deutsches forschungsnetz

IdP Grundlagen-Workshop

Andreas Borm

Doreen Liebenau

Vorstellungsrunde

- Name
- Einrichtung
- Teilnahme an der DFN-AAI
- IdP-Erfahrung
- Bevorzugter Editor

Ziel des Workshops

- Zielgruppe: IdP-Newbies
- Grundlegendes Verständnis der Föderation
- IdP-Installation und –Konfiguration
- SP-Anbindung
- Hilfe zur Selbsthilfe

Ablauf Tag 1

- Einrichtung IdP
- Recap Basiswissen Föderation
- IdP-Installation
- Theorie Metadaten
- Praxis Metadaten, LDAP-Anbindung, Webinterface
- Theorie Attribute
- attribut-resolver.xml & attribut-filter.xml
- Status-Seite IdP

Ablauf Tag 2

- Übungen
- Theorie Plugins & Module
- User-Consent-Modul
- Server-Side Storage
- SAML2-Name-IDs
- Metadaten & Attributfreigaben
- Fehlerbehandlung
- Schema
- Abschluss & Feedbackrunde

Onboarding

- Wie ist die Internetverbindung?
- Funktioniert die Schulungs-VM?
- Anleitung verfügbar?
- Hausaufgaben erledigt?

Workshop-Spielregeln

Schaltet eure Kamera ein.

Teilt eure Fragen und Fehler per Share.

Kündigt Fragen per Handzeichen an.

Lasst das Alltagsgeschäft außen vor.

Einführung in die DFN-AAI

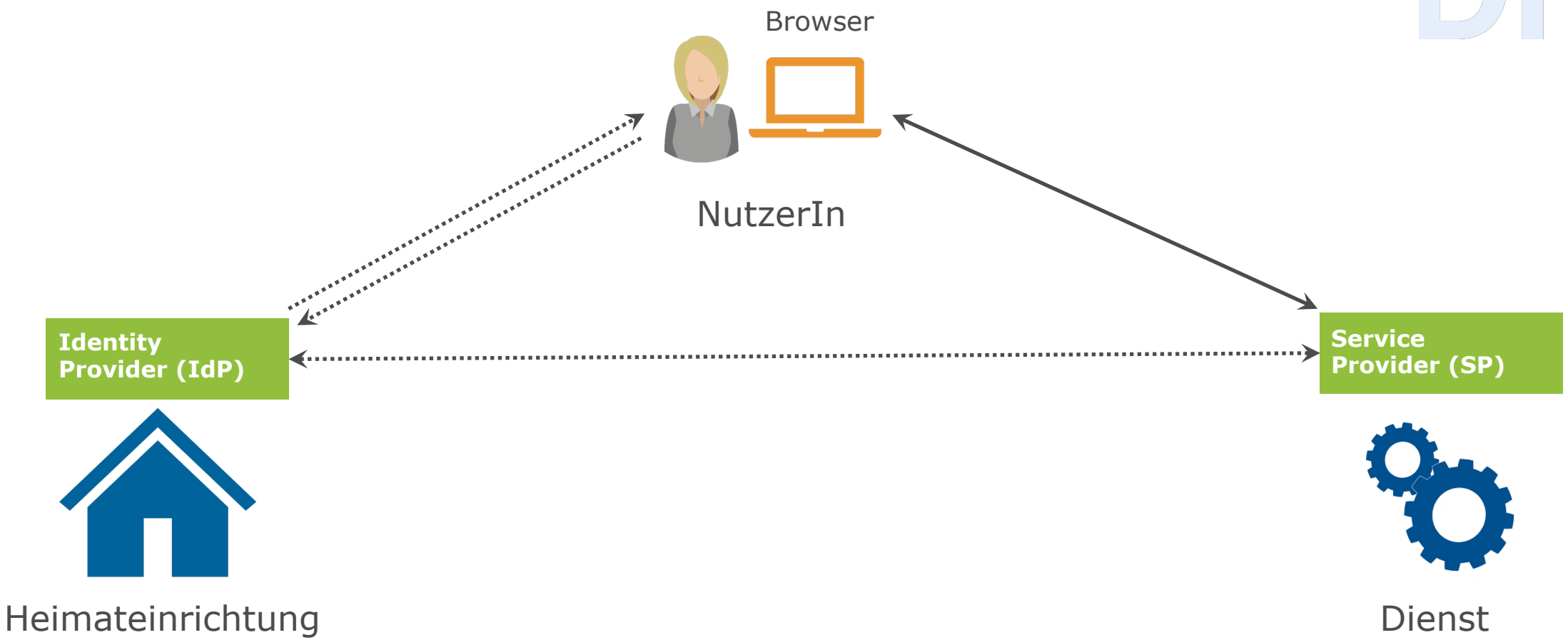
Agenda

- Terminologie Föderation
- Funktionsweise Föderation
- Arten von Föderationen
- Teilnahme an der DFN-AAI

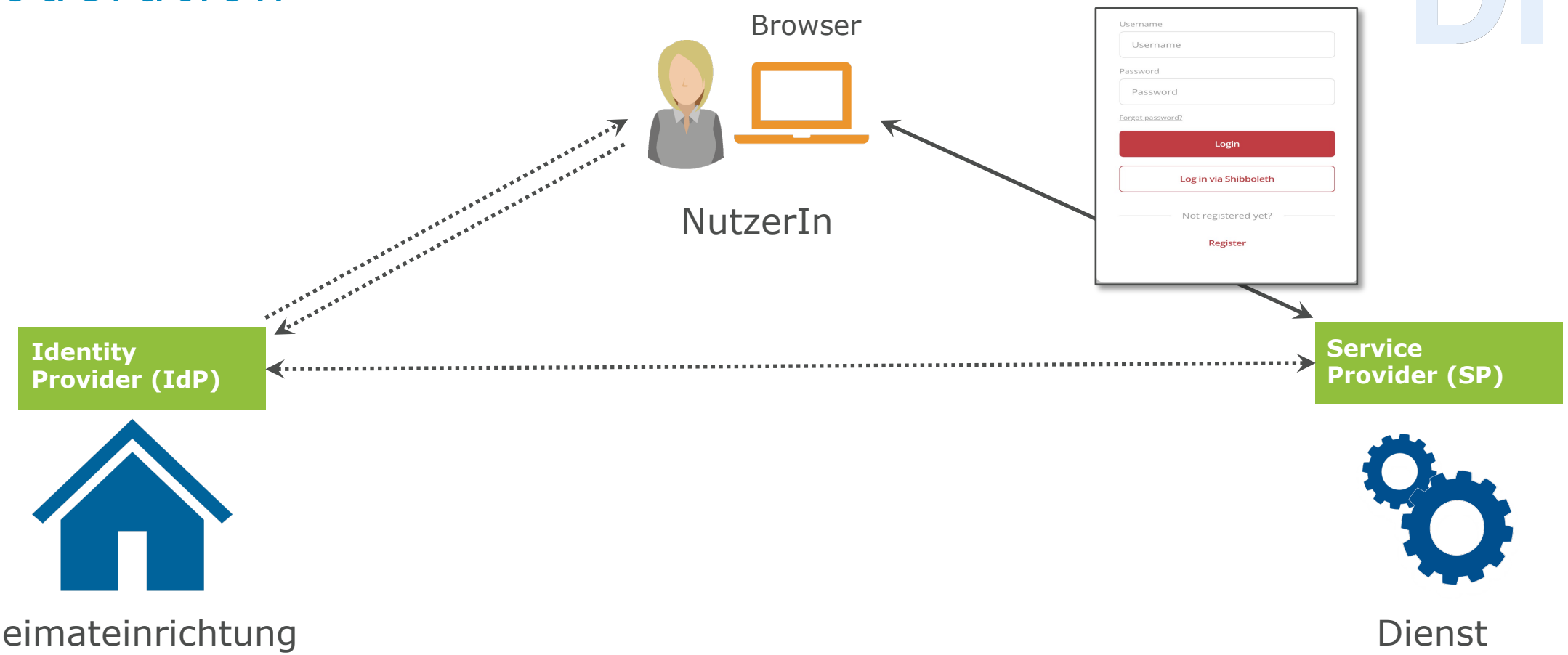
Begriffsbestimmung (1)

- Web-SSO
  - ist die Möglichkeit, sich bei mehreren Anwendungen und Webseiten mit einer Kennung anzumelden
- IDM – Identitäts-Management
  - User-Datenbank und User-Verwaltung in einer Organisation
- IdP – Identity Provider
  - Identitätsverwaltung der Heimateinrichtung, inkl. Login-Seite
- SP – Service Provider
  - ein Dienst / regelt den Zugriff

