

DEN
deutsches forschungsnetz

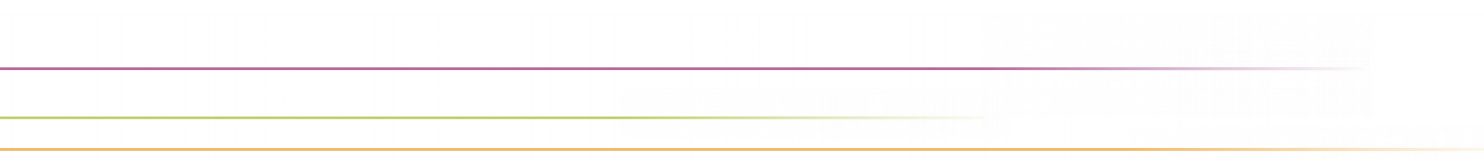


DFN

Einführung in die DFN-AAI

DFN-AAI Workshop

Silke Meyer (smeyer@dfn.de)



Heute

- ▶ Was ist die DFN-AAI?
- ▶ Shibboleth in a Nutshell
- ▶ Metadaten und SAML2
- ▶ Der Discovery Service
- ▶ Einführung in eduGAIN
- ▶ Shibboleth IdP 3.x – Fertigstellung der Grundinstallation

Morgen

- ▶ Vertiefung: Attribute und Attributfreigaben (Wolfgang Pempe)
- ▶ Shibboleth-Konfigurationsübungen
- ▶ Fragen aus der Praxis

Was ist die DFN-AAI?

Klassisch: Dienstspezifische Identitäten

- ▶ User haben ein Login pro Dienst, viele Passwörter und ggf. TANs/Tokens.
- ▶ Jeder Dienst muss sicheres Login implementieren.
- ▶ Verteilte Hacking-Versuche sind schwer zu korrelieren.
- ▶ erleichtertes Phishing, weil jede Anmeldeseite anders aussieht

Single Sign-On

- ▶ User haben nur noch einen Username + Passwort.
- ▶ User sind nach *einem* Login z.B. für 1 Tag an *allen* Diensten angemeldet.
- ▶ Die zentrale Loginseite kann alle aktuellen Technologien für sicheres Login umsetzen (z.B. Smartcard, Token, ...).
- ▶ nur eine Nutzer-DB nötig, die dafür besser geschützt werden kann
- ▶ (Identitäts-)Hacking-Angriffe können nur an einer Stelle auftreten → leichter zu erkennen
- ▶ erleichterter Support und Passwort-Reset

Begriffsklärungen (1)

- ▶ **AAI** = **A**uthentication and **A**uthorization **I**nfrastructure
 - ▶ lokal oder einrichtungsübergreifend
 - ▶ im letztgenannten Fall: **zentrale Instanz** (AAI-Betreiber) stellt Einhaltung der technischen und rechtlichen Rahmenbedingungen sicher
- ▶ Identity Federation / „**Föderation**“
- ▶ Eine solche Föderation ist die DFN-AAI.

Begriffsklärungen (2)

- ▶ **Web-SSO** = Web **S**ingle **S**ign-**O**n
 - ▶ browserbasiert
 - ▶ *eine* Anmeldung für alle Dienste, für die man zugriffsberechtigt ist
 - ▶ keine dienstspezifischen Credentials, Login findet immer bei Heimateinrichtung statt
- ▶ **SAML** = **S**ecurity **A**ssertion **M**arkup **L**anguage
- ▶ **Shibboleth** ist eigentlich eine Software...
- ▶ ... wird aber häufig synonym für SAML-basiertes Web-SSO verwendet.

Worum geht es in der (DFN-)AAI?

- ▶ Zugriff auf Dienste via Web-Single Sign On
- ▶ lokale, einrichtungs- und föderationsübergreifende Zusammenarbeit
- ▶ Datenschutz bzw. Datensparsamkeit: Nutzernamen + Passwörter werden nicht an Dienste übertragen
- ▶ Organisatorische Basis: Vertrauen (bzw. Verträge)
- ▶ Technische Basis: Metadaten

Typen von Entitäten in einer AAI (1)

- ▶ **IdP** = Identity Provider
 - ▶ liefert Informationen über Nutzer an Service Provider
 - ▶ Authentifizierung erfolgreich
 - ▶ Übertragung weiterer Attribute (zur Autorisierung am SP bzw. zur Personalisierung des Dienstes)
- ▶ **Attribute Authority** = „abgespeckter IdP“
 - ▶ liefert nur Attribute
 - ▶ direkter Zugriff seitens des SP

