SHIBBOLETH MIDDLEWARE AUTHENTICATION IN FINLAND

IGELU 2006
Stockholm
Ere Maijala & Ari Rouvari
TOPICS

• HAKA – National Identity Federation
• Shibboleth Middleware Technology
• EZproxy
• The Point
NATIONAL HAKA FEDERATION

• **Aims:**
  – More secure
  – **Easier** to use
  – Single Sign On (all services)
  – Happy people

• **HAKA federation**
  – The identity federation of Finnish universities, polytechnics and research institutions
  – Members: identity providers & service providers
MEMBERS OF HAKA

• 10 of our 20 universities
• 7 of our 29 polytechnics
• 8 using Shibboleth with Nelli
• Two using Shibboleth with ILS
• A lot of bubbling under
MAINLY USED WITH AUTHENTICATION

• Nelli portal (MetaLib)
  - Access to licensed DBs
  - Personalized services
    - My space (My Nelli)

• ILS (Voyager)
  - Requests, renewals, book bag …

• eLearning environments
  – (local systems)
Challenges of Authorization

- Full texts
- Access by IP address
- Proxies (välivouhkat)
- Shibboleth not there yet
  - Too difficult in practice
  - Pilot project with Elsevier ScienceDirect
Shibboleth Technology – Identity Providers

• Each institution has own Identity Provider (IdP)
• Setup is a local responsibility
• HAKA federation offers help and guidelines
  – Rules for user account management such as retention period
  – Logout implemented with a custom solution
• Different platforms and configurations in each institution
Shibboleth Technology – Service Provider

- **Nelli is a single Service Provider (SP)**
  - Only one Shibboleth application
  - Separate directories and session initiators for all IdP’s
  - A script to limit access per institution
  - No Shibboleth configuration changes needed when a new member joins

- **When IdP is up and running, implementing Shibboleth in MetaLib very easy**
  - Libraries don’t need to do anything but test it

- **Shibboleth WAYF is bypassed**
  - MetaLib UI instance dictates institution
  - No cross-domain logins at the moment
EZproxy Solution

• **EZproxy used in authorization**
  - Plain Shibboleth is not ready yet
    • Login at vendor’s site too complicated

• **Locally administered**

• **Authorization can be done**
  - Directly with Shibboleth
  - With a custom solution
  - Via our PDS/MetaLib authentication adapter
    • PDS provides single sign-on support for non-Shibboleth institutions too (=happy people)

• **Two libraries are using EZproxy with PDS**
The Point

• Customer-oriented services
  – Single Sign-on
  – One login is enough
  – Happy users

• Based on decision by IT directors

• Standard, unified system

• Easy to implement for the libraries

• Modern

• Wider acceptance expected
  – Discounts automatically when buying train tickets

• Not easy to pronounce correctly
It’s so easy to make people happy!