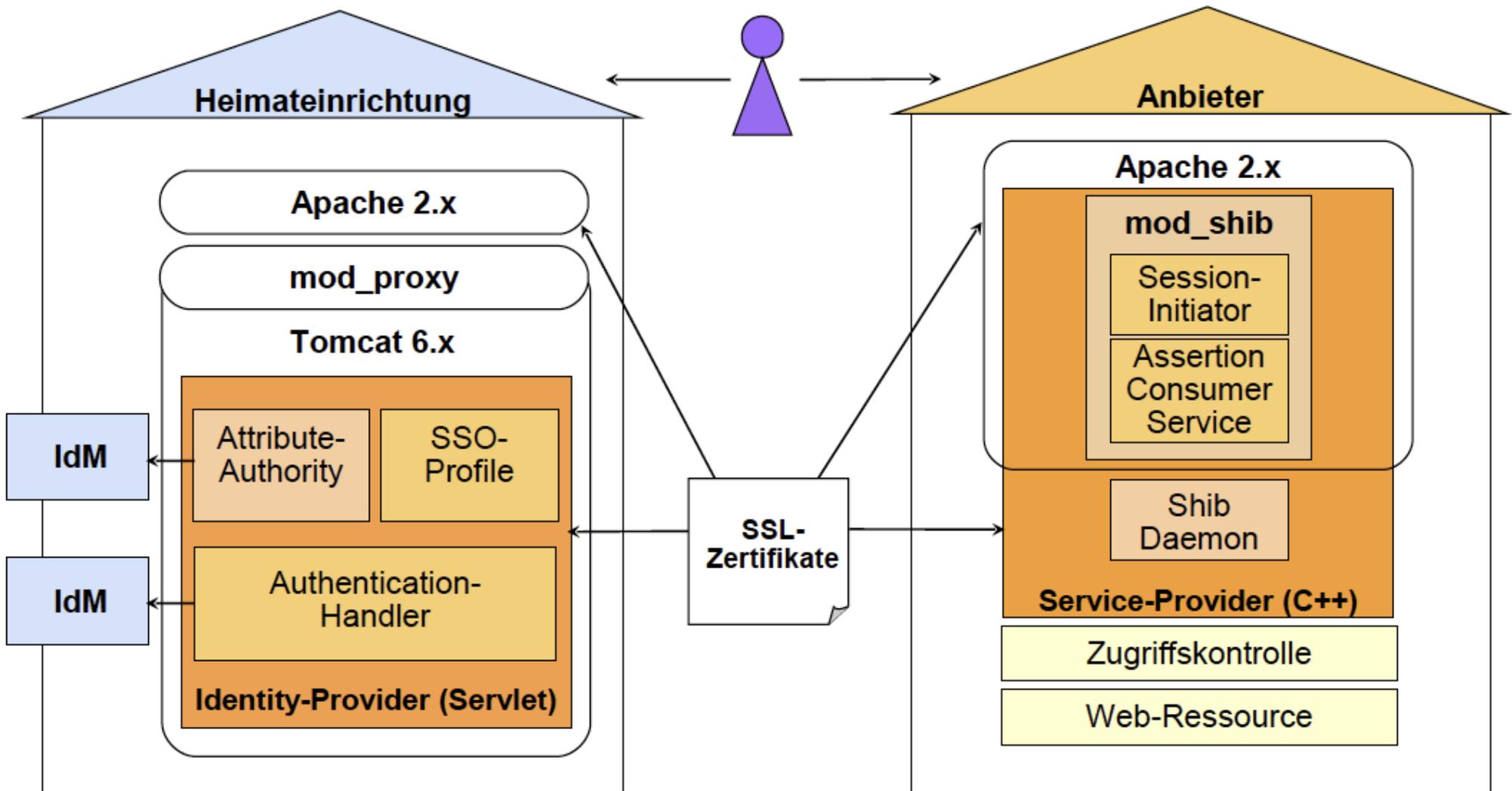


Shibboleth Service Provider

Installation, Konfiguration, Anwendungen schützen

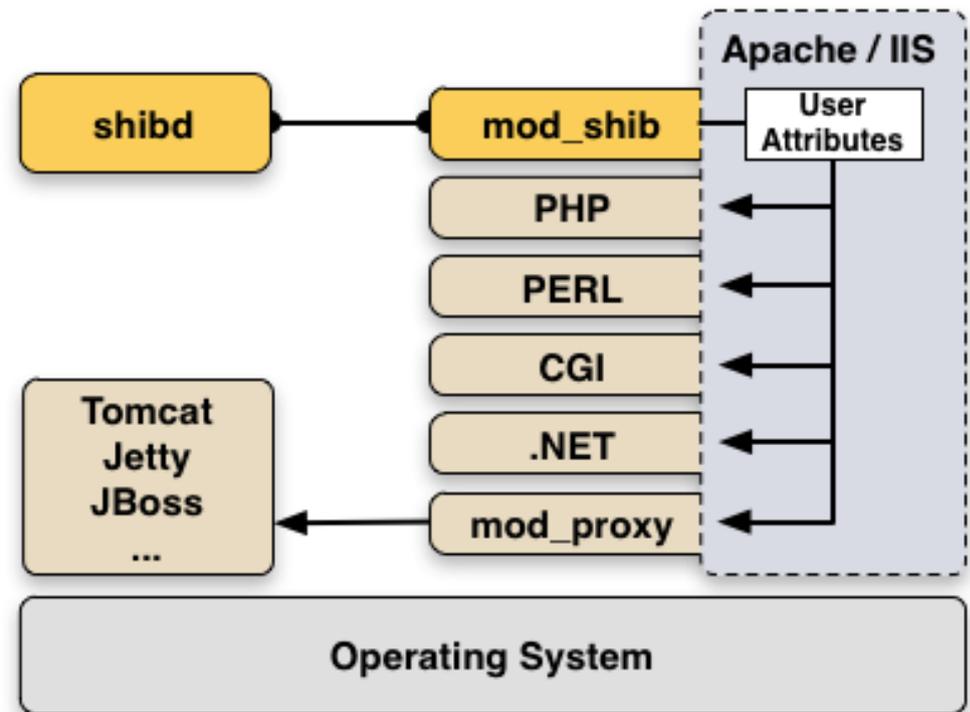
Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DFN-AAI Workshop
5./6. September 2017, FH Westküste



Quelle: Bernd Oberknapp, Universitätsbibliothek Freiburg i.Br.

- Implementiert in C++
- Zwei Komponenten:
 - `mod_shib` Modul für Apache und IIS Web Server (+ Nginx):
Schützt Files, Directories, Locations und erzwingt AAI-basierte Authentifizierung sowie ggf. bestimmte Attribute und -Werte
 - `shibd` Daemon:
Stateful,
Initiiert AuthnRequests,
Verarbeitet Assertions, wertet
Zugriffsregeln aus
- Attribute werden auf Umgebungsvariablen abgelegt, auf die alle Anwendungen zugreifen können, die im Web Server laufen, z.B. PHP: `$_SERVER['mail']`



Quelle: <https://www.switch.ch/aai/guides/sp/>

- Aktuelle Version: 2.6
- Debian + Ubuntu Repositories werden von SWITCH gepflegt
- Installationsanleitungen für alle Plattformen unter <https://www.switch.ch/aai/guides/sp/installation/>
(Shib Wiki: <https://wiki.shibboleth.net/confluence/x/T4BC>)
- Unter Debian muss i.d.R. anschließend noch manuell `a2enmod shib2` ausgeführt werden
- Test der shibd-Konfiguration: `sudo shibd -t`
nach Änderungen: `sudo service shibd restart`
- Nach Neustart des Web Servers sollte bereits der Session Handler verfügbar sein:
<https://sp.uni-musterstadt.de/Shibboleth.sso/Session>

- **/etc/shibboleth/**
 - Zentrale Konfiguration in `shibboleth2.xml`
 - **Attribute:** `attribute-map.xml`, `attribute-policy.xml`
 - **Logging:** `native.logger`, `shibd.logger`, `syslog.logger`
 - **HTML Templates** (`*.html`)
 - Lokal generierte Zertifikate + Keys
- **/var/cache/shibboleth/**
 - Backup Remote Metadata
- **/var/log/shibboleth/**
 - `shibd.log` und `transaction.log`
 - `native.log` (← `mod_shib` Modul, in Unterverzeichnis `./apache2`)

