deutsches forschungsnetz

Grundlagen:
AAI, Web-SSO, Metadaten und Föderationen

DFN-AAI Workshop, FH Dortmund | 28./29. August 2018

Wolfgang Pempe (pempe@dfn.de)

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** = **A**uthentication and **A**uthorization **I**nfrastructure
- 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.)

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
- Speicher- und Filesharing-Dienste (Gigamove, sciebo, bwSync&Share, …)
- Webkonferenzen u.a.m.

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

Dienste und Nutzergruppen

2007 → heute

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

Verteilung lizenzierter Software – Microsoft Dreamspark, Kivuto, etc.

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

Speicher-, Kommunikationsdienste – Gigamove, WebConf …

Landesdienste – bwIDM, SaxID, sciebo, hessenbox, …

E-Research – CLARIN, DARIAH, ELIXIR …

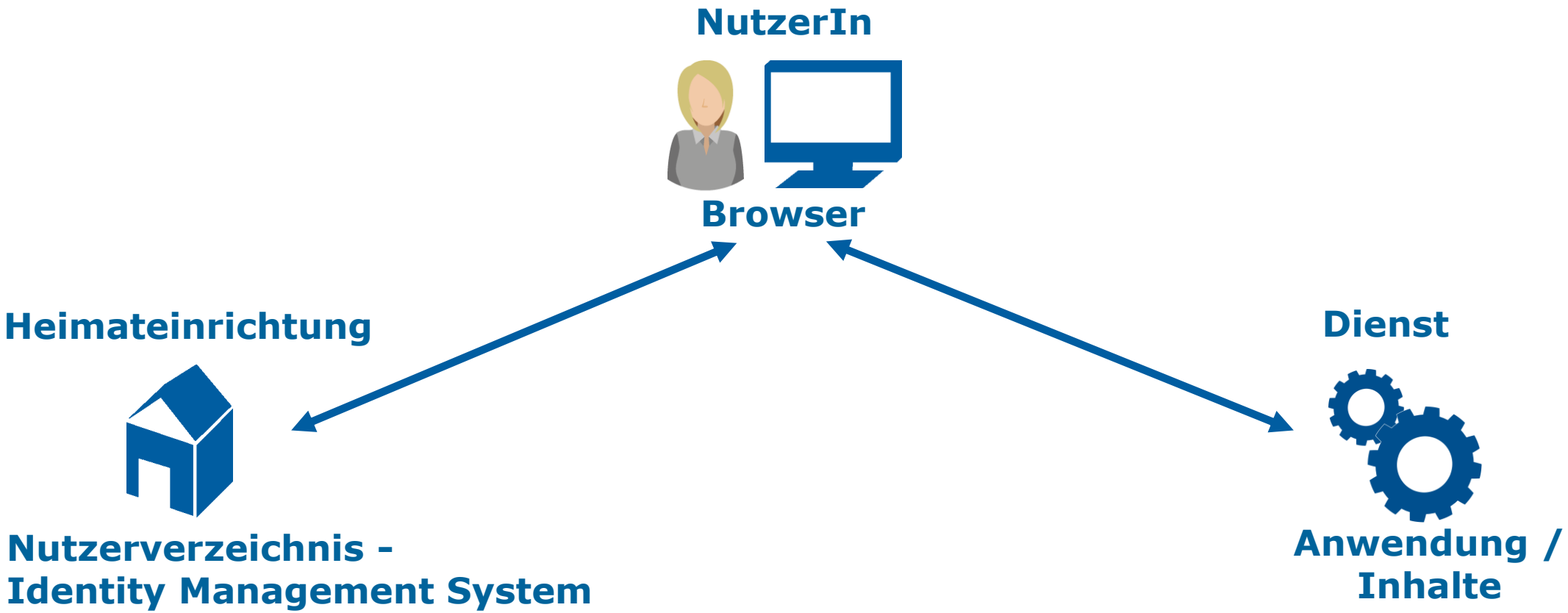
Internat. Forschungscommunities (→ eduGAIN)