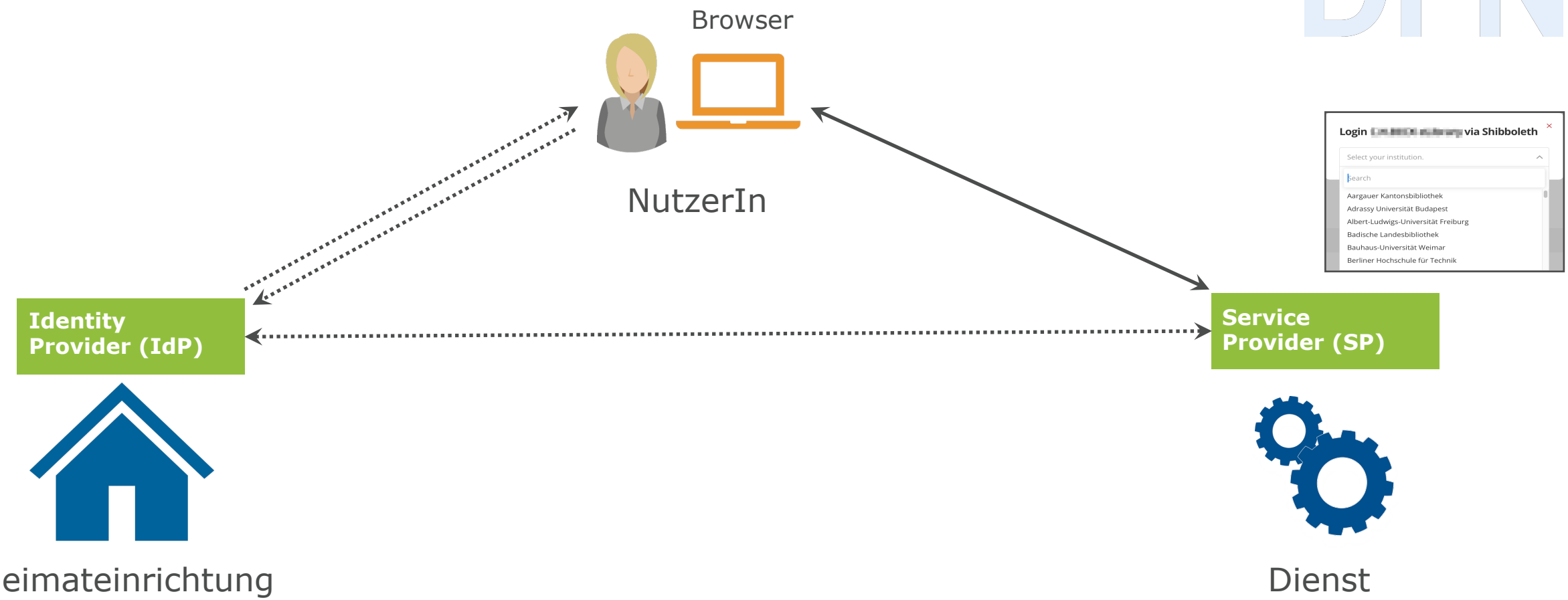
Föderation


Browser
NutzerIn
Identity Provider (IdP)
Service Provider (SP)
Heimateinrichtung
Dienst

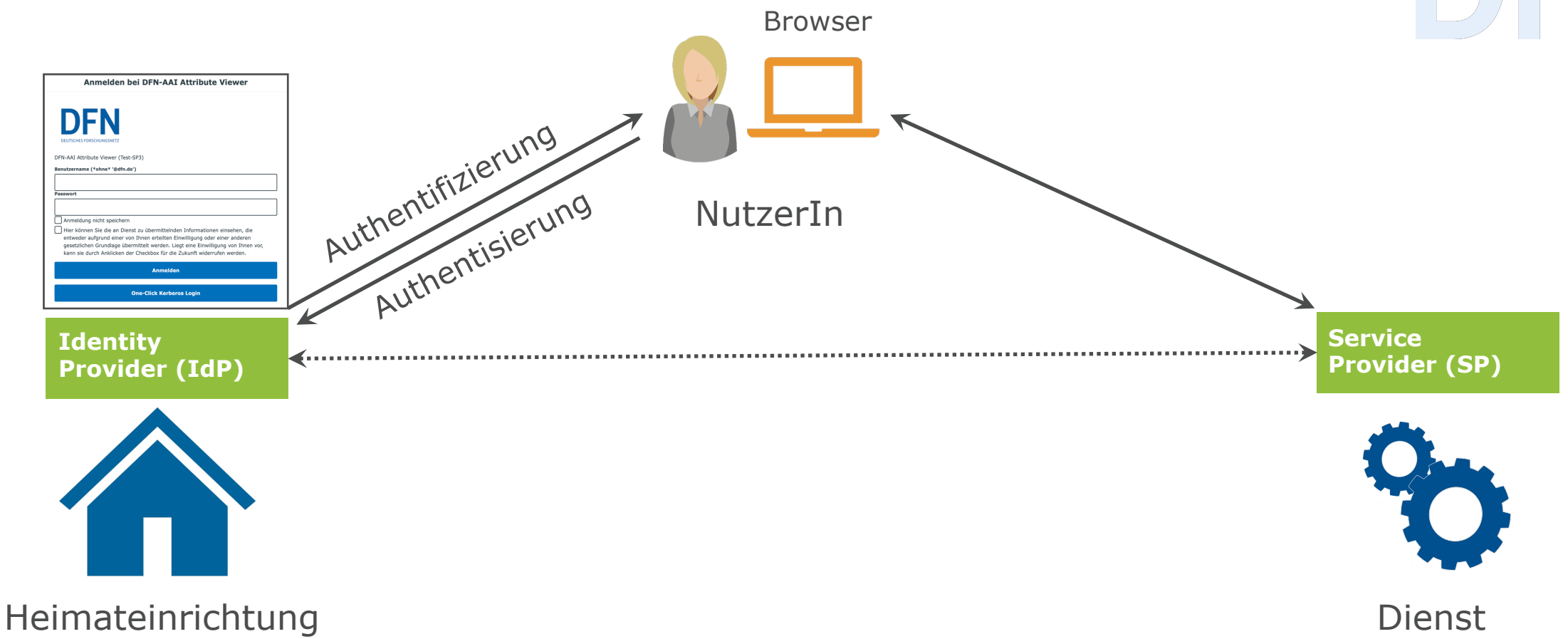
Föderation


Browser
NutzerIn
Username
Username
Password
Password
Forgot password?
Login
Log in via Shibboleth
Not registered yet?
Register
Identity Provider (IdP)
Service Provider (SP)
Heimateinrichtung
Dienst

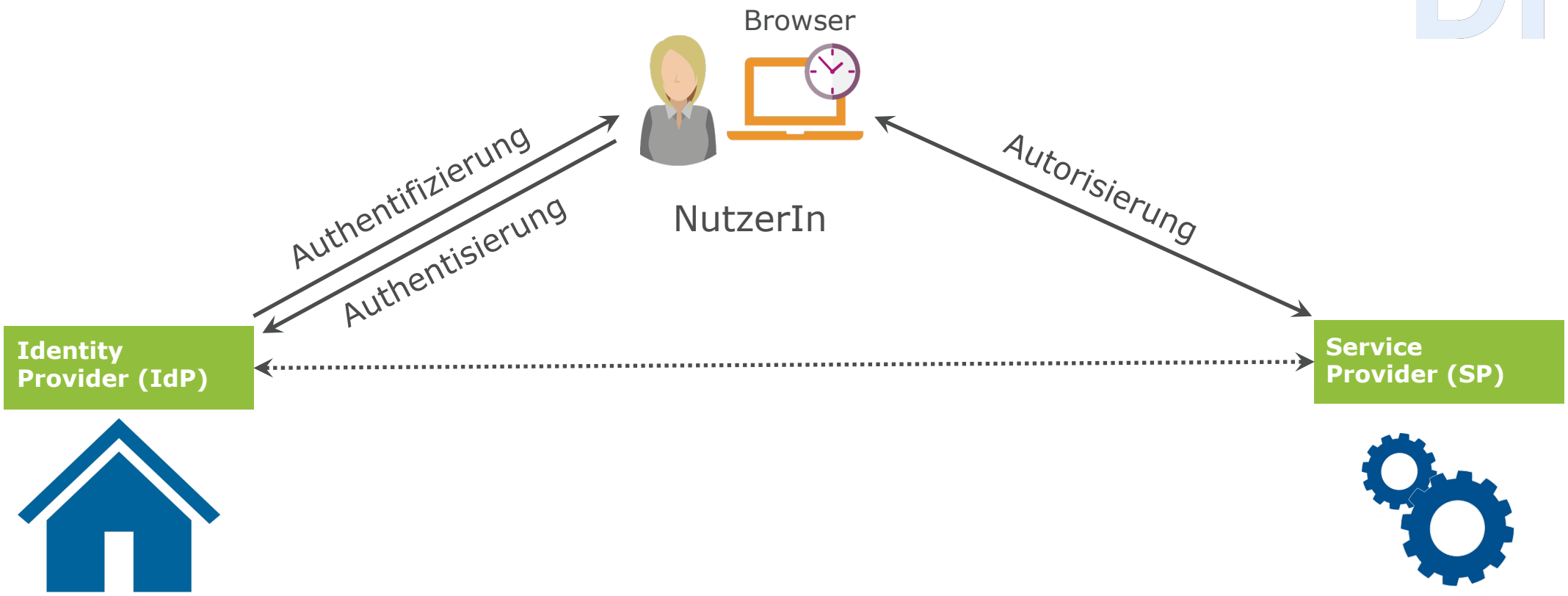
Föderation


Browser
NutzerIn
Login via Shibboleth
Select your institution.
Search
Aargauer Kantonsbibliothek
Adrassy Universität Budapest
Albert-Ludwigs-Universität Freiburg
Badische Landesbibliothek
Bauhaus-Universität Weimar
Berliner Hochschule für Technik
Identity Provider (IdP)
Service Provider (SP)
Heimateinrichtung
Dienst

