AAI for German higher education
The library's perspective

AAI Info-Day 2006

Bern, 21 November 2006

Bernd Oberknapp

University Library Freiburg

E-Mail: bo@ub.uni-freiburg.de

Outline

- **Project AAR:**
  - Motivation
  - Objectives
  - Why Shibboleth?
  - Use cases
  - Project plan
  - ReDI and vascoda
- **Shib-enabling providers**
- **AAI activities in Germany**
- **DFN-AAI**
- **Challenges**

Project AAR

- AAR stands for **A**uthentication, **A**uthorization and **R**ights management ("rights" in the sense of "license information", not DRM)
- AAR is run by
  - University Library Freiburg (AA*)
  - University Library Regensburg (*AR)
- Funded by the Federal Ministry of Education and Research (BMBF, PT-NMB+F)
- Infrastructure project for vascoda
- Duration: 1/2005-6/2008
- Web page: http://aar.vascoda.de/

Motivation

- Libraries are licensing more and more electronic content: e-journals, databases, e-books, …

- Integration of all this content in a "digital library" is a big challenge for the libraries

- Access to the content today is often controlled by IP authentication which
  - is insecure (open proxies)
  - severely limits the options for authn/authz, especially when private networks and proxies are involved
  - requires special solutions for off-campus access

Motivation

Solutions for off-campus access with IP authentication:

- VPN: complex technical solution, problems with software installation and configuration and firewalls

- Proxies: require a special browser configuration, problems with users in private networks that require a different proxy for internet access

- Rewriting proxies:
  - Require special links for accessing the content (in catalogs, link resolvers, portals, … – everywhere)
  - Make the integration of the content even more difficult
  - Don't scale well – imagine setting up and managing special links for 10000-20000 journals...
  - Problems with reference linking

Objectives

The objectives of the AAR project are to improve and simplify access to electronic content:

- For users: access to all content and services anywhere, anytime, in any way, with just one login (single sign-on, SSO)

- For institutions (identity providers): free choice of the identity management system and the authentication methods, easy integration with the existing infrastructure

- For publishers (service providers): secure method for protecting content, easy integration with the existing infrastructure, personalized services without user registration

Why Shibboleth?

- Inter-institutional SSO
- Federated administration
- Access control based on attributes
- Support for anonymous/pseudonymous access
- Based on well-known software (Apache, Tomcat, OpenSSL) and standards (SAML)
- Easy integration with identity management systems and (web based) applications
- Broad support both in higher education and by commercial providers (Elsevier, JSTOR, EBSCO, CSA, Ovid, GENIOS-GBI, …)

Use Cases

- Access to licensed content:
  e-journals, databases, e-books, …

- Portals: ReDI, vascoda, virtual libraries, …

- Repositories: MyCoRe, EPrints, …

- e-Learning

- Library systems

- In-house applications

- Administrative applications

Project Plan

The original AAR project plan included:

- Building a Shibboleth test environment

- Getting into production with some important applications (ReDI, vascoda)

- Convincing higher education institutions and (commercial) providers to implement Shibboleth and supporting them in doing so

- Proposing a long-term solution for using Shibboleth in German higher education

Extended Project Plan

- At the end of 2005 it became clear that we needed a federation for German higher education as soon as possible. The DFN has agreed to run that federation (DFN-AAI).

- The extended project plan now includes building the federation in cooperation with the DFN and other interested communities (grid, e-learning, administration).

- AAR has become the testbed for DFN-AAI.

Pilot Application: ReDI

- ReDI (Regionale Datenbank-Information) is the central database service for the higher education institutions in the federal state of Baden-Württemberg, it is funded by the Ministry of Science, Research and the Arts.

- ReDI offers access to more than 500 databases including about 350 windows databases and CrossFire Beilstein and Gmelin hosted on ReDI server systems in Freiburg und Stuttgart.

- ReDI is used by about 50 sites in Baden-Württemberg and an increasing number of sites from other federal states in Germany.

- ReDI is in service since 1999.

- Web page: http://www.redi-bw.de/

Shib-enabling ReDI

- ReDI already includes
  - a proprietary distributed authn/authz system
  - an authn/authz gateway for providing access to providers (similar to the AAI Portal)
- First steps in shib-enabling ReDI:
  - Adding Shibboleth authn/authz and a WAYF
  - Setting up IdPs for all sites that are using ReDI on the central servers (for a quick start)
  - Replacing the old authn/authz system with Shibboleth
- In production since April 2006
- Demo

ReDI: The Next Steps

- "Outsourcing" the IdPs:
  - Heidelberg is already in production with its own IdP
  - Other universities will follow within the next months
  - IdPs for the smaller sites in Baden-Württemberg with a Horizon library system will be hosted by the Library Service Centre (BSZ) in Konstanz

- Replacing the authn/authz gateway with Shibboleth:
  - Tests with commercial providers: CSA (pilot), GENIOS-GBI, Elsevier, Infoconnex, …
  - The "ReDI federation" is ok for testing, but for production we need the DFN-AAI!

vascoda

- vascoda is an internet portal for scientific and scholarly information (not only for higher education)
- Funded by the BMBF and the German Research Foundation (DFG)
- Lots of (commercial) providers, virtual libraries, library networks and libraries involved
- Highly complex environment with
  - a central portal (http://vascoda.de/) and virtual library portals
  - commercial content providers
  - metasearch and search engine technology
  - access to free and licensed content, including nationally licensed content (for everybody with residence in Germany)
  - at least two VHOs

Shib-enabling vascoda

- vascoda is a "killer application":
  - Lots of institutions involved
  - Everybody interested in scientific and scholary information is a potential customer, including all higher education institutions
  - There's a lot of potential for improvements by using Shibboleth
- The IPS portal software used for the central portal is already shib-enabled
- Test environment with the central portal (hbz Cologne), at least two content providers (IZ Soz/Infoconnex and DIPF/German Education Portal) and a VHO should be up and running by the end of March 2007
- Shibboleth will be implemented in the central portal before the vascoda relaunch in mid 2007

Shib-enabling Providers

How can the adoption rate be improved?

- International coordination of the activities (Internet2 and federations)

- Standardization of attributes (for example: urn:mace:dir:entitlement:common-lib-terms)

- Ask the providers to implement Shibboleth during (consortia) contract negotiations!

- Pilot installations with commercial providers (AAR: CSA Illumina, GENIOS-GBI – much more to come)

AAI Activities in Germany

- Lots of identity management projects – this will improve the basis for Shibboleth in many institutions
- Some activities at the institution level, including projects for introducing Shibboleth as a campus SSO solution (for example at the LMU and TU Munich)
- Only few inter-institutional projects (for example SaxIS: AAI for higher education in Saxony with an e-learning portal as pilot application)
- More and more activities by the library networks, especially by the BSZ and the GBV (the common library network of 7 federal states in Germany)
- DFN-AAI

DFN-AAI

- DFN-AAI will be the national federation for German higher education
- DFN-AAI will be run by the DFN, Germany's National Research and Education Network
- There will be a
  - service agreement for DFN members (like for internet access and other DFN services)
  - service partner agreement for (commercial) providers
- First version of the service (partner) agreements and policy documents should be available before the end of 2006
- DFN-AAI should be operational within the second quarter of 2007

Challenges

- Identity management

- IdP discovery

- Login/logout look and feel (SSO as a service)

- User control of attribute release (ArpViewer, ShARPE/Autograph)

- Walk-in Patrons, Guest access

- Adoption by publishers/service providers