Konzept zum Shibboleth-Einsatz für E-Learning in Bayern

4. Shibboleth-Workshop, Berlin

28. Februar 2007

Wolfgang Hommel, Leibniz-Rechenzentrum

Agenda

- Überblick über das Vorhaben
  - Virtuelle Hochschule Bayern (vhb)
  - Bisherige Lösungsansätze
  - Projektziele
  - Herausforderungen

- Datenschutz mit Shibboleth
  - Attribute Release Policies
  - Verwendung von XACML als Policysprache

Erweiterte Zielsetzung

- AAI wörtlich genommen:
  - Authentifizierung: *„Benutzer wurde authentifiziert“*
  - Autorisierung: *„Benutzer darf Dienst nutzen“*
- Benutzerprofile, z.B. für E-Learning:

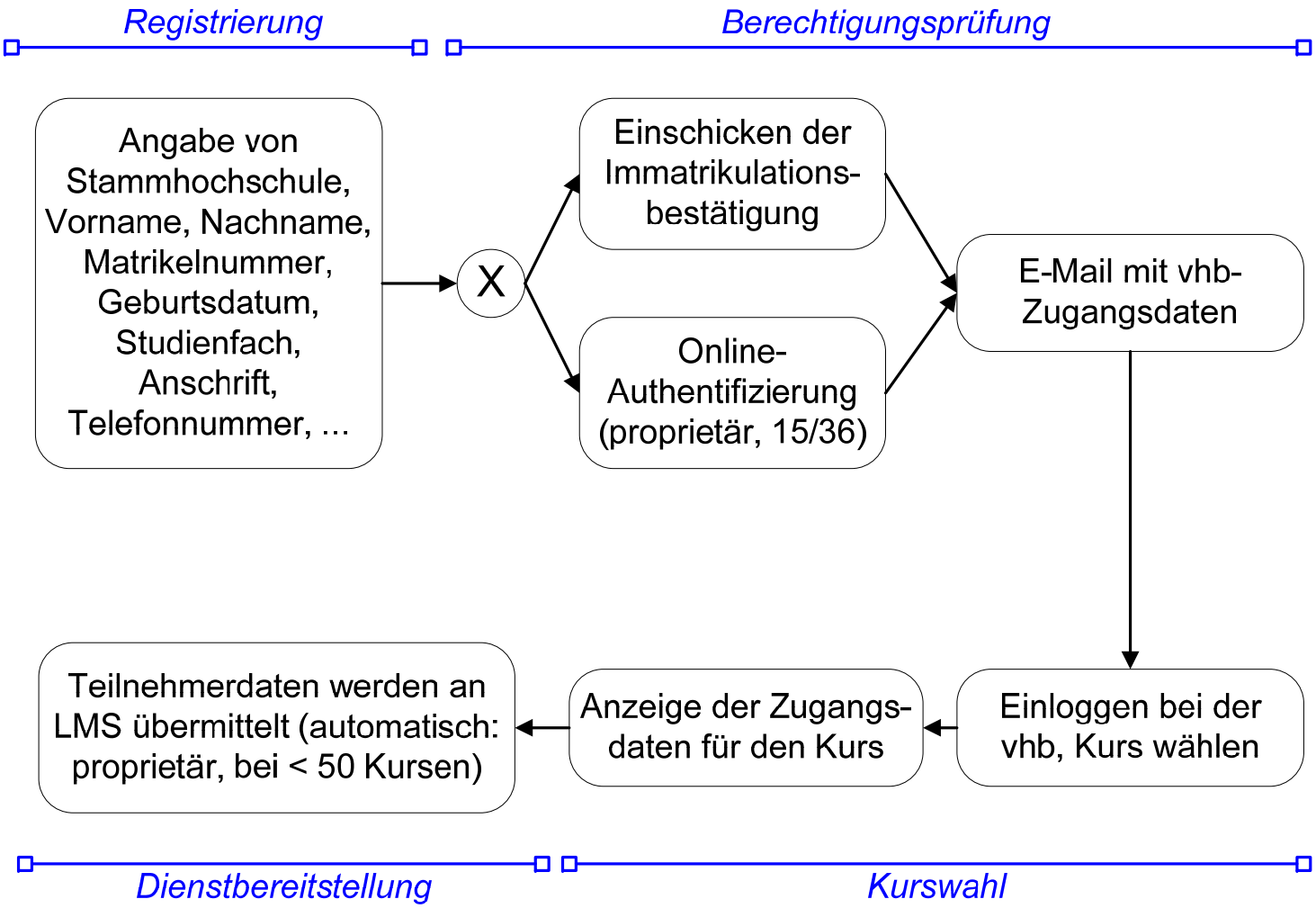
  - *„Herr Max Mustermann, geboren am 28.02.1987, hat die Matrikelnummer 1234567 und studiert im 3. Semester Maschinenbau (Master).“*