Föderation

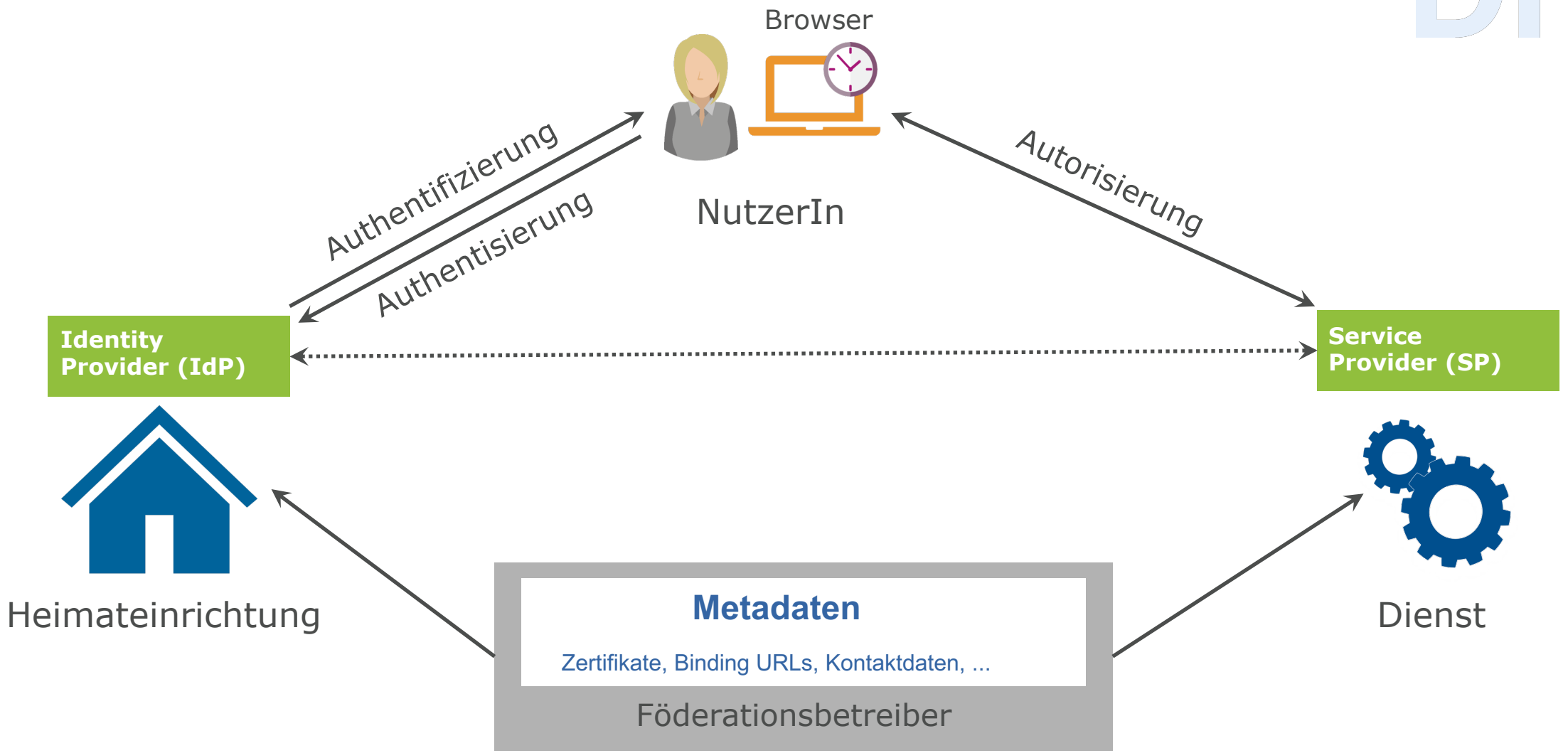

Browser
Anmelden bei DFN-AAI Attribute Viewer
DFN
DFN-AAI Attribute Viewer (Test-SP3)
Benutzername (*ohne* '@dfn.de')
Passwort
Anmeldung nicht speichern
Anmelden
One-Click Kerberos Login
Authentifizierung
Authentisierung
NutzerIn
Identity Provider (IdP)
Service Provider (SP)
Heimateinrichtung
Dienst

Föderation



Attribute
Name
Mail
Zugehörigkeit
...

Föderation


Browser
NutzerIn
Authentifizierung
Authentisierung
Autorisierung
Identity Provider (IdP)
Service Provider (SP)
Heimateinrichtung
Metadaten
Zertifikate, Binding URLs, Kontaktdaten, ...
Föderationsbetreiber
Dienst

Die Rolle des Föderationsbetreibers

- Der DFN als Föderationsbetreiber schafft das notwendige Vertrauensverhältnis:
  - 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!

Begriffsbestimmung (2)

- Föderiertes Login
  - Die Anmeldung über den IdP der Heimateinrichtung ermöglicht Nutzenden den Zugriff auf Dienste innerhalb der Föderation
- AAI = Authentication and Authorization Infrastructure
  - Bildet den technischen und rechtlichen Rahmen für föderiertes Login

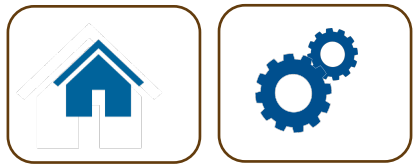
Begriffsbestimmung (3)

- SAML = Security Assertion Markup Language
- Shibboleth ist eigentlich eine Software...
  - … wird aber häufig synonym für SAML-basiertes Web-SSO verwendet.
- PHP SimpleSAML
  - ein weniger bekannte SAML-Implementierung
- Discovery-Service
  - Auswahl-Dialog aller in der AAI vertretener Identity-Provider (IdP); aka WAYF (Where-Are-You-From)

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.
- Admin-Dienste (DFN Mail Support, eduroam CAT)
- siehe auch DFN-Metadata Viewer und https://doku.tid.dfn.de/de:access_services („Dienste nutzen“)

Teilnahme an der DFN-AAI



Einrichtung / Anbieter

Vertrag

Metadaten

Erfassung

Testsystem in Testföderation

IdP

SP

Metadatenverwaltung

DFN

Prüfung von Vertrag und Metadaten

Erfolgreiche Attributübertragung auf Testsystem

Metadaten

Produktivföderation

Shibboleth IdP Installation

Installationsschritte

- Download als tar-Archiv ins Verzeichnis /opt/install
- Interaktives Installer-Script ausführen
  - Hostname: `idp.local`

Schulungs-VM

Metadaten und SAML2

Agenda

- Begriff Metadaten
- Entity ID
- Elemente der Metadaten
- Nutzungsmöglichkeiten (lokal, national, international)

Metadaten als „Rückgrat der Föderation“

- Abbildung des Vertrauensverhältnisses zwischen den teiln. Organisationen
- DFN gibt stündlich signierte Metadaten heraus: Wer nimmt an AAI teil, unter welchen Adressen, mit welchen Zertifikaten?
- IdP / SP: Informationsabgleich der Informationen der Gegenseite mit den Föderationsmetadaten
- Abbruch der Kommunikation bei Nichtübereinstimmung

Metadaten bei der SAML-basierten Kommunikation(1)

- Auszug aus Metadaten am Beispiel des DFN-IdP https://idp.dfn.de/idp/shibboleth

```
<EntityDescriptor entityID="https://idp.dfn.de/idp/shibboleth">…
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">…

<KeyDescriptor use="signing">
<ds:KeyInfo>
…
<ds:X509SubjectName>CN=idp.dfn.de</ds:X509SubjectName>
<ds:X509Certificate>
          MIIE8DCCAtigAwIBAgIUQ8ZM3aGQMOLuXsR5viqX9yE2MFowDQYJKoZIhvcNAQEL…                    …
</ds:X509Certificate>
..
</KeyDescriptor>

<ArtifactResolutionService Binding=”…"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" …
Location="https://idp.dfn.de/idp/profile/SAML2/POST/SSO"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-
 … Location="https://idp.dfn.de/idp/profile/SAML2/POST-SimpleSign/SSO"/>
<SingleSignOnService …
</IDPSSODescriptor>
<ContactPerson contactType="technical">
<GivenName>DFN OS Team</GivenName>
<EmailAddress>mailto:os@dfn.de</EmailAddress>
</ContactPerson>

</EntityDescriptor >
```

