
Authentifizierung, Autorisierung
und Rechteverwaltung

# Das Projekt AAR

## Integration von Informationsdiensten in einem föderativen System

*Frühjahrssitzung des ZKI vd-ak*

*Oldenburg, 8. Mai 2005*

Bernd Oberknapp, UB Freiburg
E-Mail: bo@ub.uni-freiburg.de

# Übersicht

- Das Projekt AAR
- Warum AAR?
- Was sind AAR und Shibboleth?
- Wie funktioniert Shibboleth?
- Warum Shibboleth?
- Attribute
- Identity-Provider
- Service-Provider
- Ausblick

# Das Projekt AAR

- Partner: **UB Freiburg** und **UB Regensburg**
- finanziert durch das **BMBF** (PT-NMB+F)
- eingebettet in **vascoda** (http://www.vascoda.de/)
- Laufzeit **3 Jahre** bis Ende 2007:
  - 2 Jahre Entwicklungs- und Testphase mit der Regionalen Datenbank-Information Baden-Württemberg (**ReDI**) **und vascoda als Pilotanwendungen**
  - 1 Jahr Unterstützung von Einrichtungen und Anbietern bei der Einführung des Systems

# Warum AAR?

- **Bibliotheken** kaufen Nutzungslizenzen für vielfältige elektronische **Informationsangebote**: Zeitschriften, Datenbanken, Bücher, ...
- Der **Zugang** zu den Informationsangeboten ist heute zum Teil nur **eingeschränkt** möglich (IP-Kontrolle, VPN, Proxies).
- Die Einbindung der Informationsangebote in das Angebot der Bibliotheken und ihre **Verknüpfung** (Stichwort: Reference Linking) ist teilweise sehr **aufwendig**.

# Warum AAR?

Ziel ist die **Verbesserung und Vereinfachung des Zugangs** zu den Informationsangeboten:

- **Nutzer**: Zugriff auf lizenzierte Inhalte **unabhängig vom gewählten Arbeitsplatz und dem Zugriffsweg**, Zugriff auf alle Angebote nach nur einmaliger Authentifizierung und Autorisierung (**Single Sign-on**)
- **Einrichtungen**: freie Wahl des Authentifizierungssystems, möglichst geringer Aufwand für die Rechteverwaltung
- **Anbieter**: Schutz der Inhalte vor unberechtigtem Zugriff, einfacheres Angebot von personalisierten Diensten

# Was ist AAR?

- **AAR** ist eine **Infrastruktur** zur Authentifizierung, Autorisierung und Rechteverwaltung.
- **AAR** ist ein **Single Sign-on System**, mit dem verschiedene Ressourcen mit einem einzigen Login genutzt werden können.
- **AAR** basiert auf einem **föderativen Ansatz**: Die Einrichtung verwaltet und authentifiziert ihre Mitglieder und der Anbieter kontrolliert den Zugang zu seinen Ressourcen.
- **AAR** baut auf **Shibboleth** auf.


# Was ist Shibboleth?

- **Shibboleth** ist ein **Internet2/MACE**-Projekt
  (MACE = Middleware Architecture Committee for Education)
- Shibboleth entwickelt eine
  - **Architektur** (Protokolle und Profile),
  - **Richtlinien-Strukturen** und eine
  - **Open Source-Implementierung**

  für den einrichtungsübergreifenden Zugriff auf geschützte (Web-)Ressourcen

# Woher kommt „Shibboleth“?

Hintergrund ist eine Stelle aus dem **Alten Testament, Buch Richter, Kapitel 12**, Vers 5ff:

> Und die Gileaditer nahmen ein die Furt des Jordans vor Ephraim. Wenn nun sprachen die Flüchtigen Ephraims: Laß mich hinübergehen, so sprachen die Männer von Gilead zu ihm: Bist du ein Ephraiter? Wenn er dann antwortete: Nein, so hießen sie ihn sprechen: **Schiboleth**, so sprach er: **Siboleth**, und konnte es nicht recht reden. So griffen sie ihn und schlugen ihn an der Furt des Jordans, daß zu der Zeit von Ephraim fielen zweiundvierzigtausend.
>
> (Zitat http://www.spiritproject.de/orakel/magie/lyrik/bibel/richter.htm)

Das Wort „Shibboleth“ war somit wohl das erste **biometrische Autorisierungsverfahren**!