Virtuelle Hochschule Bayern (vhb)

- Verbund von 36 Trägerhochschulen
- Mehr als 300 Kurse, 15.000 Studenten und 40.000 Kursbelegungen pro Jahr
- vhb als Vermittler: Learning Management Systeme (LMS) dezentral betrieben

Bildquelle: vhb

Bisheriger Ablauf

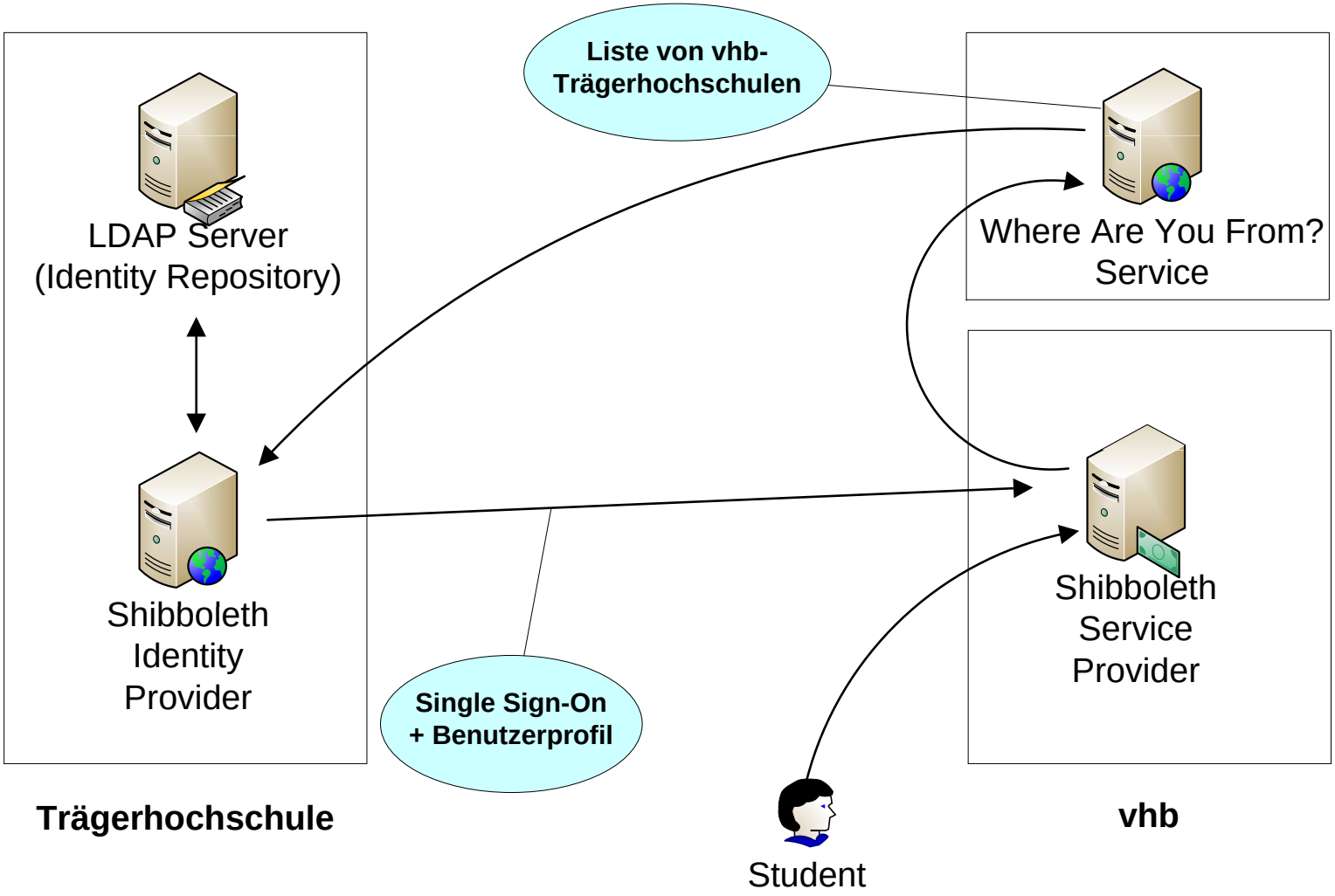


Resultat: Verschiedene Benutzernamen/Passworte bei der Heimathochschule, vhb und pro Kurs