Entity ID

- 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 das Entity entsprechen
  - Einrichtung sollte Rechte an der Domain besitzen
- zur Einführung: SAML v2.0 Metadata Guide von Oasis

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

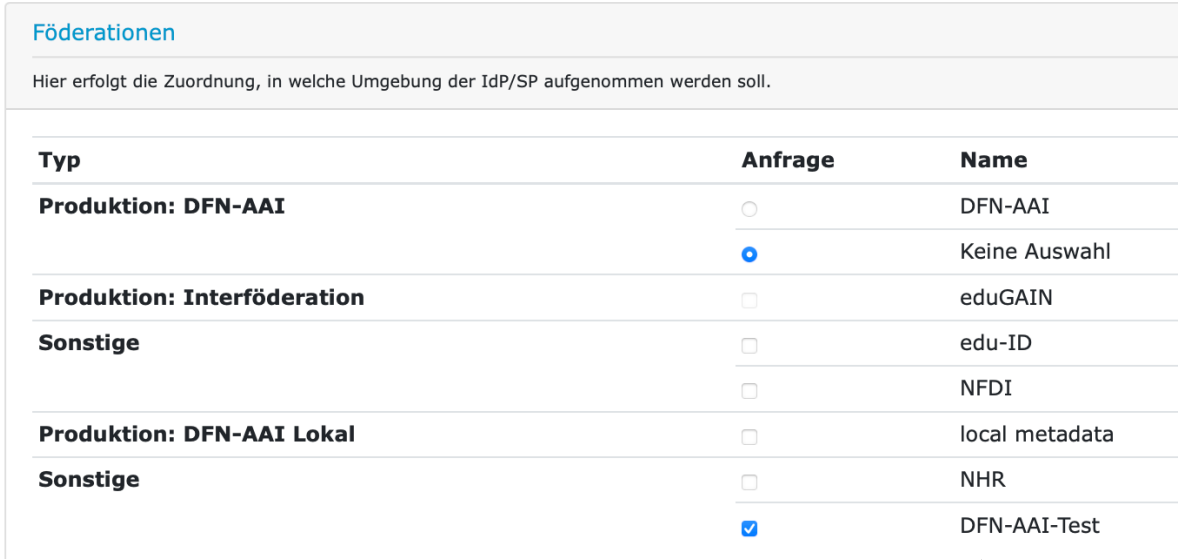
- IdP Single Sign-On Descriptor (nur IdP): `<IDPSSODescriptor>`
- „Scope“ (Geltungsbereich / Name der Einrichtung):
  - `<saml1md:Scope regexp=“false“>dfn.de</saml1md:Scope>`
- Bindings für SSO und SLO: `<SingleSignOnService>, <SingleLogoutService>`
- weitere optionale Elemente z.B.
  - Bindings für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

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:

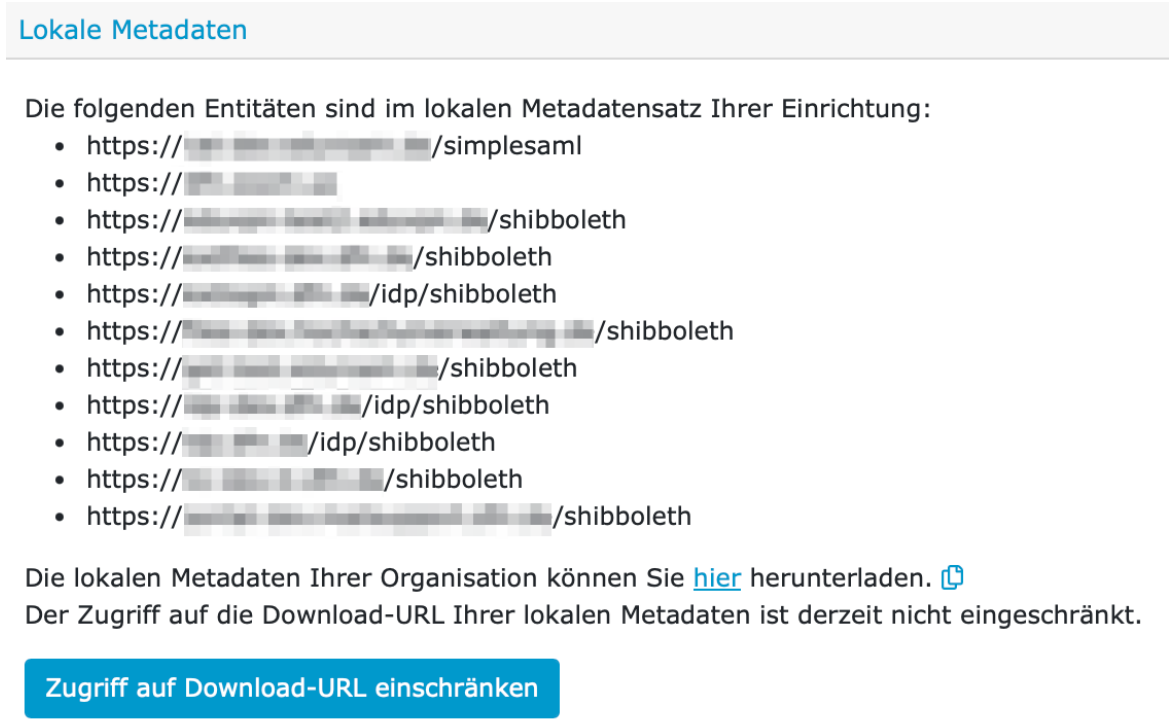
	IdP/AA	SP
DFN-AAI-Test	dfn-aai-test-metadata.xml	
DFN-AAI	dfn-aai-sp-metadata.xml	dfn-aai-idp-metadata.xml
eduGAIN	dfn-aai-edugain+sp-metadata.xml	dfn-aai-edugain+idp-metadata.xml
Lokale Metadaten	dfn-aai-local-999-metadata.xml*	

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

- Mit Aufnahme des ersten SP in die lokalen Metadaten wird der Datensatz generiert
- Metadatenverwaltung

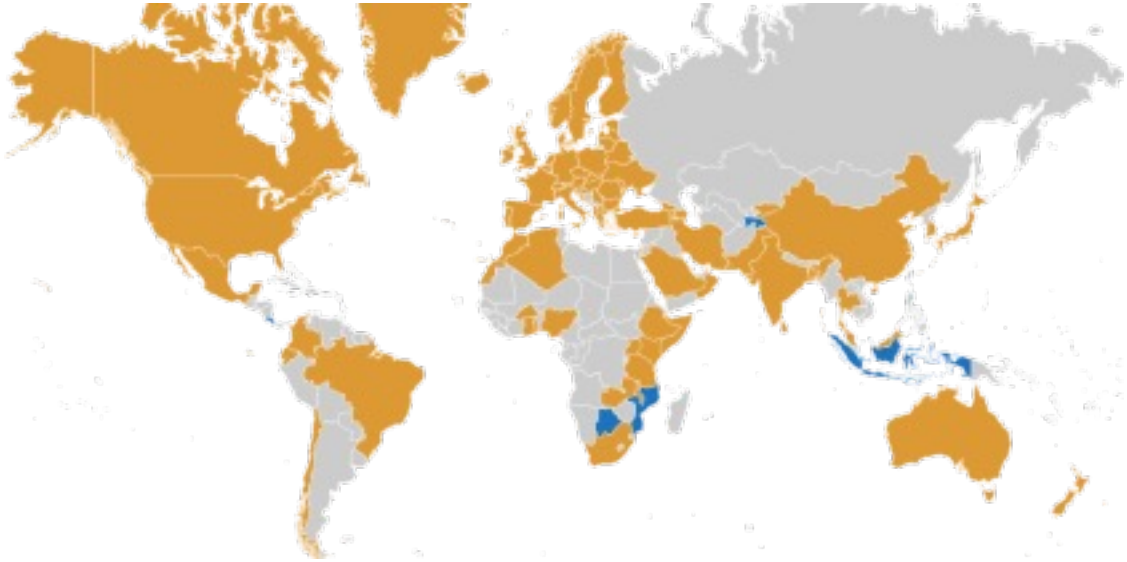


Einführung in eduGAIN

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 – beteiligte Föderationen



Stand: 02.01.2026

eduGAIN – Beteiligung in der DFN-AAI

- Teilnahme an eduGAIN ist in der DFN-AAI Opt-in
- 89% der IdPs (374/417)
- 22% der SPs (186/832) (Stand: 02.01.2026)

eduGAIN

- Teilnehmende Föderationen https://technical.edugain.org/status
- Entities Database https://technical.edugain.org/entities
- Connectivity Check https://technical.edugain.org/eccs/