# Wie funktioniert Shibboleth?

Benutzerin

(1)

Benutzerin authentifiziert?

(2)

nein

ja

(3)

Lokalisierungsdienst (WAYF)

(4)

(5)

(6)

Benutzerin berechtigt?

Heimateinrichtung (Identity-Provider)

(7)

(8)

(9)

ja

gestattet

verweigert

nein

Zugriff

Anbieter (Service-Provider)


# Warum Shibboleth?

- **einrichtungsübergreifendes Single Sign-On**
- Autorisierung und Zugriffskontrolle über **Attribute** mit der Möglichkeit zur **anonymen/pseudonymen Nutzung** von Angeboten
- basiert auf **bewährter Software und Standards** (SAML: XML, SOAP, TLS, XMLsig, XMLenc)
- **Aufwand für Integration** mit vorhandenem IdM und (webbasierten) Anwendungen in vielen Fällen **vergleichsweise gering**
- **Weltweit hohe Akzeptanz**, auch bei kommerziellen Anbietern (Elsevier, JSTOR, EBSCO, Ovid, Springer, ...)

# Anwendungsmöglichkeiten

- Zugang zu geschützten (kommerziellen) elektronischen Informationsangeboten:
  - Zeitschriften, Datenbanken, Bücher, ...
  - Portale (z.B. vascoda, ReDI)
  - DFG-Nationallizenzen
  - Repositories (z.B. MyCoRe)
- e-Learning
- e-Science
- Verwaltungssysteme
- Grid-Computing

# Attribute und Shibboleth

- Attribute bilden die **Grundlage für Autorisierung und Zugriffskontrolle** in Shibboleth:
  - Identity-Provider stellen die notwendigen Attribute für ihre Benutzer zur Verfügung.
  - Service-Provider werten die Attribute anhand ihrer Regeln aus und gestatten oder verweigern je nach Ergebnis den Zugriff.
- Hierfür sind **Absprachen zwischen Identity- und Service-Providern** notwendig, die durch Verwendung eines einheitlichen Schemas vereinfacht werden!


# Der „Shibboleth-Standard“

- **InCommon** hat mit eduPerson den Standard für den Austausch von Attributen vorgegeben: http://www.incommonfederation.org/docs/policies/federatedattributes.html
- **Internationale Anbieter** orientieren sich üblicherweise an diesem Standard.
- Die **meisten Service-Provider** kommen dabei mit einigen **wenigen Attributen** aus, typischerweise mit eduPersonScopedAffiliation, **eduPersonEntitlement**, eduPersonTargetedID oder eduPersonPrincipalName

