ARCS Summary
SAML (Security Assertion Markup Language)

Basics:

- XML standard created by Organization for Advancement of Structured Information Standards (OASIS). OASIS also specified OpenOffice document standard.
- Current Version 1.1.
- Created to solve Single Sign On (SSO) for Web (Intranet).
- The identity provider performs local authentication for the principal. SAML doesn't care about how the local authentication is performed (mechanism independent).
- *Assertions* are transferred from identity provider to service provider and contain *statements* used to make control decisions. Multiple statements can be contained within one assertion.
- *Statements* can be of the following types: Authentication, Attribute, or Authorization decision.
- *Authentication Statements* assert that the principal has been authenticated with the identity provider. These statements may contain the method of authentication as well as other data such as the principal's email address.
- *An Attribute Statement* assigns affiliations (categories) to the principal, such as student or faculty. These attributes are often stored in a directory structure.
- The *Authorization Decision Statement* is basically the service provider asking the identity provider if the principal should be allowed to access the resource at a given URI.
- The SAML protocol is simple, request and response. SAML 1.1 must implement the SAML protocol over SOAP (also version 1.1) over HTTP to be compatible. Security is not required but recommended via SSL 3 or TLS 1.
- SAML 1.1 defines two single-sign-on browser-based *profiles*, the *Browser/Artifact* and *Browser/POST*. A single-log-out profile is not defined.
- The Browser/Artifact profile is expressed as a URL (Artifact Retriever) and specifies the following steps. It uses a "pull" method (pass by reference).
    1. The principal requests an inter-site transfer at the identity provider that contains the *target* resource requested from the service provider. (GET request)
    2. Principal is redirected to the Assertion Consumer Service at the service provider and provided with an *artifact* that is a reference to an assertion that will be provided by the identity provider. It is assumed (required) that the principal has already established with the identity provider.
    3. The principal then requests the target and artifact from the Assertion Consumer Service (GET) at the service provider.
    4. The ACS then contacts (via a "back channel" using HTTP POST) the *artifact resolution service* at the identity provider with the previous artifact.

5. The ARS responds (on the same "back channel") with an SAML assertion (success/failure).
6. The ACS then responds to the principal (if success) by redirecting it to the target resource.

- The Browser/POST uses a push method (pass by value). No "back channel" communication occurs.
    1. The principal requests inter site communication via a URL to the identity provider. The target resource is included with the URL. (GET)
    2. The inter site communication mechanism returns an HTML FORM w/ACTION attribute equal to the URL of the assertion consumer service. The SAML response (success/failure) is base64 encoded as a hidden input within the FORM.
    3. Principal requests resource from the assertion consumer service (POST).
    4. The ACS examines the SAML response and redirects principal to requested resource.

Implementations

- Shibboleth – Middleware developed to help Internet2 universities to share resources between members. Written in Java. Works/Tested on Windows, Macintosh 10.x, Redhat/Fedora. Looks like a BSD type license. It uses OpenSAML.
- SourceID – Open source federation for ID management. Implemented in both Java and .NET. PingFederate Server is the commercial product. Two entities (or more) setup PingFederate servers to manage ids (and trusts) between the entities. Uses SAML for communication between servers. Server runs on Linux/Windows. Client IE 6 w/Javascript.

Organizations

- Liberty Alliance Project – "The Liberty Alliance Project is an alliance of more than 150 companies, non-profit and government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information in today's digital economy, and is a key component in driving the use of e-commerce, personalized data services, as well as web-based services. Membership is open to all commercial and non-commercial organizations." Members: American Express, RSA, Entrust, Novell, GM, SAP, Sun, and more.
- OASIS – "OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector

and for application-specific markets. Founded in 1993, OASIS has more than 4,000 participants representing over 600 organizations and individual members in 100 countries."

External References

http://en.wikipedia.org/wiki/SAML
http://www.oasis-open.org/
http://en.wikipedia.org/wiki/SOAP
http://java.sun.com/features/2002/05/single-signon.html
http://shibboleth.internet2.edu/
http://www.opensaml.org/faq.html
http://www.sourceid.org/index.html
http://www.pingidentity.com/products/pingfederate.html
http://www.projectliberty.org/index.php