IdP Konfiguration

Metadaten - Hinweise

- SP-Metadaten
  - SP ist vorinstalliert
  - lokalen Metadaten laden, statt Föderationsdaten
  - Konfiguration MetadaProvider
  - Bsp. für den produktiven Betrieb:

```
<!-- Metadaten aller SPs der DFN-AAI Produktivföderation -->
  <MetadataProvider id="dfn_aai"
      xsi:type="FileBackedHTTPMetadataProvider"
      backingFile="%{idp.home}/metadata/dfn-aai-sp-metadata.xml"
      metadataURL="http://www.aai.dfn.de/metadata/dfn-aai-sp-metadata.xml"
      maxRefreshDelay="PT2H">
    <MetadataFilter xsi:type="SignatureValidation"
      requireSignedRoot="true"
      certificateFile="/etc/ssl/aai/dfn-aai.pem"/>
  </MetadataProvider>
```

Metadaten - Hinweise

- IdP-Metadaten
  - Automatisch bei der Installation erstellt: `metadata/idp-metadata.xml`
  - Produktiv:
    - ausschließlich für das initiale Einlesen in die Metadatenverwaltung (MDV)!
    - Anschließend URL abstellen
    - Einmalige Verwendigung der idp-metadata.xml

Schulungs-VM

LDAP-Anbindung – to do

- LDAP-Verbindung manuell prüfen
- Beim Login-Versuch startet der IdP zwei LDAP-Abfragen
  - Authentisierung des Users
    - `conf/ldap.properties` → `idp.authn…`
  - Abruf der Attribute des Users
    - `conf/ldap.properties` → `ldap.attribute.resolver…`
- Bind-Passwort für den LDAP-Zugang hinterlegen
  - `credentials/secrets.properties`
- alle Usernamen im IdP in Kleinbuchstaben verarbeiten
  - `conf/c14n/subject-c14n.properties`

Schulungs-VM

Zugriff auf das Webinterface – to do

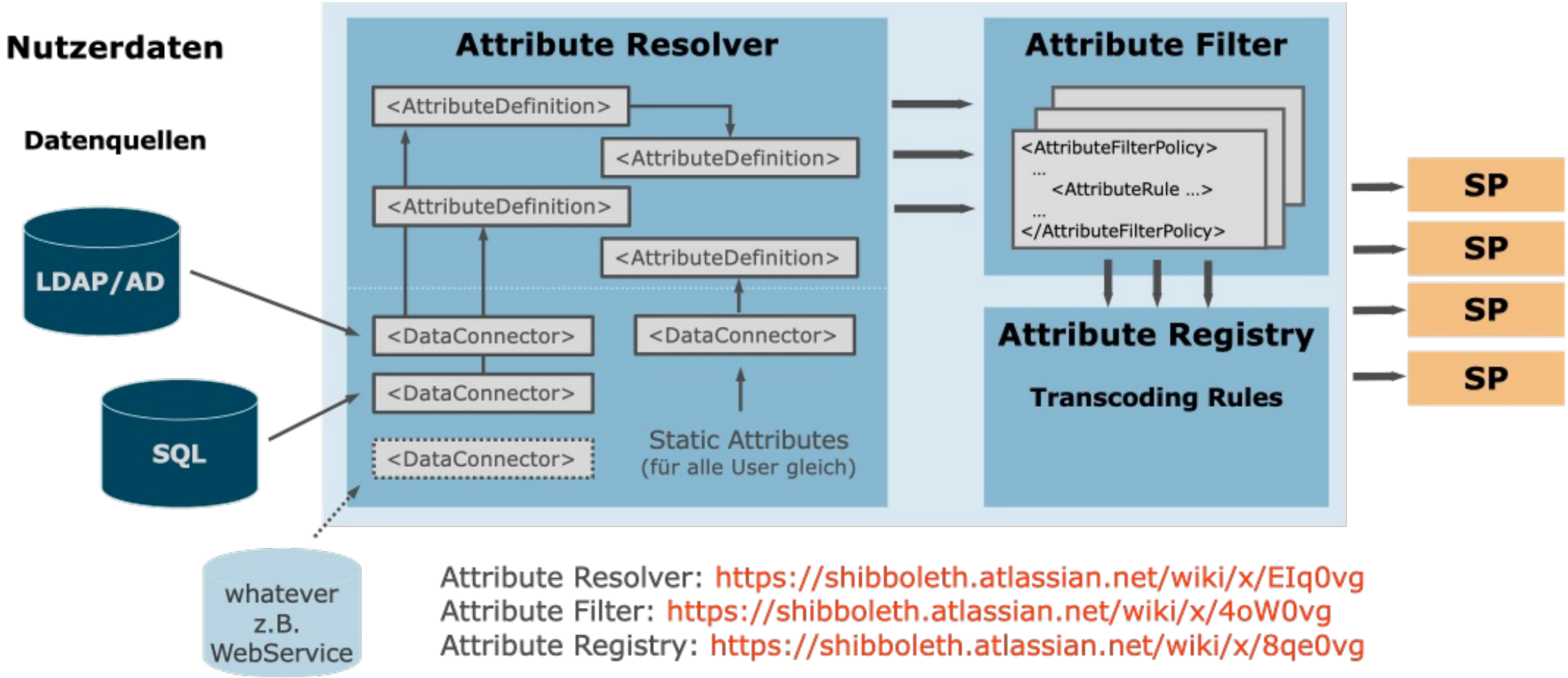
- Zugriff auf das Webinterface
  - `conf/access-control.xml`
- Zur Darstellung der Status-Seite eine aktuelle Version der Jakarta JSTL einbinden
  - `wget` & anschließendes `bin/build.sh`

Schulungs-VM

DFN

Attribute

IdP – Attribute Resolver, Filter und Encoding



Attribute Resolver: https://shibboleth.atlassian.net/wiki/x/EIq0vg
Attribute Filter: https://shibboleth.atlassian.net/wiki/x/4oW0vg
Attribute Registry: https://shibboleth.atlassian.net/wiki/x/8qe0vg

Attributeschemata

- Schema: Definition von Attribut-Mengen, den zulässigen Werten und deren Bedeutungen
- im Föderationsumfeld verbreitete Schemata:
  - eduPerson (international)
  - SCHAC (Schema for Academia, international)
  - dfnEduPerson (e-Learning, Deutschland)
  - weitere, z.B. inetOrgPerson
- Unsere Dokumentation
- Attribute für SAML-Kommunikation müssen nicht im IdM vorhanden sein!

Attribut-Handling im IdP

- IdP liest Attribute aus IdM/Nutzerverzeichnis
- Splitten, Zusammenfügen, Umschreiben von Attributen im IdP möglich
- Generierung neuer Attribute in Abhängigkeit von bereits definierten Attributen / Werten
- Attribute Filter Policies entscheiden über Weitergabe von Attributen an SPs
- Encoding der Attribute
- Einholung der Zustimmung zur Attributfreigabe (User Consent Modul)
- IdP verpackt Attribute in SAML-Assertion
- Versand der SAML-Assertion per HTTP-POST an Assertion Consumer Service (ACS) des anfragenden SPs (URL aus Föderationsmetadaten)

IdP: Auslesen der Attribute aus dem IdM

- Attribute Resolver:
  - Abschnitt “Data Connectors”
- Konfiguration:
  - conf/attribute-resolver.xml
  - conf/ldap.properties
- Unsere Doku

```
<DataConnector id="myLDAP" xsi:type="LDAPDirectory"
    ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}"
    baseDN="%{idp.attribute.resolver.LDAP.baseDN}"
    principal="%{idp.attribute.resolver.LDAP.bindDN}"
    principalCredential="%{idp.attribute.resolver.LDAP.bindDNCredential}"
    useStartTLS="%{idp.attribute.resolver.LDAP.useStartTLS:true}"
    connectTimeout="%{idp.attribute.resolver.LDAP.connectTimeout}"
    responseTimeout="%{idp.attribute.resolver.LDAP.responseTimeout}"
exportAttributes="uid givenName sn mail displayName">
    <FilterTemplate>
        <![CDATA[
            %{idp.attribute.resolver.LDAP.searchFilter}
        ]]>
    </FilterTemplate>
    <ConnectionPool
        minPoolSize="%{idp.pool.LDAP.minSize:3}"
        maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
        blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
        validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
        validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
        expirationTime="%{idp.pool.LDAP.idleTime:PT10M}" />
</DataConnector>
```

