UNIVERSITÄTS-
BIBLIOTHEK
HEIDELBERG

Shibboleth-Erfahrungsbericht UB Heidelberg

- Motivation
- Realisierung/Erfahrungen
- Wünsche

Zugang zu den elektronische Medien:

- IP-Authentifizierung für Klinika HD + MA
- Authentifzierung über Bibliothekskennung vom Campus bzw. weltweit (wo vertraglich erlaubt)

Authentifizierung über Bibliothekskennung bislang:

Eigenentwicklung mit

- SSO
- Berechtigungsgruppen, Zuordnung abhängig von
  - Benutzertyp
  - Organisationseinheit
  - Standort (IP-Adresse)

Shibboleth Erfahrungsbericht UB Heidelberg

Authentifizierung über Bibliothekskennung bislang:

✔ eigen-gehostete Anwendungen

✔ Anwendungen unter ReDI

✗ **Problem: Hosting durch andere Einricht. (z.B. Elektra)**

✗ **Problem: von Verlagen gehostete Anwendungen**

Bisherige Lösung für Verlagsanwendungen:

Authentifzierung mit Kennung → Nutzung der IP-Freischaltung

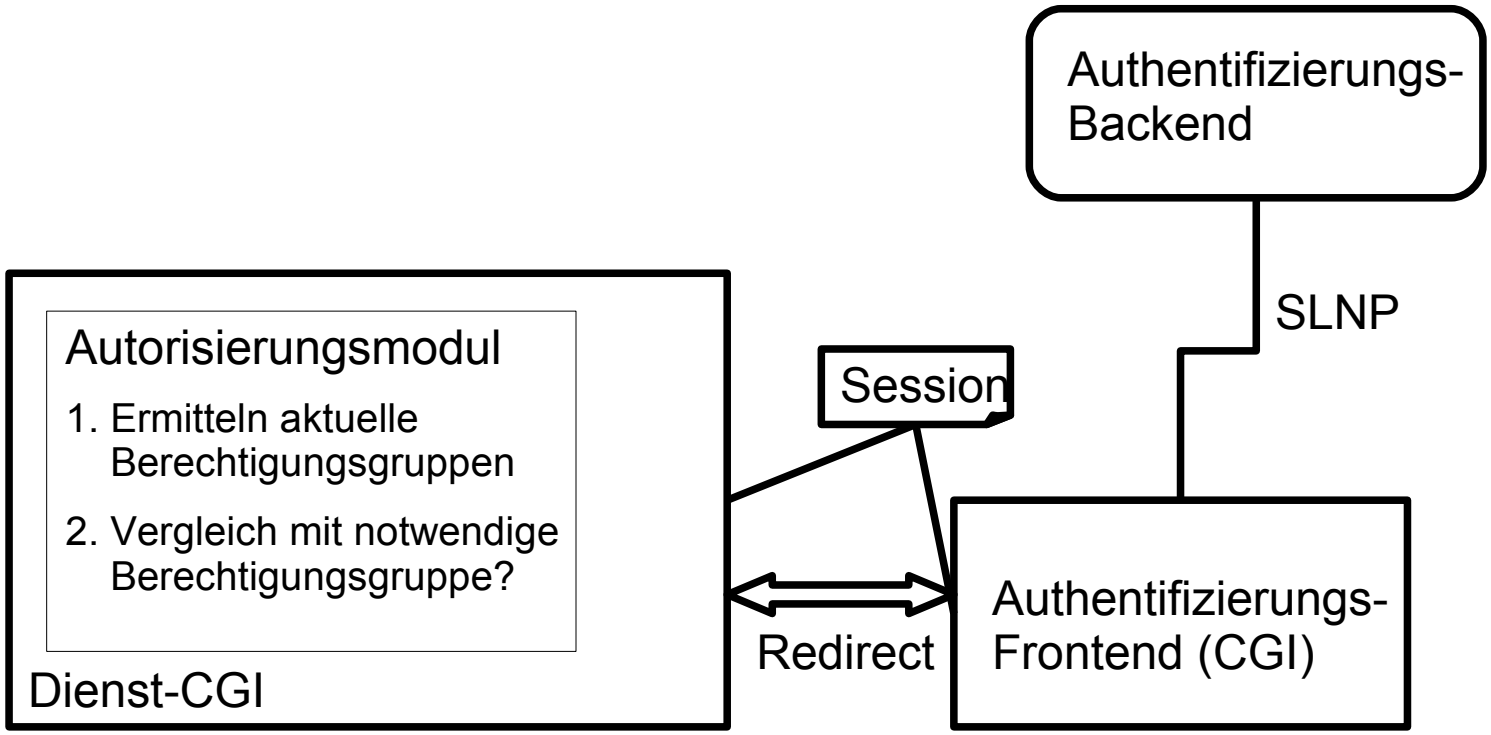
- Proxy
- VPN
- Rewriting Proxy/Aufruf über lokale (P)URL

