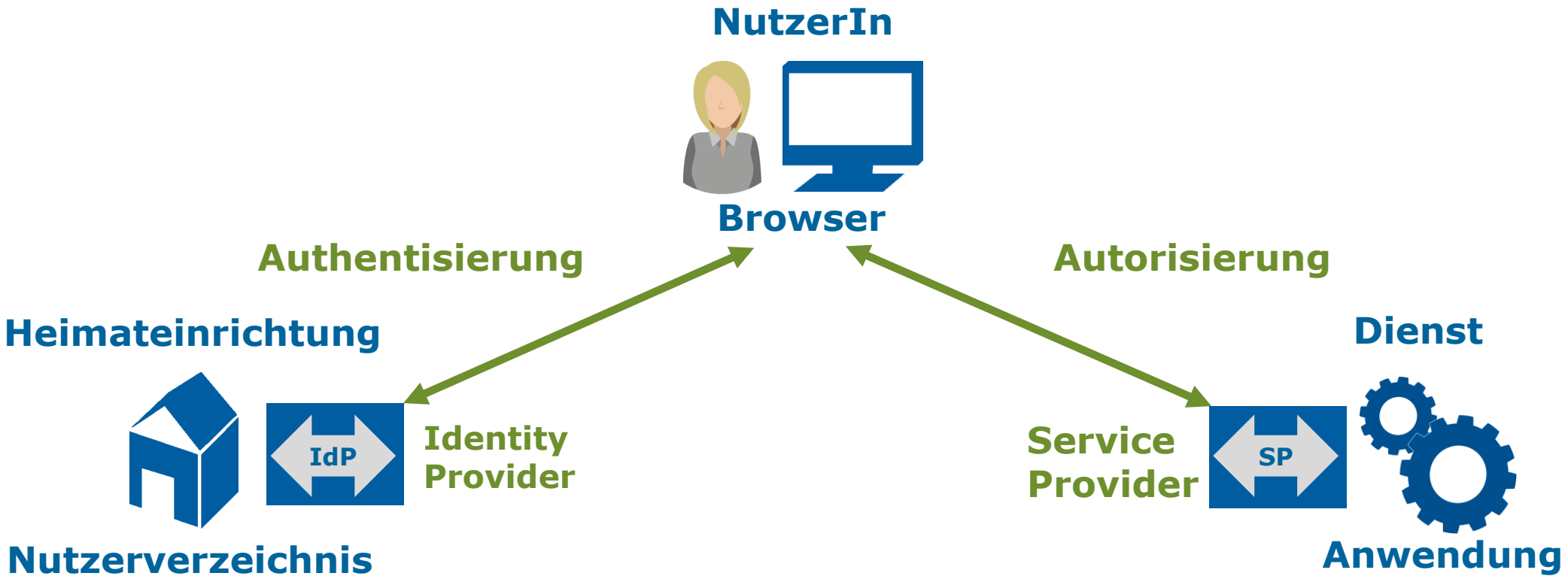
Studierende, Lehrpersonal

Forschende

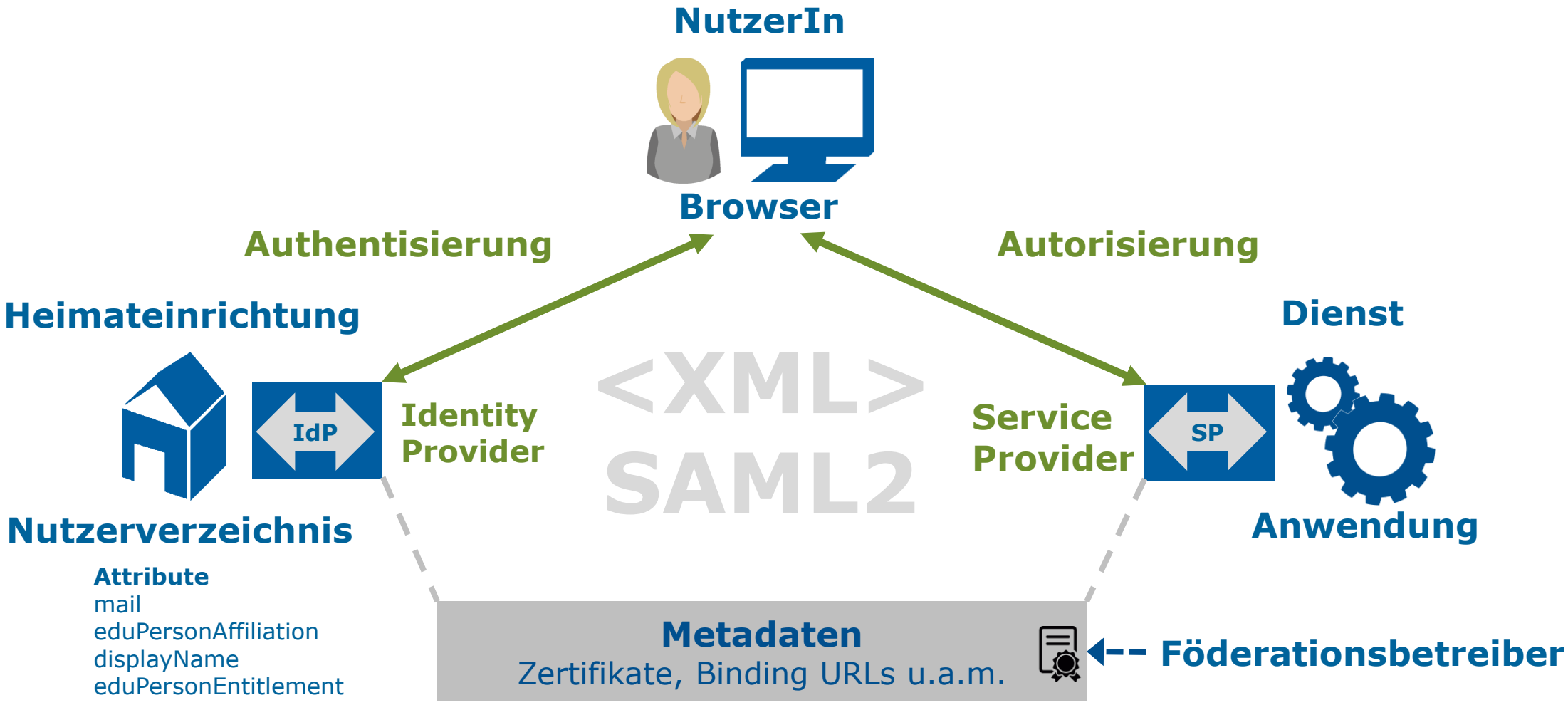
Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail



Lingua franca: SAML (bzw. SAML2)



