



Global Research and Education Federations with SAML and Shibboleth

Scott Cantor
cantor.2@osu.edu
Internet2/The Ohio State University

(Re)Definition

- Shibboleth Project
 - An umbrella of activities around federated authentication and access management managed by Internet2 and its international partners, still ad hoc but moving toward some formalism
- Shibboleth Specifications
 - The wire protocols and conformance requirements that define "Shibboleth Compatible", currently derived in large part from SAML 1.1 with additions supporting user-centric privacy-preserving interactions
- Shibboleth System
 - Internet2-developed open source implementation of the specification and value-added components
 - Not the only extant or planned implementation (at least 2-3 other implementations known, lots of smaller projects based on the code base)
 - <Your Consulting Opportunity Here>

Timeline

- Project formation - Feb 2000
- OpenSAML prerelease – July 2002
- Shib v1.0 April 2003
- Shib v1.2 April 2004
- Shib v1.3 June 2005 (finally SAML 1.x compatible)
- ...
- OpenSAML 2.0 – Second half of 2005
- Shib 2.0 – First half of 2006

Shibboleth Project View of Federations

- Persistent enterprise-centric trust facilitators
- Sector-based, nationally-oriented
- Federated operator handles enterprise I/A, management of centralized metadata operations
- Members of federation exchange SAML assertions bilaterally using a federated set of attributes
- Members of federation determine what to trust and for what purposes on an application level basis
- Steering group sets policy and operational direction
- Note the “discovery” of widespread internal federations

InCommon Federation

- Federation membership – US .edu and those we do business with
- Federating standards – SAML 1.1 now, SAML 2.0 soon, potentially others
- Federating software – Shibboleth 1.2 and above
- Federation operations – Internet2
- Federation data schema - eduPerson200210 or later and eduOrg200210 or later
- Federated approach to security and privacy, with policies posted by members in common formats
- Became fully operational 9/04; currently around 15 members
- Precursor federation, InQueue, has been in operation (by some definition) for several years and will feed into InCommon and possibly be shutdown; approximately 150 participants
- <http://www.incommonfederation.org/>



InCommon Members 5/10/05

Dartmouth College

Elsevier ScienceDirect

Cornell University

Georgetown University

Internet2

OCLC

OhioLink - The Ohio Library and Information Network

The Ohio State University

Penn State

SUNY Buffalo

University of California, Irvine

University of California, Los Angeles

University of California, Office of the President

University of California, San Diego

University of Chicago

University of Rochester

University of Southern California

University of Washington

InCommon Uses / Value

- Institutional users acquiring content from popular providers (Napster, etc.) and academic providers (Elsevier, JSTOR, EBSCO, Pro-Quest, etc.)
- Institutions working with outsourced service providers, e.g. grading services, scheduling systems, software sales
- Inter-institutional collaborations, including shared courses and students, research computing sharing, etc.
- Extending the range of services offered to more and more managed identities (prospectives, alumni)...
- Shared network security monitoring, interactions between students and federal applications, peering with international activities, etc.

InCommon Evolution

- Learning how to do this as we go along (it's what we do...)
- Searching for the value the federation can add to federated identity...
 - Facilitating PKI
 - Playing the /etc/hosts role until something better exists
 - Providing testbeds for IdP and SP testing
 - Supporting and prodding the software upgrade process
 - Representing the members' interests in the broader world of federated identity
 - Facilitating the introduction of new standardized/interoperable technologies into the environment

Other Federations

- US Govt establishing a federation-like entity for inter-agency activity, currently SAML 1.0-based
- Outside the US, political and social models result in different evolutionary paths.
- Europe seeing a number of national federations organizing around research networks (SWITCH, SURFnet)
- Others organizing bottom-up
- Interfederation peering starts to look like international peering
- Shib now running on at least 4 continents, penguins are stubborn but we do support Linux

A Multi-Federation World...

- Naming
- Cryptography
- Attribute Agreement
- Software choice vs. software compatibility
- Growing into a community responsive to its stakeholders but driven by its core contributors
- Discovery...

Multi-Federation IdP Discovery

- Early view...we'll run a server where the user can select and IdP and remember the choice (WAYF)
- Oops...
 - Not every IdP is usable by every SP
 - Building multi-level hierarchical WAYF is questionable, even if everybody trusted the same group to run it (DNS is hard, reinventing it seems like a bad idea)
 - Single point of failure
 - SPs want control over look and feel anyway
- Elsevier taking a lead role in designing a workable UI for their service to enable IdP selection
- Futures
 - SP-customizable discovery tools built-in to software
 - i-Names or something like them?
 - Browser plugins to manage discovery cookies?
 - All stop-gaps until an open federation aware client exists