Bibliotheksnutzer

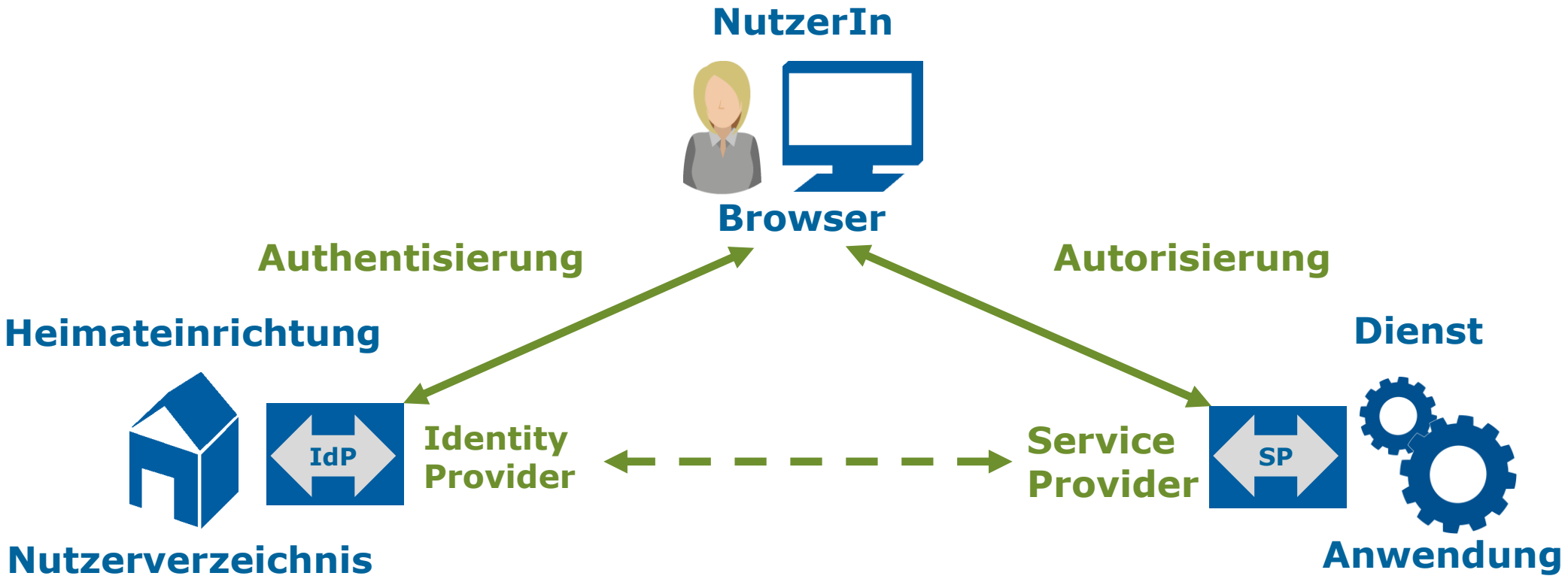
Studierende, Lehrpersonal

Forschende

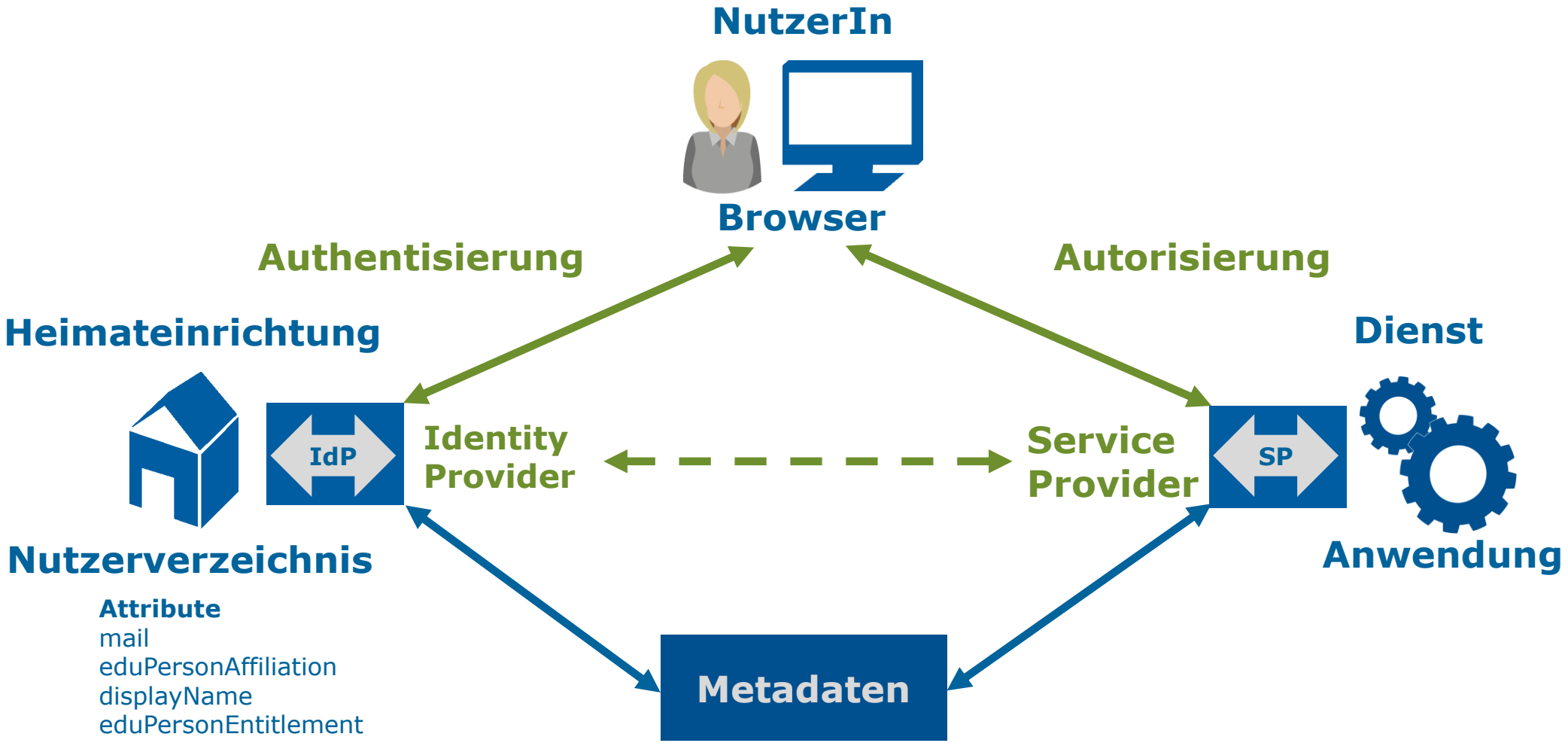
Web-SSO = Dreiecksbeziehung



Dreiecksbeziehung im Detail



Lingua franca: SAML (bzw. SAML2)