Motivation für den Shibboleth-Einsatz

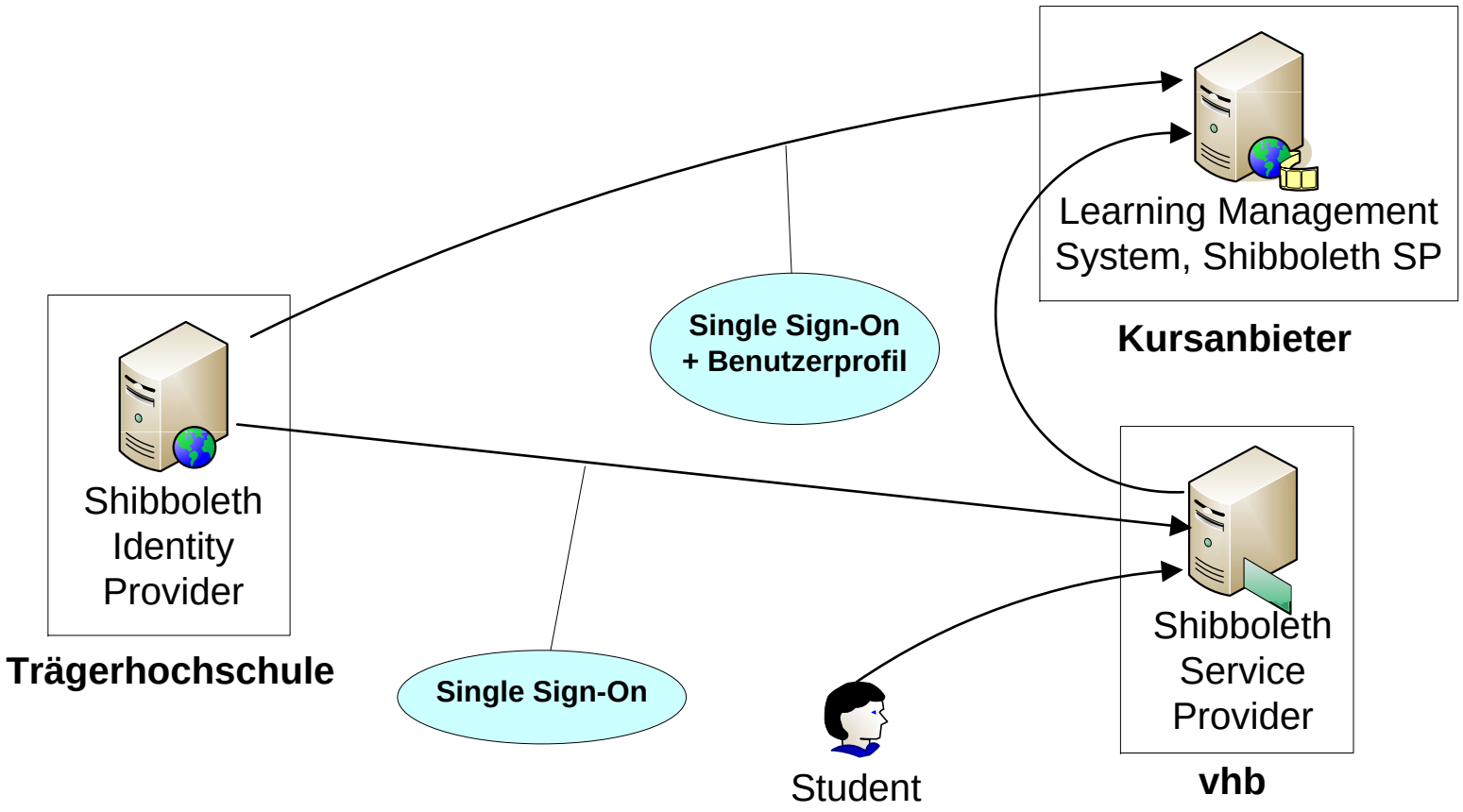
- Einheitliches technisches Verfahren für möglichst viele Dienste:
  - Erspart initialen Mehraufwand
  - Nachhaltigkeit und effizienter Dauerbetrieb
- De-facto Standard:
  Argument für Schnittstellenimplementierung durch Hersteller von Learning Mgmt. Systemen
- Frühere Shibboleth-Projekte und Testumgebungen vielversprechend