IdP: Attributdefinitionen im IdP

- Umschreiben und Neugenerierung von Attributen wird ebenfalls in `conf/attribute-resolver.xml` konfiguriert
- Abschnitt: „`Attribute Definitions`“
- Typen von Attribute Definitions (Auswahl)
  - Simple
  - Mapped
  - ScriptedAttribute
  - Scoped
- Shibboleth-Dokumentation

```
<AttributeDefinition xsi:type="Simple" id="ou">
    <InputDataConnector ref="myLDAP" attributeNames="ou"/>
</AttributeDefinition>
```

IdP: Attribute Encoding

- IdP wandelt seine Attribute um, damit der empfangende SP sie versteht.
- Konfiguration in der Attribute Registry, unterhalb von `conf/attributes`
  - z.B. “ou” in inetOrgPerson.xml

```
<bean parent="shibboleth.TranscodingProperties">
    <property name="properties">
        <props merge="true">
            <prop key="id">ou</prop>
            <prop key="transcoder">SAML2StringTranscoder SAML1StringTranscoder</prop>
            <prop key="saml2.name">urn:oid:2.5.4.11</prop>
            <prop key="saml1.name">urn:mace:dir:attribute-def:ou</prop>
            <prop key="displayName.en">Organizational unit</prop>
            <prop key="displayName.de">Organisationseinheit</prop>
            <prop key="displayName.fr">Unité organisationnelle</prop>
            ….
        </props>
    </property>
</bean>
```

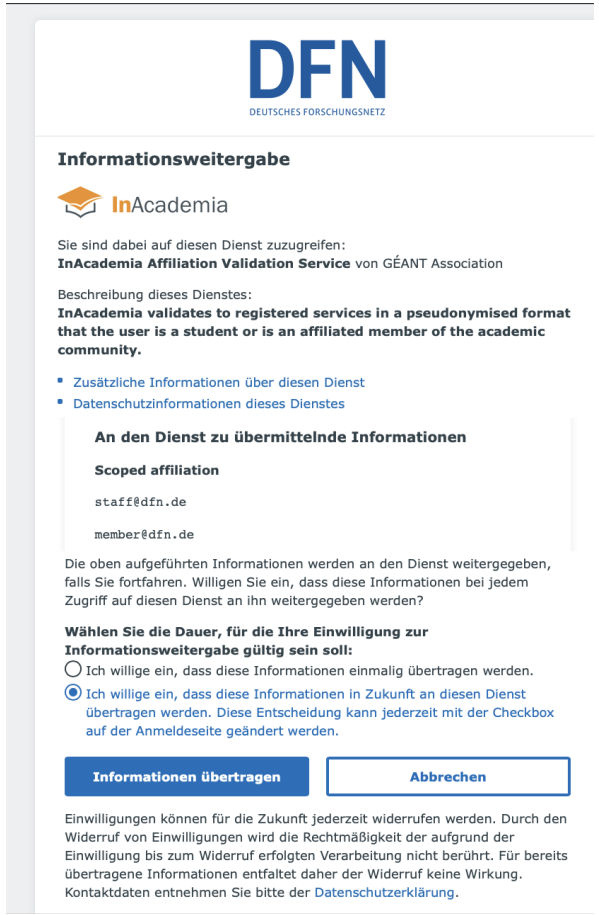
IdP: Attribut-Filter

- legt fest, welche Attribute an einen SP oder eine Gruppe von SPs versendet werden
- Attribute werden anhand der ID aus Attribute Resolver referenziert
- sehr flexibel, Regeln anhand vieler Kriterien möglich, z.B.
  - SP (EntityID)
  - Föderation
  - Entity Attribute
  - User
  - Attribut-Werte
- Doku im Shib-Wiki

```
<AttributeFilterPolicy id="dfn_test_sps">
    <PolicyRequirementRule xsi:type="OR">
        <Rule xsi:type="Requester" value="https://testsp2.aai.dfn.de/shibboleth" />
        <Rule xsi:type="Requester" value="https://testsp3.aai.dfn.de/shibboleth" />
    </PolicyRequirementRule>
    <AttributeRule attributeID="uid"                    permitAny="true"/>
    <AttributeRule attributeID="ou"                     permitAny="true"/>
    <AttributeRule attributeID="sn"                     permitAny="true"/>
    <AttributeRule attributeID="givenName"              permitAny="true"/>
</AttributeFilterPolicy>
```

IdP: Attributfreigabe

- User Consent-Modul
- Nachweispflicht!
- Informationen zur Einwilligung der Endnutzenden zur Attributfreigabe werden im Logfile `idp-consent-audit.log` abgelegt
  → gut aufheben



User Identifier

Identifikation von Usern (Subjects)

Entwicklung Identifier

- SAML1
  - <NameIdentitfier>- Element
- SAML2.0
  - <NameID>-Element
  - Mehrere NameID-Formate
    - <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="https://idp.local/idp/shibboleth" SPNameQualifier="https://sp1.local/shibboleth" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">HFgOn7tH2rKS1pmtzVARvEDOUUk=</saml2:NameID>
- SAML2.0 (neu)
  - <Attribute>- Element
  - Subject Identifier Attributes Profile
    - <saml2:Attribute FriendlyName="samlPairwiseID" Name="urn:oasis:names:tc:SAML:attribute:pairwise-id" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"> <saml2:AttributeValue>M22SVWRXLZIVUONQ55M522POYCQRIGJ4@local</saml2:AttributeValue></saml2:Attribute>

Übersicht der Entwicklung

Phase	Mechanismus	Typischer Identifier	Kommentar (siehe Best Practice)
SAML 1.x	NameIdentifier (im Subject)	E-Mail, lokale User-ID	- Wenig Datenschutz, - keine Pairwise-IDs
SAML 1.1	SAML 1.1 Attribut (als Attribut)	eduPersonTargetedID	- pairwise-like - aus Kompatibilitätsgründen noch verbreitet - komplexes XML-Konstrukt
SAML 2.0	NameID (im Subject)	persistent, transient, emailAddress, unspecified	- Mehr Formate, - komplex, - Datenschutzprobleme
SAML 2.0 (neu)	Subject Identifier Attribute (als Attribut)	subject-id, pairwise-id	- Klare Semantik, - Datenschutz, - Interoperabilität

Konfiguration Attribute Resolver – to do

- Zentrale Konfigurationsdatei: `conf/attribute-resolver.xml`
- Definition folgender Attribute:
  - `uid, givenName, sn, mail, displayName`
  - `o, schacHomeOrganisation`
  - `eduPersonScopedAffiliation=member@scope`
  - `eduPersonEntitlement=urn:mace:dir:common-lib-terms`
- Data Connectors
  - `staticAttributes`
  - `myLDAP`
- Für scripted Attribute:
  - Nashorn Plugin

Schulungs-VM

Konfiguration von Attributfreigaben – to do

- Zentrale Konfigurationsdatei `conf/attribute-filter.xml`
- Freigabe folgender Attribute für den lokalen Service Provider “`https://sp1.local/shibboleth`“
  - eduPersonScopedAffiliation
  - sn
  - givenName
  - mail
  - uid
- Orientierung an der Vorlage:

```
<!-- Datei: /opt/shibboleth-idp/conf/attribute-filter.xml -->
  <!-- Release an additional attribute to an SP. -->
    <AttributeFilterPolicy id="SPs_locals">
      <PolicyRequirementRule xsi:type="Requester" value="https://sp.example.org" />
      <AttributeRule attributeID="uid" permitAny="true" />
      </AttributeFilterPolicy>
```

Schulungs-VM

Dateirechte & IdP-Status – to do

- Letzte Aufräumarbeiten
  - Tomcat-Benutzeraccount besitzt das Installationsverzeichnis
- Neustart
  - Tomcat
  - Shibboleth-SP
- Erreichbarkeit Statusseite IdP https://idp.local/idp/shibboleth
- Erstes Login am lokalen SP https://sp1.local

Schulungs-VM

Tipps und Tricks

- Tomcat Servlet neu laden
  - `touch /opt/shibboleth-idp/war/idp.war`
- War-File neu bauen
  - `/opt/shibboleth-idp/bin/build.sh`
- Intervalle für automatischen Neuladen der Konfiguration anpassen
  - Standardwerte:
    - `conf/attribute-resolver.xml`, `conf/attribute-filter.xml` uvm.: 15 min
  - Anpassung in `conf/services.properties`
- Reload-URLs, zum Neuladen der Konfiguration
- Aufruf von bestimmter Handler über URLs, z.B. Logout-Handler