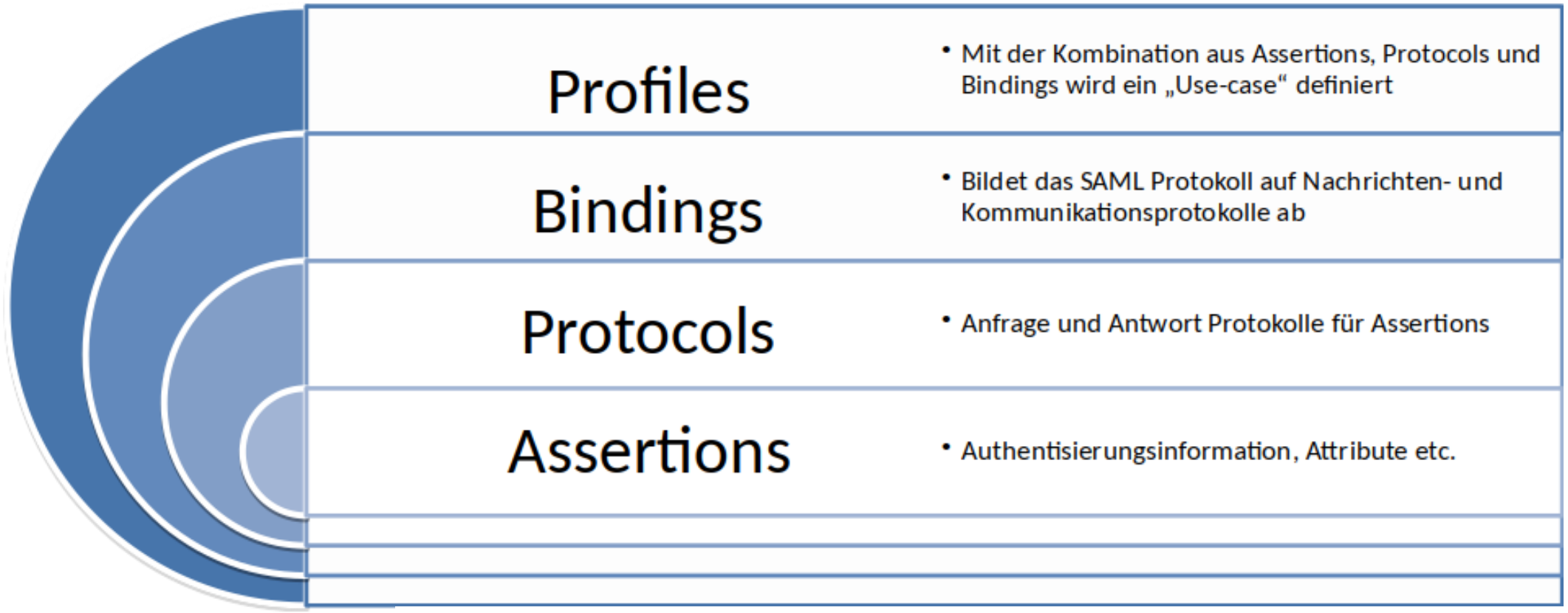
Siehe auch: https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

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

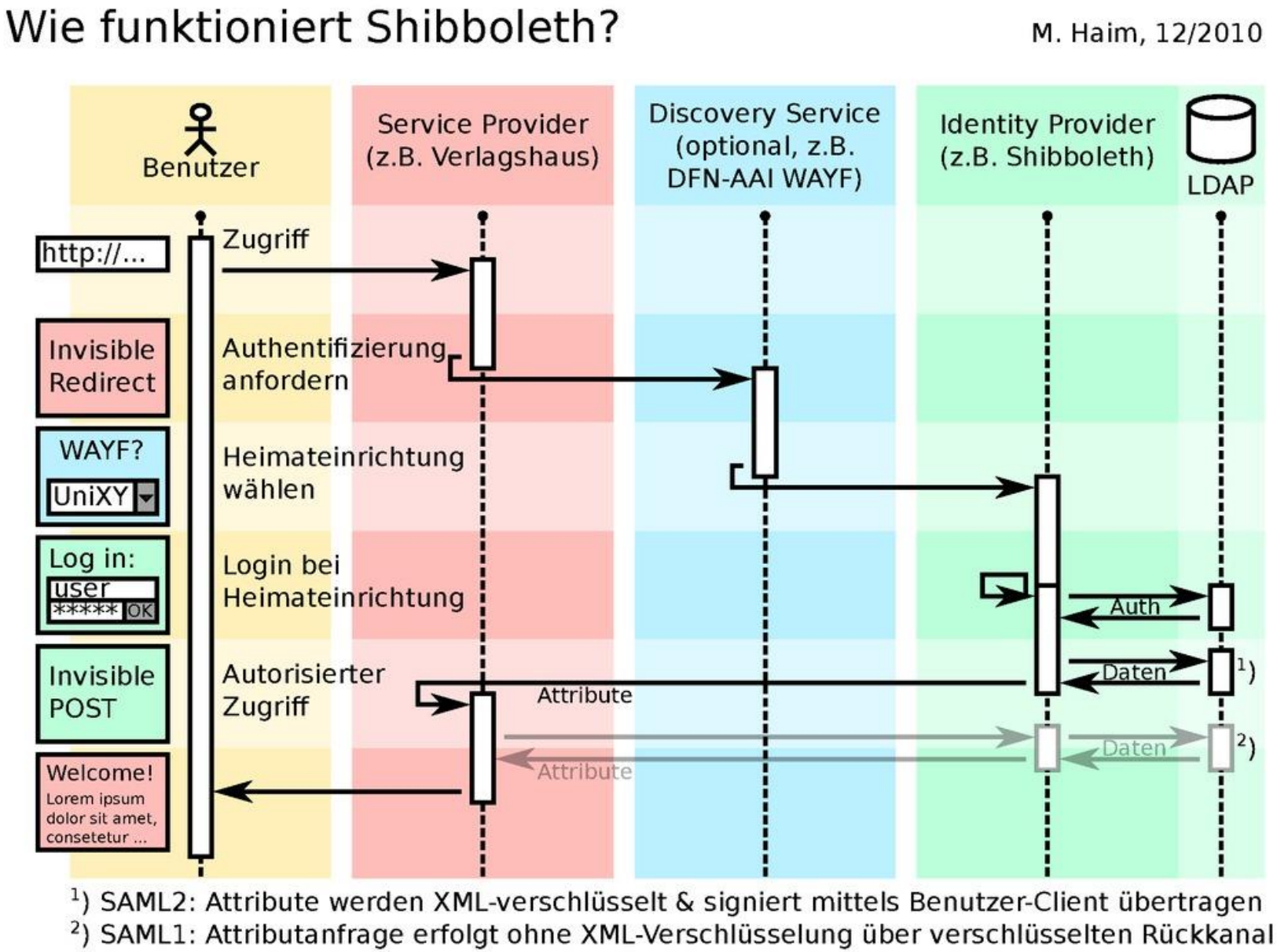
- Konfigurationsdaten für Service- und Identityprovider

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://idp.fh-dortmund.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

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>` (Typ: technical, administrative, support, security)