Projektziel 1/3



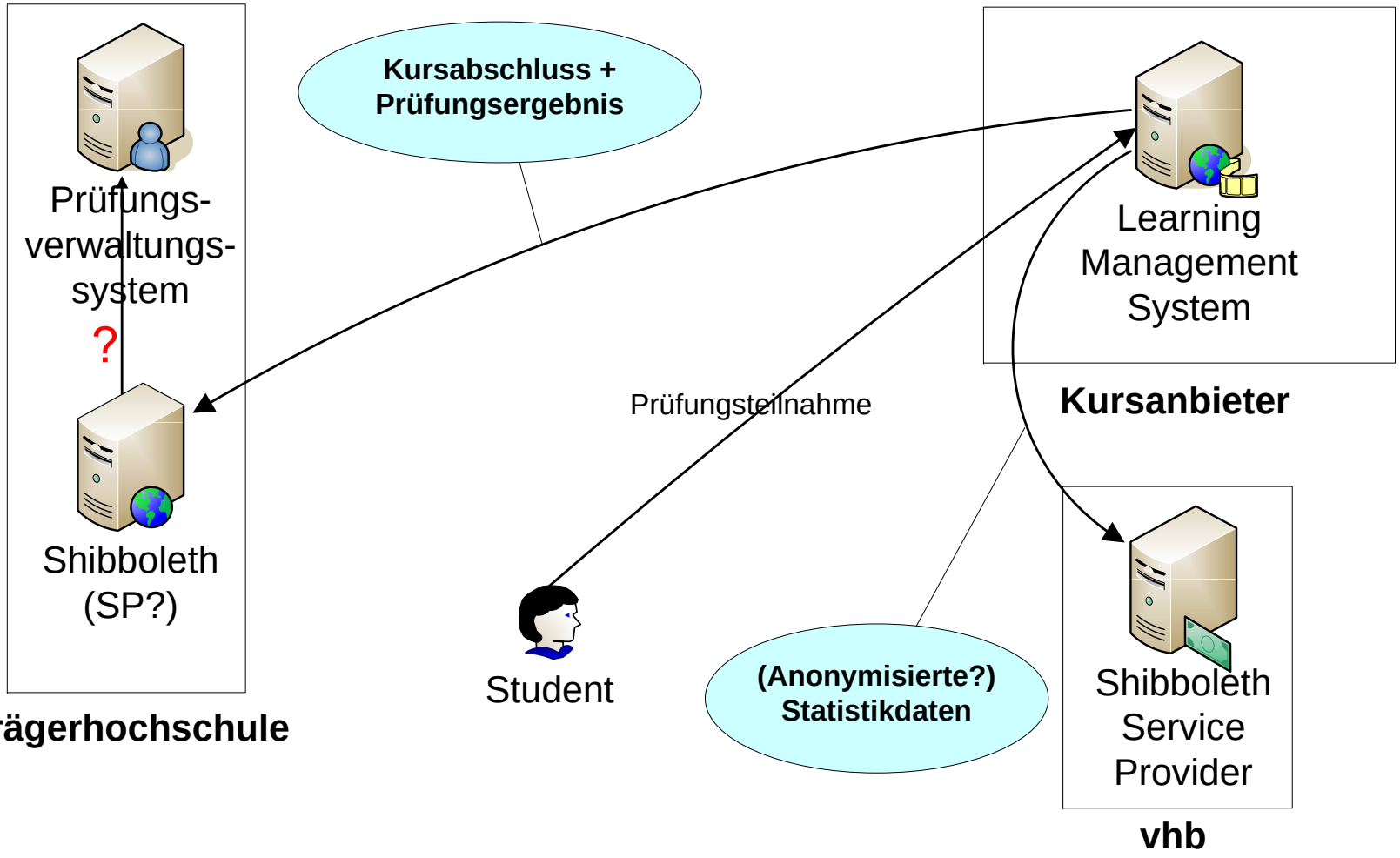
Shibboleth-basierte Übermittlung von Benutzerdaten an die vhb

Projektziel 2/3



Shibboleth-basierte Nutzung dezentraler E-Learning Systeme

Projektziel 3/3



Übermittlung von Leistungsnachweisen an die Heimathochschulen

Föderationskontext

- Aufwand für eigene vhb-AAI schreckt ab
- Nutzung der DFN-AAI sehr reizvoll
- Aber:
  - Europaweite, shibboleth-basierte Kommunikation schon jetzt benötigt
  - Voraussetzungen für bi-/multilaterale Hochschulkooperationen schaffen (z.B. gemeinsame Studiengänge)

Datenmodell

- DFN-AAI Schema (v0.8) als Ausgangsbasis
- Diverse für LMS-Zwecke fehlende Attribute:
  - Geburtsdatum
  - Geschlecht
  - Semester-Rückmeldestatus
  - Studienfächer / angestrebter Abschluss
  - ...
- Aussagen zur Erweiterbarkeit?