- **In der Regel sind nur wenige Anpassungen in shibboleth2.xml erforderlich:**
- Entity ID des SP
- Security-Einstellungen für SP-Sessions (Cookies, https, Timeout, etc.)
- Session Initiator: definiert, wie die Weiterleitung der Nutzer*innen zum IdP erfolgt (→ Discovery Service)
- Kontakt-Informationen
- (Föderations-)Metadaten
- Zertifikat(e) und Private Key(s) für Signierung und Ver-/Entschlüsselung der SAML-basierten Kommunikation

- Application Defaults:

```
<ApplicationDefaults entityID="https://loa-check.aai.dfn.de/shibboleth"  
    REMOTE_USER="eppn persistent-id mail eduPersonUniqueId">
```

- Session Konfiguration:

```
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"  
    checkAddress="false" consistentAddress="true"  
    handlerSSL="true" cookieProps="https">
```

- Session Initiator:

```
<SSO discoveryProtocol="SAMLDS"  
    discoveryURL="https://wayf.aai.dfn.de/DFN-AAI-Test/wayf">  
    SAML2  
</SSO>
```

- Hart mit IdP verdrahtet (z.B. lokale Metadaten)

```
<SSO entityID="https://testidp2.aai.dfn.de/idp/shibboleth">  
    SAML2  
</SSO>
```

- Embedded Discovery Service: <https://wiki.aai.dfn.de/de:shibeds>

(zu DS und Metadaten s.u. <https://wiki.aai.dfn.de/de:production>)

- Kontaktdaten für die Anzeige von Fehlerseiten:

```
<Errors supportContact="helpdesk@uni-musterstadt.de"  
        helpLocation="/about.html"  
        styleSheet="/shibboleth-sp/main.css"/>
```

- (Föderations-)Metadaten, mehrere Metadata Provider möglich:

```
<MetadataProvider type="XML"  
    uri="https://www.aai.dfn.de/fileadmin/metadata/dfn-aai-test-metadata.xml"  
    backingFilePath="dfn-aai-test-metadata.xml" reloadInterval="3600">  
    <MetadataFilter type="Signature" certificate="/etc/shibboleth/dfn-aai.g2.pem"/>  
</MetadataProvider>
```

- Zertifikate und Private Keys:

```
<CredentialResolver type="File" key="/etc/ssl/private/sp-key.pem"  
    certificate="/etc/ssl/localcerts/sp-crt.pem"/>
```

Certificate Rollover:

<https://www.aai.dfn.de/dokumentation/zertifikate/zertifikat-erneuern/>

- Der Blick aufs Ganze: <https://wiki.aai.dfn.de/de:shibsp>

<SPConfig> Document root element

Outer elements of the shibboleth.xml configuration file:

<OutOfProcess> / <InProcess>	(Optional) Log settings, extensions
<UnixListener> / <TCPLListener>	(Optional) Communication shibd/mod_shib
<StorageService>	(Optional) Where session information is stored
<SessionCache>	(Optional) Session timeouts and cleanup intervals
<ReplayCache>	(Optional) Where replay cache is stored
<ArtifactMap>	(Optional) Timeout of artifact messages
<RequestMapper>	(Optional) Session initiation and access control
<ApplicationDefaults>	Contains the most important settings of SP
<SecurityPolicyProvider>	Define various security options
<ProtocolProviders>	Defines supported protocols (SAML, ADFS, ...)

Quelle: <https://aarc-project.eu/training/training-for-service-provider-operators/>

Elemente unterhalb `<ApplicationDefaults>`

<code><Sessions></code>	Defines handlers and how sessions are initiated and managed. Contains <code><SSO></code> , <code><Logout></code> , <code><Handler></code>
<code><Errors></code>	Used to display error messages. E.g. logo, email and CSS
<code><RelyingParty></code>	(optional) To modify settings for certain IdPs/federations
<code><MetadataProvider></code>	Defines the metadata to be used by the SP
<code><AttributeExtractor></code>	Attribute map file to use
<code><AttributeResolver></code>	Attribute resolver file to use
<code><AttributeFilter></code>	Attribute filter file to use
<code><CredentialResolver></code>	Defines certificate and private key to be use
<code><ApplicationOverride></code>	(Optional) Can override any of the above for certain applications

