SP-seitiges Rechtemanagement mit Shibboleth-Bordmitteln

– Werkstattbericht –

Wolfgang Pempe, DFN-Verein
pempe@dfn.de

AAI-Forum, 59. DFN-Betriebstagung,
15. Oktober 2013, Berlin

Ausgangssituation

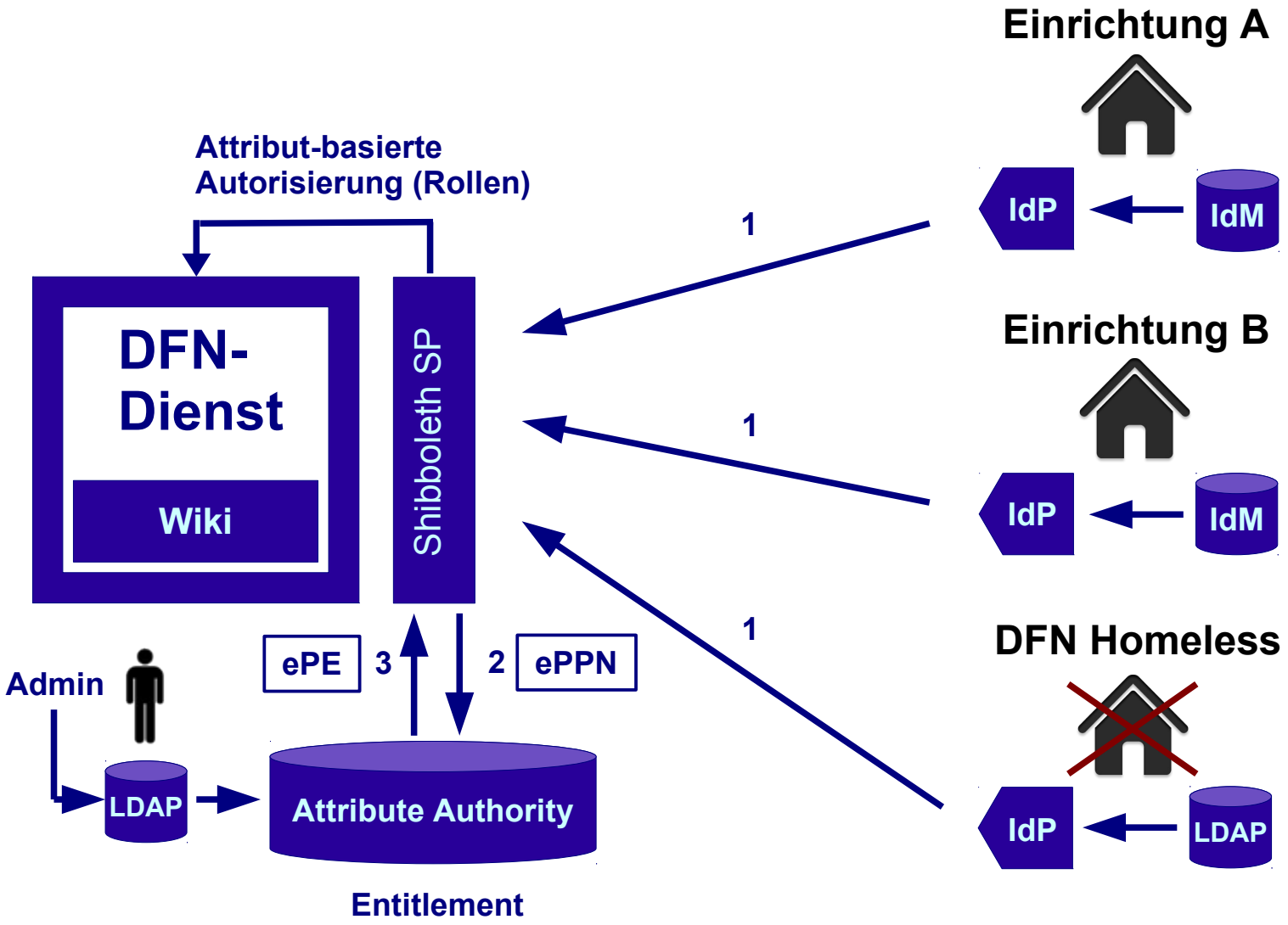
Föderierter Zugang zu DFN-Dienst (Wiki)