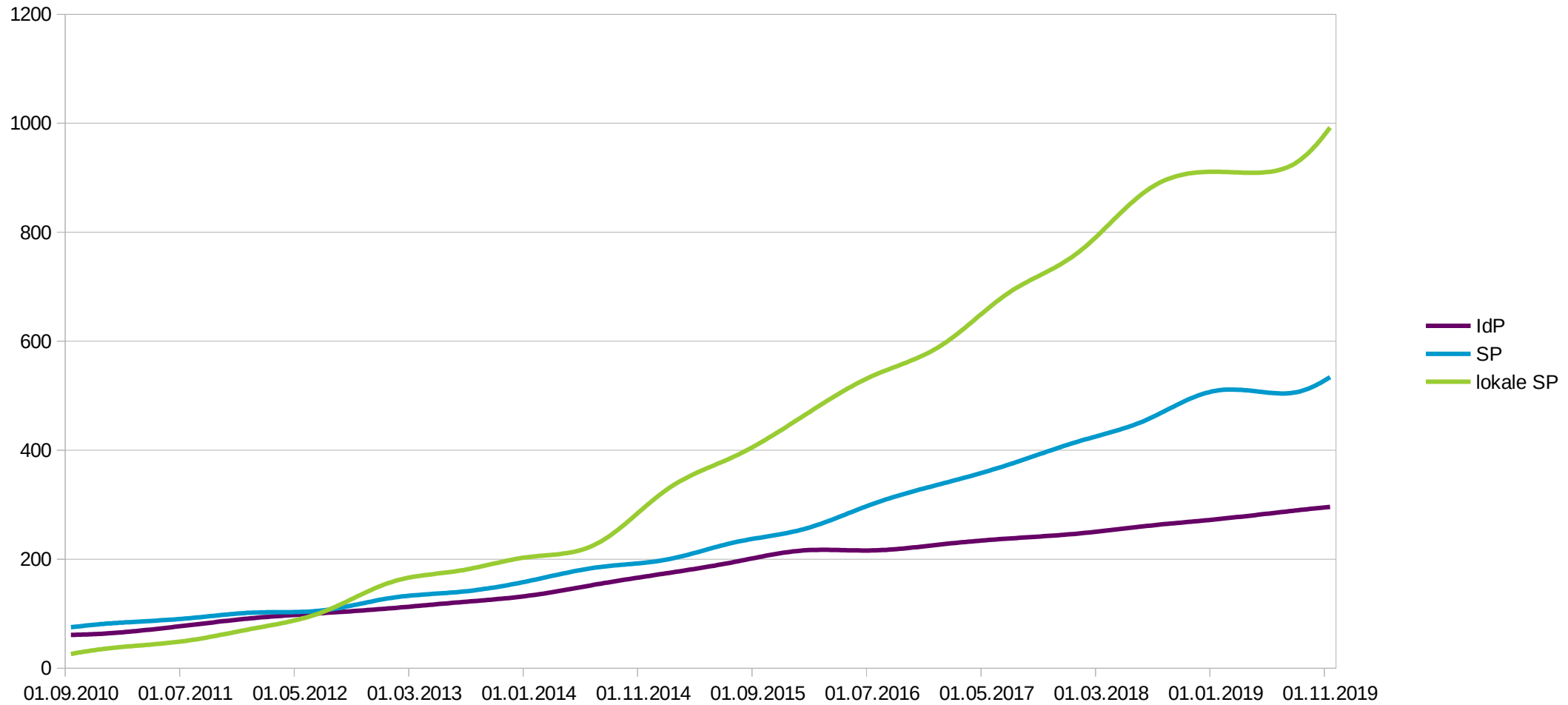
Typen von Entitäten in einer AAI (2)

- ▶ **SP** = Service Provider
 - ▶ schützt Ressourcen
 - ▶ wertet SAML-Assertions aus
 - ▶ reicht Attribute an die dahinter liegende Anwendung weiter
- ▶ Unser Schwerpunkt heute: Identity Provider

Dienste

- ▶ Zielgruppe: Angehörige von Bildungs- und Forschungseinrichtungen
- ▶ Verlage und Bibliotheken
- ▶ Verteilung lizenzierter Software
- ▶ Hochschulinterne Dienste
- ▶ E-Learning-Plattformen
- ▶ Forschungsprojekte und -infrastrukturen
- ▶ Speicher- und Filesharing-Dienste, Webkonferenzen u.v.m.
- ▶ [Verzeichnis](#) der Dienste in der DFN-AAI, AAI-Doku: [Dienste nutzen](#)

Die DFN-AAI in Zahlen



Die Rolle des Föderationsbetreibers

- ▶ Der Föderationsbetreiber schafft den vertraglichen und technischen Rahmen:
 - ▶ Verträge mit allen Teilnehmern
 - ▶ Metadatenverwaltung
 - ▶ Zertifikatsüberprüfung und -überwachung
 - ▶ **signierte Metadaten**

