



</update> Shib-SAML & InCommon-Federal eAuthentication: </update>

Ken Klingenstein
Director, Internet2 Middleware and Security



Topics

- The basic ingredients
 - Shibboleth and SAML
 - Federations and InCommon, a US R&E federation
 - The Federal e-Authentication Initiative
- Interactions
 - Phase 1/2 – Certifying Shib, Shaping Policy Issues, etc
 - Phase 3/4 – SAML 2.0 Profile, USperson deliverables, interederation peering
- Related activities
 - Work with Microsoft
 - International federations

- Security Access Markup Language – an OASIS standard
- SAML 1.0 current eAuth standard; SAML 1.1 widely embedded
- SAML 2.0 recently ratified by OASIS earlier this year
 - Combines much of the intellectual contributions of the Liberty Alliance with materials from the Shibboleth community – a fusion product
 - Scott Cantor of Ohio State was the technical editor
 - Adds some interesting new capabilities, eg. privacy-preservation, actively linked identities
 - Possibly a plateau product

- An **architecture**, consisting of both a payload definition (using SAML) of attributes and a set of privacy-preserving methods of exchanging such payloads.
- A **project** that has managed the development of the architecture and code
- A **code package**, running on a variety of systems, that implements the architecture.
- (Note that other code sets are under development)

Shib Timeline

- Project formation - Feb 2000
- Inception of SAML effort in OASIS – December 2000
- OpenSAML release – July 2002
- Shib v1.0 April 2003
- Shib v1.2 April 2004
- Shib v1.3 April 2005 – non web services, e-Auth certified,
- Shib v1.3.x WS-Fed compliant
- OpenSAML 2.0 – relatively soon, we hope
- Refactored Shib 2.0 – 4Q05?

Shibboleth-enriched Applications

- Via a web browser
 - Rich access to content providers, including Elsevier, OCLC, Napster, JSTOR, ArtStor, ExLibris etc...
 - Access to services such as WebAssign, Scholarsworkbench, HigherMarkets, etc.
 - Blackboard and WebCT
- Embedded in applications
 - Lionshare, Fedora
 - Globus and Grids
 - Darwin streaming video server, ArtStor Java client
 - Sympa list proc
- Still more at <http://shibboleth.internet2.edu/seas.html>
- Note that applications can obtain identity via a number of identifiers – ePPN, ePTargetedId, etc.

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 bi-laterally 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

Federations and PKI

- The rough differences are payload format (SAML vs X.509) and typical length of validity of assertion (real-time vs long-term)
- Federations use enterprise-oriented PKI heavily and make end-user PKI both more attractive and more tractable – adding privacy (secrecy), ease of verification, addition of role, etc.
- The analytic framework (evaluation methodologies for risk in applications and strength of credentials) and infrastructure developed for PKI is useful for federations.
- The same entity can offer both federation and PKI services

Shibboleth based Federations

▪ In the US

- InQueue – several hundred enterprises globally in development, testing (and a little production)
- InCommon – 12-15 institutions and partners in production service and posted operational practices
- State and system federations beginning

▪ Internationally

- Full production federations in Switzerland, Finland, United Kingdom, etc.
- “League of federations” has been established to address development and peering

InCommon federation

- Federation operations – Internet2
- Federating software – Shibboleth 1.2 and above
- 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 for about six months and will feed into InCommon; approximately 150 members
- <http://www.incommonfederation.org>



InCommon Members 4/10/05

Dartmouth College
Elsevier ScienceDirect
Cornell 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 Rochester
University of Southern California
University of Washington



InCommon Uses

- 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.
- (Shared network security monitoring, interactions between students and federal applications, peering with international activities, etc.)

InCommon pricing

▪ Goals

- Cost recovery
- Manage federation “stress points”

▪ Prices

- Application Fee: \$700 (largely enterprise I/A, db)
- Yearly Fee
 - Higher Ed participant: \$1000 per identity management system
 - Sponsored participant: \$1000
 - All participants: 20 Resourceproviderids included; additional resourceproviderids available at \$50 each per year, available in bundles of 20

InCommon Management

▪ Operational services by I2

- Member services
- Backroom (CA, WAYF service, etc.)

▪ Governance

- Steering Committee – drawn from CIO level leadership in the community - sets policies, priorities, etc.
- Project manager – Internet2

▪ Contractual and policy issues were not easy and will evolve

▪ Initially a LLC; likely to take 501(c)3 status in the long term

Trust in InCommon - initial

- Members trust the federated operators to perform its activities well
 - The operator (Internet2) posts its procedures
 - Enterprises read the procedures and decide if they want to become members
 - Contracts address operational and legal issues
- Origins and targets establish trust bilaterally in out-of-band or no-band arrangements (using shared posting of practices)
 - Origins must trust targets dispose of attributes properly
 - Targets must trust origins to provide attributes accurately
 - Risks and liabilities managed by end enterprises, in separate ways
 - Collaborative apps are generally approved within the federation
 - Higher risk apps address issues through contractual and legal means

Members trust InCommon operations

- The federation operations presents limited but real exposures in identity proofing members properly and in the metadata management
- InCommon publishes its procedures for identity proofing and its operational procedures
 - InCommon CA CP/CPS
 - Metadata management process
- Individual enterprises read the policies and decide whether to trust the federation operations and how to assign liability



