SAML, Liberty Alliance, openLiberty, and Concordia

Eve Maler
Sun Microsystems, Inc.
www.xmlgrrl.com/blog
Federated identity means distributing **identity tasks and information** across domains

Great! I like being in control of my valuable users and their attributes!

How do I trust the relying parties that approach me? How can I better authn my users?...

Great! I can simplify my user management and authn architecture!

How valuable a service can I offer based on authn quality and transaction security?...

Great! I can authn only once (**single sign-on**) and still get to use multiple web sites!

(Am I being phished? Should I allow my attributes to be sent to and stored at these websites?...)
SAML in a verbal nutshell

• XML-based framework standardized at OASIS for:
  > Marshaling security and identity information
  > Exchanging it across domain boundaries

• Out-of-the-box profiles for:
  > Single sign-on, single logout, privacy-preserving account linking, simple arbitrary attribute exchange...

• At SAML's core: assertions about subjects
  > Authentication, attributes, entitlements
  > SAML assertions are reused in many other specs

• SAML V2.0 + business guidelines + interop certification testing = “Liberty Federation”
SAML in a pictorial nutshell

Operational modes for use in conformance testing and RFPs

- IdP
- IdP Lite
- SP
- SP Lite
- Enhanced client
- ...

Metadata to describe provider abilities and needs

Profiles combining binding, assertion, and protocol use to support defined use cases

- Web browser SSO
- Enhanced client SSO
- IdP discovery
- Single logout
- ...
- Custom

Protocols to get assertions and do identity mgmt

- Assertion request
- Authentication request
- Name ID management
- Single logout
- ...
- Custom

Assertions of authn, attribute, and entitlement information

- Authentication statement
- Attribute statement
- Authz decision statement
- Custom

Bindings onto standard communications protocols

- SOAP over HTTP
- PAOS
- HTTP redirect
- HTTP POST
- HTTP artifact
- SAML URI
- Custom
SAML, Shibboleth, and Liberty Federation Framework convergence timeline

- **Liberty “Phase 1”**
  - SAML1
  - 2002
  - Liberty bases new federation standard on emerging SAML standard

- **Liberty ID-FF 1.1,1.2**
  - SAML1.1
  - 2003
  - Liberty tracks SAML evolution; Internet2 Shibboleth bases its solutions on SAML also

- **Liberty Federation**
  - SAML2
  - 2005
  - Liberty endorses SAML2 as its identity federation solution and provides interop and conformance testing; Shibboleth is working on new SAML2-based APIs

- **Shibboleth 1.0,1.1**
  - 2004
  - Liberty contributes ID-FF to OASIS for SAML2 convergence; Shibboleth also takes part

- **Shibboleth 1.2**
  - 2004
  - Shibboleth bases its solutions on SAML also

X → y = design of X feeds into Y (with direct dependencies except in the SAML2 case)
Liberty Alliance in a verbal nutshell

• A **community** of ~150 businesses, organizations, government agencies – and now individuals
  > With a long list of .org relationships...

• Its mission since 2001:
  > Foster a ubiquitous, interoperable, privacy-respecting federated identity layer for web applications and services

• Deliverables are the result of three work streams:
  > Gathering requirements from deployers and users
  > Gathering privacy policy and global regulatory requirements
  > Developing open technology standards (and testing software for interop)

• Tackles business and technical requirements for “trust”
Liberty in a pictorial nutshell

**ID-WSF**: Identity Web Services Framework
- Focused on application-to-application interaction
- Permission-based attribute sharing and user-absent scenarios

**ID-SIS**: Identity Service Interface Specifications
- Focused on ID-based services
- Personal profile, geolocation...
- Uses WSP/WSC terminology
- Liberty Web Services = ID-WSF + ID-SIS

**IDSAFE**: Identity Strong Auth Framework
- Interoperable strong auth
- In the requirements phase

**ID-FF**: Identity Federation Framework
- Focused on human-to-application interaction
- Now converged with SAML2

**openLiberty.org**: open source for web service consumers
- Eventually other projects too

**Identity provider** (login site)

**Relying party** (web application or community)

**Advanced Client**
- Client as extension of the IdP
- Strong local authn, and local-hosted services
- More features coming soon