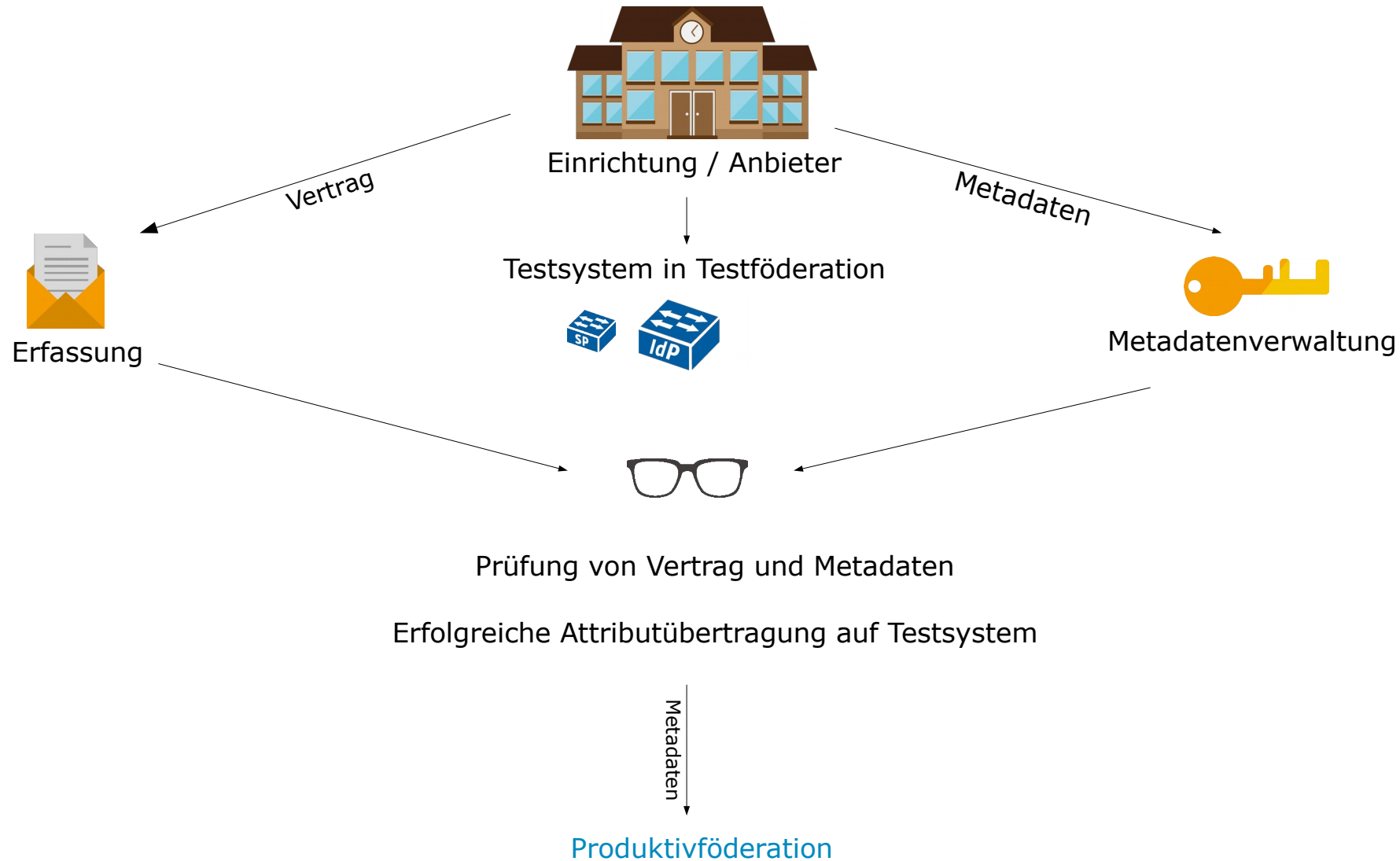
Metadaten: Technisches Rückgrat einer Föderation

Nur wenn auf beiden Seiten (IdP/AA, SP) die Metadaten des jeweiligen Kommunikationspartners bekannt sind, funktioniert die Kommunikation!

Teilnahme an der DFN-AAI

- ▶ Dokumentation
- ▶ Teilnahme für DFNInternet-Teilnehmer
 - ▶ Rahmenvertrag
 - ▶ Dienstvereinbarung für DFN-AAI (deckt Betrieb von SPs mit ab)
- ▶ Kosten
 - ▶ im **Entgelt für DFNInternet** enthalten (ab Kategorie Portanschluss I02)

Aufnahme in die DFN-AAI



Weitere Dienste und Leistungen

- ▶ Testumgebung: Testföderation mit Test-IdPs und -SPs
- ▶ Discovery Services, stündlich aktualisiert
 - ▶ auch für Testföderation
- ▶ Support und Beratung: hotline@aai.dfn.de
- ▶ Workshops / Schulungen
- ▶ Mailinglisten