FOPS 2: InCommon CA Ops

- CA_Disaster_Recovery_Procedure_ver_0.14
 - An outline of the procedures to be used if there is a disaster with the CA.
- cspguide
 - Manual of the CA software planning to use.
- InCommon_CA_Audit_Log_ver_0.31
 - Proposed details for logging related to the CA.
- Internet2_InCommon_CA_Disaster_Recovery_from_root_key_compromise_ver_0.2
 - An outline of the procedures to be used if there is a root key compromise with the CA.
- Internet2_InCommon_CA_PKI-Lite_CPS_ver_0.61
 - Draft of the PKI-Lite CPS.
- Internet2_InCommon_CA_PKI-Lite_CP_ver_0.21
 - Draft of the PKI-Lite CP.
- Internet2_InCommon_Certificate_Authority_for_the_InCommon_Federation_System_Technical_Reference_ver_0.41
 - Document describing the CA.



Members Trusting Each Other: Participant Operational Practice Statement

- Basic Campus identity management practices in a short, structured presentation
 - Identity proofing, credential delivery and repeated authn
 - Provisioning of enterprise-wide attributes, including entitlements and privileges
- Basic privacy management policies
 - Standard privacy plus
 - Received attribute management and disposal
- No audit, unclear visibility of policies

- Relatively straightforward
 - Syntax and semantics of exchanged attributes (Eduperson)
 - Set up and operation of federation
 - Selling the concept and value
- More challenging
 - Having applications make intelligent use of federated identity
 - Handling indemnification
 - Finding scalable paths for LOA components

- Key driver for e-government, operating under the auspices of GSA
- Leveraging key NIST guidelines
- Setting the standard for a variety of federated identity requirements
 - Identity proofing
 - SAML bindings
 - Credential assessment
 - Risk assessment
- Technical components driven through the InterOp Lab
- <http://www.cio.gov/eAuthentication/>

eAuthentication Key Concepts

- Approved technologies
- Credential assessment framework
- Trusted credential service providers

Federal eAuthentication federation

- Original model was to certify a few key Credential Service Providers (CSP's) to a variety of federal applications, both agency to agency and citizen to agency
- Evolving model includes a federation of federal agencies, peering with other sector-based federations
- Peering is intended to leverage other peering vehicles for trust
- Peering could also include operational components such as attribute and identifier mappings, and correlation of contractual and financial approaches

Phase 1/2 of Interaction

- Phase 1/2 work commissioned to identify issues and opportunities for interactions between higher ed and federal eAuthentication
- Deliverables include
 - Policy framework comparison submitted Oct 7
 - Technical interop of Shib demonstrated October 14
 - CAF/POP comparison submitted Jan 28
 - Next stages scope of work submitted mid-Feb

Phase 3/4 of the Interactions

- Deliverables include:
 - Recommended e-Authentication SAML 2.0 profile.
 - Recommendations concerning a USperson object class
 - Recommendations on the formation of a US Government federation
 - Draft approach to interfederation peering
- Deliverables due Sept 30, 2005

- New territory...
- Technical
 - Mapping LOA's
 - Mapping attributes
 - SAML technical issues
 - PKI technical issues
- Policy
 - What agreements need to be in place
 - Where does liability flow
 - What audit requirements will be needed

- Initial focus is on citizen-agency interactions
- Extensible architecture; likely a UML model with various bindings
- Intended for use by CSP's, either directly, via peering mappings, etc.
- Deliverables may include a small core of attributes, organizational superstructure, discussions on mechanisms for extensions, maintenance, authoritative sources, etc.
- WACOW

International federation peering

- Shibboleth-based federations in the UK, Netherlands, Finland, Switzerland, Australia, Spain, and others
- International peering meeting October 14-15 in Upper Slaughter, England
- Issues include agreeing on policy framework, comparing policies, correlating app usage to trust level, aligning privacy needs, working with multinational service providers, scaling the WAYF function
- Leading trust to Slaughter...

Upper Slaughter



Three types of issues

- **Internal federation issues**
 - Business drivers – educational, research, admin – helping each country find a reason
 - Cookbook – key issues and common touchpoints
 - Alignment with other trust services such as PKI
- **Inter-federation issues**
 - Needs for agreements
 - Authncontext, attributes
 - Needs for legal frameworks
 - Assignment of roles within federation between
 - Treaties/MOU between federations
 - Privacy
- **Union of federations issues (brand, membership, etc..)**

Immediate International Issues

- **“International WAYF” – management of the user experience**
 - List of Federations that contain IdP’s
 - Where to put multi-nationals?
 - Handling of exceptions in a consistent fashion
- **Privacy**
 - EU Privacy directives intended for attributes associated with identity
 - Rules for interior and exterior privacy may be different for EU
 - And then there’s the Swiss...

WS-Fed and Shib

- Agreements to build WS-Fed interoperability into Shib
 - Contracts signed; work to begin later this spring
 - WS-Federation + Passive Requestor Profile + Passive Requestor Interoperability Profile
- Discussions broached, by Microsoft, in building Shib interoperability into WS-Fed; no further discussions
- Devils in the details
 - Can WS-Fed-based SPs work in InCommon without having to muck up federation metadata with WS-Fed-specifics?
 - All the stuff besides WS-Fed in the WS-* stack

Next Steps

- The GUI's and the diagnostics
- Getting the applications enabled
- Building the federations
- Federation peering
- Federated network security
- Use with virtual organizations
- Federated authorization