

deutsches forschungsnetz

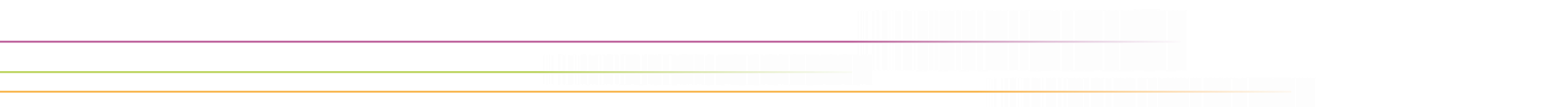


Shibboleth IdP 3.x

Hinweise zu Installation und Konfiguration

AAI- und Shibboleth-Workshop | Berlin, 18./19. Februar 2019

Wolfgang Pempe (pempe@dfn.de)



Installation

- ▶ Shibboleth Wiki:

<https://wiki.shibboleth.net/confluence/display/IDP30/Installation>

- ▶ DFN-AAI Wiki mit Schritt-für-Schritt Doku:

<https://doku.tid.dfn.de/de:shibidp3>

- ▶ Virtuelle Maschine und Materialien:

https://download.aai.dfn.de/ws/2019_cc/

- ▶ Installationsfahrplan: <https://download.aai.dfn.de/ws/2019/>

- ▶ Trainingsunterlagen von SWITCH:

<https://www.switch.ch/aai/support/presentations/shibboleth-training-2015/>

Überblick Konfigurationsdateien (1)

- ▶ ... liegen unter **./conf**
- ▶ .xml und .properties Dateien
- ▶ Zentral: **idp.properties** - wird bei Installation teilweise mit Werten belegt
- ▶ (Föderations-)Metadaten: **metadata-providers.xml**
- ▶ LDAP-Parameter für Login und Attribute Resolver: **ldap.properties**
- ▶ Attribute: **attribute-resolver.xml** und **attribute-filter.xml**
- ▶ SQL-DB für Storage (Session Storage, SAML2 persistent NameID, User Consent):
global.xml
- ▶ SAML Profile: **relying-party.xml**

Überblick Konfigurationsdateien (2)

- ▶ Login / Authentifizierungsmodule unter **./conf/authn** (LDAP, Username+Passwort, x509, Kerberos etc.)
- ▶ Logging: **logback.xml**
- ▶ SAML2 Name IDs: **saml-nameid.properties** und **saml-nameid.xml**
- ▶ Intervalle, in denen Konfigurationsänderungen diverser IdP-interner Dienste geprüft werden: **services.properties**
- ▶ Subject Canonicalization: unter **./conf/c14n**, insbesondere **simple-subject-c14n-config.xml** (Groß-/Kleinschreibung)
- ▶ Zugriff (IP-Bereiche) auf bestimmte Verwaltungsseiten: **access-control.xml**, Zuordnung unter **./conf/admin/general-admin.xml**

Weitere Anpassungsmöglichkeiten

- ▶ Velocity Templates für HTML-Seiten (Login, Logout, User Consent etc.) im Verzeichnis **./views**
- ▶ Sprachspezifische Properties, Beschriftungen unter **./messages**
- ▶ CSS Stylesheets, Grafiken, zusätzliche JARs, angepasste web.xml unter **./edit-webapp**
→ Änderungen erfordern Neu-Generierung des IdP-Servlets: **./bin/build.sh**
- ▶ Zur IdP-Installation und -Konfiguration siehe unter <https://doku.tid.dfn.de/de:shibidp3>

Admin-Interface

- ▶ Neuladen bestimmter Dienste/Konfigurationen: Attribute Resolver, Attribute Filter, Relying Party, Logging, Metadata Resolver etc. via URL, z.B.
<https://idp.local/idp/profile/admin/reload-service?id=shibboleth.LoggingService>
- ▶ Doku im Shib Wiki:
<https://wiki.shibboleth.net/confluence/display/IDP30/ReloadableServices>
- ▶ Regeln festlegen, nach denen der Zugriff erfolgen darf: `./conf/access-control.xml` mit `./conf/admin/general-admin.xml`
- ▶ <https://wiki.shibboleth.net/confluence/display/IDP30/AccessControlConfiguration>

Logging

- ▶ Konfiguration in ./conf/logback.xml
- ▶ `<appender>`: Wohin wird wie geloggt? Z.B. Datei, syslog, Mail, ...
- ▶ `<logger>`: Was wird geloggt? Z.B. Packages, nach Logger-Namen, ...
- ▶ Direkt auf spezifische `<appender>` mit
`<appender-ref ref="<appender-name>" />`
- ▶ `<root>`: zentraler Verteiler für alle `<logger>`
- ▶ Level: TRACE, DEBUG, INFO, WARN, ERROR, OFF, ALL
- ▶ <https://wiki.shibboleth.net/confluence/display/IDP30/LoggingConfiguration>

Wartung und Pflege (1)

- ▶ Abfrage Status-Seite unter `https://idp.uni-musterstadt.de/idp/status`, IP-basierter Zugriff wird über `./conf/access-control.xml` konfigurierbar
- ▶ Certificate / Key Rollover:
<https://www.aai.dfn.de/dokumentation/zertifikate/zertifikat-erneuern/>
- ▶ Update (https://wiki.shibboleth.net/confluence/x/JoIgAQ_):
 - ▶ Zuvor unbedingt die Release Notes lesen!!!
<https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes>
 - ▶ Download der aktuellen Version unter <https://shibboleth.net/downloads/identity-provider/latest/>
 - ▶ Entpacken und `./bin/install.sh -Didp.conf.filemode=644` ausführen
 - ▶ Als Zielverzeichnis die bestehende Installation auswählen (zuvor Backup erstellen!)
 - ▶ Dateien unter `./conf`, `./views`, `./messages` und `./edit-webapp` werden nicht überschrieben
 - ▶ Siehe auch <https://doku.tid.dfn.de/de:shibidp3upgrade>

Wartung und Pflege (2)

- ▶ Web (Admin) Interfaces

<https://wiki.shibboleth.net/confluence/display/IDP30/WebInterfaces>

- ▶ Monitoring und Statistiken: <https://doku.tid.dfn.de/de:shibidp3monitoring>

- ▶ Abwehr Brute Force mit fail2ban: <https://doku.tid.dfn.de/de:shibidp3fail2ban>

- ▶ Troubleshooting: <https://doku.tid.dfn.de/de:shibidp3troubleshoot>

- ▶ User Deprovisionierung via Attribute Query

<https://doku.tid.dfn.de/de:shibidp3userdepro>

Vielen Dank! Fragen? Kommentare?

DFN

► 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