- Wiki durch Shibboleth SP geschützt
- Kleiner, überschaubarer Nutzerkreis
- Nutzer aus unterschiedlichen Institutionen
- Nicht jede dieser Institutionen mit IdP in DFN-AAI
- Unterschiedliche Rechte/Rollen (Entitlements)
- Diese Attribute sollten **nicht** von der HO verwaltet werden

→ Homeless IdP für Nutzer von DFN-Diensten

→ **Attribute Authority für dienstspezifische Entitlements**

Umsetzung – Überblick



Umsetzung – SP (1)

Simple Aggregation Attribute Resolver

- Gut dokumentiert, siehe Shibboleth-Wiki
  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeResolver
- Für das Attribut-Mapping wird ein eindeutiger Identifier benötigt, hier eduPersonPrincipalName (ePPN)
- Neben der Konfiguration des Attribute Resolvers sind weitere Zurichtungen erforderlich
  - Whitelist für ”berechtigte” IdPs (Metadata Filter)
  - Zugang zum Wiki nur, wenn Entitlement gesetzt ist (Webserver, Apache)
  - Entitlements nur von der Attribute Authority (AA) entgegennehmen (attribute filter policy)

Umsetzung – SP (2)

Attribute Resolver

```
<AttributeResolver type="SimpleAggregation" attributeId="eppn"
        format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
    <Entity>https://attributes.dfn.de/idp/shibboleth</Entity>
    <Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        FriendlyName="eduPersonEntitlement"/>
</AttributeResolver>
```

Umsetzung – SP (3)

Metadata Filter

```
<MetadataProvider type="Chaining">
      <MetadataProvider type="XML"
           uri="https://www.aai.dfn.de/fileadmin/metadata/DFN-AAI-metadata.xml" ...>
      <MetadataFilter type="RequireValidUntil" maxValidityInterval="604800"/>
      <MetadataFilter type="Signature" certificate="/etc/shibboleth/dfn-aai.pem" />
      <MetadataFilter type="Whitelist">
          <Include>https://idp.uni-abc.de/idp/shibboleth</Include>
          <Include>https://idp.uni-xyz.de/idp/shibboleth</Include>
          <Include>https://idp.dfn.de/idp/shibboleth</Include>
          <Include>https://extlogin.dfn.de/idp/shibboleth</Include>
          <Include>https://attributes.dfn.de/idp/shibboleth</Include>
      </MetadataFilter>
</MetadataProvider>
```

Umsetzung – SP (4)

Webserver / Apache

```
<Directory /var/www/vhosts/...>
  ...
  AuthType shibboleth
  ShibRequireSession On
  ShibRequireAll On
  require valid-user
  require entitlement ~ ^https://www.dfn.de/entitlement/syncandshare/.*$
</Directory>
```

Umsetzung – SP (5)

Attribute Filter Policy

shibboleth2.xml

```
<AttributeFilter type="XML" validate="true" path="attribute-authority-policy.xml" reloadChanges="true" />
```

attribute-authority-policy.xml

```
<afp:AttributeFilterPolicyGroup ...>
    <afp:AttributeFilterPolicy id="getAttributesFromAlmostAnyone">
        <afp:PolicyRequirementRule xsi:type="basic:ANY" />
        <afp:AttributeRule attributeID="eppn">
            <afp:PermitValueRule xsi:type="basic:ANY" />
        </afp:AttributeRule>
        ...
        <afp:AttributeRule attributeID="entitlement">
            <afp:PermitValueRule xsi:type="basic:AttributeIssuerString"
                value="https://attributes.dfn.de/idp/shibboleth"/>
        </afp:AttributeRule>
    </afp:AttributeFilterPolicy>
</afp:AttributeFilterPolicyGroup>
```

Umsetzung – AA (1)

AA = IdP mit eingeschränkter Funktionalität

- Setup als solches nicht sehr gut dokumentiert (?)
- Metadaten-technisch wird nur <AttributeAuthorityDescriptor> benötigt
- Nur AttributeQuery Profile erforderlich, kein SSO
- RemoteUser Authentication
- ePPN als Direct Principal Connector (attribute-resolver.xml), siehe auch https://wiki.shibboleth.net/confluence/display/SHIB2/DirectPrincipalConnector
- Attribute Query nur seitens berechtiger SPs!