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

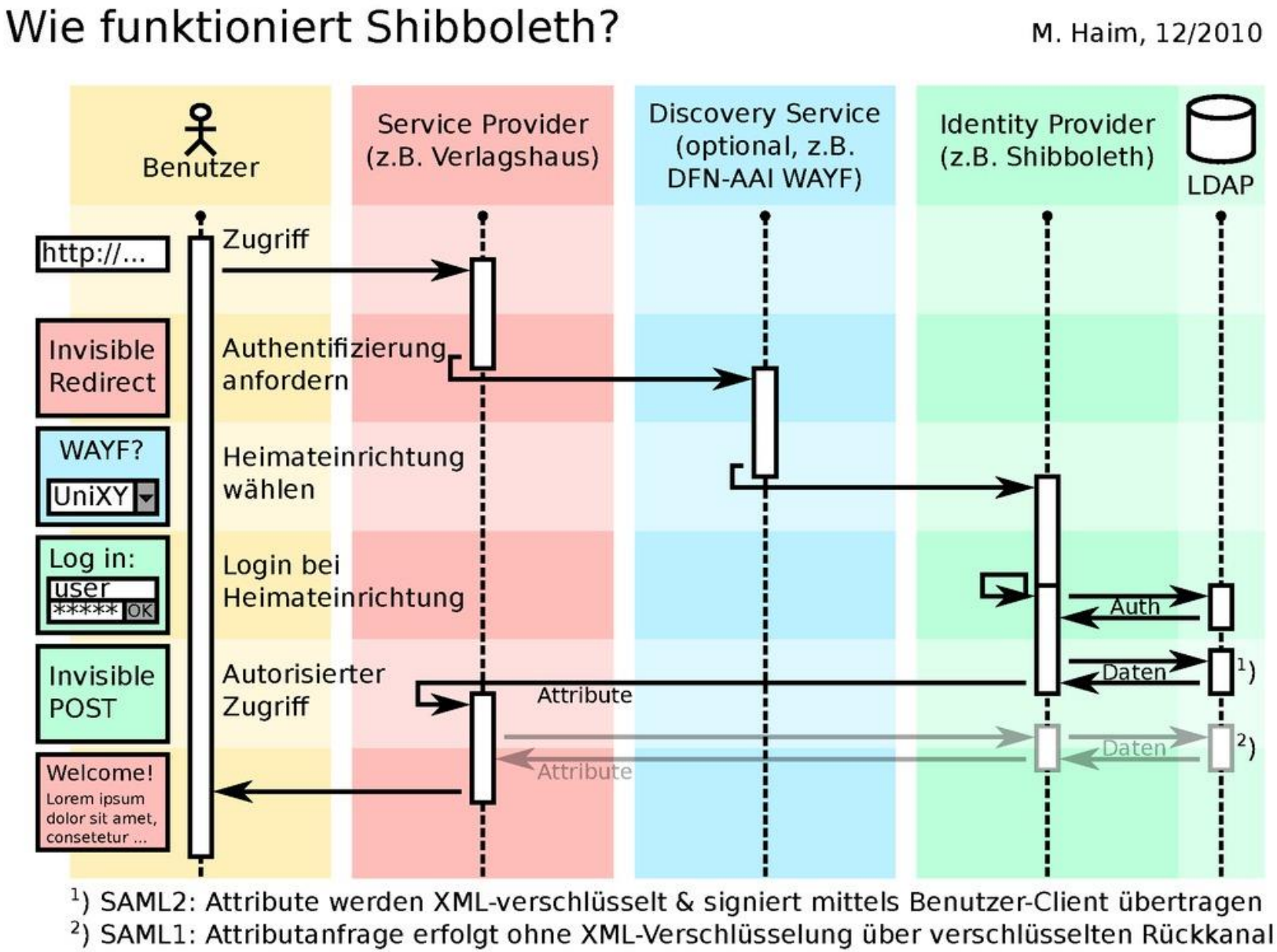
SAML und SAML Metadaten

- 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
- **Metadaten** enthalten alle Informationen, die für eine sichere Kommunikation zwischen den beteiligten Entities (IdPs, SPs) benötigt werden

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 (SP sendet AuthnRequest)
- ... authentisiert sich am IdP (IdP sendet Response inkl. Assertion an SP)
- ... 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

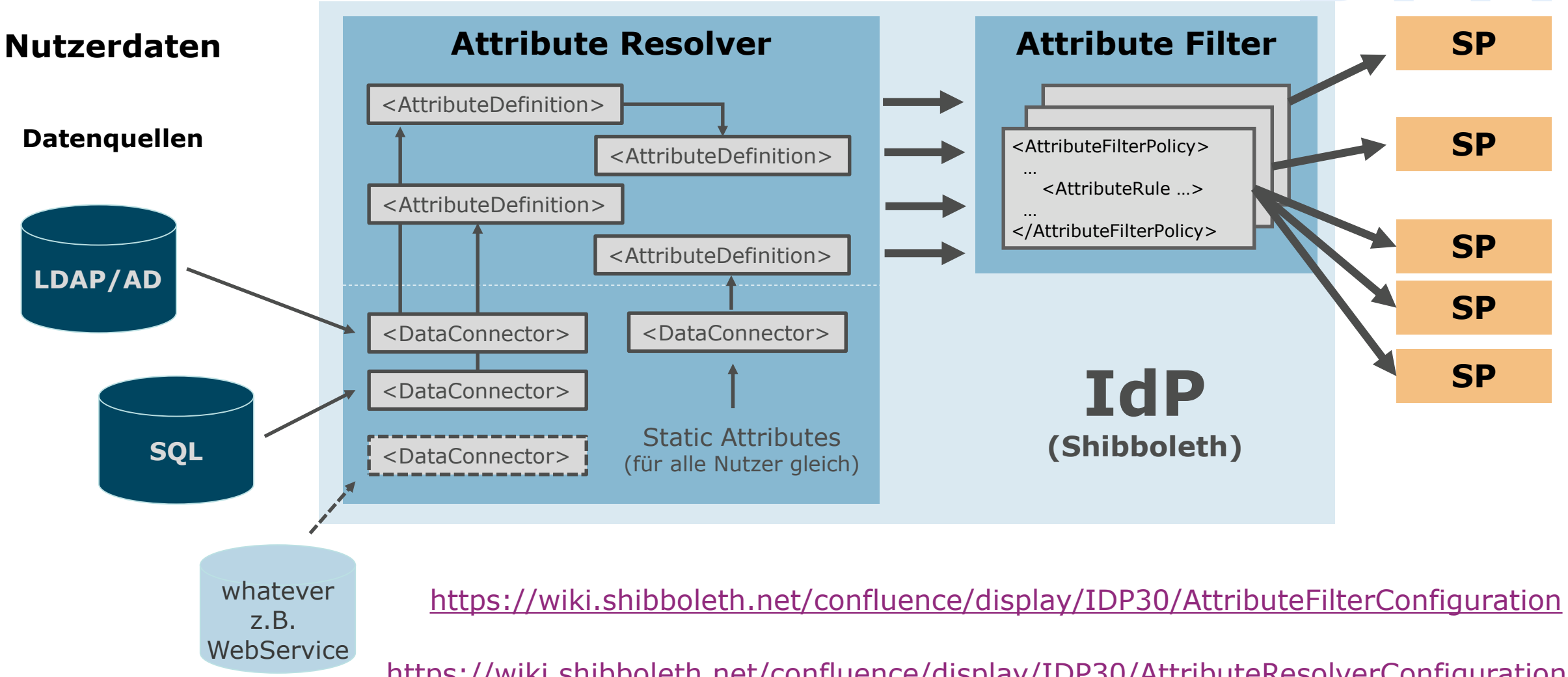


Quelle: Manuel Haim, Uni Marburg

Exkurs: Single Sign-On (SSO)