Datenschutz

- Essentiell aufgrund der Übertragung personenbezogener Daten
- DFN-AAI Vorlagen für Shibboleth Attribute Release Policies wären hilfreich
- Im konkreten Fall: Shibboleth-basierte Umsetzung bereits bestehender Prozesse

Vor-/Nachteile von Shibboleth ARPs

Angabe, welches Attribut an welchen Dienst (providerId) herausgegeben wird

Keine Zweckbindung

Keine Gruppierung von Attributen

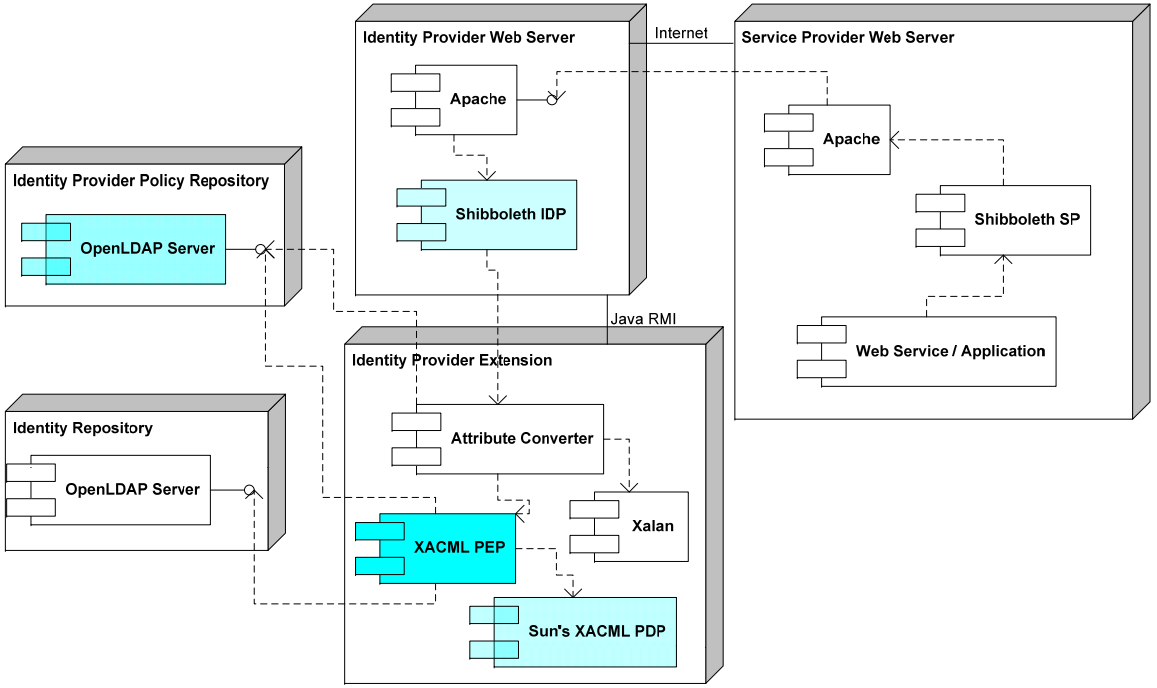
Als Bedingungen nur Zeichenkettenvergleich

Keine Benachrichtigungen / Protokolle

→ Motivation für umfassendere Policysprache

Shibboleth-ARPs mit XACML

- Diplomarbeit Matthias Ebert, 12/2006
  `https://spaces.internet2.edu/display/SHIB/ShibXACML`
- eXtensible Access Control Markup Language (XACML 2.0, OASIS-Standard)



Details: XACML für Shibboleth ARPs

- Hierarchische, prioritätsgesteuerte ARPs (→ mehr als eine Site ARP)
- Optionale Unterscheidung von Zugriffsarten und –zwecken
- Gruppen von Attributen und Benutzern
- XACML-Funktionen in Bedingungen
- Protokolldateien, E-Mail-Versand

Vor- und Nachteile von XACML ARPs

Beheben die genannten Defizite

Mangel an Frontends zum Editieren der ARPs

Support und nachhaltiger Betrieb noch unklar

Aber:

Demonstriert die Machbarkeit eigener Shibboleth-Modifikationen

Zusammenfassung

- Geplanter Shibboleth-Einsatz im vhb-Kontext
  - Ablösung des bisherigen Verfahrens
  - Shibboleth als de-facto Standard naheliegend
  - Nahtlose Integration in DFN-AAI angestrebt
- Herausforderungen
  - Schwerpunkt: Übertragung von Benutzerprofilen
  - Schema, Datenschutz und ARPs
  - Organisation, Schnittstellen zur Prüfungsverwaltung