Shibboleth: Linking campus and Grid infrastructures

Keith Hazelton: Sr. IT Architect, UW-Madison; Internet2 Middleware Architecture Committee for Education
Chicago, Dec. 7, 2006
Topics

- Identity federations defined
- Shibboleth: SAML for higher education and research
- The US higher education federation, InCommon as example
- Shibboleth, SAML, federations and the Grid community
Identity Federations

• Enroll locally...

• Authenticate locally...

• Assign attributes locally...

• Act federally
The federated identity dance partners
(courtesy of SWITCH)
Dance steps
Identity Federations

- Simplified usability for all collaborations
- Home organizations carefully manage the release of personal information
- On-line resource providers focus on the protection and authorization of use of their on-line resources.
Identity Federations

- Most widely adopted technical basis: Security Assertion Markup Language (SAML)
- Message exchanges between Identity Providers (IdPs) and Service Providers (SPs)
- Federation operations as a source of trusted metadata about IdPs and SPs (supports scalability)
The Shibboleth system is

- An Open Source implementation of the OASIS SAML standard (Internet2 project; NMI-EDIT product)
  - Interoperates with commercial implementations
  - Implements the Shibboleth profile -- extensions to SAML 1.1 specification to preserve the browser user’s privacy

- A web single-signon (SSO) system

- Attribute-Based Access Control
  - Attributes Describe the Browser User
  - Are typically used for Access Control, and to Personalize the Session
The Shibboleth system:

- Relies on pre-existing Authentication Mechanisms and Attribute Sources at the Identity Provider (IdP) site
- Is Portable to a variety of operating systems and web servers
The Shibboleth system is also

- Management of privacy
  - Site, Groups, and the User can control release of Attributes on a per-SP basis

- Framework for a variety of policy and management models
  - federations
  - bi-lateral agreements

- Extensible authentication and attribute sharing
  - two parties can define custom attributes
InCommon

A federation of higher education, by higher education, for higher education (in US)
InCommon Federation

- Created to support US Higher Education and its research and business partners
- Federation operator is an LLC operated by Internet2
- Builds on existing campus identity management and single sign-on systems
- Makes use of open industry standards (SAML) and open source federating software (Shibboleth)
InCommon Participation Requirements

- Common descriptive information
- Software Guidelines
  - http://www.incommonfederation.org/ops/softguide.html
- Transparency of Policy and Practices
  - POP (Participant Operational Practices)
- Participation Agreement
  - Minimal “bar” to enter
  - Limited Liability; No Indemnification
  - General Liability Insurance
- Modest application and annual fee
Current InCommon Participants

- Case Western Reserve University
- Cornell University
- Dartmouth
- Duke University
- Elsevier ScienceDirect
- Georgetown University
- Houston Academy of Medicine - Texas Medical Center Library
- Internet2
- Miami University
- Napster, LLC
- OCLC
- Ohio University
- OhioLink - The Ohio Library & Information Network
- Penn State
- ProtectNetwork
- Stanford University
- SUNY Buffalo
- Symplicity Corporation
- The Ohio State University
- The University of Chicago
- Turnitin
- University of Alabama at Birmingham
- University of California, Irvine
- University of California, Los Angeles
- University of California, Merced
- University of California, Office of the President
- University of California, Riverside
- University of California, San Diego
- University of Maryland, Baltimore
- University of Rochester
- University of Southern California
- University of Virginia
- University of Washington
- WebAssign
World-wide: higher education shibboleth federations operational in:

- Australia
- Belgium
- Canada
- China
- Denmark
- Finland
- France
- Germany
- Greece
- New Zealand
- Norway
- Spain
- Sweden (Nov 2006)
- Switzerland
- The Netherlands
- United Kingdom
- United States
What does Shib/SAML/fed. offer to Grid Community?

• User population scalability

• Authentication service for whole campus population (local “NetID” authN behind Shib IdP)

• e.g., SWITCH gLite Phase I shows how to use Shib to feed a short-lived credential service

• SP and IdP scalability (federation-signed metadata)
What does Shib/SAML/fed. offer to Grid Community?

- Access to campus-maintained attributes

- GridShib (Standard X.509 authN, attributes from Shib IdP)

- GT4 new AuthZ framework

- Basis for possibly multi-tier SAML exchanges between IdP and Grid resources

- Multi-tier will take us beyond SSO-centric SAML to related approaches like Liberty Alliance ID-WSF
What does Shib/SAML/fed. offer to Grid Community?

- Indirect: Support for Virtual Organization (VO)-maintained identity information (VO hosting)

- Emergence of campus middleware tools to manage

  - ad hoc populations,

  - groups / roles

  - privileges

- In a distributed administration mode
Q&A

- http://www.incommonfederation.org
- http://shibboleth.internet2.edu
- hazelton@wisc.edu