Shibboleth-Erfahrungsbericht UB Heidelberg

- Motivation
- Realisierung/Erfahrungen
- Wünsche

Motivation

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)

Motivation

Authentifizierung über Bibliothekskennung bislang:

✔ eigen-gehostete Anwendungen

✔ Anwendungen unter ReDI

✗ **Problem:** von Verlagen gehostete Anwendungen

Bisherige Lösung:

Authentifzierung mit Kennung → Nutzung der IP-Freischaltung

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

Jeweils mit Nachteilen verbunden...

Motivation

Probleme der bisherigen Lösungen:

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

Motivation

Wir brauchen eine Lösung, die folgende Bedingungen erfüllt:

- Campus + Extern
- sicher
- einfach für Benutzer
- einfach zu administrieren und zu verhandeln (Standard)
- Nach Möglichkeit: Bisheriges System weiter nutzbar

Shibboleth mit JAAS

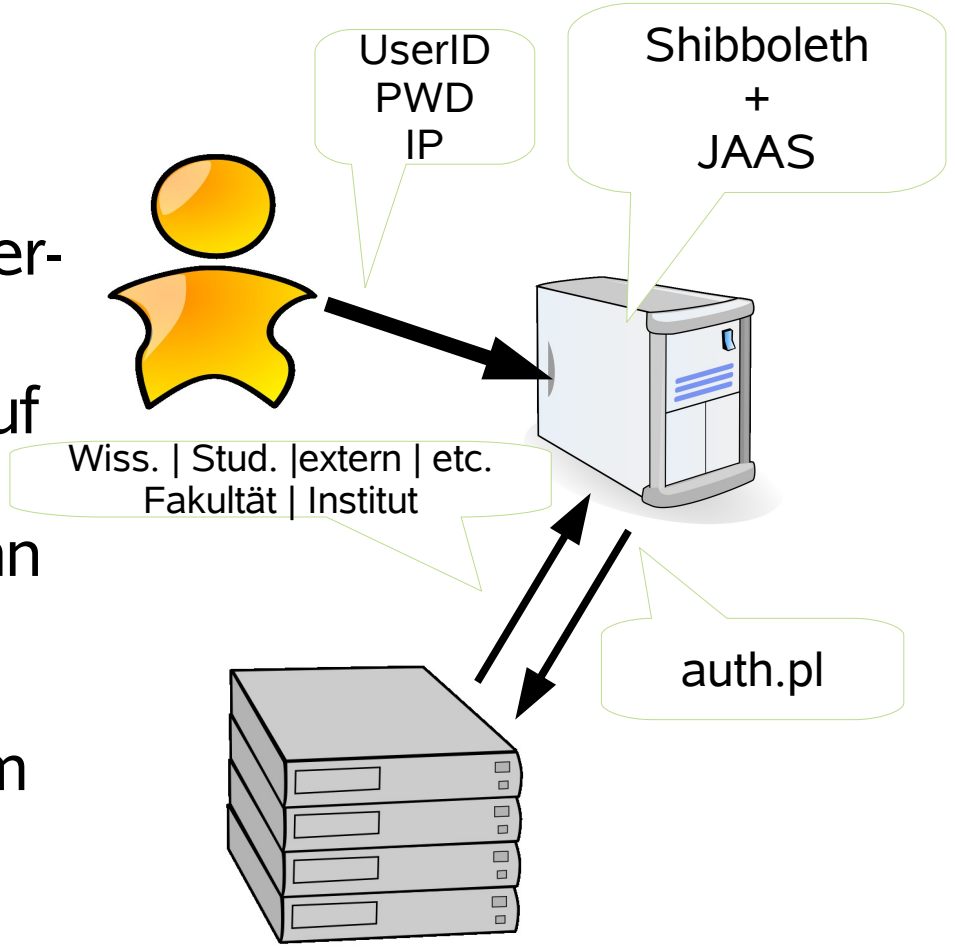
- Motivation:
  - Benötigt wird neben Benutzer-ID+Passwort auch die IP-Adresse
  - IP-Adresse wird z. B. bei Lizenzmodellen benötigt die einen Zugriff nur innerhalb des Campus zulassen
  - IP-Adresse nur bei der **Authentifizierung** verfügbar
  - LDAP Resolver wurde nur benutzt um individuelles Authentifizierungsskript aufzurufen

