Shibboleth Identity Provider 2.4.x

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

DFN-AAI IdP-Workshop,
24./25. Juni 2015, HS Amberg-Weiden

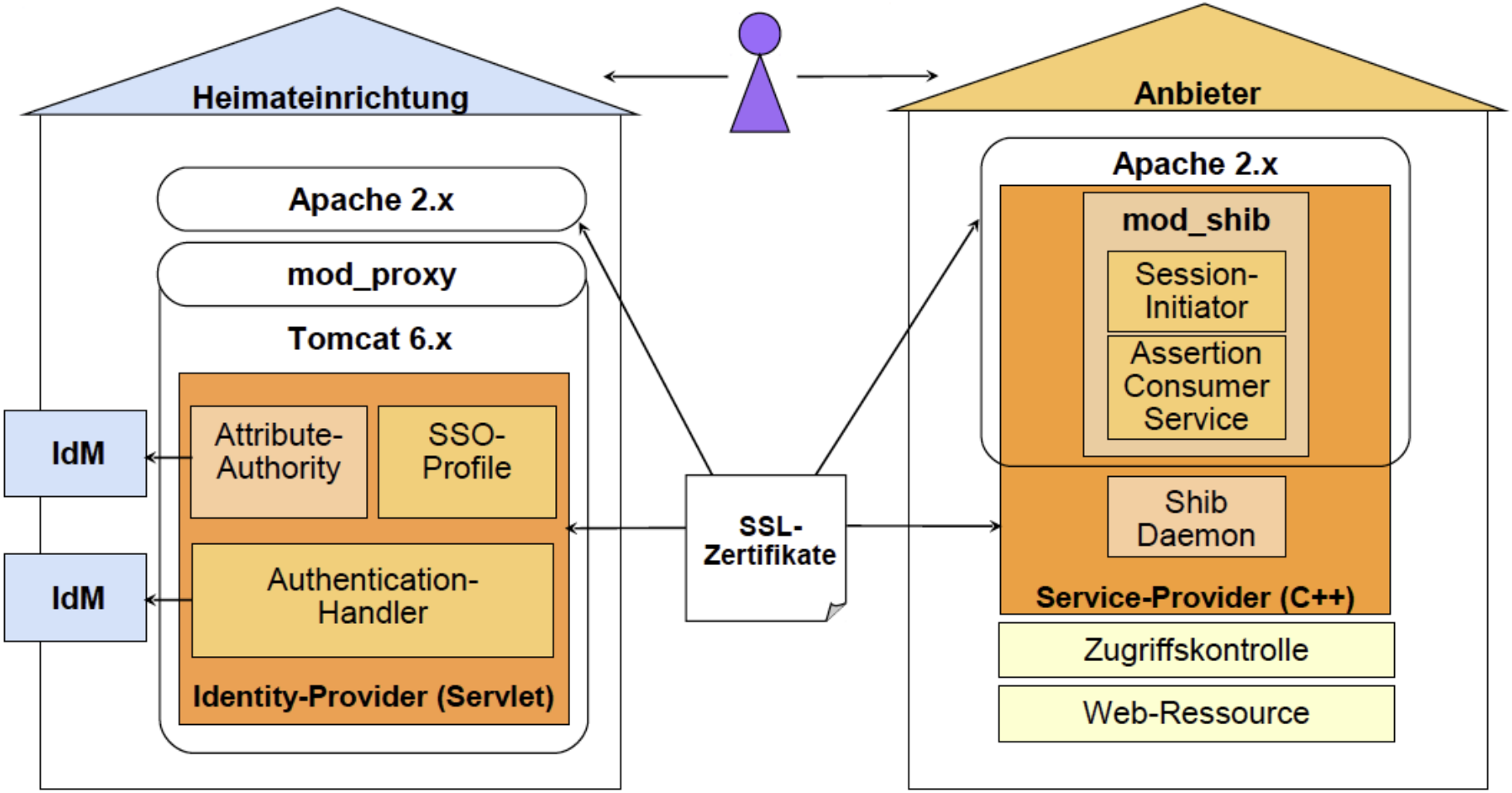
Inhalt

- Überblick
- Konfiguration