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>`

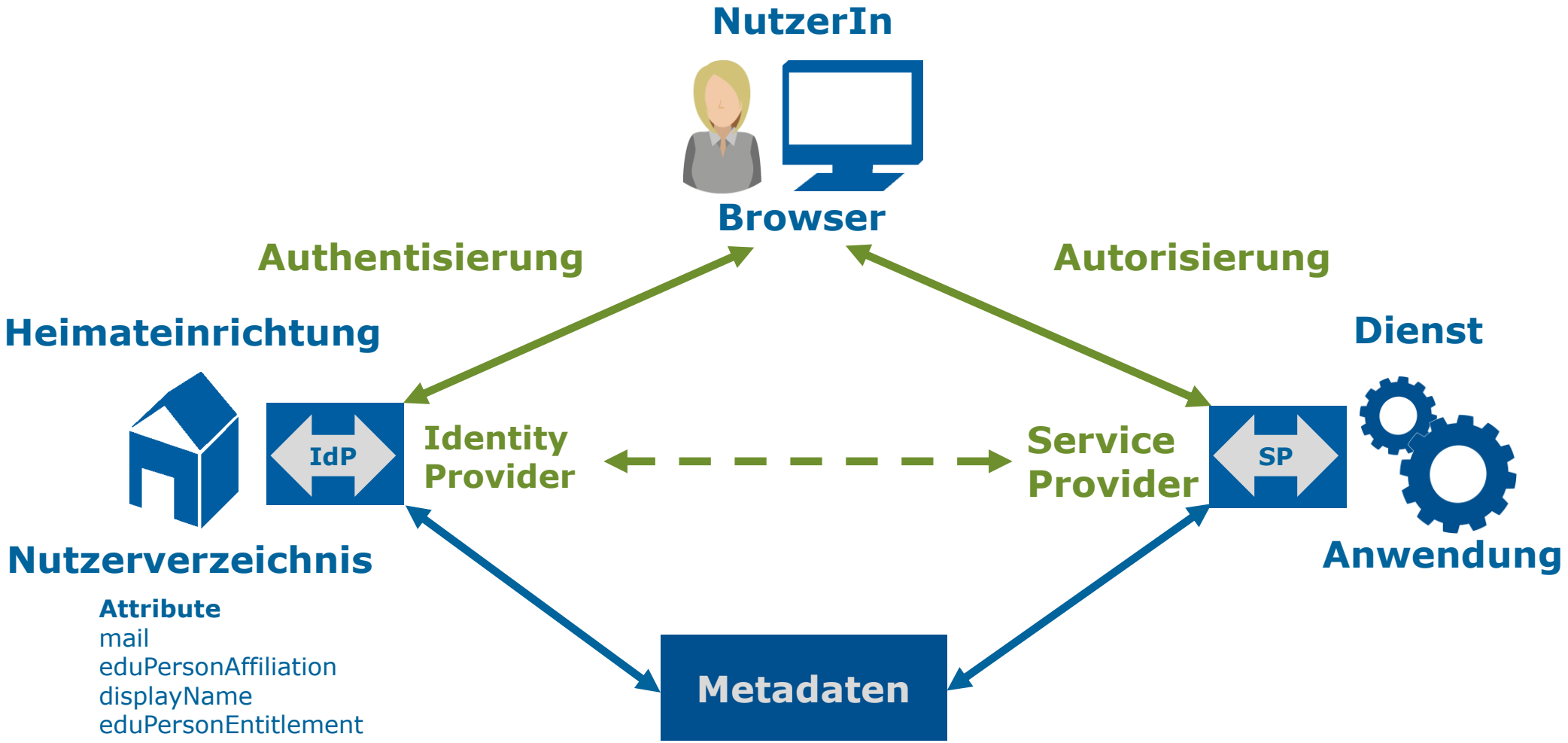
Bindings für SLO (Single Log-out)

`<SingleLogoutService>`

Deklaration der vom SP benötigten Attribute

`<AttributeConsumingService>`

Wir erinnern uns…



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

SAML Security Features - Example

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]**

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

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)