Umsetzung – AA (2)

Profil-Konfiguration in relying-party.xml

```
<rp:AnonymousRelyingParty provider="https://attributes.dfn.de/idp/shibboleth"
    defaultSigningCredentialRef="IdPCredential"/>
<rp:DefaultRelyingParty provider="https://attributes.dfn.de/idp/shibboleth"
    defaultSigningCredentialRef="IdPCredential"/>
<rp:RelyingParty id="https://collab.dfn.de/shibboleth"
            provider="https://attributes.dfn.de/idp/shibboleth"
            defaultSigningCredentialRef="IdPCredential">
   <rp:ProfileConfiguration xsi:type="saml:SAML2AttributeQueryProfile"
                    assertionLifetime="PT5M" assertionProxyCount="0"
                    signResponses="conditional" signAssertions="never"
                    encryptAssertions="conditional" encryptNameIds="never"
                    includeConditionsNotBefore="true"/>
</rp:RelyingParty>
```

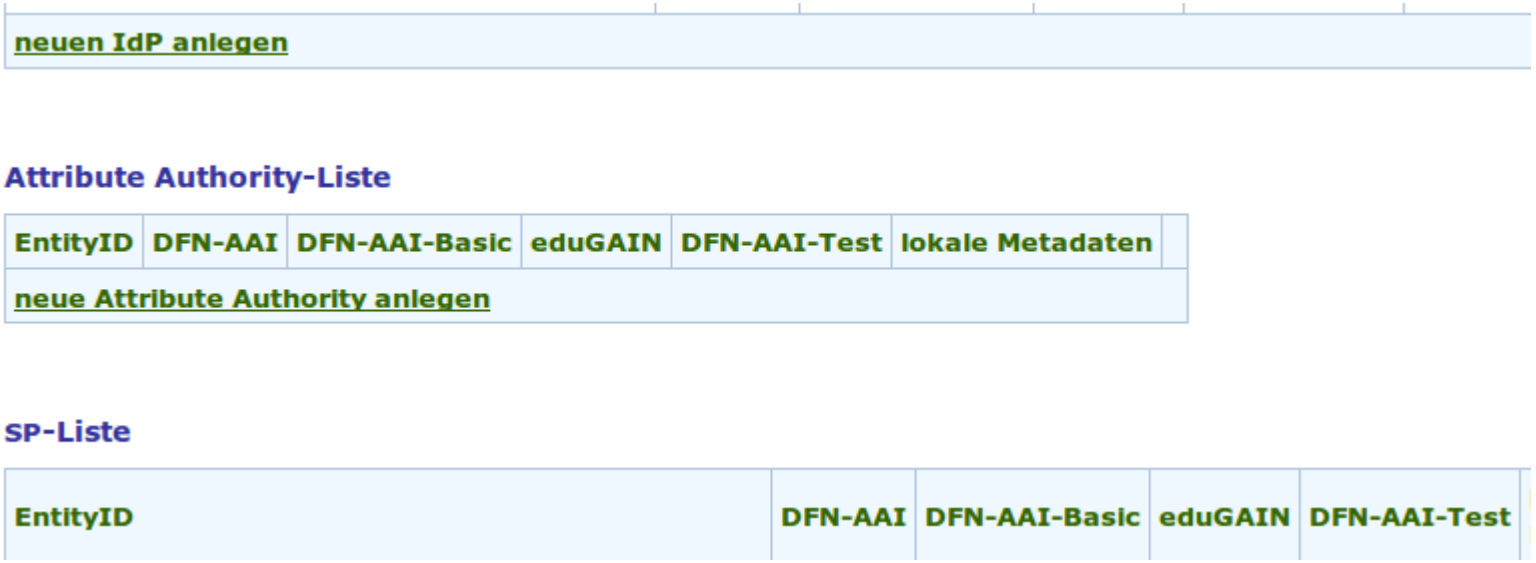
Umsetzung – AA (3)

Attribute Filter Policy (attribute-filter.xml)

```
<afp:AttributeFilterPolicy id="releaseEverythingToDfnSP">
    <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
        value="https://collab.dfn.de/shibboleth" />
    <afp:AttributeRule attributeID="eduPersonEntitlement">
        <afp:PermitValueRule xsi:type="basic:ANY" />
    </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

Metadatenverwaltung: AA als eigener Typ?

- Metadaten-technisch saubere Lösung
- DFN-Policy: Nur ein produktiver IdP pro Einrichtung
  → aber mehrere Attribute Authorities
- WAYF-Generierung → nur Entities mit IdPSSODescriptor



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