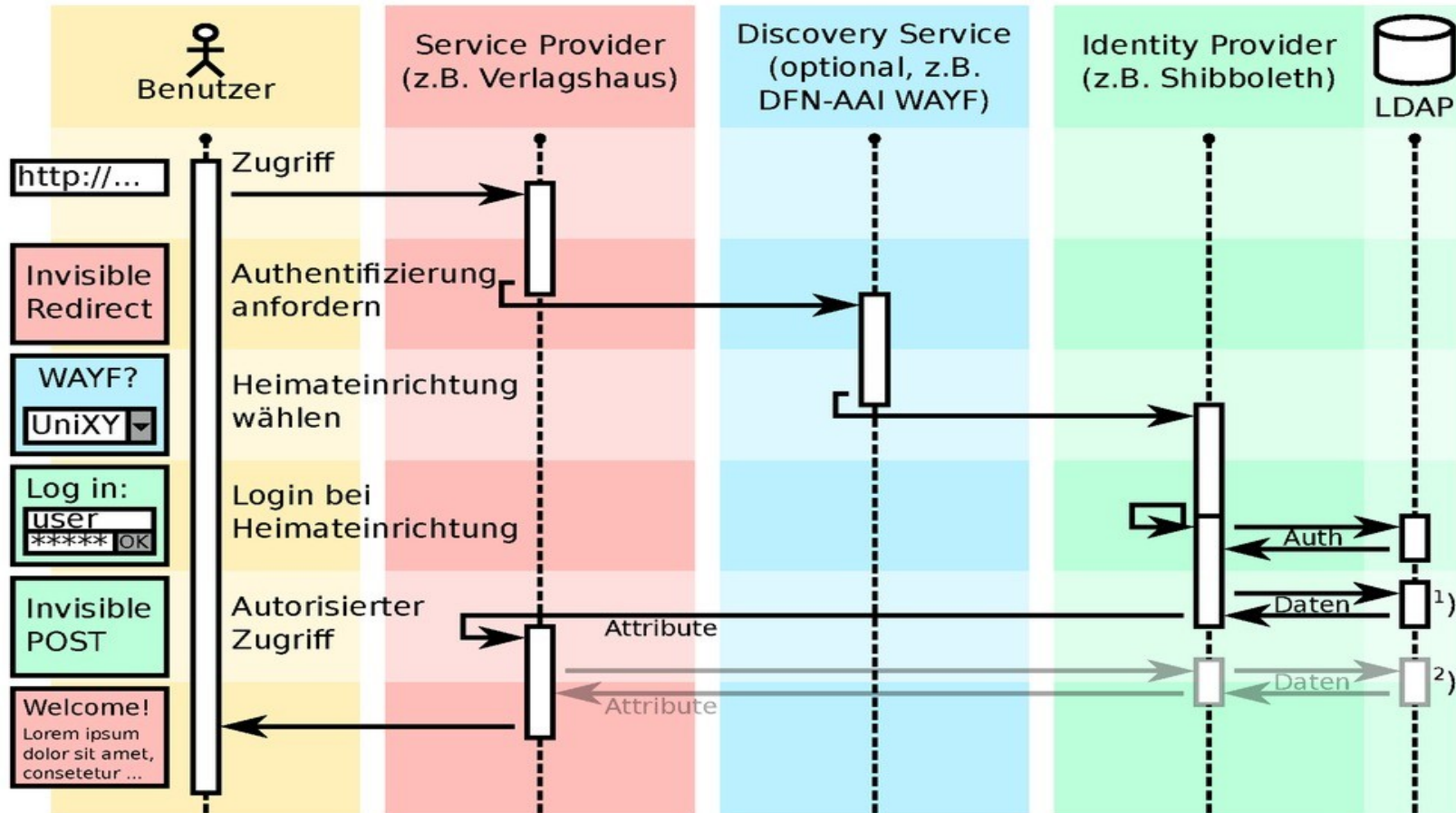
Shibboleth in a Nutshell



Die Kommunikation im Detail

Wie funktioniert Shibboleth?

M. Haim, 12/2010



1) SAML2: Attribute werden XML-verschlüsselt & signiert mittels Benutzer-Client übertragen

2) SAML1: Attributanfrage erfolgt ohne XML-Verschlüsselung über verschlüsselten Rückkanal

Quelle: Manuel Haim, Uni Marburg

Kurze Einführung in Attribute

- ▶ IdP übermittelt Attribute an SP, Infos über NutzerInnen
- ▶ Attribute bilden die Grundlage für Autorisierung („Was darf ich hier?“)
- ▶ Manche Attribute dienen der eindeutigen Identifizierung von NutzerInnen und der Personalisierung des Dienstes
- ▶ SP übermittelt sie an die geschützte Anwendung
- ▶ SP und/oder Anwendung entscheiden über Zugriff

Attributschemata

- ▶ Schemata definieren Attribute, ihre zulässigen Werte und deren Bedeutung
- ▶ Etablierte Schemata im Föderationsumfeld ([Dokumentation](#)):
 - ▶ EduPerson (international)
 - ▶ SCHAC (Schema for Academia, international)
 - ▶ dfnEduPerson (e-Learning, Deutschland)
 - ▶ Weitere Attribute aus dem inetOrgPerson-Schema
- ▶ Die Schemata können, müssen aber nicht im IdM existieren!