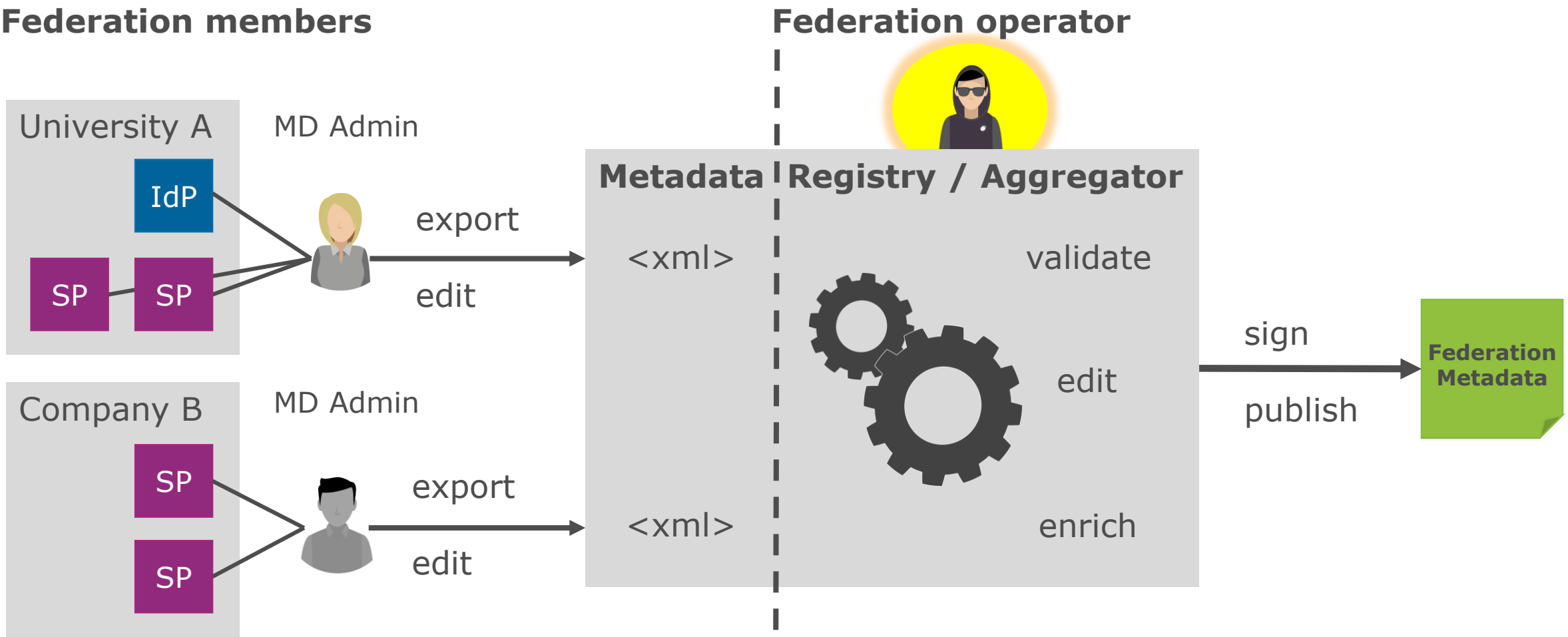
Föderationen – DFN-AAI

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**

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

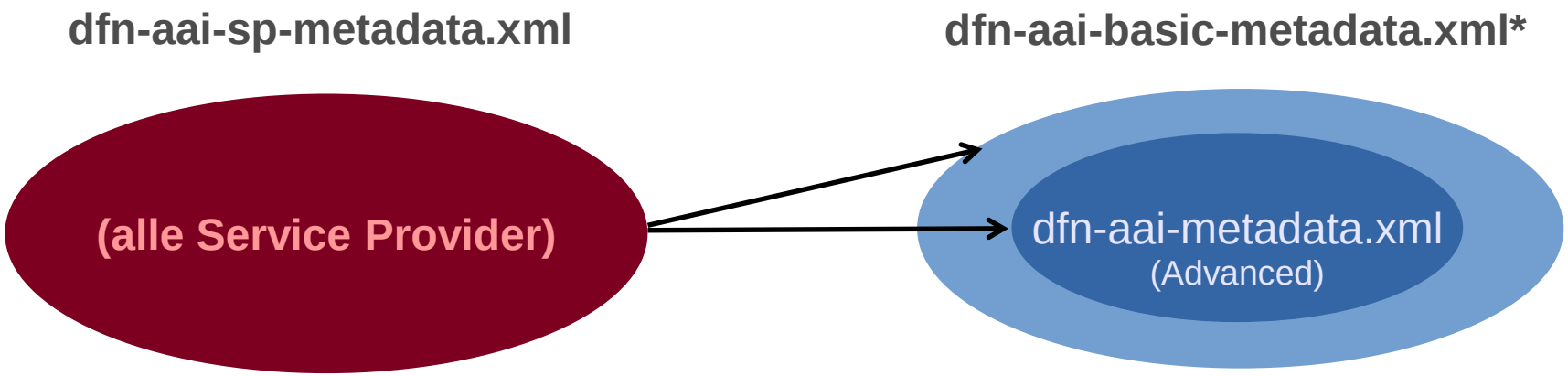
Verlässlichkeitsklassen in der DFN-AAI (1)

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 Zertfikat-Checks