Quelle: <https://aarc-project.eu/training/training-for-service-provider-operators/>

- Eine Art API, die verschiedene Funktionen über URLs zur Verfügung stellt:
<https://sp.uni-musterstadt.de/Shibboleth.sso/...>

- Binding URLs

- Metadaten: `.../Shibboleth.sso/`**Metadata**

- Request Initiator: `.../Shibboleth.sso/`**Login**

- Session-Info: `.../Shibboleth.sso/`**Session**

```
<Handler type="Session" Location="/Session"  
        showAttributeValues="true"/>
```

- Status-Abfrage: `.../Shibboleth.sso/`**Status**

```
<Handler type="Status" Location="/Status"  
        acl="127.0.0.1 YOUR_DESKTOP_IP"/>
```

- /etc/shibboleth/attribute-map.xml
- Bildet Attribute auf interne Variablen ab
- Variablenname wird in **id** definiert

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" id="affiliation">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
<Attribute name="urn:mace:dir:attribute-def:eduPersonScopedAffiliation" id="affiliation">
  <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" id="unscoped-affiliation">
  <AttributeDecoder xsi:type="StringAttributeDecoder" caseSensitive="false"/>
</Attribute>
<Attribute name="urn:mace:dir:attribute-def:eduPersonAffiliation" id="unscoped-affiliation">
  <AttributeDecoder xsi:type="StringAttributeDecoder" caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" id="entitlement"/>
<Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement" id="entitlement"/>
```

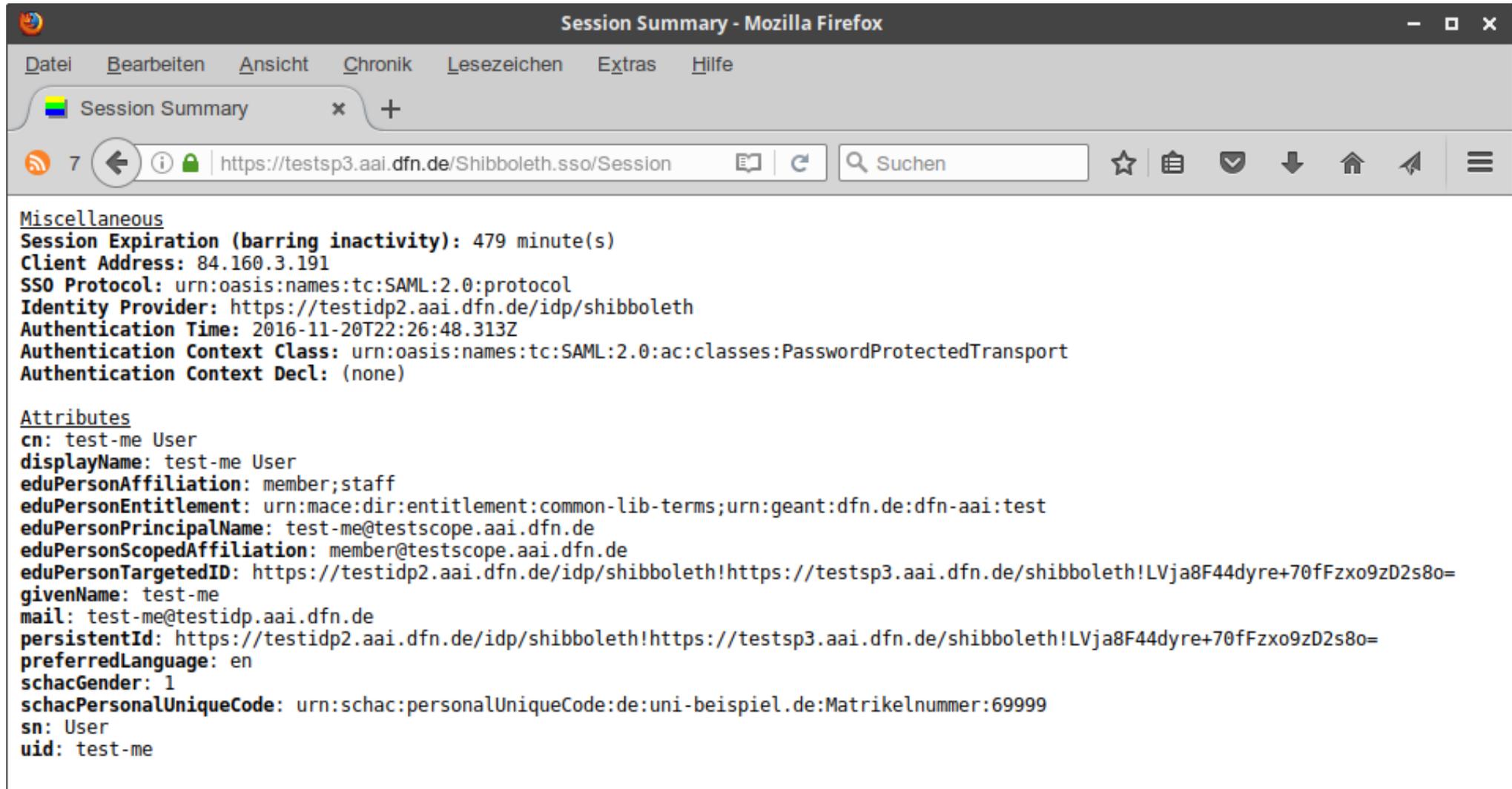
- /etc/shibboleth/attribute-policy.xml
- Filtert Variablen und deren Werte, i.d.R. genügen die Default-Einstellungen