IdP übersetzt IdM-Attribute in SAML2

- ▶ IdP liest Attribute aus Nutzerverzeichnis aus und schreibt sie um auf eduPerson, SCHAC, dfnEduPerson etc.
- ▶ IdP kann neue Attribute aus bestehenden Attributen generieren
- ▶ IdP arbeitet mit konfigurierbaren Attributdefinitionen:
 - ▶ Simple
 - ▶ Mapped
 - ▶ ScriptedAttribute
 - ▶ weitere

Metadaten und SAML2

Metadaten als „Rückgrat der Föderation“

- ▶ Abbildung des Vertrauensverhältnisse zwischen den teiln. Organisationen
- ▶ DFN gibt stündlich signierte Metadaten heraus: Wer nimmt an AAI teil, unter welchen Adressen, mit welchen Zertifikaten?
- ▶ „Sprecht nur mit denen, die in den Metadaten stehen!“
- ▶ IdP / SP: Informationsabgleich der Informationen der Gegenseite mit den Föderationsmetadaten
- ▶ Abbruch der Kommunikation bei Nichtübereinstimmung

Metadaten-Abgleich bei der SAML-basierter Kommunikation

SP

stellt AuthnRequest an

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"
  [...]>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
</samlp:AuthnRequest>
```

Metadaten-Abgleich bei der SAML-basierter Kommunikation

SP

stellt AuthnRequest an

IdP

1. Lesen der Entity Id des SP

```
<?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"
  [...]>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
</samlp:AuthnRequest>
```

Metadaten-Abgleich bei der SAML-basierter Kommunikation

SP

stellt AuthnRequest an

IdP

1. Lesen der Entity Id des SP

```
<?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"
  [...]>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
</samlp:AuthnRequest>
```

2. Nachschlagen in Föderationsmetadaten

Federation
Metadata

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

Metadaten-Abgleich bei der SAML-basierter Kommunikation

SP

stellt AuthnRequest an

IdP

1. Lesen der Entity Id des SP

```
<?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"
  [...]>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
</samlp:AuthnRequest>
```

2. Nachschlagen in Föderationsmetadaten

Federation Metadata

```
<EntityDescriptor entityID="https://testsp2.aai.dfn.de/shibboleth">
  <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. Vergleich mit ACS URLs im AuthnRequest

Metadaten-Abgleich bei der SAML-basierter Kommunikation

SP

stellt AuthnRequest an

IdP

1. Lesen der Entity Id des SP

```
<?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"
  [...]>
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://testsp2.aai.dfn.de/shibboleth</saml:Issuer>
</samlp:AuthnRequest>
```

2. Nachschlagen in Föderationsmetadaten

Federation Metadata

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

3. Vergleich mit ACS URLs im AuthnRequest

Weiter

ja

nein

Abbruch [ERROR]

SAML-Metadaten

- ▶ enthalten alle für die Kommunikation benötigten Informationen
- ▶ eindeutiger Identifier: entity ID
 - ▶ Datentyp: anyURI (Bsp: <https://idp.dfn.de/idp/shibboleth>)
 - ▶ Entity ID muss nicht auf Web-Ressource verweisen bzw. dem Hostname der Entity entsprechen
 - ▶ Einrichtung sollte Rechte an der Domain besitzen
 - ▶ Best Practice: Entity ID verweist auf IdP-/SP-Metadaten
- ▶ zur Einführung: [SAML V.20 Metadata Guide](#) von Oasis

Beispiele für Metadaten

- ▶ IdP: <https://idp.dfn.de/idp/shibboleth>
- ▶ Attribute Authority: <https://attributes.dfn.de/idp/shibboleth>
- ▶ SP: <https://clarin.ids-mannheim.de/shibboleth>

Metadaten – typunabhängige Elemente

- ▶ Wurzelelement: `<EntityDescriptor entityID="https://entity-xyz.de">`
- ▶ Informationen für User Interfaces: `<UIInfo>`
- ▶ Zertifikate: `<KeyDescriptor>`
- ▶ Benötigte / unterstützte Name Identifier: `<NameIDFormat>`
- ▶ Kontaktdaten: `<Organization>`, `<ContactPerson>` (Typ: technical, administrative, support, security)

Metadaten – IdP / AA

- ▶ IdP Single Sign-On Descriptor (nur IdP): `<IDPSSODescriptor>`
- ▶ „Scope“ (Geltungsbereich / Name der Einrichtung):
`<saml1md:Scope regexp="false">dfn.de</saml1md:Scope>`
- ▶ Bindings für SSO und SLO: `<SingleSignOnService>`, `<SingleLogoutService>`
- ▶ weitere optionale Elemente, z.B. Bindings für Attribute Queries
`<AttributeService>` oder Attribute Authority Descriptor
`<AttributeAuthorityDescriptor>`

Metadaten – SP

- ▶ SP Single Sign-On Descriptor: `<SPSSODescriptor>`
- ▶ Bindings für Entgegennahme von Assertions: `<AssertionConsumerService>`
- ▶ Bindings für SLO: `<SingleLogoutService>`
- ▶ Deklaration der vom SP benötigten Attribute: `<AttributeConsumingService>`

SAML Profile


- ▶ Kombinationen aus Assertions, Protocols und Bindings für bestimmte Anwendungsfälle
- ▶ Beispiel 1: SAML-Komponenten, die bei **Web-SSO** zum Einsatz kommen:
 - ▶ Protocol: Authentication Request Protocol
 - Binding: HTTP Redirect, HTTP POST
- ▶ Beispiel 2: **ECP** (nicht browserbasierte Anwendungen)
 - ▶ Protocol: Authentication Request Protocol
 - Bindings: PAOS, SOAP