- Lohnt sich vor allem für Einrichtungen mit vielen lokalen SPs (z.B. FU Berlin über hundert SPs)
- Angebot wird derzeit (21.8.2018) von 133 Einrichtungen mit insgesamt 884 SPs genutzt
- Doku: https://doku.tid.dfn.de/de:metadata_local

Konfiguration lokale Metadaten

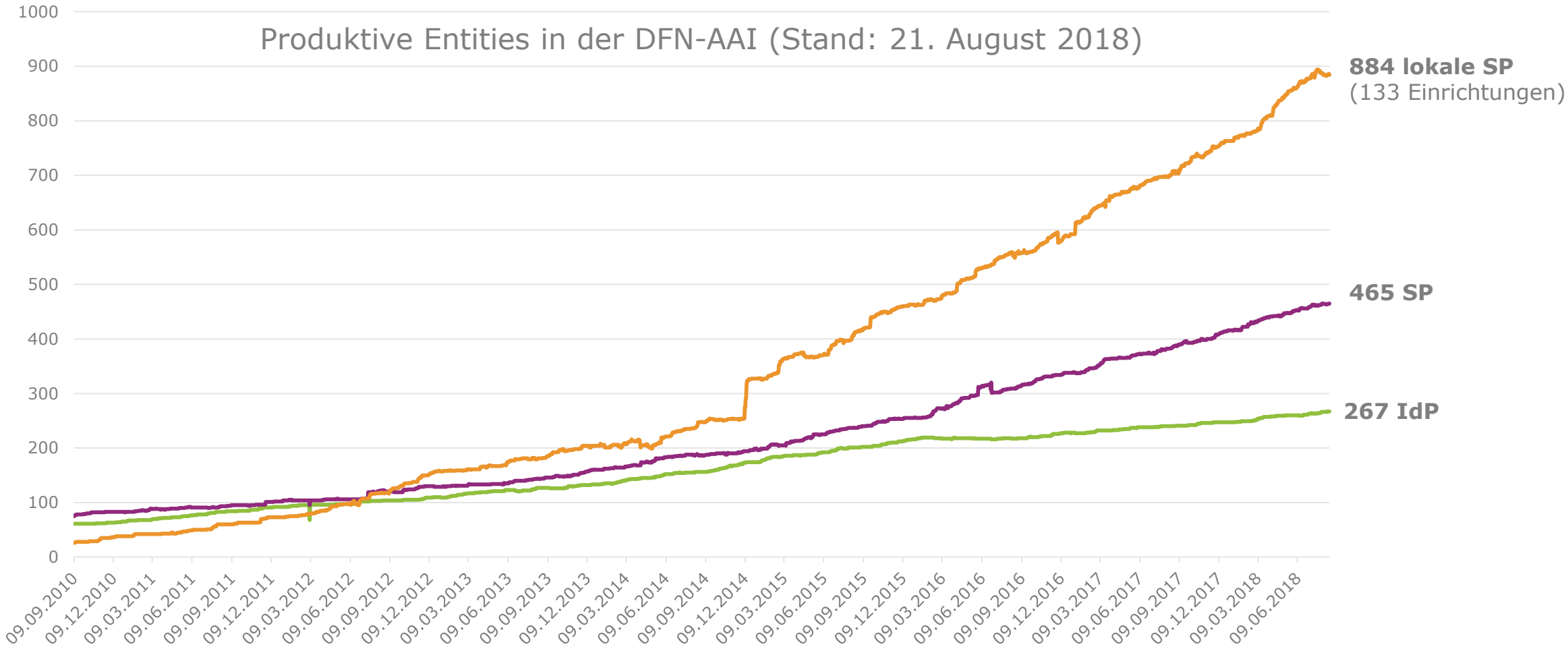
Konfiguration über Schaltfläche in Vertragsdaten verfügbar:

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**

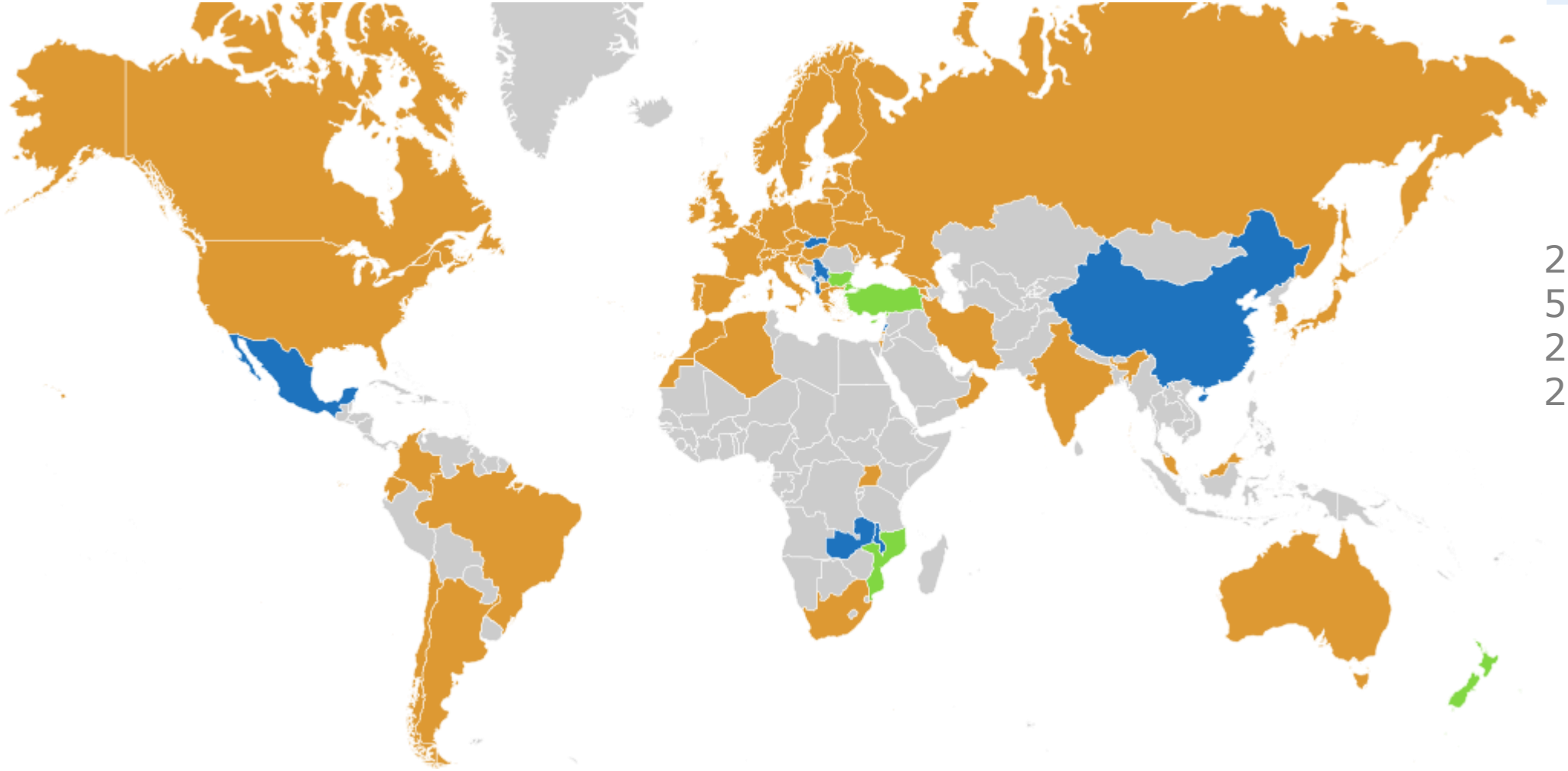
Aktuelle Zahlen DFN-AAI



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

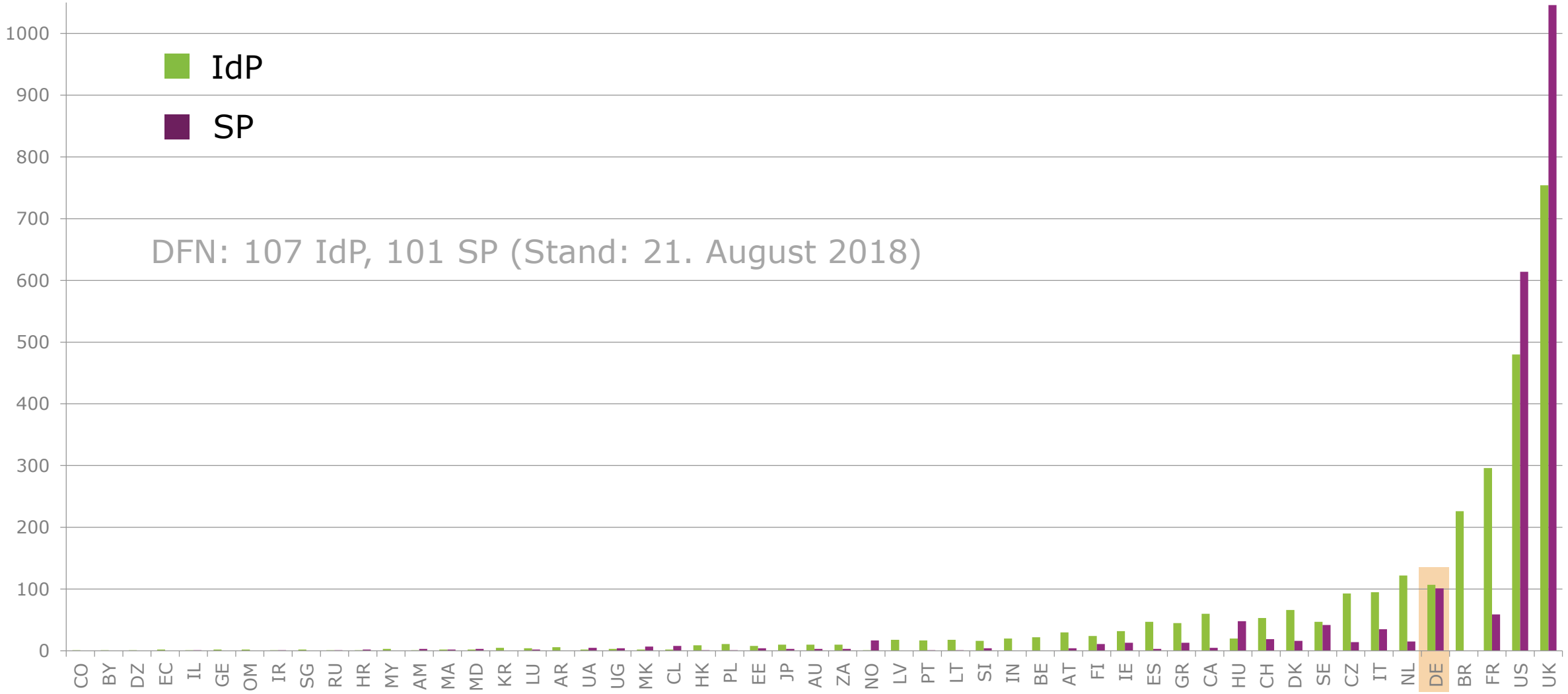


21. August 2018:
53 Föderationen
2813 IdP
2138 SP

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

Quelle: https://technical.edugain.org/

eduGAIN – Beteiligung je Föderation



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 Subföderationen (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

Virtuelle Subföderation, Metadatenverwaltung

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-Attribute/-Kategorien

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

☐ **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.

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 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)

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

Sonstiges

Aktivitäten und Kooperationen international

- DFN-Verein ist eduGAIN-Mitglied der ersten Stunde
- GÉANT Project (GN4-2): Beteiligung an Tasks in JRA3, Trust and Identity Development:
  - Task 2: Research and Service Providers
  - Task 3: Next Generation Trust and Identity Technology Development (→ OIDC)
- AARC2 - Authentication and Authorisation for Research and Collaboration
  - Anforderungen der Research Communities erheben und Lösungen erarbeiten
- 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://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework+round+2
  - 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

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 (→ GN4-2, JRA3)
- DFN-AAI: Bridging-Elemente für lokale Installationen (SAML-Proxy)?
- Shibboleth IdP: OIDC-Unterstützung wird derzeit implementiert