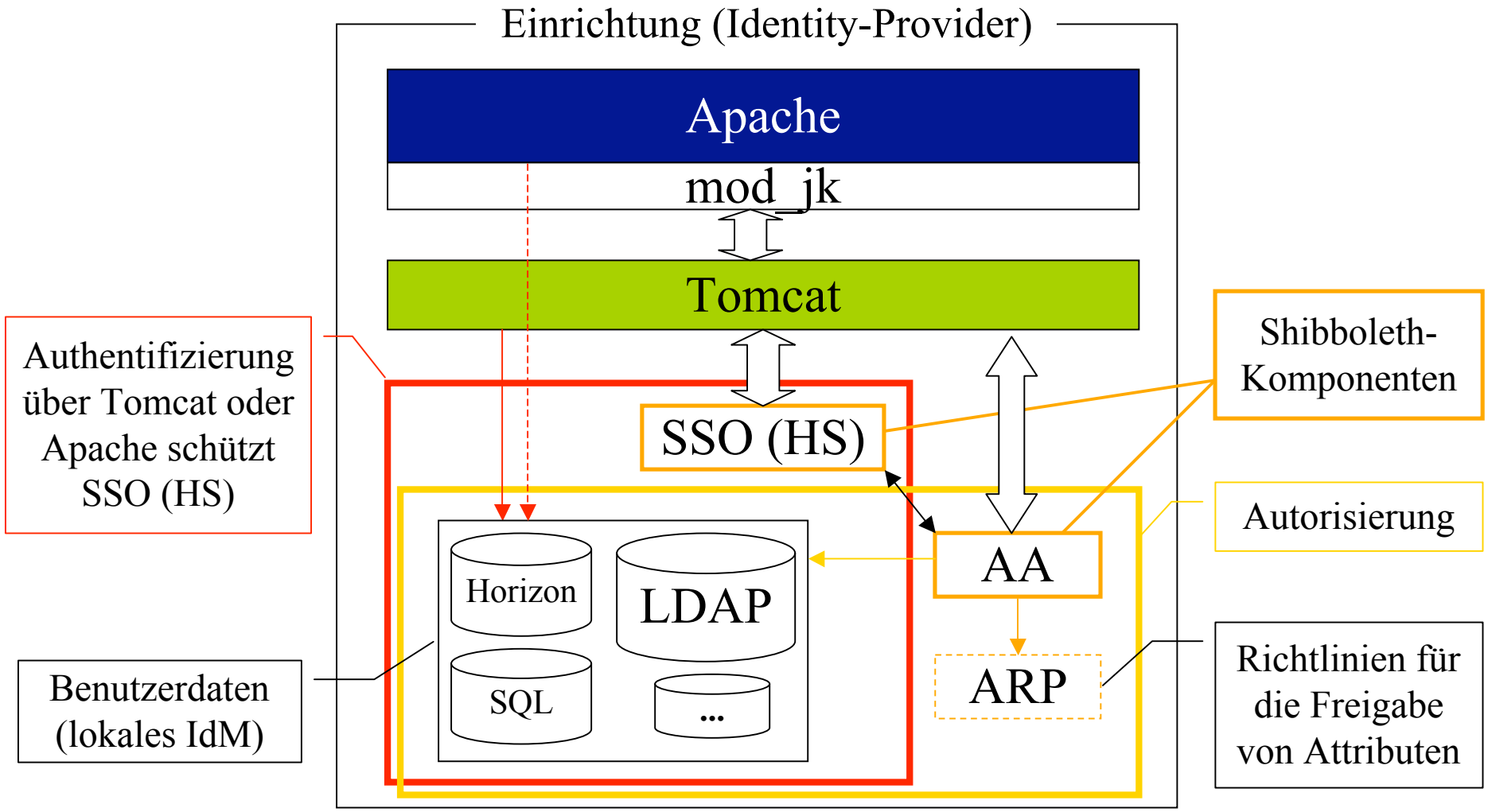

# Attribute und Datenschutz

- Attribute können **personenbezogene Daten** sein (Beispiele: Benutzerkennung, E-Mailadresse).
- Bei Verwendung personenbezogener Daten sind die (EU-) **Datenschutzbestimmungen** zu beachten!
- Personenbezogene Daten dürfen nur dann weitergegeben werden, wenn dies
  - für die Erbringung des Dienstes **notwendig** ist und
  - der **Benutzer** der Weitergabe **ausdrücklich zustimmt**.
- Die Weitergabe der Attribute wird über **Attribute Release Policies** (ARPs) gesteuert (dreistufig auf Einrichtungs-, Gruppen- und Benutzerebene)


# Attribute Release Policies

- MAMS (Meta-Access Management System, Australien) hat Werkzeuge für die **Verwaltung der ARPs** entwickelt (siehe http://tinyurl.com/dzhfk):
  - **ShARPE** (Shibboleth Attribute Release Policy Editor, Administrationsschnittstelle) und
  - **Autograph** (Benutzerschnittstelle)
- Die Attribute, die an einen Service-Provider weitergegeben werden, werden den Benutzern in Form von **Visitenkarten** präsentiert.
- Die Benutzer können für jeden Service-Provider **sehr intuitiv** individuelle Visitenkarten erstellen.