- Einmal am IdP authentisieren → 1..n Dienste ohne weitere Anmeldung nutzen
- Parameter:
  - Sitzungsdauer am IdP (Authn Default Lifetime/Timeout, Session Timeout)
  - Sitzungsdauer am SP
  - SP kann erneute Anmeldung am IdP verlangen
- An den teilnehmenden Einrichtungen sehr unterschiedlich gehandhabt
- Komplexes Zusammenspiel, Dokumentation im Shibboleth Wiki
  https://wiki.shibboleth.net/confluence/display/CONCEPT/Sessions
  https://wiki.shibboleth.net/confluence/display/IDP30/SessionConfiguration

Der Weg der Attribute



https://wiki.shibboleth.net/confluence/display/IDP30/AttributeFilterConfiguration

https://wiki.shibboleth.net/confluence/display/IDP30/AttributeResolverConfiguration

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://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
- 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 (oder eines Äquivalents)

SP = Service Provider

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

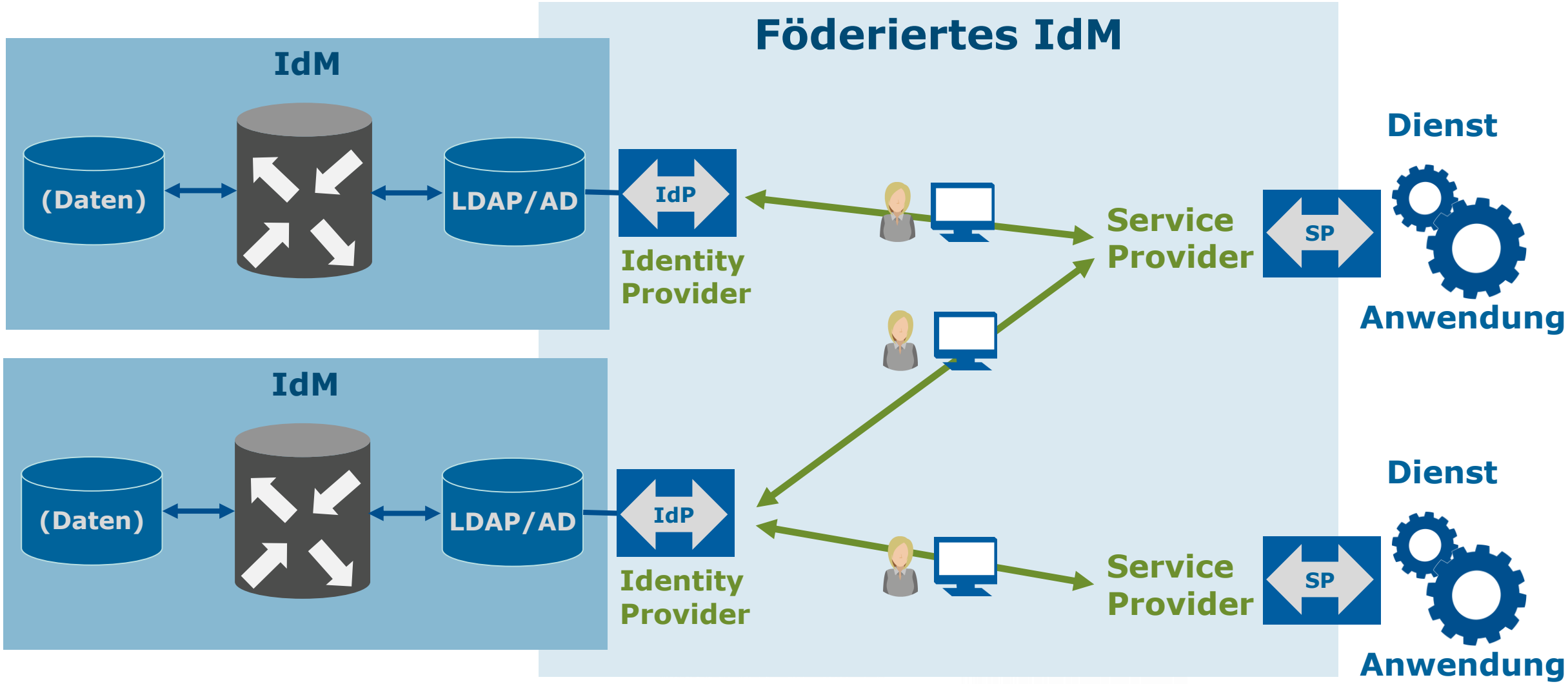
Beispiele

- SAML-Kommunikation zw. SP und IdP/AA
- Metadaten
  - IdP (https://idp.dfn.de/idp/shibboleth)
  - Attribute Authority (https://attributes.dfn.de/idp/shibboleth)
  - SP (https://clarin.ids-mannheim.de/shibboleth)
  - Föderationsmetadaten - siehe unter https://doku.tid.dfn.de/de:metadata

SAML und X.509-Zertifikate

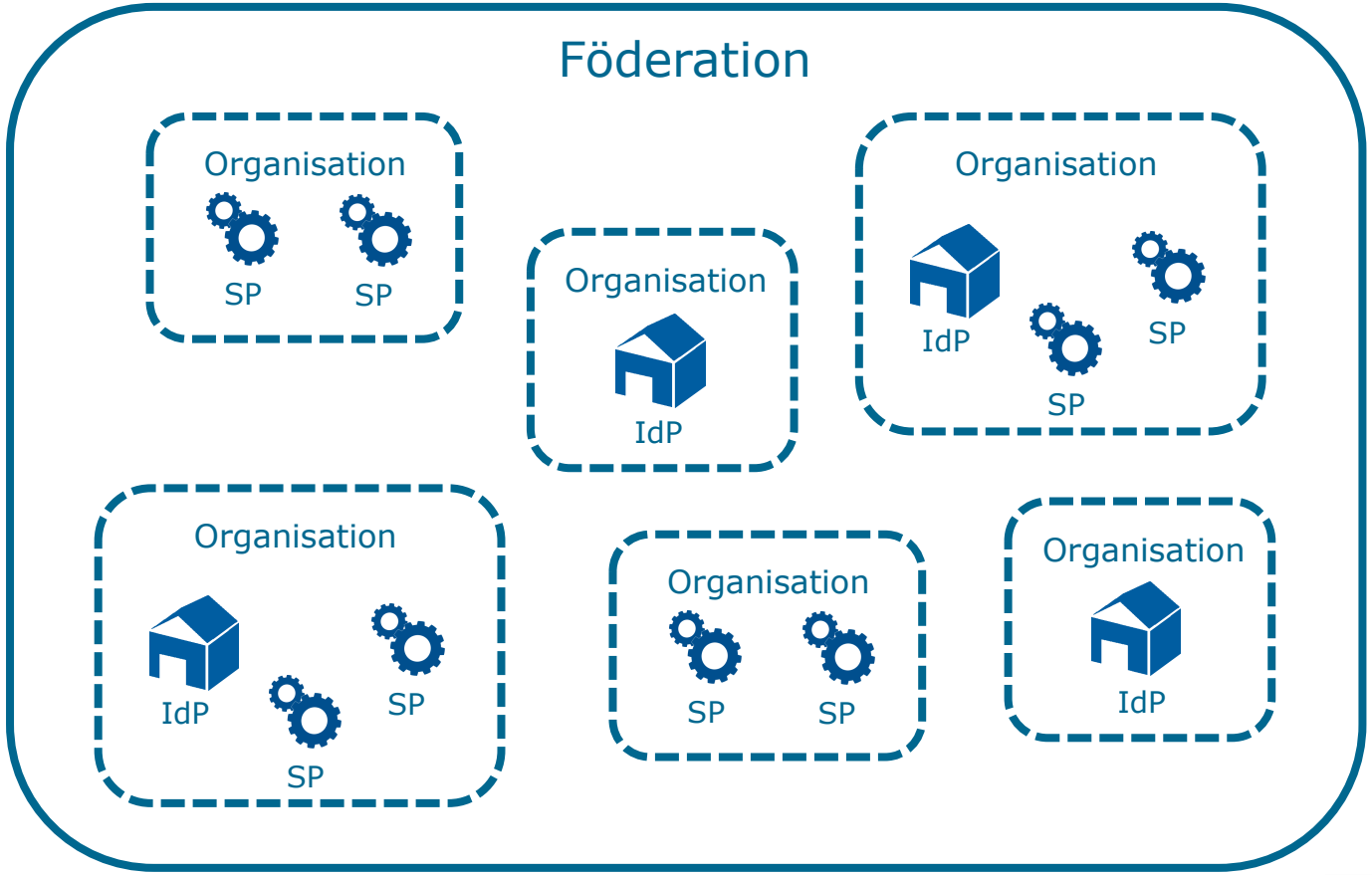
- Absicherung der Kommunikation durch XML-Signaturen und -Verschlüsselung
- Eigener Private Key: Signieren, Entschlüsseln
- Zertifikat der Gegenstelle: Signatur-Validierung, Verschlüsselung
- **Kann** identisch mit TLS-Zertifikat in Webserver-Konfiguration sein
- Einrichtungen, die an der DFN-AAI teilnehmen → Zertifikate aus der DFN-PKI
- https://doku.tid.dfn.de/de:certificates
- https://www.oasis-open.org/committees/download.php/56776/sstc-saml-core-errata-2.0-wd-07.pdf