```
<afp:PermitValueRule id="eduPersonAffiliationValues" xsi:type="OR">
  <Rule xsi:type="AttributeValueString" value="faculty"/>
  <Rule xsi:type="AttributeValueString" value="student"/>
  <Rule xsi:type="AttributeValueString" value="staff"/>
  <Rule xsi:type="AttributeValueString" value="alum"/>
  <Rule xsi:type="AttributeValueString" value="member"/>
  <Rule xsi:type="AttributeValueString" value="affiliate"/>
  <Rule xsi:type="AttributeValueString" value="employee"/>
  <Rule xsi:type="AttributeValueString" value="library-walk-in"/>
</afp:PermitValueRule>

<afp:PermitValueRule id="ScopingRules" xsi:type="AND">
  <Rule xsi:type="NOT">
    <Rule xsi:type="AttributeValueRegex" regex="@"/>
  </Rule>
  <Rule xsi:type="saml:AttributeScopeMatchesShibMDScope"/>
</afp:PermitValueRule>

<afp:AttributeFilterPolicy>
  <!-- This policy is in effect in all cases. -->
  <afp:PolicyRequirementRule xsi:type="ANY"/>
  <!-- Filter out undefined affiliations and ensure only one primary. -->
  <afp:AttributeRule attributeID="affiliation">
    <afp:PermitValueRule xsi:type="AND">
      <RuleReference ref="eduPersonAffiliationValues"/>
      <RuleReference ref="ScopingRules"/>
    </afp:PermitValueRule>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="unscoped-affiliation">
    <afp:PermitValueRuleReference ref="eduPersonAffiliationValues"/>
  </afp:AttributeRule>
  <!-- Catch-all that passes everything else through unmolested. -->
  <afp:AttributeRule attributeID="*" permitAny="true"/>
</afp:AttributeFilterPolicy>
```

Session Handler URL Extension bei Shibboleth SP: /Shibboleth.sso/Session



Session Summary - Mozilla Firefox

File Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

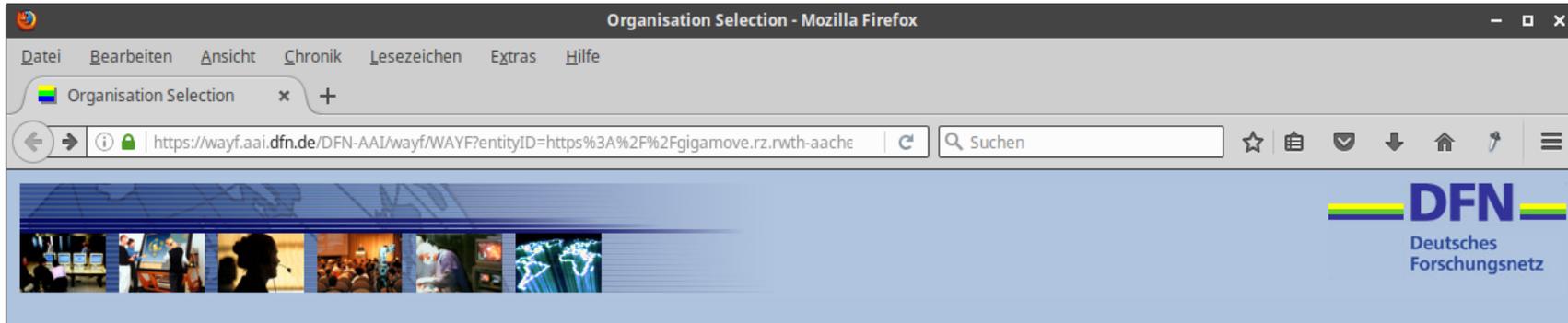
Session Summary x +

7 | https://testsp3.aai.dfn.de/Shibboleth.sso/Session

Miscellaneous
Session Expiration (barring inactivity): 479 minute(s)
Client Address: 84.160.3.191
SSO Protocol: urn:oasis:names:tc:SAML:2.0:protocol
Identity Provider: https://testidp2.aai.dfn.de/idp/shibboleth
Authentication Time: 2016-11-20T22:26:48.313Z
Authentication Context Class: urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport
Authentication Context Decl: (none)

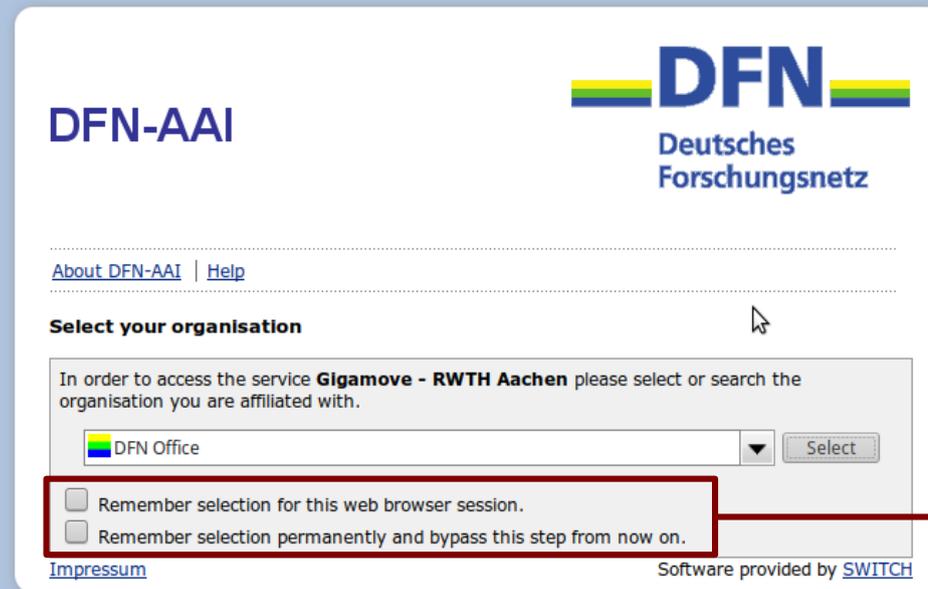
Attributes
cn: test-me User
displayName: test-me User
eduPersonAffiliation: member;staff
eduPersonEntitlement: urn:mace:dir:entitlement:common-lib-terms;urn:geant:dfn.de:dfn-aai:test
eduPersonPrincipalName: test-me@testscope.aai.dfn.de
eduPersonScopedAffiliation: member@testscope.aai.dfn.de