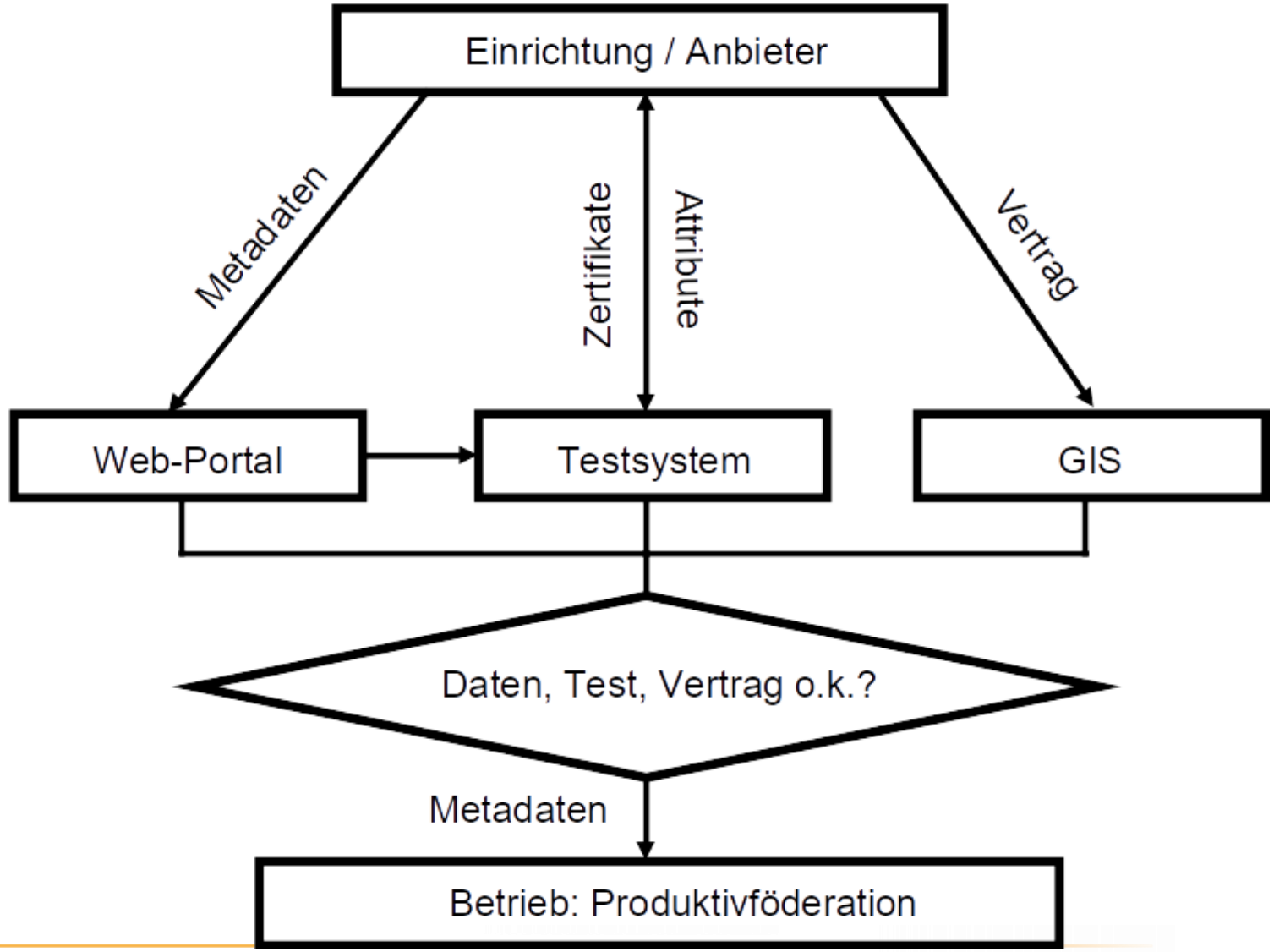
Incident Response

- AAI-spezifische Szenarien
  - IdP: Identitätsdiebstahl und unberechtigter Zugriff (z.B.) auf Forschungsdaten
  - SP: Hackerangriff mit Diebstahl dienstlokaler Nutzer- und/oder Forschungsdaten
- Zusammenarbeit mit DFN-CERT
- Entwurf mit Handlungsanweisungen für Vorfälle innerhalb der DFN-AAI
- Metadaten: Separate Kontakte für Sicherheitsvorfälle
- Prozesse kompatibel mit Sirtfi-Empfehlungen (Security Incident Response Trust Framework for Federated Identity, https://refeds.org/sirtfi)
- Geplanter Testlauf mit ausgewählten Hochschulen und Diensten in der DFN-AAI, Ende 2018 Teilnahme an internationalem Sirtfi-Testlauf

Teilnahme

- Die wichtigsten Schritte sind im DFN-AAI Wiki unter https://doku.tid.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)

Aufnahme in Produktivföderation



Vielen Dank! Fragen? Kommentare?

- Kontakt
  - DFN-AAI Team

    E-Mail: aai@dfn.de
    Tel.: +49-30-884299-9124
    Fax: +49-30-884299-370

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

Informationsquellen (1)

- DFN-AAI Wiki: https://doku.tid.dfn.de/de:dfnaai:start
- Änderungsfeed: https://doku.tid.dfn.de/feed.php
- Materialien aus anderen Veranstaltungen (Betriebstagungen, Workshops, etc.) https://www.aai.dfn.de/aktuelles/archiv/ und https://doku.tid.dfn.de/de:shibidp3documents
- Shibboleth Wiki: https://wiki.shibboleth.net
- Online Doku SWITCHaai: https://www.switch.ch/aai/guides/

Informationsquellen (2)

- OpenID Connect

  https://openid.net/connect/, https://wiki.geant.org/x/KxKIAw

- OpenID Connect Federation

  http://openid.net/specs/openid-connect-federation-1_0.html

  Implementierung am Shibboleth IdP:

  https://github.com/CSCfi/shibboleth-idp-oidc-extension

- Shibboleth Consortium

  https://www.shibboleth.net/

Hier ist erstmal Schluss…

Backup-Folien

Verlässlichkeitsklassen in der DFN-AAI

- **Nachteile des bisherigen Ansatzes:**
- Eine Verlässlichkeitsklasse / *Level of Assurance* (LoA) pro IdP → Speziallösungen (Attribute Filter Policies) für Identitäten, die nicht den Anforderungen genügen
- Verlässlichkeitsklasse = Kombination unterschiedlicher Kriterien, diese können nicht einzeln von SP adressiert werden
- Umständliches Handling der verschiedenen Metadaten-Dateien, ideal wäre eine Datei mit SP- und eine mit IdP-Metadaten
- Insellösung, auf die DFN-AAI beschränkt, keine Interoperabilität mit anderen Föderationen, die genau das selbe Problem haben
- Ziel: LoA-relevante Infos pro Login-Vorgang/Identität an SP mitteilen

Verlässlichkeitsklassen in der DFN-AAI (4)

- Zukünftiger internationaler Standard: REFEDS Assurance Framework (RFA)
- Informationen als Attribute übertragen (eduPersonAssurance)
- Ergänzt durch Multifactor Authentication Profile (MFA) und Single Factor Authentication Profile (SFA)
- Primäre Zielgruppe: E-Research Community

Value	Cappuccino	Espresso
$PREFIX$	X	X
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/low	X	X
$PREFIX$/IAP/medium	X	X
$PREFIX$/IAP/high		X
$PREFIX$/IAP/local-enterprise		
$PREFIX$/ATP/ePA-1m	X (*)	X (*)
$PREFIX$/ATP/ePA-1d		

Exkurs: GÉANT Data Protection Code of Conduct

- Verhaltenscodex für Service Provider: https://wiki.refeds.org/display/CODE
- Aktueller Überblick: https://monitor.edugain.org/coc/
- Version 2 („GDPR Version“) derzeit in Arbeit, bezieht sich auf Art. 40 (2) „Verhaltensregeln“ – Verbände und andere Vereinigungen
- Soll dem *European Data Protection Board* (ehem. Art. 29 WP) vorgelegt werden
- Geltungsbereich:
  - SPs in EU and EEA (EU28 + Norway, Iceland, Liechenstein)
  - SPs in EC whitelist countries and international organizations (”providing adequate protection”)
  - SPs in other countries and international organizations (Art. 46.2(e): ”together with binding and enforceable commitments”)