Wir rekapitulieren…



Föderationen

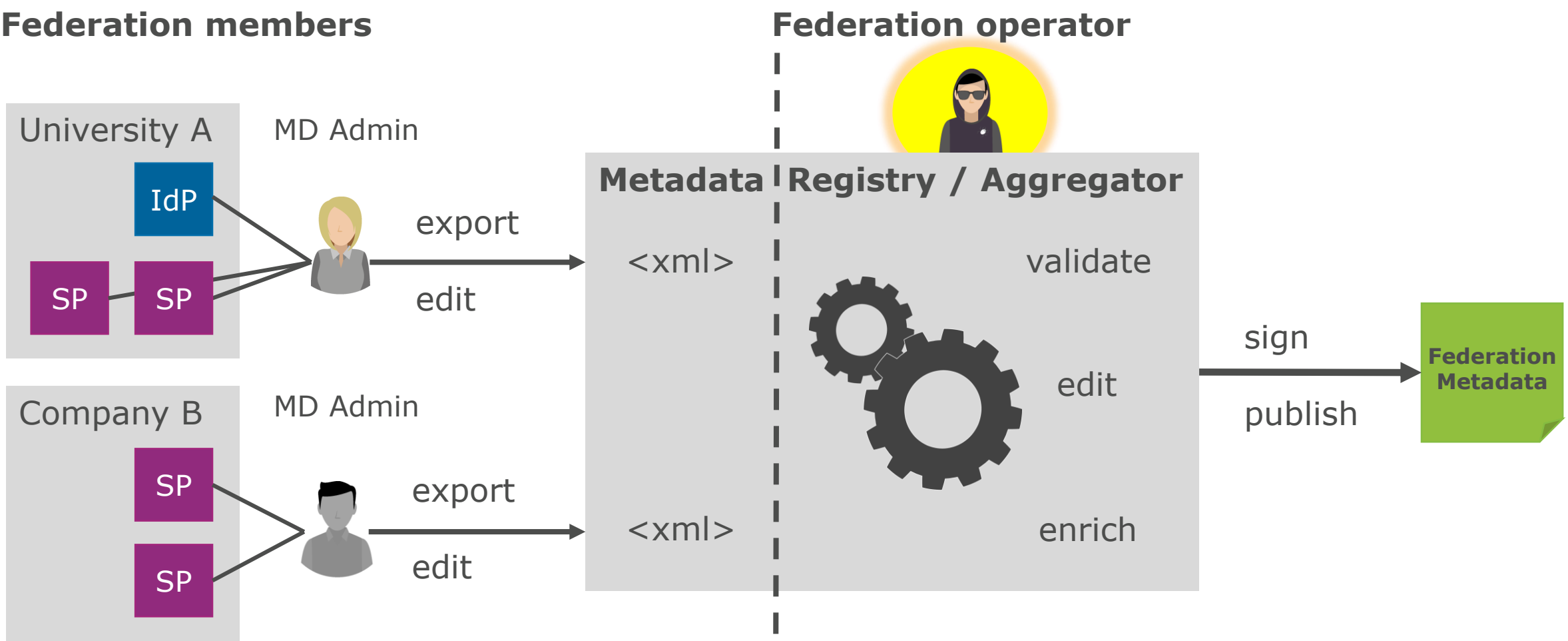
z.B. DFN-AAI



Metadaten und 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
    - Zertifikatprüfung und –überwachung (u.a.m.)
    - Signierte Metadaten

Metadata Aggregation and Management



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://doku.tid.dfn.de/de:metadata
- Testföderation
- Lokale Metadaten
- Produktivföderation, nach Verlässlichkeitsklassen, SP- und IdP-spezifisch, siehe https://doku.tid.dfn.de/de:production

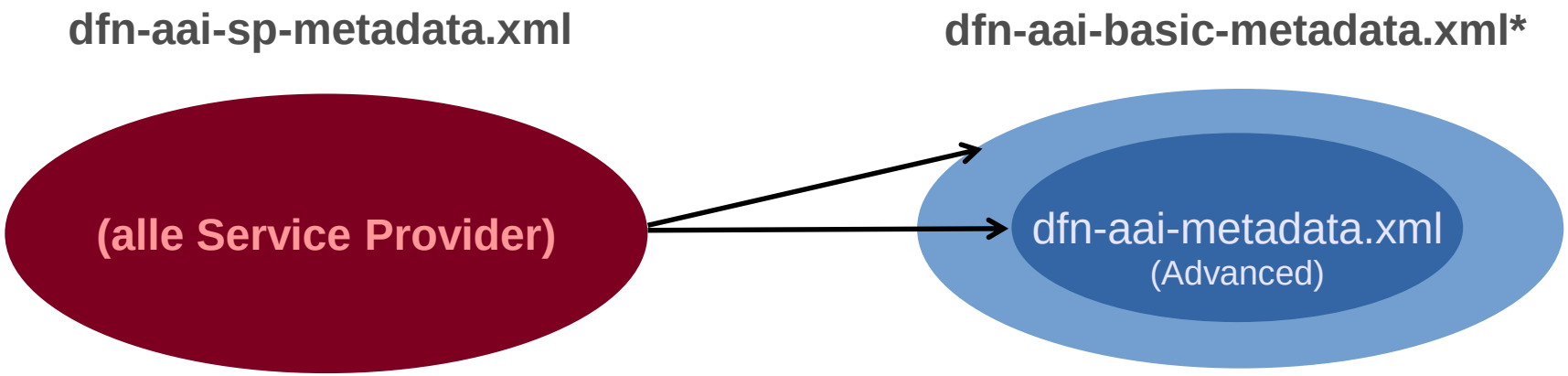
Verlässlichkeitsklassen in der DFN-AAI (1)

