Standard-Attribute für Shibboleth, Status ausgewählter Anbieter

MPG-AAI Workshop

Stuttgart, 26. Juli 2007

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

Teil 1: Standard-Attribute für Shibboleth

Attribute und Shibboleth

- Attribute bilden die Grundlage für Autorisierung und Zugriffskontrolle in Shibboleth:
  - Identity-Provider stellen die notwendigen Informationen über ihre Nutzer in Form von Attributen zur Verfügung.
  - Service-Provider werten die Attribute anhand ihrer Regeln aus und gestatten oder verweigern je nach Ergebnis den Zugriff.
- Hierfür sind Absprachen zwischen den Identity- und Service-Providern notwendig, die durch Verwendung eines einheitlichen Vokabulars, d.h. Schemata, vereinfacht werden!

eduPerson-Schema

- Schemata legen eine Menge von Attributen, die zulässigen Werte und deren Bedeutung fest.
- Die für Shibboleth verwendeten Schemata basieren üblicherweise auf **eduPerson**:
  - eduPerson (InCommon)
  - swissEduPerson (SWITCH)
  - funetEduPerson (HAKA)
- InCommon hat den auf eduPerson basierenden Standard für den Austausch von Attributen gesetzt: http://www.incommonfederation.org/ docs/policies/fed

Attribute in der DFN-AAI

- Die Anforderungen an die Attribute in der DFN-AAI basieren auch auf eduPerson (sowie inetOrgPerson, organizationalPerson und person).
- Die Liste der Attribute kann bei Bedarf erweitert werden, als Grundlage dafür kämen z.B. SCHAC (für den Datenaustausch auf europäischer Ebene) und ggf. hisPerson (innerhalb Deutschlands) in Frage.
- Nur wenige Attribute sind obligatorisch, und viele Anwendungen – insbesondere im Bibliotheksbereich – kommen mit ganz wenigen Attributen aus!

eduPersonScopedAffiliation

- Ermöglicht die Zuordnung der Nutzer einer Einrichtung zu einigen grundlegenden Rollen.
- Zulässige Werte sind: **member**, **faculty**, **staff**, **employee**, **student**, **alum** und **affiliate**.
- Beispiel: **member@uni-freiburg.de**
- Erste Implementierungen kommerzieller Anbieter basierten auf diesem Attribut.
- Probleme:
  - Die Bedeutung der Werte ist auf internationaler Ebene nicht wirklich einheitlich festgelegt (z.B.: Was ist ein student?).
  - Es fehlen wichtige Rollen wie „Walk-in Patron“.

eduPersonEntitlement

- Ermöglicht den Austausch praktisch beliebiger Rechteinformationen.
- Zulässige Werte: URIs, d.h. URNs oder URLs, wobei momentan meistens URNs verwendet werden.
- Die Bedeutung der Entitlement-Werte muss zwischen Identity- und Service-Providern abgesprochen werden!
- Absprachen auf Föderationsebene oder sogar föderationsübergreifend sind wünschenswert!
- Problem: „eierlegende Wollmilchsau“

eduPersonEntitlement

- Wichtigster Entitlementwert im Bibliotheksbereich: urn:mace:dir:entitlement:common-lib-terms
- Bedeutung: „Nutzer ist berechtigt, die von seiner Einrichtung im Rahmen einer Standardlizenz lizenzierten Inhalte zu nutzen“ (bei Hochschulen: Mitglied der Hochschule oder Walk-in Patron).
- Die meisten (kommerziellen) Anbieter unterstützen oder erwarten sogar, dass dieser Entitlementwert in Standardfällen verwendet wird.
- Alternative für nicht Standardfälle, z.B. bei Ovid: „urn:mace:ovid.com:<Ovid-Account>”

eduPersonPrincipalName

- Eindeutiger, persistenter Identifier des Nutzers inklusive Domain („NetID“).
- Beispiel: **oberknap@uni-freiburg.de**
- Sollte aus Datenschutzgründen nur verwendet werden, wenn die Nutzung eines Dienstes nicht anonym oder pseudonym erfolgen kann!
- Beispiel: Schreibender Zugriff auf eine Anwendung, z.B. ein Wiki oder Forum, für den der Nutzer sich zu erkennen geben muss.