eduPersonTargetedID: https://testidp2.aai.dfn.de/idp/shibboleth!https://testsp3.aai.dfn.de/shibboleth!LVja8F44dyre+70fFzxo9zD2s8o=
givenName: test-me
mail: test-me@testidp.aai.dfn.de
persistentId: https://testidp2.aai.dfn.de/idp/shibboleth!https://testsp3.aai.dfn.de/shibboleth!LVja8F44dyre+70fFzxo9zD2s8o=
preferredLanguage: en
schacGender: 1
schacPersonalUniqueCode: urn:schac:personalUniqueCode:de:uni-beispiel.de:Matrikelnummer:69999
sn: User
uid: test-me

- Auch bekannt als WAYF, „**Where Are You From**“
- 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)
 - Emdeded Discovery Service (am SP)
 - WAYFless URLs
- DFN-AAI Wiki: <https://wiki.aai.dfn.de/de:discovery>



- Vom DFN betrieben
- Stündlich neu aus den jew. Metadatenätzen generiert
- DFN-AAI ("Advanced")
- DFN-AAI-Basic
- DFN-AAI-Basic+eduGAIN
- DFN-AAI-Test
- projektspezifische DS' anhand Whitelist

DFN-AAI



DFN-AAI

Deutsches
Forschungsnetz

[About DFN-AAI](#) | [Help](#)

Select your organisation

In order to access the service **Gigamove - RWTH Aachen** please select or search the organisation you are affiliated with.

Remember selection for this web browser session.
 Remember selection permanently and bypass this step from now on.

[Impressum](#) Software provided by [SWITCH](#)

Cookies!

- Nutzerfreundlich, da nur IdPs gelistet, die tatsächlich für den Dienst relevant sind
- Wird lokal am SP anhand der eingelesenen Metadaten konfiguriert
- Üblicherweise JavaScript Anwendung
- Filterfunktion: Listet nur die IdPs, die für den jeweiligen SP bzw. Dienst relevant sind
- Beispiele
 - SWITCH EDS
<https://www.switch.ch/aai/guides/discovery/embedded-wayf/>
 - Shibboleth EDS
<https://wiki.aai.dfn.de/de:shibeds>
- Best Practice Empfehlungen: **NISO ESPRESSO**,
REFEDS Discovery Guide

- 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://wiki.aai.dfn.de/Shibboleth.sso/Login?entityID=https://idp.dfn.de/idp/shibboleth>
- Siehe auch unter
<https://wiki.aai.dfn.de/de:shibwayfless>

- Die Regeln für die Zugriffskontrolle können auf unterschiedliche Arten definiert werden:
 - Web Server / Apache-Konfiguration: **Apache Access Rules**
 - SP-Konfiguration: **XML Access Control**
 - Anwendung (SP: Lazy Session)
 - SP-Handler: Attribute Checker
- Apache Access Rules ermöglichen einfache AND/OR-Verknüpfung von Bedingungen
- XML Access Control erlaubt komplexere Regeln
- Empfehlung: Die o.g. Varianten nicht mischen und, falls möglich, Apache Access Rules verwenden.

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPProtectContent>

- Schützt Files, Directories, Locations
- Im einfachsten Fall dürfen alle authentifizierten Nutzer auf ein Verzeichnis zugreifen:

```
<Location /protected>  
  AuthType shibboleth  
  Require shibboleth  
  ShibRequestSetting requireSession true  
</Location>
```

- In der Praxis gelten i.d.R. weitere Anforderungen, z.B. gewisse Attribute zur Personalisierung und Autorisierung:

```
<Location /protected>  
  AuthType shibboleth  
  ShibRequestSetting requireSession true  
  <RequireAll>  
    Require shib-attr affiliation staff  
    Require shib-attr mail .*  
  </RequireAll>  
</Location>
```

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApacheConfig>

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPhtaccess>

- Zwei Spezialfälle
(können auch global in `shibboleth2.xml`, Element `<SSO>` gesetzt werden):
 - `ShibRequestSetting forceAuthn true`
(erzwingt erneuten Login am IdP)
 - `ShibRequestSetting isPassive true`
(wenn SSO Session vorhanden, wird eine SP Session ohne weitere Interaktion gestartet, d.h. kein „Sign In“ Button o.ä.)
- Einen Pfad von `mod_shib` ausnehmen, falls z.B. bereits ab `"/` aktiv:

```
<Location /public>  
  AuthType Shibboleth  
  ShibRequestSetting requireSession false  
  Require shibboleth  
</Location>
```

- Zugriffsregeln in XML-Syntax außerhalb der Apache bzw. Web Server Konfiguration (externe Datei kann aber über die Direktive `ShibAccessControl` referenziert werden)
- Üblicherweise in `/etc/shibboleth/shibboleth2.xml`:

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="sp.uni-musterstadt.de">
      <Path name="protected" authType="shibboleth" requireSession="true">
        <AccessControl>
          <AND>
            <Rule require="unscoped-affiliation">staff</Rule>
            <RuleRegex require="mail">.*</RuleRegex>
          </AND>
        </AccessControl>
      </Path>
    </Host>
  </RequestMap>
</RequestMapper>
```

Obacht! In Apache muss `UseCanonicalName On` gesetzt sein!