Nutzungsmöglichkeiten von Metadaten

- ▶ auf nationaler Ebene (z.B. DFN-AAI)
- ▶ „virtuelle Subföderationen“ (z.B. Bundesländer, Forschungsprojekte)
- ▶ auf lokaler Ebene (innerhalb einer Einrichtung)
- ▶ auf internationaler Ebene / Interföderation (eduGAIN)

Föderation(en) und Metadaten in der DFN-AAI

- ▶ Organisatorisch ist die DFN-AAI *eine* Identity Federation.
- ▶ Wir stellen aber *mehrere* Metadatensätze zur Verfügung:

Föderationen					
Typ	Aktivierung	Name	Status	Kommentar	
Produktion: DFN-AAI	<input checked="" type="radio"/>	DFN-AAI	zugelassen		
	<input type="radio"/>	DFN-AAI-Basic			
	<input type="radio"/>	keine			
	<input type="checkbox"/>	lokale Metadaten			
Produktion: Interföderation	<input type="checkbox"/>	eduGAIN			
Test	<input checked="" type="checkbox"/>	DFN-AAI-Test	zugelassen		

Verlässlichkeitsklassen in der DFN-AAI

Verlässlichkeitsklasse	Identifizierung durch Heimateinrichtung	Verfahren zum Ausweis einer Identität	Prozesse zur Pflege der Identitäten
Test	Verfahren freigestellt	Verfahren freigestellt	Verfahren freigestellt
Basic	Rückantwort von eindeutiger Adresse (E-Mail, Post etc.)	Anhand eindeutig zuzuordnender digitaler Adresse	Aktualisierung innerhalb von 3 Monaten
Advanced	Pers. Vorsprechen unter Vorlage amtlicher Dokumente, Post-Ident, eID, universitäre Einschreibungs-/Einstellungsprozesse	Pers. Account bzw. digitales Zertifikat (sichere Vergaberichtlinie)	Aktualisierung innerhalb von 2 Wochen

[Dokumentation](#)

Lokale Metadaten (= lokale Mini-Föderation)

- ▶ für Einrichtungen mit vielen lokalen/internen SPs
- ▶ einrichtungsspezifischer Metadatensatz mit IdP und internen SPs
- ▶ Auch lokale Metadatensätze werden stündlich generiert und signiert.
- ▶ bei Bedarf Zugriff nur für bestimmte IP-Bereiche
- ▶ Validierung, automatische Zertifikatsprüfungen
- ▶ Dokumentation

Konfiguration lokaler Metadaten

- ▶ Aktivieren über Schaltfläche im Abschnitt „Vertragsdaten“

Verlässlichkeitsklasse	lokale Metadaten	
Advanced	aktiviert download	

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	<input type="radio"/> Basic <input checked="" type="radio"/> Advanced
Service Provider	Vertrag vorhanden / Vertragssoption aktiviert
lokale Metadaten	<input checked="" type="checkbox"/> aktivieren
Zugang zu lokalen Metadaten auf IP Bereich(e) beschränken (Hinweise zur Syntax)	<input type="text"/>
<input type="button" value="schreiben"/>	zurück zur Übersicht

Überblick über die Metadatenansätze

► Technische Umsetzung über getrennte Metadatenansätze ([Doku](#)):

	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 (alle IdP)
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*