# Identity-Provider (IdP 1.3)



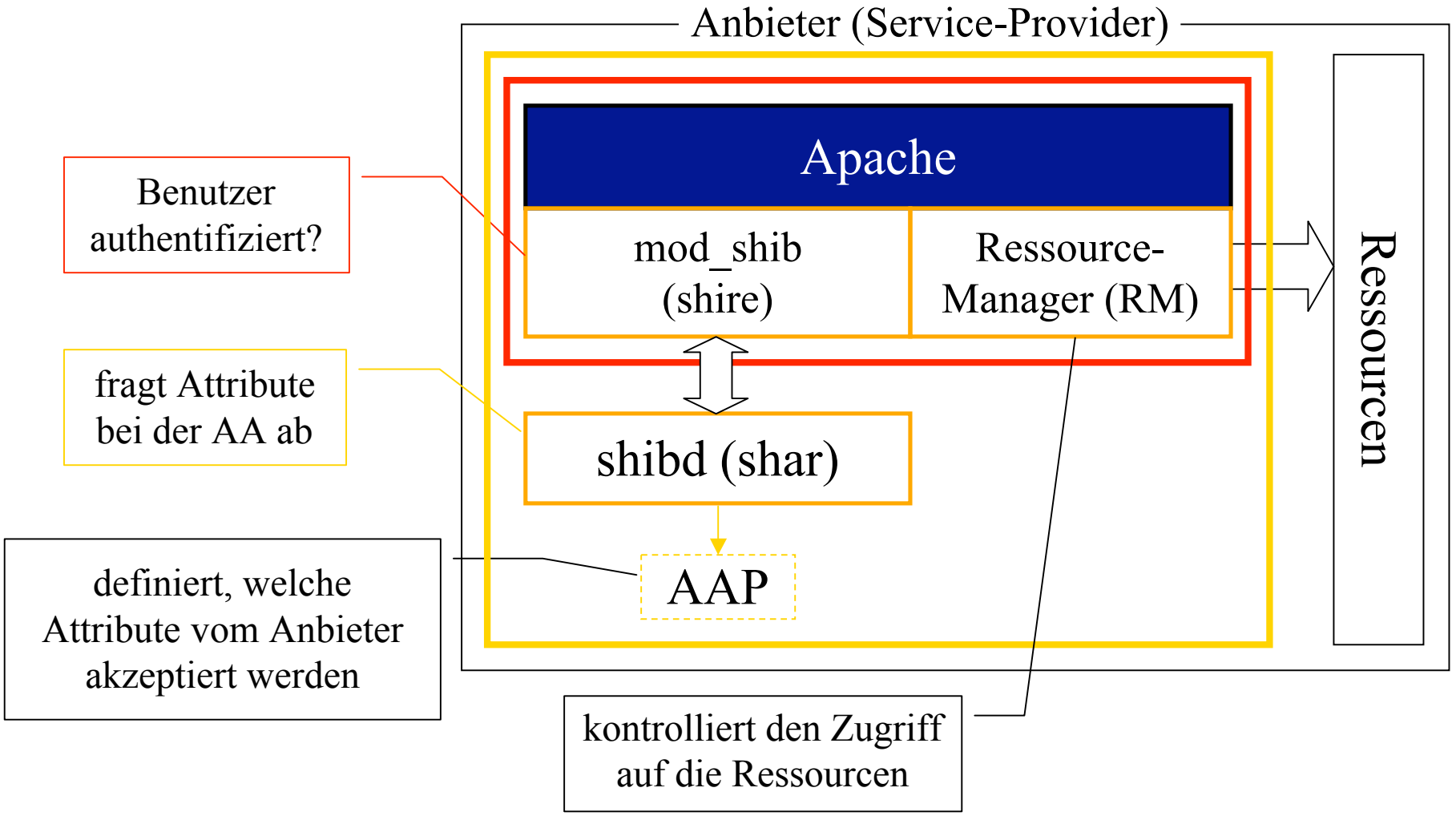

# Arbeitsschwerpunkte IdP

- **Integration des IdP mit lokalem IdM**:
  - Authentifizierung: LDAP, SQL, diverse Bibliothekssysteme und ReDI (JAAS)
  - Autorisierung: LDAP, SQL, eigene Resolver
- **IdPs für mehr als 50 ReDI-Teilnehmer**:
  - zunächst zentral installiert
  - Übernahme in lokalen Betrieb zum Teil bereits in Arbeit (Heidelberg, Konstanz, Stuttgart, Hohenheim, BSZ)
- Virtual Home Organization (VHO)
- **Beratung und technische Unterstützung** von Hochschulen, Bibliotheksverbünden, ...


# Beispiel: IdP der Uni Freiburg

- **Tomcat-Authentifizierung** mit Anbindung an drei Benutzerdatenbanken über **eigenen JAAS-Realm**:
  - LDAP-Server des Rechenzentrums
  - Ausleihsystem der Bibliothek
  - LDAP-Server des Klinikums
- **Autorisierung** über Attribute aus dem **LDAP-Server** und einer **eigenen Rechtedatenbank** (SQL)
- Lösung für **Problemfälle** wie Walk-in Benutzer in der Bibliothek: Mapping von IP-Adressen auf Pseudo-Accounts oder Login über Ausleihsystem?
- **Single Sign-on als eigener Dienst**!

# Service-Provider (SP)



# Arbeitsschwerpunkte SP

- **Anwendungen Shibboleth fähig machen**:
  - ReDI (Hauptentwicklung: integrierter WAYF)
  - vascoda (IPS-Portalsoftware): bis Herbst 2006 Testumgebung mit Hochschulbibliothekszentrum Köln und Informationszentrum Sozialwissenschaften aufbauen
  - Bibliotheksanwendungen (z.B. Standortkatalog)
  - Systemanwendungen (z.B. Nagios und Backup)
  - interne Webseiten der UB Freiburg, ...
- weitere (kommerzielle) **Anbieter überzeugen**