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPXMLAccessControl>

- Shibboleth ist zwar aktiv, d.h. alle Attribute / Umgebungsvariablen sind verfügbar, aber die Anwendung ist dafür zuständig, eine Authentifizierung zu triggern
→ Session Initiator / Login Handler

- Apache Konfiguration:

```
<Location /Lazy>  
    AuthType shibboleth  
    Require shibboleth  
</Location>
```

- Session initialisieren:

```
https://sp.uni-musterstadt.de/Shibboleth.sso/Login?  
target=https://sp.uni-  
musterstadt.de/protected&entityID=https://idp.uni-  
musterstadt.de/idp/shibboleth
```

- Dieser Handler wird aktiv, bevor eine Weiterleitung auf eine geschützte Ressource erfolgt
- `/etc/shibboleth/shibboleth2.xml`

```
<ApplicationDefaults entityID="https://sp.uni-musterstadt.de/shibboleth"
    REMOTE_USER="eppn"
    sessionHook="/Shibboleth.sso/AttrChecker">
```

```
<!-- hier kommt noch allerlei zwischendurch -->
```

```
<Handler type="AttributeChecker" Location="/AttrChecker" template="attrChecker.html"
    attributes="eppn displayName" flushSession="true"/>
```

- Kann auch `access control policy` enthalten (Element `<AccessControl>` → XML Access Control)
- Siehe unter <https://wiki.shibboleth.net/confluence/x/8IBC>
- Ausführliches Beispiel im eduGAIN Wiki:
https://wiki.edugain.org/How_to_configure_Shibboleth_SP_attribute_checker

- Spezielle CGI-Variable, in der die Identität des Users transportiert wird.
- Eine oder mehrere der in attribute-map.xml definierten Variablen können verwendet werden
- wird gesetzt in shibboleth2.xml:

```
<ApplicationDefaults entityID="https://loa-check.aai.dfn.de/shibboleth"  
    REMOTE_USER="eppn persistent-id mail eduPersonUniqueId">
```

- Damit lassen sich auch Applikationen durch Shibboleth schützen, die keine direkte Shibboleth-(Attribut-)Unterstützung mitbringen
→ Alternative zu Basic Auth
- Siehe auch unter <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication>

- Für das Umstellen von Anwendungen auf Web-SSO via Shibboleth gibt es kein Patentrezept
- Checkliste:
 - Wie wird die Anwendung bisher geschützt (Apache, Tomcat, eigenes Verfahren, ...)?
 - Existiert ein eigenes Session-Management?
 - Kann dieses an SP Sessions gekoppelt werden?
 - Kann Single Logout unterstützt werden?
 - Existiert eine eigene Rechteverwaltung?
 - Können die dafür notwendigen Informationen über Attribute transportiert werden?
 - Können IdPs diese Informationen überhaupt liefern?

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPEnableApplication>

- DFN-AAI Wiki mit einfacher Beispiel-Konfiguration:
<https://wiki.aai.dfn.de/de:shibsp>
- Doku SWITCHaai:
<https://www.switch.ch/aai/guides/sp/>
Installation: <https://www.switch.ch/aai/guides/sp/installation/>
Access Control: <https://www.switch.ch/aai/guides/sp/access-rules/>
- Shibboleth Wiki, Konfiguration:
<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPConfiguration>
- AARC Training for Service Providers
<https://aarc-project.eu/training/training-for-service-provider-operators/>
- SWITCHaai Shibboleth Training 2015:
<https://www.switch.ch/aai/support/presentations/shibboleth-training-2015/>
- Bernd Oberknapp, Anwendungen schützen mit dem Shibboleth Service Provider:
<https://www.aai.dfn.de/uploads/media/20120523-AAIWS-03-service-provider.pdf>
- Shibboleth SP mit Nginx:
<https://wiki.shibboleth.net/confluence/x/VAHN>

Vielen Dank für Ihre Aufmerksamkeit!

Ideen? Fragen? Anmerkungen?

Kontakt

Portal: <https://www.aai.dfn.de>

E-Mail: aai@dfn.de

Tel.: +49 30 884299-9124