- Fehlersuche
- Wartung

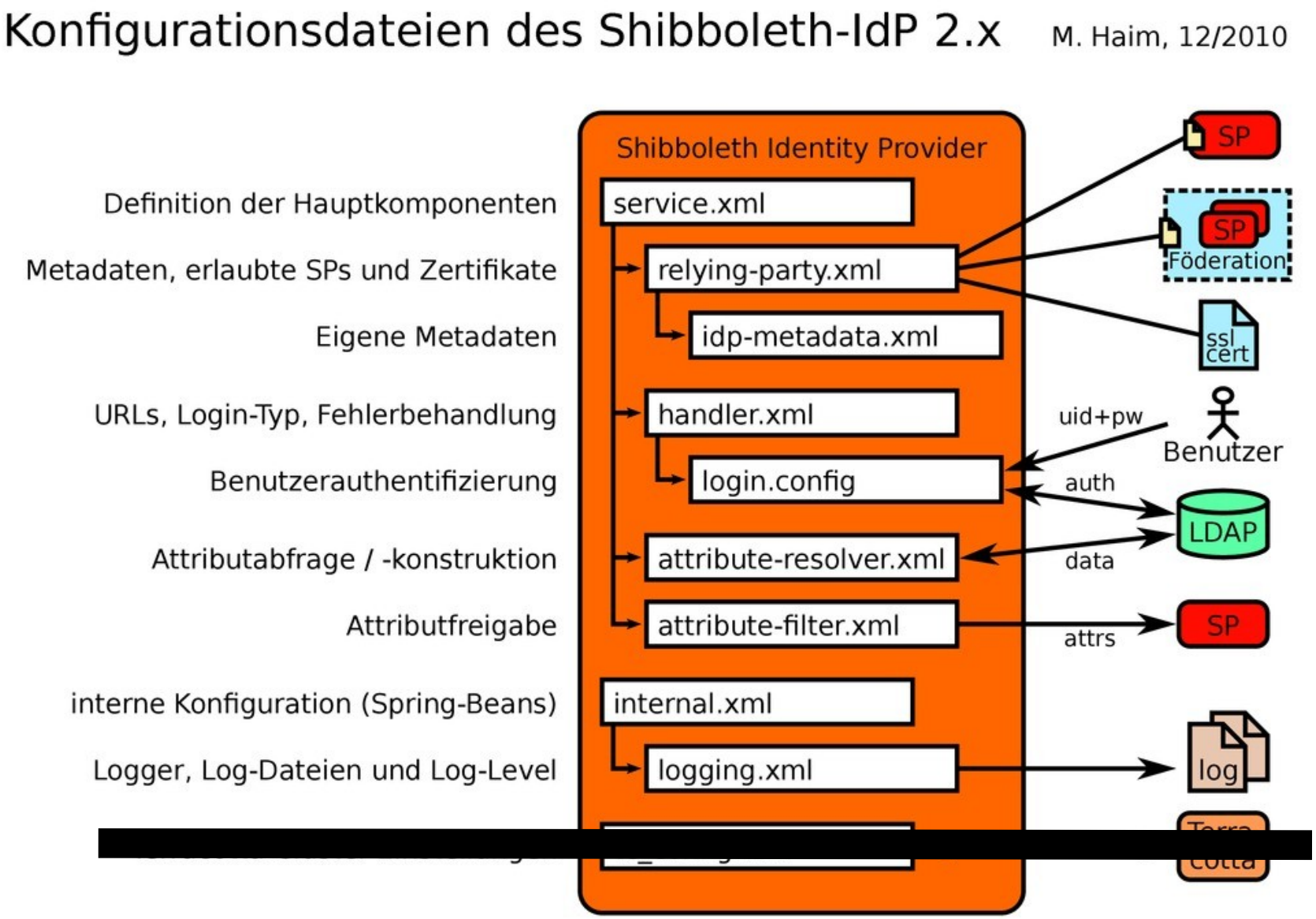
Dokumentation

- Shibboleth Wiki
  https://wiki.shibboleth.net/confluence/display/SHIB2/Configuration
- DFN-AAI
  https://www.aai.dfn.de/dokumentation/