* einrichtungsspezifische Nummer statt „999“

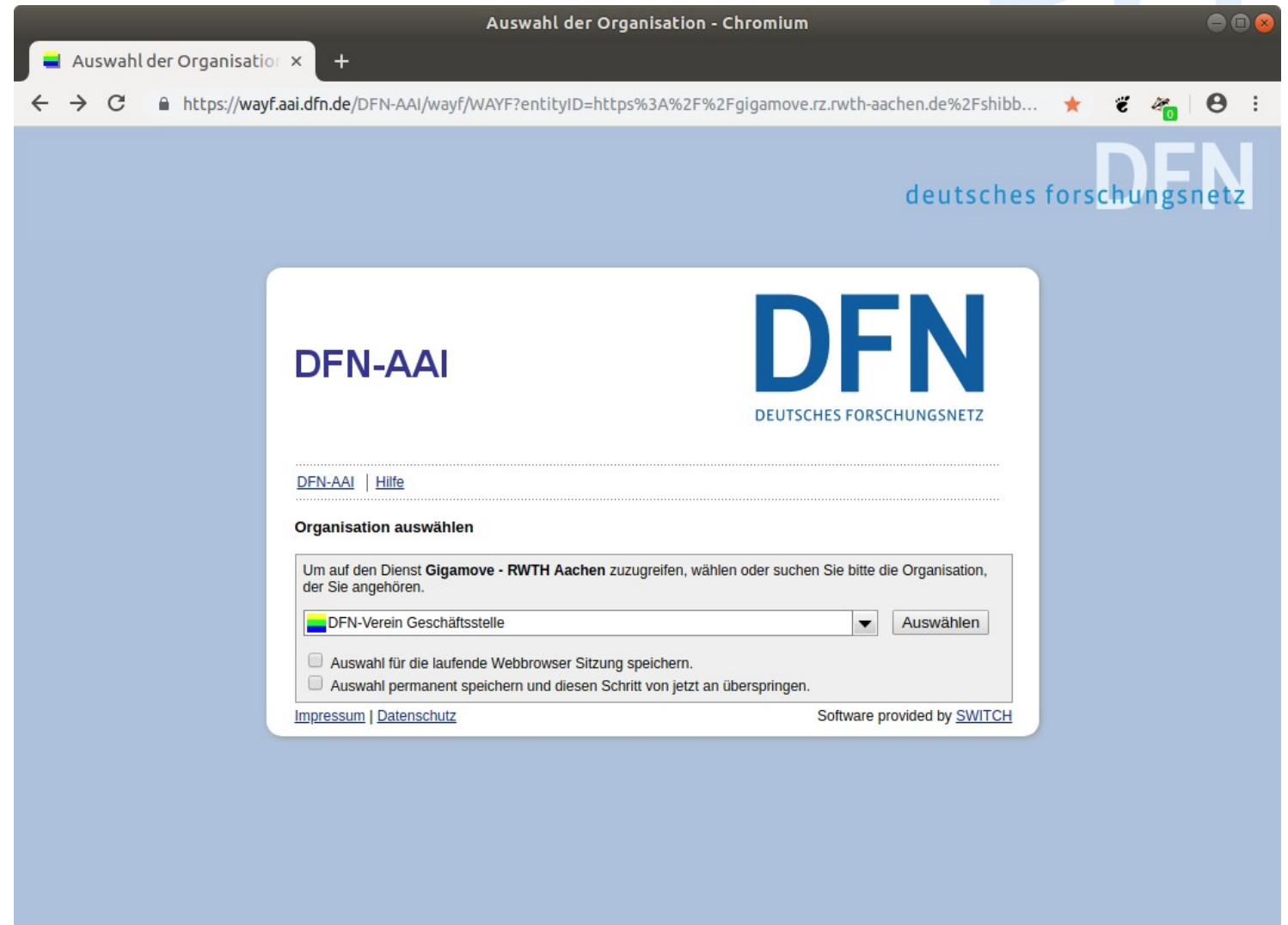
Der Discovery Service

Discovery Service

- ▶ auch bekannt als **WAYF** („**W**here **a**re **y**ou **f**rom?“)
- ▶ Browser-gestützte Auswahl der Heimateinrichtung
- ▶ Herstellung einer Verbindung zwischen SP und IdP
- ▶ Varianten:
 - ▶ zentraler Discovery Service (z.B. vom Föderationsbetreiber)
 - ▶ Embedded Discovery Service (am SP)
 - ▶ „WAYFless URLs“
- ▶ **Dokumentation**

Beispiel zentraler Discovery Service

- ▶ vom DFN betrieben
- ▶ stündliche Aktualisierung
- ▶ abgestimmt auf die verschiedenen Metadatensätze



Embedded Discovery Service (EDS)

- ▶ lokal am SP anhand von eingelesenen Metadaten
- ▶ nutzerfreundlich, nur relevante IdPs gelistet
- ▶ Filtermöglichkeiten über Black-/Whitelisting
- ▶ Beispiele
 - ▶ SWITCH EDS
 - ▶ Shibboleth EDS
- ▶ Best Practice: NISO ESPReSSO, REFEDS Discovery Guide, RA21 Initiative

WAYFIess URLs

- ▶ komplettes Wegfallen der Einrichtungsauswahl
- ▶ IdP und SP sind hart verdrahtet (unflexibel)
- ▶ URL löst direkt Authentication Request bei einem bestimmten IdP aus
- ▶ Beispiel: `https://doku.tid.dfn.de/Shibboleth.sso/Login?entityID=https://idp.dfn.de/idp/shibboleth`
- ▶ **Dokumentation**

Einführung in eduGAIN

- ▶ föderationsübergreifende AAI / Interföderation
- ▶ Use case: Anmeldung bei SP in anderem Land / anderer Föderation
- ▶ Betrieben von GÉANT, produktiv seit 2011
- ▶ Aggregation der Metadaten aller teilnehmenden Föderationen durch eduGAIN/GÉANT („Upstream Metadata“)
- ▶ Verteilung dieser Metadaten innerhalb der eigenen Föderation durch einzelne Föderationsbetreiber („Downstream Metadata“)

EduGAIN – Beteiligung in der DFN-AAI

- ▶ Teilnahme an eduGAIN ist in der DFN-AAI Opt-in
- ▶ 69% der IdPs (204/296)
- ▶ 22% der SPs (118/534)

(Stand: 25.11.2019)

Vielen Dank! Gibt's Fragen?