Shibboleth mit JAAS

- Voraussetzungen
  - Datenbank Connector (z.B. mysql-connector-java.jar) in $TOMCAT/common/lib
  - Bibliothek $TOMCAT/server/lib/jaas-scriptlogin.jar vom AAR Team
  - $TOMCAT /bin/setenv.sh für erweiterte JAVA_OPTS
  - $SHIB/etc/jaas-scriptlogin.conf - hier wird der Pfad zur jaas-scriptlogin.xml gesetzt.
  - in $SHIB/etc/jaas-scriptlogin.xml wird schließlich der Pfad zum Perl Skript angegeben
  - Neuer Security Realm in der server.xml

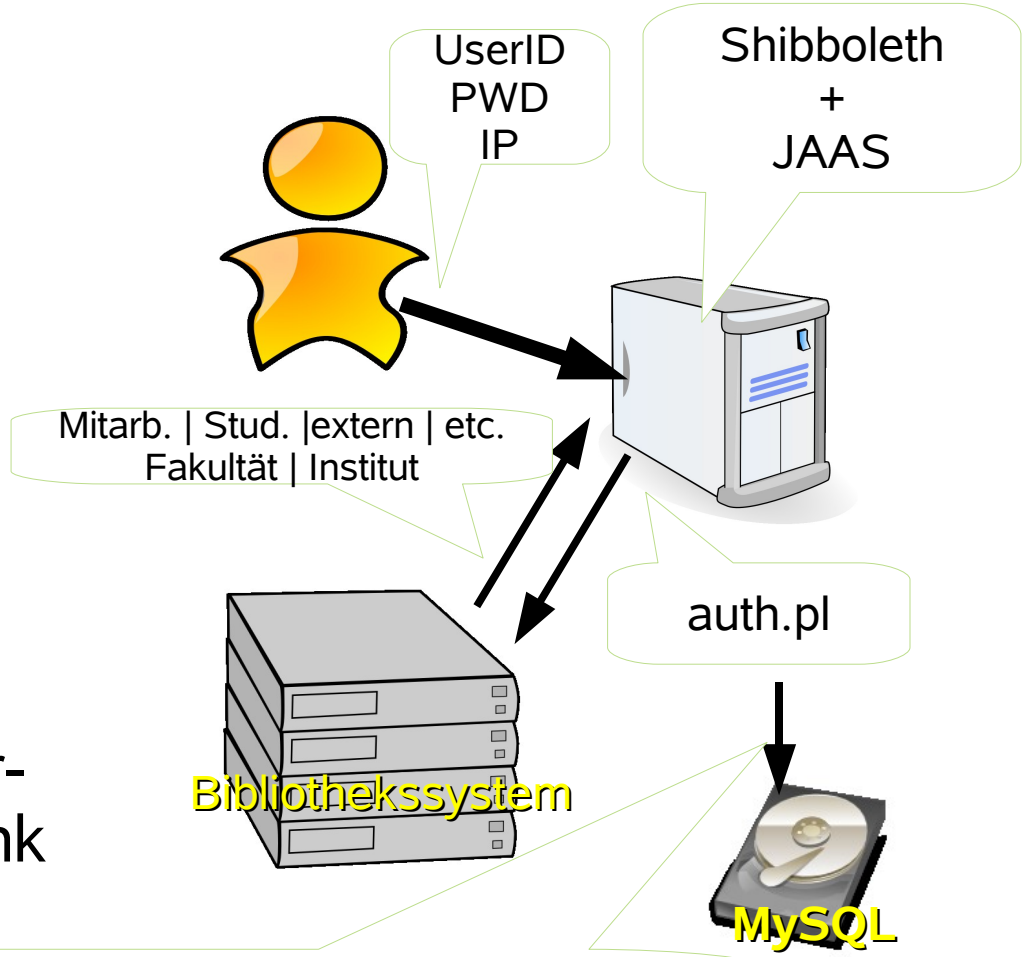
Shibboleth mit JAAS

- Ablauf:
  1. Benutzer gibt Benutzer-ID und Passwort ein
  2. JAAS ruft ein Skript auf das den Benutzer authentifiziert und dann Benutzertyp und Organisationseinheit vom Bibliothekssystem holt



Shibboleth mit JAAS

- Ablauf (forts.):
  3. Das Skript ermittelt mit der IP und den Daten des Bibl.-systems die Berechtigungs-gruppen
  4. => Attribute für alle Provider; diese werden mit der User-ID in einer Datenbank gespeichert.



Shibboleth mit JAAS

Aufbau der Datenbanktabelle

```
+---------+-----------+-----------------------------------------------+-----------------------------+
| userid  | attname | attvalue                                                                  | timestamp  |
+---------+-----------+-----------------------------------------------+-----------------------------+
                                                .
                                                .
                                                .
00123123 | entit   | urn:mace:ub.uni-freiburg.de:entitlement:unihd:redi:all   | 1160052091 |
00123123 | entit   | urn:mace:ub.uni-freiburg.de:entitlement:unihd:redi:juris | 1160052091 |
                                                .
