

Single SignOn mit Shibboleth

Andreas Jobs

6. April 2011



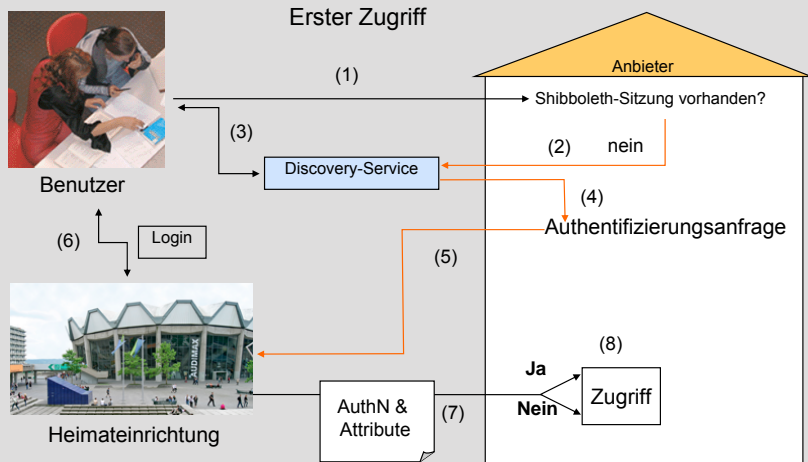
Was ist Shibboleth?

- Shibboleth ist ein einrichtungsübergreifender Single-SignOn Dienst für den Zugriff auf geschützte Web-Ressourcen
- Wird von Internet2 entwickelt
<http://shibboleth.internet2.edu>
- Basiert auf SAML (Security Assertion Markup Language)
- Ist Open-Source

Wie sieht das dann aus?

Demo

Wie funktioniert Shibboleth?



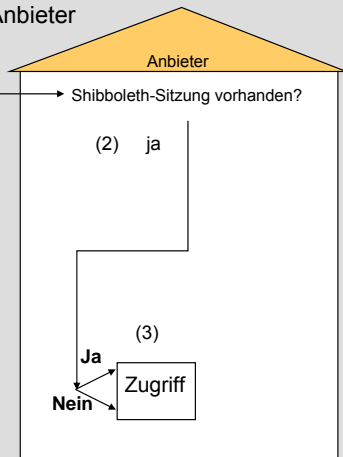
Wie funktioniert Shibboleth?



Benutzer

Zweiter Zugriff gleicher Anbieter

(1)



Anbieter

Shibboleth-Sitzung vorhanden?

(2) ja

(3)

Ja

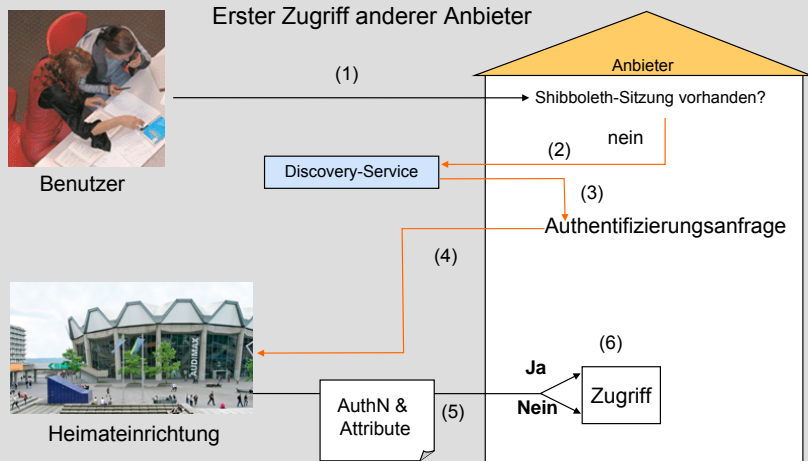
Nein

Zugriff



Heimatinstitution

Wie funktioniert Shibboleth?