Verlässlichkeits-klasse	Identifizierung durch Heimateinrichtung	Verfahren zum Ausweis einer Identität	Datenhaltung und Prozesse zur Pflege der Identitäten
n.a. / Test	Verfahren freigestellt	Verfahren freigestellt	Verfahren freigestellt
Basic	Rückantwort von eindeutiger Adresse (E-Mail, Tel.-Nr., Postanschrift, etc.)	Anhand eindeutig zuzuordnender digitalen Adresse	Verpflichtung bzgl. Aktualität innerhalb von 3 Monaten
Advanced	pers. Vorsprechen gegenüber Vertrauens-instanz unter Vorlage amtlicher Dokumente (alternativ: Post-Ident, eID/nPA). Die an den Hochschulen etablierten Einschreibungs- und Einstellungsprozesse werden als gleichwertig akzeptiert	pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Verpflichtung bzgl. Aktualität innerhalb von 2 Wochen

Vgl. https://doku.tid.dfn.de/de:degrees_of_reliance

Verlässlichkeitsklassen in der DFN-AAI (2)

Technische Umsetzung: getrennte Metadatensätze



* enthält **alle** IdP

	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`*

https://doku.tid.dfn.de/de:metadata

* „999“ wird durch einrichtungs-spezifische Nummer ersetzt

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 Zertifikat-Checks
- Lohnt sich vor allem für Einrichtungen mit vielen lokalen SPs (z.B. FU Berlin über hundert SPs)
- Angebot wird derzeit (11.11.2019) von 147 Einrichtungen mit insgesamt 975 SPs genutzt
- Doku: https://doku.tid.dfn.de/de:metadata_local

Konfiguration lokale Metadaten

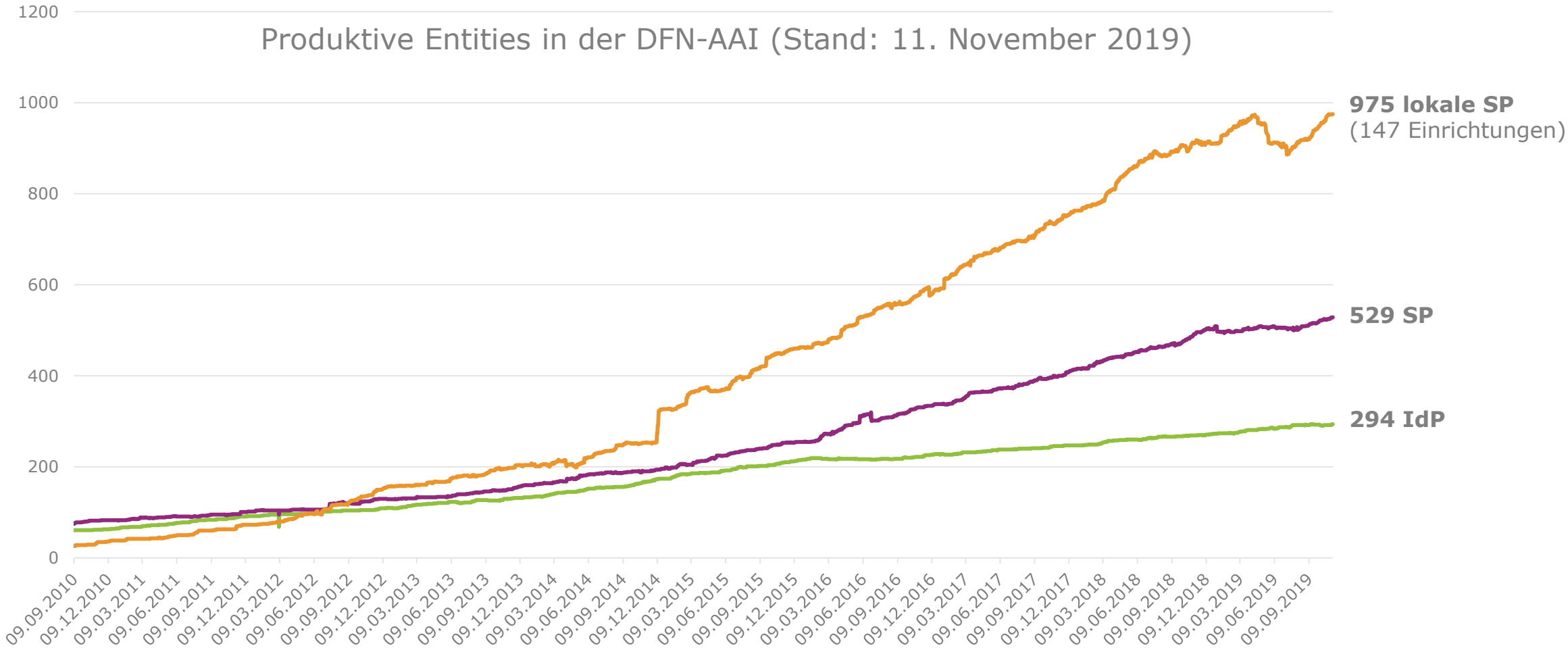
Konfiguration über Schaltfläche in Vertragsdaten verfügbar:

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**

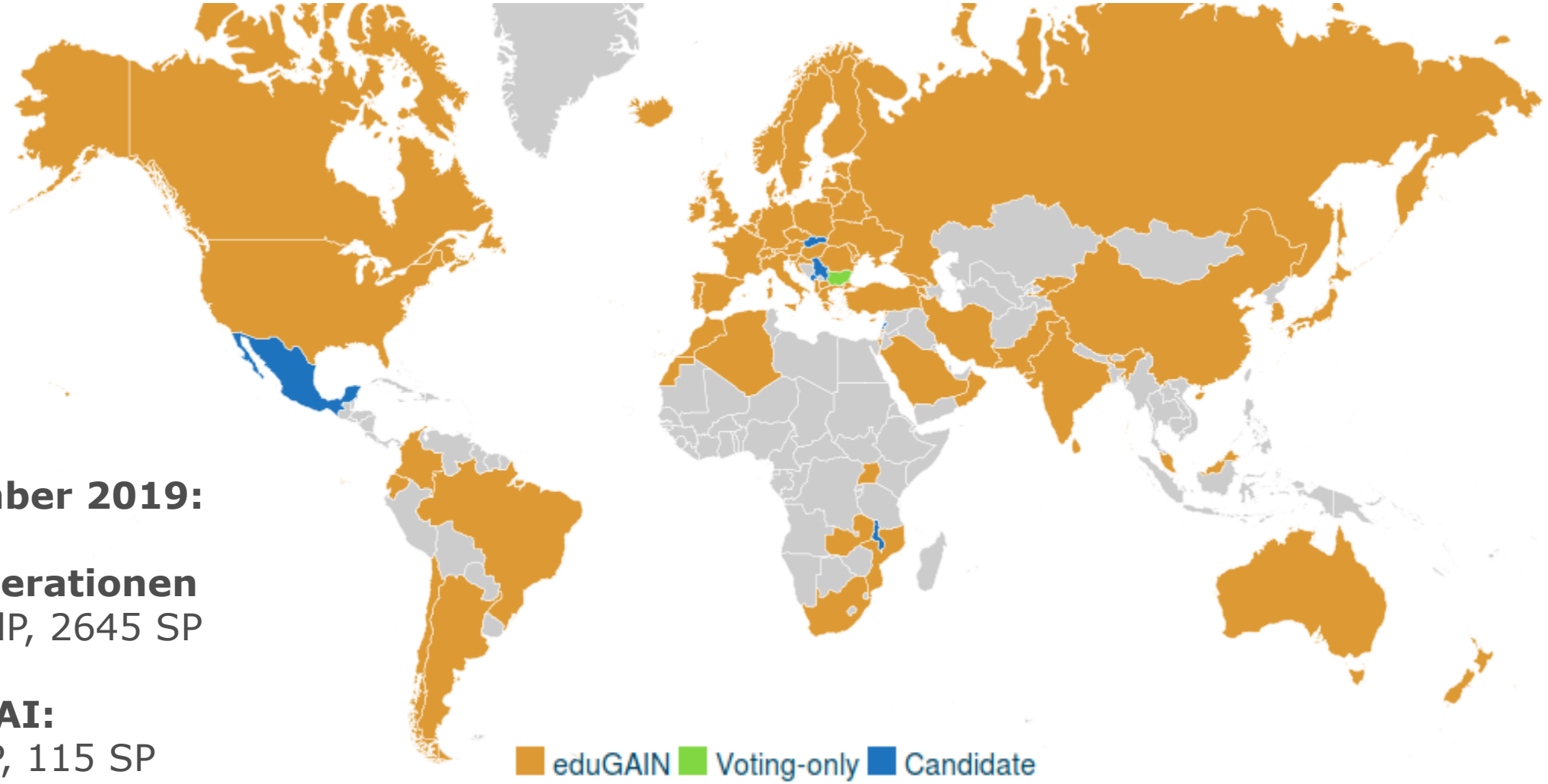
Aktuelle Zahlen DFN-AAI



eduGAIN

- Föderationsübergreifende AAI
- Betrieben von GÉANT, seit Ende 2011 im Produktivbetrieb
- Aggregation der Metadaten der teilnehmenden Föderationen („Upstream Metadata“)
- Teilnehmende Föderationen verteilen diese Metadaten intern („Downstream Metadata“)
- Upstream Metadata: Opt-in vs. Opt-out; DFN-AAI verfolgt eine Opt-in Policy, d.h. Teilnahme nur auf expliziten Wunsch
- Keine Vertragsbeziehungen zwischen DFN und IdP/SP anderer Föderationen(!)

eduGAIN – beteiligte Föderationen

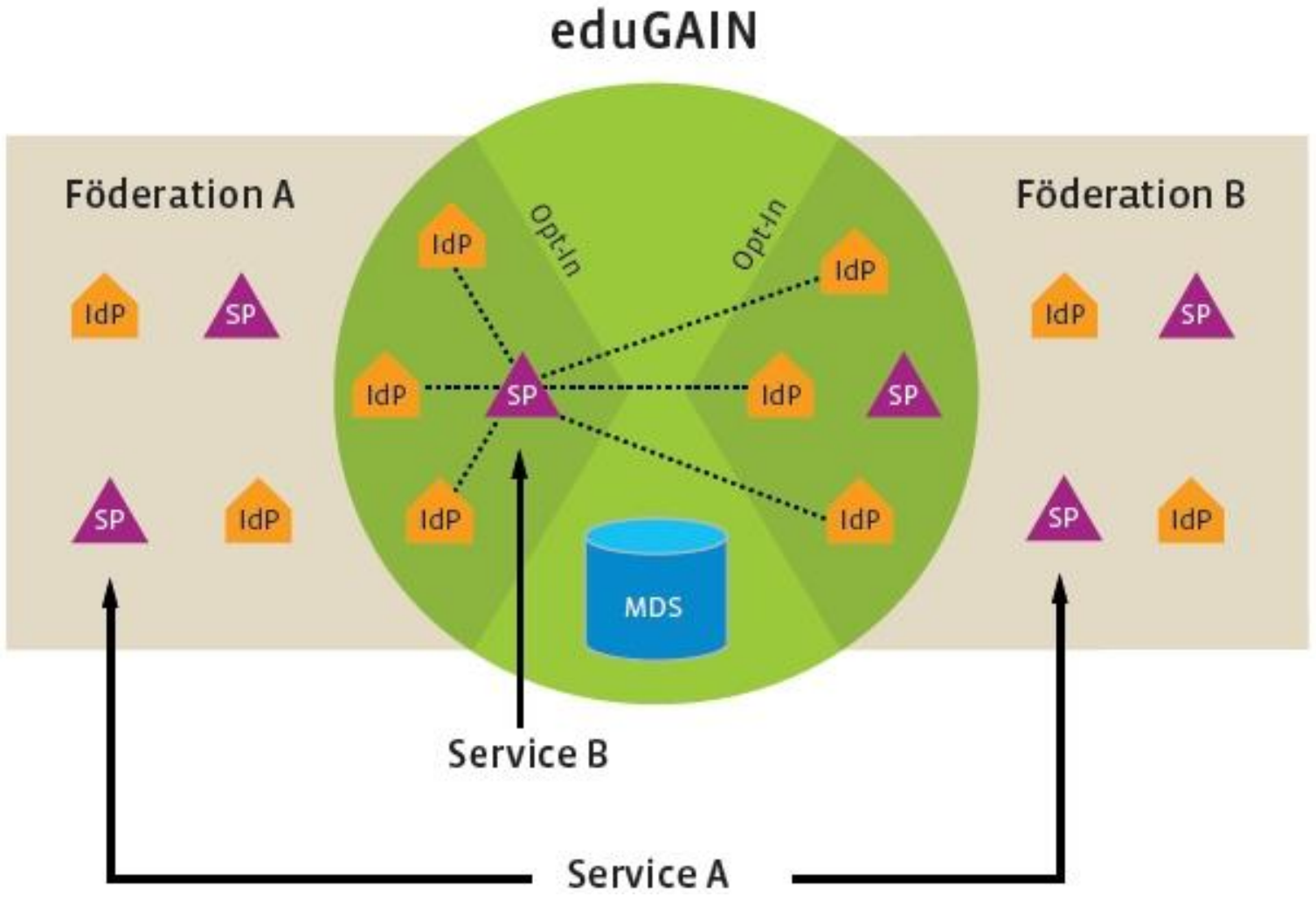


November 2019:

66 Föderationen
3152 IdP, 2645 SP

DFN-AAI:
198 IdP, 115 SP

eduGAIN Metadata Distribution Service



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)

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)
  - Embedded Discovery Service (am SP)
  - WAYFless URLs
- DFN-AAI Wiki: https://doku.tid.dfn.de/de:discovery

Beispiel zentraler Discovery Service

- Vom DFN betrieben
- Stündlich neu generiert
- DFN-AAI (”Advanced”)
- DFN-AAI-Basic
- DFN-AAI-Basic+eduGAIN
- DFN-AAI-Test
- ...