Shibboleth Architektur



Überblick Konfiguration



Quelle: Manuel Haim, Uni Marburg

Konfigurationsdateien

- Beispiele aus der Konfiguration eines DFN Test-IdP (außerhalb der Folien)
- Die Folien behandeln nur (mehr oder minder) wichtige Details

service.xml

- Automatisches Nachladen der Konfigurationsdateien `attribute-filter.xml` und `attribute-resolver.xml`
- Parameter ”configurationResourcePollingFrequency”
- Kein Neustart bei Konfigurationsänderungen erforderlich
- Bei (Syntax-)Fehlern wird die bestehende Konfiguration weiterverwendet → minimales Risiko

```
<srv:Service id="shibboleth.AttributeResolver" xsi:type="attribute-resolver:ShibbolethAttributeResolver"
    configurationResourcePollingFrequency="PT10M">
    <srv:ConfigurationResource file="/opt/shibboleth-idp/dfn-testidp-config/attribute-resolver.xml" xsi:type="resource:FilesystemResource"/>
</srv:Service>

<srv:Service id="shibboleth.AttributeFilterEngine" xsi:type="attribute-afp:ShibbolethAttributeFilteringEngine"
    configurationResourcePollingFrequency="PT10M">
    <srv:ConfigurationResource file="/opt/shibboleth-idp/dfn-testidp-config/attribute-filter.xml" xsi:type="resource:FilesystemResource"/>
</srv:Service>
```

- Bei `relying-party.xml` kommt es erfahrungsgemäß zu Problemen
- `logging.xml` wird per default alle 10 Minuten nachgeladen, falls Änderungen erfolgt sind → erleichtert Debugging

relying-party.xml

- Konfiguration einer oder mehrerer Entity IDs – in Abhängigkeit von bestimmten SPs
- Angabe, welche Profile gegenüber welchen Relying Parties (SPs) verwendet ...
- … und welche Identifier übertragen werden:

```
<rp:AnonymousRelyingParty provider="https://testidp2.aai.dfn.de/idp/shibboleth" defaultSigningCredentialRef="IdPCredential"/>

<rp:DefaultRelyingParty provider="https://testidp2.aai.dfn.de/idp/shibboleth" defaultSigningCredentialRef="IdPCredential"
    nameIDFormatPrecedence="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
    <!--
        Each attribute in these profiles configuration is set to its default value,
        that is, the values that would be in effect if those attributes were not present.
        We list them here so that people are aware of them (since they seem reluctant to
        read the documentation).
    -->
```

- MetadataProvider und Zertifikate

handler.xml

- Profiles: Bindings und Binding URLs
- URLs → Metadaten
- SP vergleicht die URLs aus der SAML Assertion mit denen aus den Föderationsmetadaten (+ vice versa)
- Definition der/des Login Handler(s), siehe

  https://wiki.shibboleth.net/confluence/display/SHIB2/IdPUserAuthn

```
<!--  Username/password login handler -->

<ph:LoginHandler xsi:type="ph:UsernamePassword"
                 jaasConfigurationLocation="file:///opt/shibboleth-idp/login.config">
    <ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</ph:AuthenticationMethod>
</ph:LoginHandler>
```

Weitere Konfigurationsdateien

- `attribute-filter.xml`
  `attribute-resolver.xml`
  → siehe Präsentation zu Attributen
- `logging.xml`
  → siehe Fehlersuche + Debugging
- `internal.xml`
  in der Regel keine Anpassungen erforderlich,
  ggf. Session-Timeout modifizieren
  https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthnSession

Fehlersuche, Debugging (1)

- In logging.xml Loglevel hochsetzen:

```
<!--
    Loggers define indicate which packages/categories are logged, at which level, and to which appender.
    Levels: OFF, ERROR, WARN, INFO, DEBUG, TRACE, ALL
-->
<!-- Logs IdP, but not OpenSAML, messages -->
<logger name="edu.internet2.middleware.shibboleth" level="DEBUG" />

<!-- Logs OpenSAML, but not IdP, messages -->
<logger name="org.opensaml" level="WARN" />

<!-- Logs LDAP related messages -->
<logger name="edu.vt.middleware.ldap" level="WARN" />

<!-- uApprove -->
<logger name="ch.SWITCH.aai.uApprove" level="WARN"/>

<!-- Logs inbound and outbound protocols messages at DEBUG level -->

<logger name="PROTOCOL_MESSAGE" level="DEBUG" />
```