Übermittelte Attribute dienen der Autorisierung. Die meisten Serviceprovider kommen mit den folgenden Attributen aus:

- eduPersonAffiliation
- eduPersonEntitlement
- eduPersonPrincipalName
- eduPersonTargetedID

- Zugehörigkeit / Rolle des Nutzers
- Mögliche Werte: member, faculty, staff, employee, student, alum, affiliate, library-walk-in

- Ermöglicht Austausch beliebiger Informationen (meist in Form von URNs)
- Wichtigster Wert im Bibliotheksumfeld:
urn:mace:dir:entitlement:common-lib-terms
- Bedeutung: Nutzer darf die in einer Standardlizenz lizenzierten Inhalte nutzen

- Eindeutige Identität des Nutzers
- an der RUB: loginID@ruhr-uni-bochum.de
- Sollte aus Datenschutzgründen nur verwendet werden, wenn der Dienst nicht anonym oder pseudonym genutzt werden kann.

- Eindeutiges Pseudonym des Nutzers
- Ermöglicht die Wiedererkennung eines Nutzers ohne seine Identität zu kennen
- Ist für jeden Serviceprovider unterschiedlich

Für (interne) Dienste können weitere Attribute ausgeliefert werden:

`email` Email Adresse

`givenName` Vorname

`surname` Nachname

`uid` LoginID

`ou` LDAP-Gruppenzugehörigkeit

Unter `https://aai.ruhr-uni-bochum.de/partner.html` befindet sich eine Liste welche Attribute welchem Serviceprovider übermittelt werden.

- Shibboleth ermöglicht den Schutz von Anwendungen mit dem Shibboleth Service Provider (SP).
- Der SP ist in C++ implementiert, aktuell ist Version 2.1.
- Folgende Webserver werden unterstützt:
 - Apache (mod_shib, shibd)
 - IIS (ISAPI-Filter, shibd)
 - weitere Webserver über FastCGI
- Die Installation kann erfolgen über:
 - Binärpakete (Debian, Red Hat, Windows, Solaris 8, MacOS X)
 - SRPMs (z.B. für openSUSE zu empfehlen)
 - Sources

- Eindeutige Kennzeichnung (entityID) des Dienstes
- SSL-Zertifikate für SSL und SAML Kommunikation
- Eine Hand voll Änderungen an der Standardkonfiguration
- Einen Eintrag im Föderationsverzeichnis

Metadatenverwaltung beim DFN







Metadaten-Verwaltung

Vertragsdaten










Um IdP's bzw SP's in die DFN-AAI-Föderation aufzunehmen ist pro Provider-Typ jeweils ein eigener Vertrag notwendig. Die Vertragsdaten werden in der [Teilnehmerliste](#) veröffentlicht. Wenden Sie sich bitte in allen vertraglichen Angelegenheiten an unsere [Hotline](#).

Typ	Nummer	Einrichtung	Kontakt	Verlässlichkeitsklasse	lokale Metadaten	
IdP	AAI85	Ruhr-Universität Bochum	Rainer Wojcieszynski, (02 34) 3 22 40 01, rainer.wojcieszynski@ruhr-uni-bochum.de	Advanced	aktiviert download	
SP	ACP127	Ruhr-Universität Bochum	Rainer Wojcieszynski, (02 34) 3 22 40 01, rainer.wojcieszynski@ruhr-uni-bochum.de			

IdP-Liste

EntityID	DFN-AAI	DFN-AAI-Basic	DFN-AAI-Test	lokale Metadaten	
https://aai.ruhr-uni-bochum.de/idp/shibboleth	 XML		 XML	 XML	  
neuen IdP anlegen					

SP-Liste

EntityID	DFN-AAI	DFN-AAI-Basic	DFN-AAI-Test	lokale Metadaten	
https://icinga.noc.ruhr-uni-bochum.de/shibboleth-sp				 XML	  
https://nagios.ruhr-uni-bochum.de/shibboleth-sp				  XML	  
neuen SP anlegen					

Vielen Dank für die Aufmerksamkeit