Federated Identity Management and Shibboleth

Noreen Hogan
Asst. Director Enterprise Admin. Applications
Federated Identity Management

- Management of digital identity/credentials (username/password)
- Access management policies and procedures
- Authentication/SSO
- Scaled to provide interactions between an association of organizations
InCommon Federation

- Higher Ed Federation (200+ HE members)
  - Common attributes, practices, policies for information exchange
  - UO joined in February 2010
- Identity Providers, Service Providers
- Participant Operating Practices (POP)
  - Documents your organizations IdM practices
- Identity Assurance Program
  - Bronze and Silver Identity Assurance Profiles
Standards & Recommendations

• Security Assertion Markup Language (SAML)
  – XML based open standard for communicating authentication, entitlement, and attribute information.

• Eduperson Object Class
  – Common attribute definitions

• Discovery Service
  – To select your Identity Provider for service access

• uApprove
  – Allows user to view and approve release of attribute data (developed by SWITCHaii)
Current Federated UO IdM

• Duck ID based access to
  – EDUCAUSE
  – Internet2 wiki
  – Qualtrix

• Service Providers on campus that are allowing federated access to UO resources?
  – Wireless access PSU, OSU, UO
    • Not taking advantage of InCommon federation, but a type of federated access
Shibboleth

- Standards based, open source federated single sign-on and attribute exchange software developed by Internet2
  - Uses SAML V2.0
  - Web single sign-on
  - Attribute delivery for authorization decisions and/or application customization
  - Recommended and supported by InCommon
Shibboleth Advantages

• **SSO functionality**
  – No need to manage usernames and passwords locally
  – Things to be aware of
    – Session management
    – No central logout, must close browser

• **Attribute delivery**
  • Don’t need to store or manage data locally
  • Common attribute definitions
Shibboleth Components

• Service Provider (SP)
  – Managed by application owner
  – Daemon and loadable module for web server
  – Apache, IIS, iPlanet, FastCGI

• Identity Provider (IdP)
  – Managed by IS
  - Leverages Identity Management System
  – Provides authentication, attribute data
• Shibboleth Demos
  – [http://switch.ch/aai/demo/2/simple.html](http://switch.ch/aai/demo/2/simple.html)
  – [http://switch.ch/aai/demo/2/medium.html](http://switch.ch/aai/demo/2/medium.html)
  – [http://switch.ch/aai/demo/2/expert.html](http://switch.ch/aai/demo/2/expert.html)
Getting Started with Shibboleth

1. Install Service Provider software
2. Obtain SSL certificate for the site
3. Send request to wso-request@ithelp
4. If require attributes not included in the default set, fill out Shibboleth Attribute Request form.
5. Make sure SP Metadata is available to IdP
Campus Shib Use

- aaa.uoregon.edu
- aaablogs.uoregon.edu
- vpfa-prod.uoregon.edu
- ba.uoregon.edu
- surplus.uoregon.edu
- ir.uoregon.edu
- brp.uoregon.edu
- pcs.uoregon.edu
- Profdevel.uoregon.edu
- odt.uoregon.edu
- academicaffairs.uoregon.edu
- wiki.uoregon.edu
- safetyweb.uoregon.edu
- intlsa.uoregon.edu
- network-services.uoregon.edu
- budgetmodel.uoregon.edu
- it.uoregon.edu
- libproxy.uoregon.edu (testing)
Challenges/Moving Forward

• Persistent Identifiers
  – UO currently reassigns usernames
    • Length restrictions, currently 3 - 8 characters
    • Vanity email addresses (aliases)

• Remote vetting
  – How to prove identity?

• Levels of Assurance (LOA)

• CAS, Shib, and AD?
Other Federated IdM

• Consumer Apps/Federated IdM
  – Social IDs and Open IDs
    • Facebook, Google, Yahoo
    • Level of assurance for information from these IdPs?
    • OK for low risk services?
    • IAM Online April 13, see InCommon web site

• Work in other countries
  – Switzerland - SWITCHaai
  – UK Access Management Federation
  – SURFnet - Netherlands
  – Many others
Resources

• UO IdM site - it.uoregon.edu/idm
• Incommon
  – http://www.incommon.org
• Internet2 Middleware Initiative
  – http://www.internet2.edu/middleware/index.cfm
• EDUCAUSE IAM Working Group
• Organization for the Advancement of Structured Information Standards (OASIS)