- Wichtig: Beide Werte auf DEBUG setzen, damit auch die noch nicht verschlüsselten Assertions mit geloggt werden.
- Doku: https://wiki.shibboleth.net/confluence/display/SHIB2/IdPLogging

Fehlersuche, Debugging (2)

- Bei Problemen mit Script Attribute Definitions lässt sich auch dort ein Logger definieren:

```
<ad:Script><![CDATA[
    importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);
    importPackage(Packages.org.slf4j);
    // logger = LoggerFactory.getLogger("edu.internet2.middleware.shibboleth.resolver.Script.statistics");
    logger = LoggerFactory.getLogger("HK24-Statistics");

    if (typeof cbUserType != "undefined" && cbUserType != null ){
       for ( i = 0; cbUserType != null && i < cbUserType.getValues().size(); i++ ){
          usertype = cbUserType.getValues().get(i);
          logger.info("entityID: " + requestContext.getPeerEntityId() + " userGroup: "+ usertype);
       }
    }

    // Create attribute to be returned from definition
    if (eduPersonEntitlement == null) {
          eduPersonEntitlement = new BasicAttribute("eduPersonEntitlement");
    }

    if (eduPersonAffiliation.getValues().contains("member")) {
          eduPersonEntitlement.getValues().add("urn:mace:dir:entitlement:common-lib-terms");
    }
    ]]>
</ad:Script>
```

- Siehe auch die Dokumentation im Shibboleth Wiki

Fehlersuche, Debugging (3)

IdP Status Seite

- https://idp.hs-beispiel.de/idp/status
- Zugriff für bestimmte IP Bereiche muss in web.xml konfiguriert werden, siehe https://www.aai.dfn.de/dokumentation/identity-provider/konfiguration#c2293
- Systeminformationen + Speicherverbrauch
- Verwendete Zertifikate
- Relying Party Konfiguration
- Entity IDs und Profile
- Beispiel: https://testidp2.aai.dfn.de/idp/status

Fehlersuche, Debugging (4)

Online-Ressourcen und Anlaufstellen:

- Shibboleth Wiki:
  https://wiki.shibboleth.net/confluence/display/SHIB2/Troubleshooting
- Mailinglisten - andere hatten möglicherweise die selben oder ähnliche Probleme:
  https://www.aai.dfn.de/mailinglisten/
  (aai-users@aai.dfn.de, users@shibboleth.net)
- DFN-AAI Hotline (siehe letzte Folie)

Wartung (1)

- Update verfügbar?
- Subskription einschlägiger Listen
  https://www.aai.dfn.de/mailinglisten/
  - aai-announce@aai.dfn.de
  - announce@shibboleth.net
- Übersicht über Sicherheitslücken und Security Advisories:
  https://wiki.shibboleth.net/confluence/display/DEV/SecurityAdvisories
- Lohnt sich ein Update? Was kommt demnächst?
  https://wiki.shibboleth.net/confluence/display/DEV/Project+Roadmap

Wartung (2)

- Installation neuer Plugins, Änderungen an JSP-Dateien und web.xml ...
- … idealerweise im Installations-Quellverzeichnis durchführen, also dort, wohin das Installations-Archiv entpackt und von wo aus `install.sh` ausgeführt wurde
- Je nach Konfiguration des Servlet Containers wird der IdP beim erneuten `install` automatisch neu gestartet **Obacht:** Nicht zu oft hintereinander wiederholen! (ansonsten Container neu starten)
- Updates innerhalb der 2.x Produktlinie auf die selbe Weise durchführen, siehe separate Doku

Vielen Dank für Ihre Aufmerksamkeit!

Ideen? Fragen? Anmerkungen?

Kontakt

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

EMail: hotline@aai.dfn.de

Tel.: +49 711 63314 215