Jeweils mit Nachteilen verbunden...

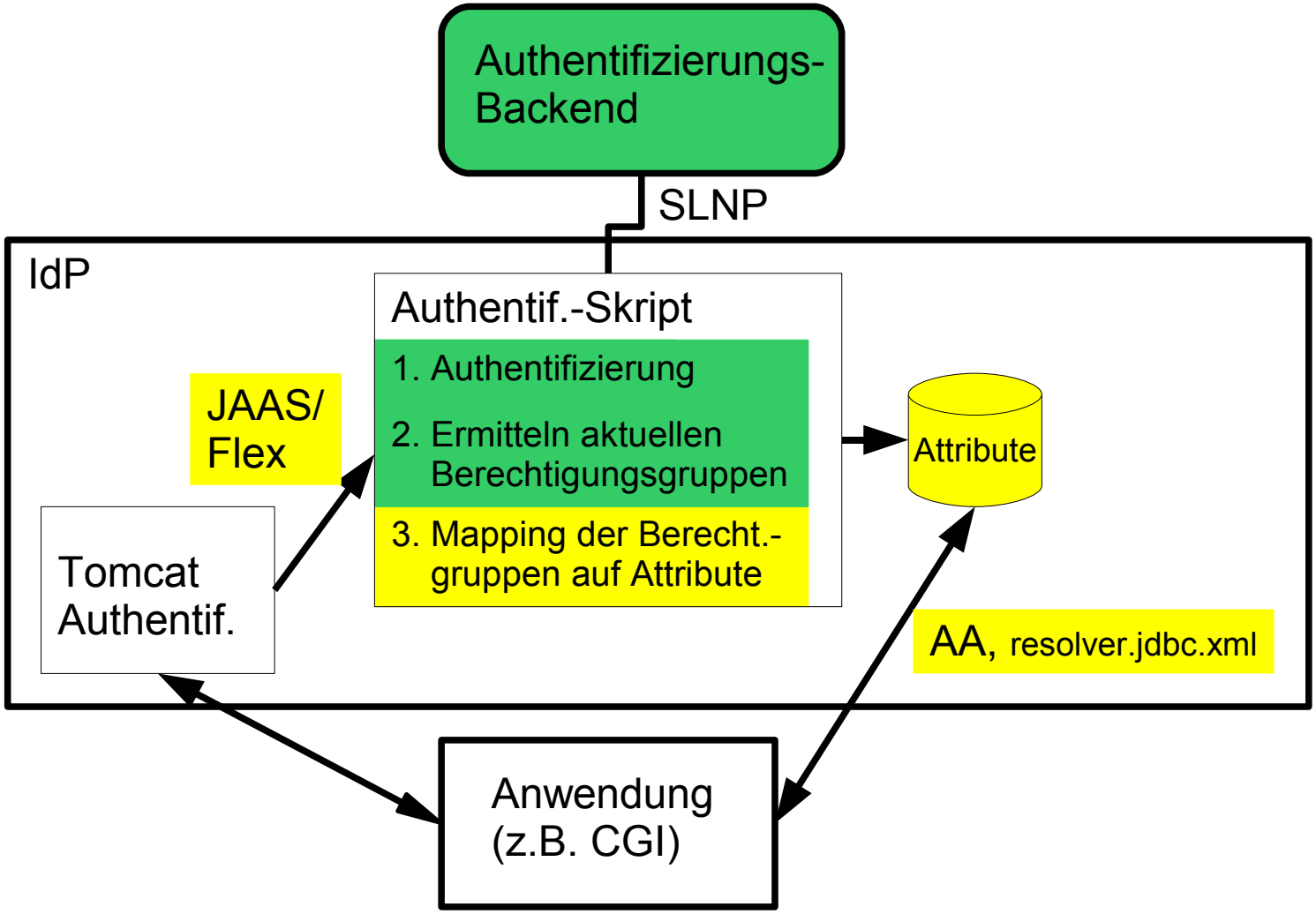
Probleme der bisherigen Lösungen:

- Verschlechterung des Benutzungskomfort
- Technisches Wissen beim Benutzer notwendig
- Technik nicht immer einsetzbar
- URLs in Nachweissystemen
- URLs bei Artikelverlinkungen
- ...

Realisierung/Erfahrungen



Shibboleth Erfahrungsbericht UB Heidelberg



Shibboleth Erfahrungsbericht UB Heidelberg

Attribut-Mapping:

```
%attribute_entitlement  =
 "urn:mace:ub.uni-freiburg.de:entitlement:unihd:redi:all" => "11,24",
 "urn:mace:ub.uni-freiburg.de:entitlement:unihd:redi:juris" => "31",
 "urn:mace:dir:entitlement:common-lib-terms" => "11,24",
);
```

11: Universitätsangehörige
24: Alle externen Nutzer – Zugriff von der UB aus
31: Universitätsangehörige – Zugriff vom Campus aus

Shibboleth Erfahrungsbericht UB Heidelberg

resolver.jdbc.xml:

```
<SimpleAttributeDefinition
   id="urn:mace:dir:attribute-def:eduPersonEntitlement"
   lifeTime="57600"
   sourceName="attvalue">
   <DataConnectorDependency requires="db1"/>
</SimpleAttributeDefinition>
<JDBCDataConnector
   id="db1"
   dbURL="jdbc:mysql://localhost:3306/ub_dienste?user=shib&amp;password=***"
   dbDriver="com.mysql.jdbc.Driver"
   maxActive="10"
   maxIdle="5">
  <Query>SELECT attvalue FROM shibboleth WHERE userid = ? AND attname = 'entit' </Query>
</JDBCDataConnector>
```

Shibboleth Erfahrungsbericht UB Heidelberg

Bislang auf Shibboleth umgestellt:

- ReDI (Datenbanken und E-Journals)
- Lokale Windows-Datenbanken (IBplus)
- Elektra

Demnächst:

- Lokal gehostete E-Books und E-Journals
- Rewriting-Proxy für Verlagsanwendungen
- Verlags-gehostete Anwendungen (?)

Langfristig:

- Umstieg auf Uni-ID.

Realisierung/Erfahrungen

- Lösungen für benötigte Anwendungsszenarien beim AAR-Team vorhanden (Tomcat-Authentifizierung: LDAP → JAAS → Flex).
- Einrichtung und lokale Anpassung im Prinzip recht einfach.
- Aber bei Problemen meist auf Expertenrat angewiesen (Logfiles + Doku. helfen nicht immer).
- Läuft stabil.

Wünsche

- Verlage:
  - Schnittstellen schaffen bzw. nutzen.
- Bibliotheken:
  - Schnittstellen bei Verlagen nachfragen.
  - Schnittstellen als Vertragsvoraussetzungen.
- AAR-Team/DFN:
  - „Rezepte“ zur Installation eines IdP bereitstellen. ☺
  - „Rezepte“ für den Betrieb (z.B. Was muss, was darf geloggt werden?) bereitstellen.
  - Aktiveres Informieren über Neuentwicklungen.
  - Dauerhafter Support durch Experten.