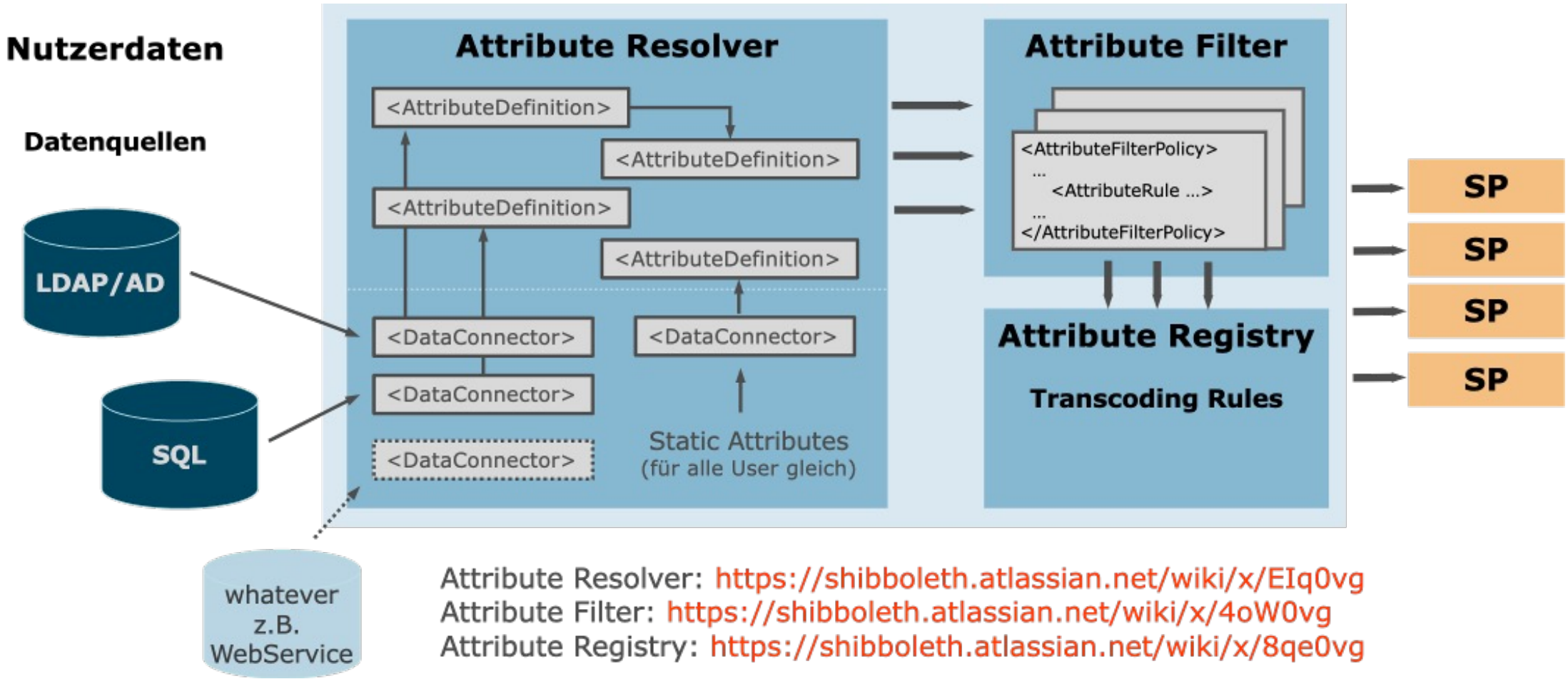
Recap Tag 1

IdP Grundlagen-Workshop – Tag 2

Andreas Borm

Doreen Liebenau

Recap & Feedback



Attribute Resolver: https://shibboleth.atlassian.net/wiki/x/EIq0vg
Attribute Filter: https://shibboleth.atlassian.net/wiki/x/4oW0vg
Attribute Registry: https://shibboleth.atlassian.net/wiki/x/8qe0vg

Ablauf Tag 2 - Übungen

- Theorie Plugins & Module
- User-Consent-Modul
- Server-Side Storage
- SAML2-Name-IDs
- Metadaten & Attributfreigaben
- Fehlerbehandlung
- Schema
- Abschluss & Feedbackrunde

Plugins und Module

- Zusätzliche Funktionalitäten für den IdP
- jede veränderte Datei ist Teil eines Moduls
- bei Upgrades werden neue Versionen der modifizierten Dateien erstellt
- Bei Upgrade
  - `Filename.idpnew-idpversion`: Default-Configs von geänderten Dateien
  - `Filename.idpsave`: Konfigs, die bei Deinstallation gesichert wurden
- Config vorhanden = module enabled
- If you're not using it, none of those files are needed.

Module

- Module werden mit dem IdP versioniert (anders als die Plugins)
- Aktivierung von Modulen (Hinterlegen spezifischer Konfigurationsdateien im Dateibaum)
  - `bin/module.sh -- enable module-ID`
- Deaktivieren von Modulen (vorhandene Konfigurationsdateien = enabled)
  - `bin/module.sh -- disable module-ID --clean`
- Detaillierte Informationen zum Modul & dazugehörigen Config-Dateien
  - `bin/module.sh -i module-ID`
- Default: drei Module
  - `idp.Core,`
  - `idp.CommandLine und`
  - `idp.EditWebApp`

Module (noreplace/replace)

bin/module.sh -i idp.Core	bin/module.sh -i idp.CommandLine
Module: idp.Core Name: Core IdP Functions (Required) … Status: ENABLED Resource: (noreplace) views/error.vm Resource: (noreplace) views/logout.vm Resource: (noreplace) conf/access-control.xml Resource: (noreplace) conf/attribute-filter.xml Resource: (noreplace) conf/attribute-registry.xml Resource: (noreplace) conf/attribute-resolver.xml Resource: (noreplace) conf/idp.properties Resource: (noreplace) conf/ldap.properties Nach Update: $ ls -la /opt/shibboleth-idp/conf/ .. idp.properties idp.properties.idpnew-511	Module: idp.CommandLine Name: Command Line Scripts … Status: ENABLED … Resource: (replace) bin/plugin.sh Resource: (replace) bin/plugin.bat … Resource: (replace) bin/status.sh Resource: (replace) bin/status.bat Resource: (replace) bin/update.sh Resource: (replace) bin/update.bat Resource: (replace) bin/version.sh Resource: (replace) bin/version.bat …

Plugins

- Zusatzpakete, die Funktionalität hinzufügen
- Upgrade IdP und Plugin werden unabhängig voneinander entwickelt & aktualisiert
- Können direkt aus dem Internet installiert & aktualisiert warden
- Müssen signiert sein
- Installation aus einer im Internet gehosteten Datei oder lokal möglich
- Hat keine Konfiguration
- Plugin-Entwickler gibt vor, ob automatisch ein Modul bei Installation aktiviert wird

Plugins II

```
/opt/shibboleth-idp/bin/plugin.sh -fl
```

```
        Plugin: net.shibboleth.idp.plugin.nashorn Current Version: 2.0.0
        Plugin Versions
        1.0.0: Min=4.1.0 Max=5.0.0 Support level: Withdrawn
        1.1.0: Min=4.1.0 Max=5.0.0 Support level: Current
        2.0.0: Min=5.0.0 Max=6.0.0 Support level: Current
```

- Support Level
  - OutOfDate: funktioniert, neue Version verfügbar
  - Secadv: es gibt Sicherheitswarnung für dieses Plugin
  - Withdrawn: zurück gezogen
  - Current: aktuell

Übung 1

Aufgabe

- Aktivierung des User-Consent-Moduls
  - Das User Consent Modul ist eine Funktion, die es ermöglicht, Nutzer*innen vor der Freigabe ihrer Attribute für SPs um deren Zustimmung zu bitten.

Umsetzung

- Modul aktivieren
  - `bin/module.sh`
- Profilkonfiguration anpassen
  - `SSO-Profile in conf/relying-party.xml ergänzen → Flow „attribute-release“`

```
<bean id="shibboleth.DefaultRelyingParty" parent="RelyingParty">
  <property name="profileConfigurations">
      <list>
          <!-- SAML 1.1 and SAML 2.0 AttributeQuery are disabled by default. -->
          <!--
          <ref bean="Shibboleth.SSO" />
          <ref bean="SAML1.AttributeQuery" />
          <ref bean="SAML1.ArtifactResolution" />
          -->
          <ref bean="SAML2.SSO" />
          <ref bean="SAML2.ECP" />
          <ref bean="SAML2.Logout" />
```

Übung 2

Aufgabe

- Einrichten einer Datenbank zum Speichern von Session-Informationen, User-Consent und Persistent-IDs

Umsetzung

- Vorbereitung der Datenbank
  - DB mit zwei Tabellen ”StorageRecords” und “shibpid” anlegen
- Konfiguration der DB-Anbindung
  - JDBC-Plugin installieren
  - `conf/global.xml`
  - `conf/idp.properties`
  - `credentials/secrets.properties`
  - `touch /opt/shibboleth-idp/war/idp.war`

Übung 3

Aufgabe

- Konfiguration von SAML2-NameIDs
  - persistentID generieren & samlPairwiseID definieren