Embedded Discovery Service (EDS)

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

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://doku.tid.dfn.de/Shibboleth.sso/Login?entityID=https://idp.dfn.de/idp/shibboleth
- Siehe auch unter https://doku.tid.dfn.de/de:shibwayfless

Teilnahme

Rollen in der DFN-AAI

- Föderationsbetreiber (DFN-AAI Team)
  - Metadatenverwaltung, Metadatenverwaltungsnutzerverwaltung
- Teilnehmer (IdP/AA → Dienstvereinbarung, SP → SP Agreement)
  - Vertrag: administrativer AP, technischer AP (beide in Vertrags-DB)
  - Metadata-Admin (in Vertrags-DB)
- Entity (IdP/AA/SP) – Kontakte in Metadaten:
  - Support
  - Administrativ
  - Technisch
  - Security

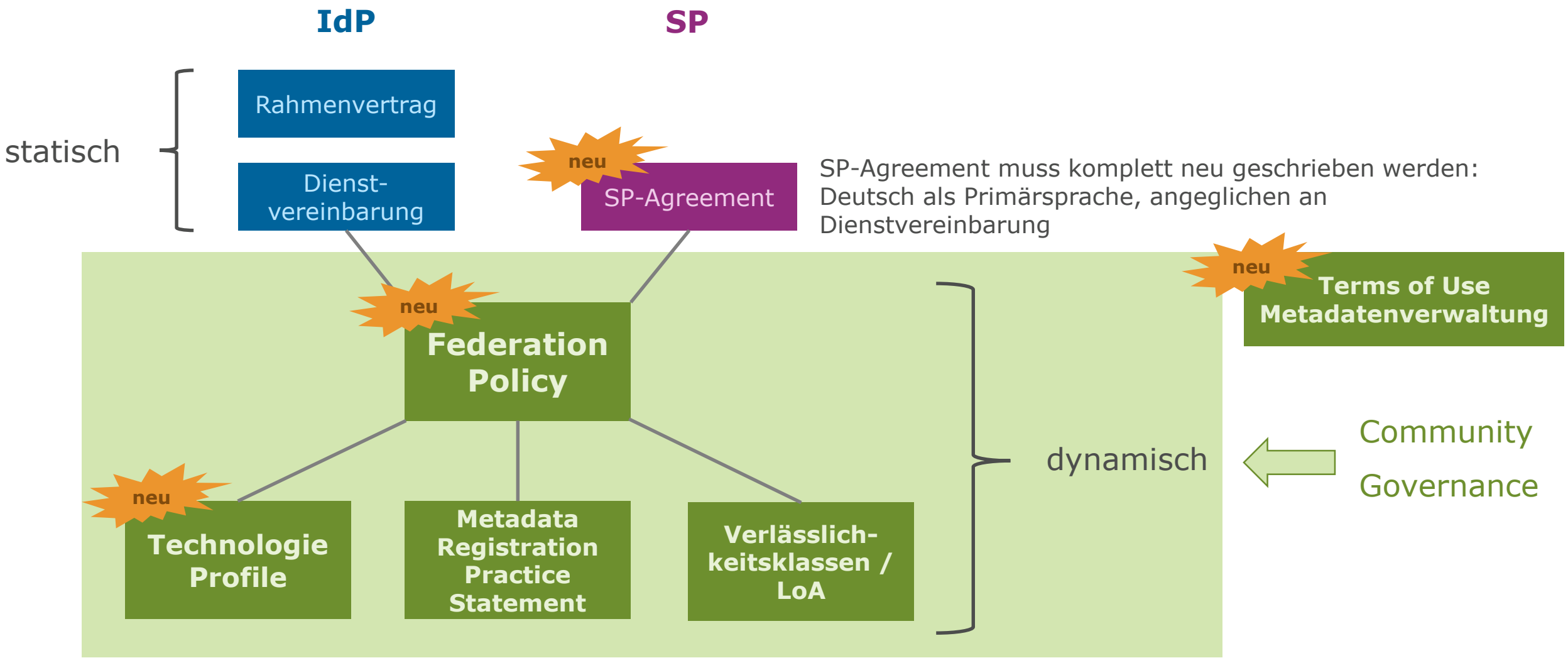
International (eduGAIN) in etwa parallele Strukturen

IR Koordination:
eduGAIN Support Team
support@edugain.org

Verträge für die Teilnahme an der DFN-AAI

- Unterschiedliche Vertragstypen, abhängig von Rolle
  - Identity Provider (IdP) – Heimateinrichtungen (Hochschulen, Forschungseinrichtungen,…)
  - Service Provider (SP) – kommerzielle und nicht-kommerzielle Dienstanbieter, aber auch Heimateinrichtungen
- Heimateinrichtungen: DFN-AAI ist ein Mehrwertdienst (DFNInternet ab I02), erforderlich sind Rahmenvertrag *und* Dienstvereinbarung
  - Dienstvereinbarung beinhaltet SP-Option
- Dienstanbieter: SP-Agreement (englisch) – keine sonstigen Voraussetzungen

DFN-AAI Policy-Framework



Sonstiges

Shibboleth

- … ist der Name eines Software-Projekts: Identity Provider (Java) und Service Provider (Apache Modul, C++)
- Ursprünglich von Internet2 entwickelt, erstes Release 2003
- Bezeichnung geht zurück auf Bibel: Richter 12,5-6 (illustrierte Version, The Brick Testament)
- Weiterentwicklung wird seit 2013 vom Shibboleth Consortium getragen (über 50 Mitglieder)
- Aktuell 8 Entwickler beschäftigt

Aktivitäten und Kooperationen national

- Mitarbeit im ZKI Arbeitskreis Verzeichnisdienste
- DFN-Betriebstagung: AAI-Forum
- Gemeinsam mit FU Berlin: seit 2015 jährlicher Shibboleth Workshop, nächster Termin: voraussichtlich Frühjahr 2020 (Berlin)
- Auf Anfrage Schulungsveranstaltungen für regionale Nutzerschaft
  - Anfang Dezember 2019: Schleswig-Holstein
- Organisation und Moderation von Ad-hoc-Arbeitsgruppen

Aktivitäten und Kooperationen international

- DFN-Verein ist eduGAIN-Mitglied der ersten Stunde
- GÉANT Project (GN4-3): Beteiligung in WP5, „Trust & Identity“
- AARC2 - Authentication and Authorisation for Research and Collaboration
  - Anforderungen der Research Communities erheben und Lösungen erarbeiten (Projektende April 2019)
- Mitgliedschaft im Shibboleth Consortium (seit 2014)
  - Wolfgang Pempe (DFN-Verein) ist als einer von zwei gewählten Members‘ Representatives Mitglied im Consortium Board

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://refeds.org/assurance
  - Ermöglicht LoAs per Identität / Login-Vorgang
- Unterstützung für OpenID Connect, http://openid.net/connect/
- Konzeption eines möglichen edu-ID-Dienstes im Rahmen einer ZKI Arbeitsgruppe, https://doku.tid.dfn.de/de:aai:eduid:start
- Konzept „AAIplus“ zur Sicherung der Zukunftsfähigkeit der DFN-AAI

Vielen Dank! Fragen? Kommentare?