                                                .
                                                .
```

Shibboleth mit JAAS

resolver.jdbc.xml

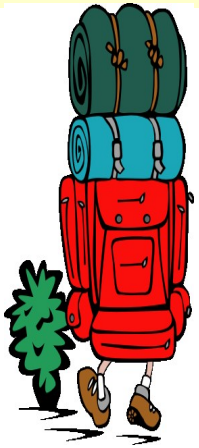
```
<JDBCDataConnector id="db1"
dbURL="jdbc:mysql://localhost:3306/ub_dienste?user..."
    dbDriver="com.mysql.jdbc.Driver"
    maxActive="10"
    maxIdle="5">
  <Query>SELECT attvalue FROM shibboleth WHERE
userid = ? AND attname = 'entit'</Query>
```

Im Resolver werden die DB - Verbindungsparameter und die SQL - Abfrage für die Attribute angegeben. Diese werden dann über den ARP gefiltert an den SP übergeben

arp.site.xml

```
<Attribute name=
   "urn:mace:dir:attribute-def:eduPersonEntitlement">
    <AnyValue release="permit"/>
</Attribute>
</Rule>
```

Erfahrungen



- Shibboleth mit JAAS ist eine komplexe Lösung, viele Konfigurationsdateien und Programmbibliotheken an verschiedenen Orten
- Aber: sehr flexibel !
- Ist der IDP erst einmal konfiguriert geht die Anpassung eines bestehenden Authentifizierungssystems schnell von statten.
- Im laufenden Betrieb ergaben sich keine Probleme

Wünsche 

- Verlage:
  - Schnittstellen schaffen bzw. nutzen
- Bibliotheken:
  - Schnittstellen bei Verlagen und Softwareherstellern nachfragen
- AAR-Team + DFN:
  - möglichst schnell geplante Föderation bereitstellen
- ReDI:
  - Bestehende ReDI-Föderation vorläufig für bilaterale Nutzung (Bibliotheken ↔ Verlage) zur Verfügung stellen

Wünsche

- AAR-Team:
  - HowTo's zur Installation eines IdP bereitstellen
  - Fertige Skripte anbieten (z.B. Aktualisierung Metadaten, Authentifzierungsskripte, JAAS-Modul, ...)
- Alle:
  - Lösungen für weiteres großes Problem im Bereich verlagsgehostete Anwendungen:

    NUTZUNGSSTATISTIK