Phase	**Mechanismus**	**Typischer Identifier**	**Kommentar** (siehe Best Practice)
SAML 1.x	NameIdentifier (im Subject)	E-Mail, lokale User-ID	- Wenig Datenschutz, - keine Pairwise-IDs
SAML 1.1	SAML 1.1 Attribut (als Attribut)	eduPersonTargetedID	- pairwise-like - aus Kompatibilitätsgründen noch verbreitet - komplexes XML-Konstrukt
SAML 2.0	NameID (im Subject)	persistent, transient, emailAddress, unspecified	- Mehr Formate, - komplex, - Datenschutzprobleme
SAML 2.0 (neu)	Subject Identifier Attribute (als Attribut)	subject-id, pairwise-id	- Klare Semantik, - Datenschutz, - Interoperabilität

Umsetzung

- Generierung der persistentID definieren
  - `conf/saml-nameid.properties`
    - Konfiguration der SAML-NameID-Formate & deren Zuordnung zu Benutzerattributen
- Aktivieren der Generierung der persistentID
  - `conf/saml-nameid.xml`
    - Steuerung der Generierung von SAML 1 NameIdentifier- und SAML 2 NameID-Content
- samlPairwiseID definieren
  - `conf/attribute-resolver.xml`
- Verarbeitung der persistentID aktivieren
  - `conf/subject-c14n.xml`
- Konfiguration der Datenbank-Anbindung

Übung 4

Aufgabe

- Einrichtung von Attribut-Freigaben für einen SP am Beispiel von easyroam

Umsetzung

- Bedarfsermittlung anhand der Metadaten
- Attribute definieren, falls noch nicht vorhanden
  - `conf/attribute-resolver.xml`
- Konfiguration der Attributfreigaben
  - `conf/attribute-filter.xml`
- Neuladen des Servlets
  - `touch /opt/shibboleth-idp/war/idp.war`

Übung 5

Aufgabe

- Freigabe der persistentID

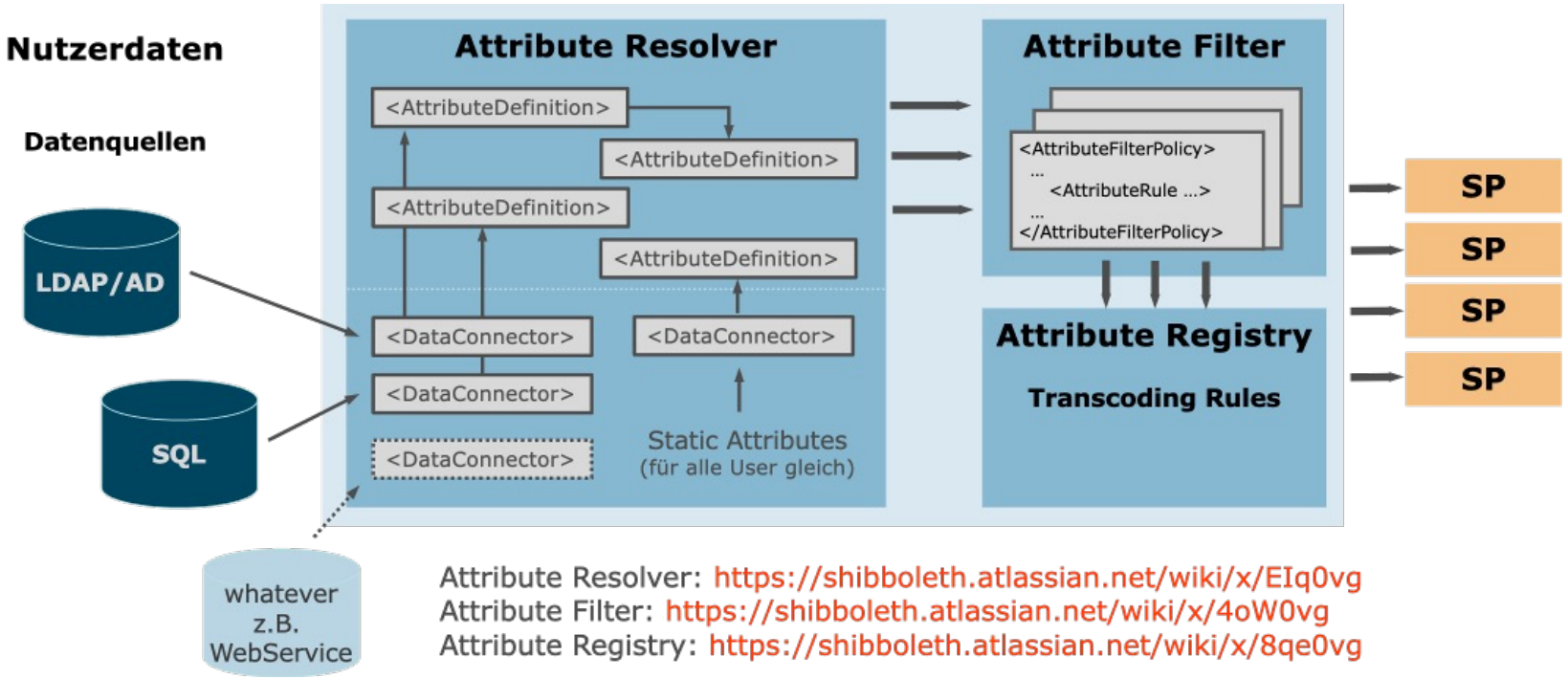
Umsetzung

- Anpassung des Profils SAML2.SSO
  - `conf/relying-party.xml`

Übung 6

Aufgabe

- Erweiterung des Attribute Registry
- Folgende Schemata sollen hinzugefügt werden
  - dfnEduPerson
  - dfnMisc



Attribute Resolver: https://shibboleth.atlassian.net/wiki/x/EIq0vg
Attribute Filter: https://shibboleth.atlassian.net/wiki/x/4oW0vg
Attribute Registry: https://shibboleth.atlassian.net/wiki/x/8qe0vg

Umsetzung

- Download der Transcoding Properties
- Einbinden des neuen Schematas
  - `conf/attributes/default-rules.xml`

Übung 7

Aufgabe

- Hinzufügen des Attributs eduPersonTagetedID
- Freigabe des Attributes für den lokalen SP

Umsetzung

- Attribute definieren, falls noch nicht vorhanden
  - `conf/attribute-resolver.xml`
- Attributefreigabe einrichten
  - `conf/attribute-filter.xml`
- Servlet neu starten

Rückblick und Ausblick

Verzeichnisstruktur

bin	• CLI-Tools & während der Installation benötigte Java-Bibliotheken • Distributions-Dateien werden bei Updates überschrieben • Zusätzlich hinzugefügte Dateien bleiben erhalten
conf[1]	• Hauptkonfiguration
credentials[1]	• Schlüssel, Zertifikate, Schlüsselspeicher und Anmeldeinformationen, z.B. Validierung v. Metadatensignaturen • Soll nur für das den IdP ausführende Benutzerkonto lesbar sein
dist	• Originalversion des Inhalts von conf, flows, messages & views • Verzeichnis wird bei jeder Installation gelöscht und neu erstellt
edit-webapp[1]	• Anpassungen an Stylesheets, Grafiken, zus. .jar-Files → nach Änderungen IdP-Servlet neubauen: ./bin/build.sh
flows[1]	• vom User editierbare Spring Web Flow Definitionen
logs	• Default-Verzeichnis für Diagnose- & Audit-Logs
messages[1]	• sprachspezifische Beschriftungen
metadata	• SAML-Metadaten • Bei Erstinstallation wird idp-metadata.xml erzeugt (Einstiegsbeispiel, keine echte Metadatenquelle!)
views[1]	• Velocity-Templates für HTML-Seiten (Login, User Consent)
war	• gepackte IdP-War-Datei für das Deployment

Rückblick

- IdP Installation & Basis-Konfiguration
- Attribute
  - User Identifier
  - Schemata
- Server-Side Storage
- Plugin-Installation
  - Nashorn & JDBC
- Modul-Aktivierung
  - User-Consent Modul
- SP-Anbindung
  - Attributefreigaben
- Logging & Fehlersuche

Ausblick & Info

- IdP Aufbau-Workshop in Planung
  - Erste Veranstaltung März 2026
- Informationen
  - DFN-Wiki
  - Mailinglisten
- Termine
  - DFN Betriebstagung, Forum AAI in Berlin (Frühjahr & Herbst)
  - ZKI AK IAM (Frühjahr & Herbst)

Vielen Dank! Fragen? Feedback?

- Kontakt
  - DFN-AAI Team

    E-Mail: hotline@aai.dfn.de
    Telefon: 0049 30 884299-9124
    Fax: 0049 30 884299-370

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz 1
    10178 Berlin

  - Andreas Borm
  - Doreen Liebenau
  - Esther Ruiz Ben
  - Heike Kaufmann
  - Wolfgang Pempe