eduPersonTargetedID

- Eindeutiges, persistentes Pseudonym des Nutzers für einen Service-Provider.
- Ermöglicht die Wiedererkennung des Nutzers (z.B. für personalisierte Anwendungen), ohne seine Identität kennen zu müssen.
- Erschwert das Zusammenführen von Informationen über einen Nutzer seitens der Service-Provider.
- Probleme:
  - Die bei Shibboleth 1.3 mitgelieferte Implementierung ist nicht für den Produktionsbetrieb geeignet.
  - Ist inzwischen „deprecated“ und soll in Shibboleth 2.0 durch persistente Name-Identifier abgelöst werden.

Teil 2: Status ausgewählter Anbieter

Status: Produktion

- Elsevier (ScienceDirect)
  - Testanfrage aus Freiburg und Heidelberg liegt seit Ende 2006 wegen Umstrukturierungen der AAI bei Elsevier auf Eis.
- Ovid (OvidWeb und ERL/WebSPIRS)
  - Test mit Teilnehmern aus der DFN-AAI ist für Ende Sommer/ Anfang Herbst geplant, nachfolgend soll so schnell wie möglich der Produktionsbetrieb aufgenommen werden.
- GENIOS/GBI (WISO)
  - ist seit Februar mit den Hochschulen in Baden-Württemberg in Produktion (mit lokaler „ReDI-Föderation“).
  - Eine Umstellung auf die DFN-AAI ist geplant.
- JSTOR

Status: Test/Planung

- EBSCO (EBSCOhost)
  - hatte die erste Implementierung überhaupt, basierend auf eduPersonAffiliation/InQueue, momentan erfolgt eine Neuimplementierung basierend auf eduPersonEntitlement.
- CSA (CSA Illumina)
  - Test mit der Uni Freiburg sowie Kunden in Kanada ist in 2006 erfolgt, der aktuelle Status ist unklar.
- FIZ Technik
  - in Planung, die Implementierung soll nach Umstellung auf die neue Oberfläche im Herbst angegangen werden.
- Proquest? Thomson Gale?
- Andere Anbieter, die Athens unterstützen?

Status: Diskussionsphase

- Springer (MetaPress)
  - Die Entscheidung von MetaPress über eine Implementierung soll bis Ende Juli fallen.
  - Die Implementierung könnte auch eine Vielzahl anderer Anbieter nutzen, die ihre Inhalte über MetaPress anbieten!
- Thomson Scientific (ISI Web of Knowledge)
  - hat im Prinzip zugesagt, Shibboleth zu implementieren, eine Aussage zum Zeitrahmen gibt es bisher aber nicht.
- Wiley
  - hat unter starkem Druck von Kunden „Shibboleth-Klauseln“ in mehreren Verträgen zugestimmt, ob und wann tatsächlich eine Implementierung erfolgen wird, ist aber unklar.

„Shib-enabling Vendors“

- Internet2 koordiniert die meisten Aktivitäten:
  - Mailinglisten shib-enable-vendor (inklusive Anbietern) und shib-enable (nur Föderationen, Hochschulen, ...)
  - urn:mace:dir:entitlement:common-lib-terms ist ein Ergebnis der Diskussion mit den Anbietern
  - „Prioritized Vendors“-Liste
- Knowledge-Exchange (DEFF, DFG, JISC, SURF)
- Unabhängig von den international koordinierten Aktivitäten zur Überzeugung der Anbieter sollte jeder Kunde beim Abschluss von Verträgen darauf drängen, dass die Anbieter sich verpflichten, Shibboleth zu implementieren!