**Browser** (or other interface)

**User**
The Liberty People Service

• A “groups and roles” service that is agnostic as to where all the identities are managed
  > You can base ACLs and other behavior on them
  > Versus today's popular web apps, which restrict the means of building ACLs

• You are effectively creating person-to-person federations between you and others

• Useful for social and business scenarios:
  > Soccer team calendar control, business networking, access-controlled collaborative spec editing, project-specific confidential material access...
Some FOSS for SAML and Liberty

- openLiberty.org ([http://www.openliberty.org](http://www.openliberty.org))
  - The new home for Liberty-related OSS
- OpenSAML ([http://www.opensaml.org](http://www.opensaml.org)) - Apache license
  - Java/C++ libraries giving low-level access to SAML 1.x functionality
- Shibboleth ([https://spaces.internet2.edu/display/SHIB/WebHome](https://spaces.internet2.edu/display/SHIB/WebHome)) - Apache license
  - SAML 1.x IdP, SP functionality
  - Plugs in to Apache httpd, IIS, Sun/iPlanet
- OpenSSO ([http://opensso.dev.java.net](http://opensso.dev.java.net)) - CDDL license based on Mozilla Public License 1.1
  - Java-based ID-FF, SAML and ID-WSF support, “Project Lightbulb” adds PHP and Ruby
  - (OpenID support now available too)
- Lasso ([http://lasso.entrouvert.org/](http://lasso.entrouvert.org/)) - GPL or commercial license
  - C libraries offering Liberty ID-FF 1.2, ID-WSF 1.x low-level support
  - SWIGified bindings for Python, Perl, Java and PHP
- ZXID ([http://www.zxid.org](http://www.zxid.org))
  - C, Perl (SWIGified) libraries with ID-FF 1.2, SAML 2, ID-WSF 1.x, 2 low-level support
  - C executable CGI, Perl and PHP scripts for acting as an SP
  - C libraries for ID-WSF 1.x, 2.0 WSC, Java WSP libraries

Thanks to John Kemp for doing most of the data compilation!
The Concordia Program

- Umbrella initiative to drive harmonization and interop of multiple identity protocols
- Based on open discussions/events to develop use cases exploring the “seams” where heterogeneous protocols meet (or don't) in deployment
- Could result in additional specs, profiles, or services being developed at Liberty or elsewhere
- Anticipates expansion of the Liberty Interoperable program
- See the wiki for use cases and to get involved
- Let's hold an IIW session on use cases...
The Venn of identity: SAML and Liberty with a bit of context (remember Saki)

**SAML, Liberty Web Services**
- SSO, single logout; permission-based attrib sharing; user-absent use cases; optimized for “circles of trust”; interop cert program
- SAML tokens in XML msgs; enterprise security & privacy; smart clients
- Can do authn against URI-based IDs; authn-method agnostic
- Supports user control/empowerment models

**OpenID**
- Distributed authentication and simple attribute sharing around URI-based IDs; low-trust scenarios; explicitly no need for preconfigured trust
- Solutions for consistent user experience

**CardSpace**
- Phishing-resistant authentication and attribute sharing through client; “card” paradigm; requires WS-Trust; can front-end various SSO systems

Thanks to Paul Madsen for the initial content and Johannes Ernst for the “three standards” paradigm!
References

- Liberty Alliance: http://www.projectliberty.org/
- ID-FF interoperability matrices: http://www.projectliberty.org/liberty/liberty_interoperable/interoperable_products
- ID-SIS specifications: http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_sis_1_0_specifications
- Advanced Client specs overview: http://www.projectliberty.org/liberty/content/download/2658/17911/file/AdvancedClient-20070122-Conor Cahill.pdf
- ID-SAFE FAQ: http://www.projectliberty.org/liberty/resource_center/faq/strong_authentication__1
- Concordia wiki: http://wiki.projectliberty.org/index.php/Concordia
Thanks!
Questions?

Eve Maler
eve.maler@sun.com
www.xmlgrrl.com/blog