- Kontakt

E-Mail: pempe@dfn.de
Tel.: +49-30-884299-308
Fax: +49-30-884299-370

Adresse:
DFN-Verein, Geschäftsstelle
Alexanderplatz 1
D-10178 Berlin

Informationsquellen

- SAML:
  https://www.oasis-open.org/standards#samlv2.0
  https://wiki.oasis-open.org/security
- DFN-AAI Wiki:
  https://doku.tid.dfn.de/de:dfnaai:start,
- Verzeichnis(se) der Teilnehmer: https://tools.aai.dfn.de/entities/
- Materialien aus anderen Veranstaltungen (Betriebstagungen, Workshops, etc.): https://doku.tid.dfn.de/de:aai:infos und
  https://doku.tid.dfn.de/de:shibidp3documents
- Shibboleth Wiki: https://wiki.shibboleth.net

Backup-Folien

SAML Security Features – Example 1

SP issues an AuthnRequest to IdP

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest
  AssertionConsumerServiceURL="https://testsp2.aai.dfn.de/Shibboleth.sso/SAML2/POST"
  Destination="https://testidp.aai.dfn.de/idp/profile/SAML2/Redirect/SSO"
  ID="_af589aa9da48910a8ba91184ab421479"
  IssueInstant="2016-11-18T23:08:00Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1"/>
</samlp:AuthnRequest>
```

1. reads SP's Entity ID…

2. performs a lookup in federation metadata…

Federation Metadata

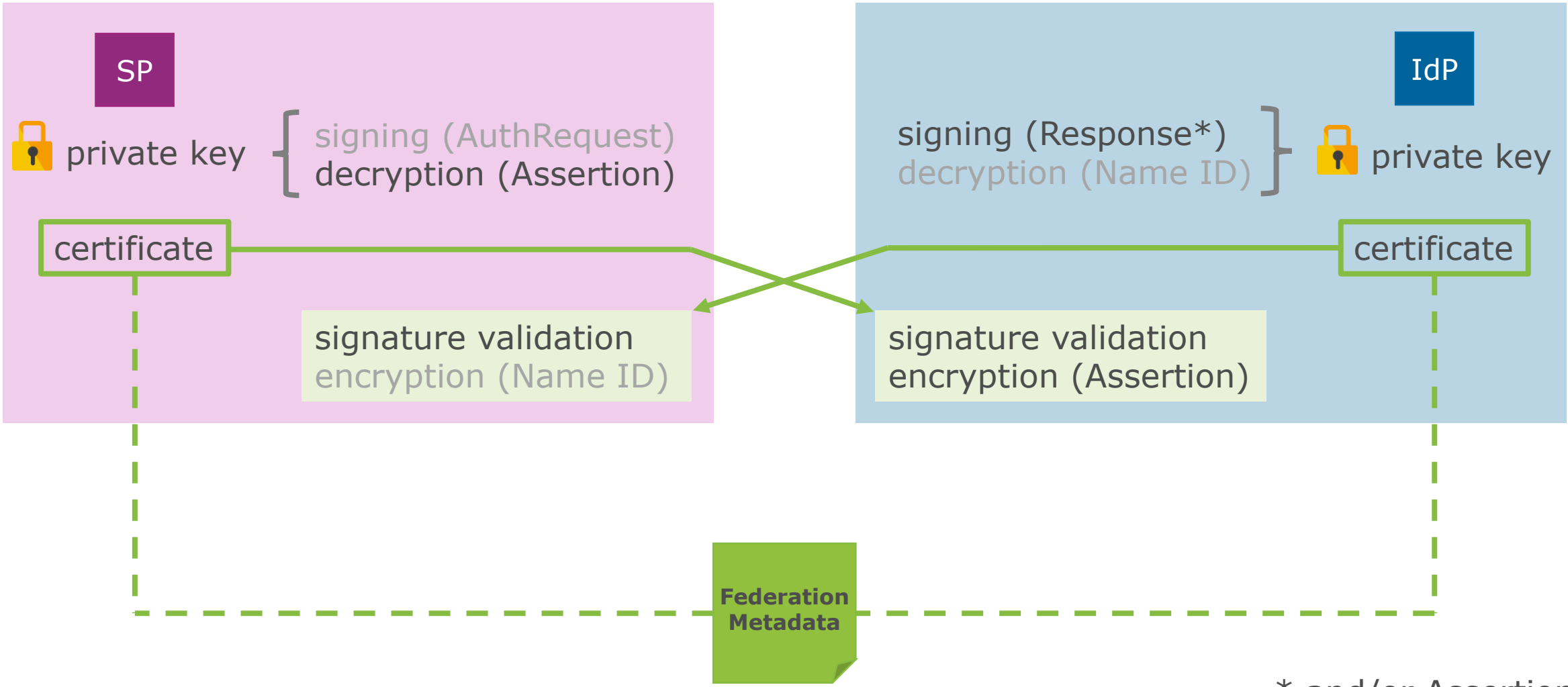
```
<EntityDescriptor entityID="https://testsp2.aai.dfn.de/shibboleth">
  <Extensions><!-- . . . --></Extensions>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <!-- . . . -->
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                              Location="https://testsp2.aai.dfn.de/Shibboleth.sso/SAML2/POST" index="1"/>
```

3. checks if any of the ACS URLs matches with the one in the AuthnRequest?

yes → **Continue**

no → **Abort [ERROR]**

SAML Security Features – Example 2



* and/or Assertion

Sonstige Dienste und Leistungen

- Discovery Service (”WAYF”), stündlich neu aus den jeweiligen 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://doku.tid.dfn.de/de:dfnaai:start, 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)

OpenID Connect

- Basiert auf OAuth 2.0, REST/JSON (also JSON anstatt XML)
- Entwicklung wurde und wird von diversen Internet-Konzernen getrieben
- Vorteil gegenüber SAML: funktioniert auch ohne Web Browser (→ mobile Endgeräte, Apps)
- Vertrauen bisher über abgeschlossenen technischen/organisatorischen Kontext gegeben
- OpenID Connect Federation: Konzept signierter Metadaten für OIDC
- Shibboleth IdP: OIDC-Unterstützung über Extension verfügbar

Incident Response

- AAI-spezifische Szenarien
  - IdP: Identitätsdiebstahl und unberechtigter Zugriff (z.B.) auf Forschungsdaten
  - SP: Hackerangriff mit Diebstahl dienstlokaler Nutzer- und/oder Forschungsdaten
  - Föderationsbetreiber: Sicherheitslücke / Identitätsdiebstahl in Metadatenverwaltung
- Metadaten: Separate Kontakte für Sicherheitsvorfälle
- Prozesse kompatibel mit Sirtfi-Empfehlungen (Security Incident Response Trust Framework for Federated Identity, https://refeds.org/sirtfi)
- Zusammenarbeit mit dem IR-Team des DFN-CERT https://www.aai.dfn.de/sicherheit/