DFN

► Kontakt

▷ DFN-AAI Team

E-Mail: aai@dfn.de

Tel.: +49-30-884299-9124

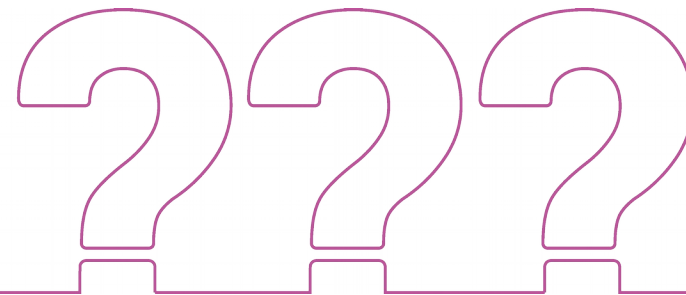
Fax: +49-30-884299-370

Anschrift:

DFN-Verein, Geschäftsstelle

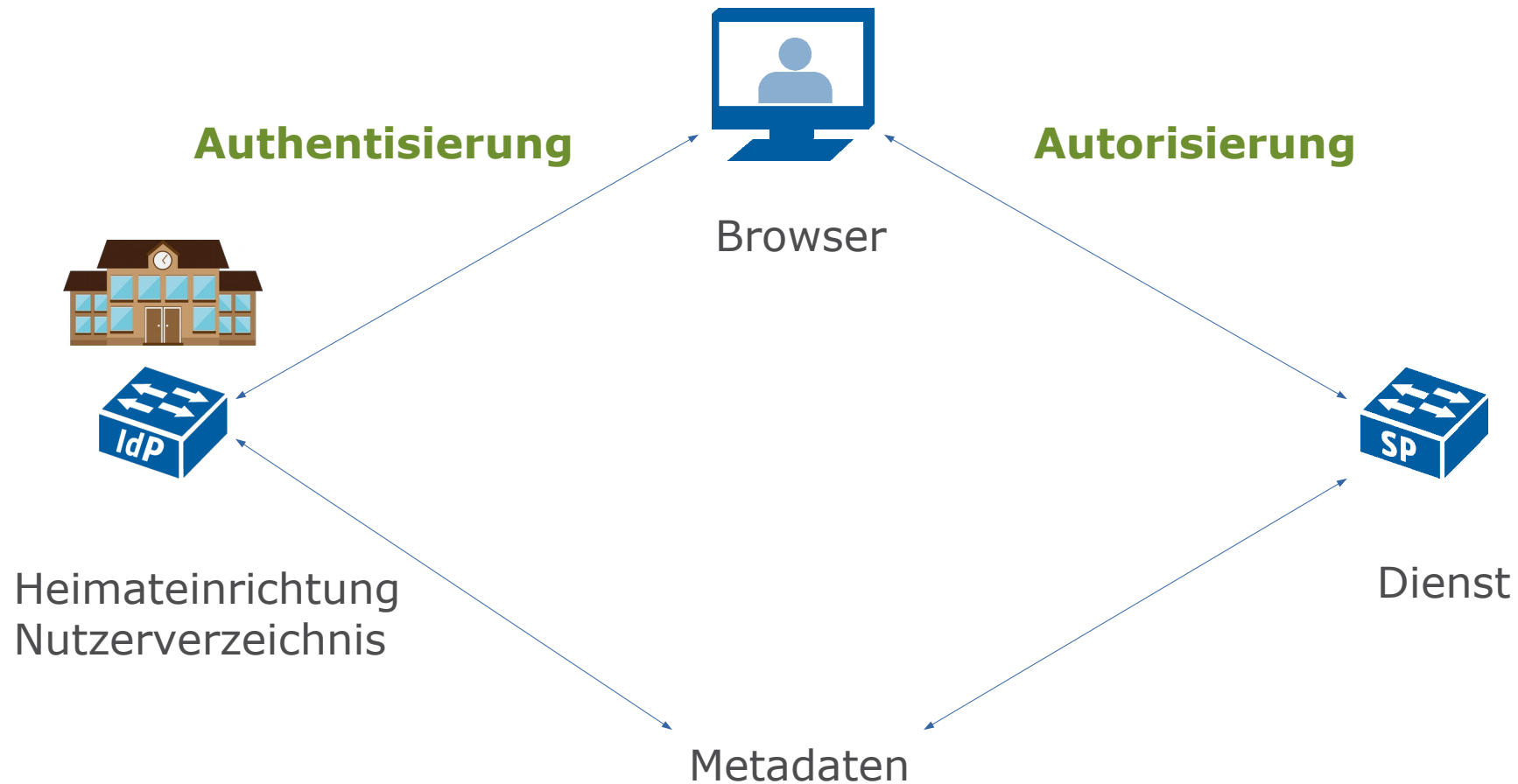
Alexanderplatz 1

10178 Berlin



- ▶ eduGAIN-Mitglied der ersten Stunde
- ▶ EU-Projekt GÉANT (GN4-2): Beteiligung an Tasks im Trust and Identity Development
- ▶ AARC2 – Authentication and Authorization for Research and Collaboration
 - ▶ Anforderungen der Communities erheben und Lösungen erarbeiten
- ▶ Mitgliedschaft im Shibboleth Consortium (seit 2014)
 - ▶ Wolfgang Pempe ist als Members' Representative im Consortium Board.
- ▶ Mitgliedschaft in der OpenID Foundation (OpenID Connect Federation)

Lingua Franca: SAML2



Aggregation und Verwaltung von Metadaten