- **Beratung und technische Unterstützung** von Einrichtungen und (kommerziellen) Anbietern


# „Migrationscheckliste“

- Wie werden die **Ressourcen** bisher **geschützt** (Apache, Tomcat, eigenes Verfahren, ...)?
- Existiert ein **Sitzungsmanagement**?
- Kann dieses weiter verwendet werden, z.B. indem eine Sitzung über Shibboleth aufgebaut wird?
- Existiert eine **Rechteverwaltung**?
- Können die dafür notwendigen Informationen per Shibboleth über **Attribute bereitgestellt** werden?
- **Können die Identity-Provider die notwendigen Attribute liefern**?


# Ausblick: Shibboleth 2.x

- Zeitrahmen für Shibboleth 2.0: Sommer 2006
- erweiterte **Authentifizierungsfunktionalität**
- Integration von **ShARPE** und **Autograph**
- **Single Logout**
- Verbessertes IdP Discovery-Verfahren?
- Delegation (WS Federation?)
- Einbindung nicht webbasierter Dienste

(siehe Shibboleth Roadmap)


# Ausblick: Föderation

- Eine **Föderation** ist ein Zusammenschluss von Einrichtungen und (auch kommerziellen) Anbietern auf Basis **gemeinsamer Richtlinien**.
- Eine Föderation schafft das für Shibboleth notwendige **Vertrauensverhältnis** zwischen Einrichtungen und Anbietern und einen **organisatorischen Rahmen** für den Austausch von Benutzerinformationen.
- Unter Koordination des DFN wird eine **deutschlandweite Föderation** aufgebaut (DFN-AAI).

# Weitere Informationen

- AAR-Webseite: http://aar.vascoda.de/
- AAR-Team: info@aar.vascoda.de
- Nächster AAR-Workshop:
  10. Oktober 2006 in Freiburg

**Vielen Dank für Ihre Aufmerksamkeit!**