SAML Executive Overview

Introduction

The credo “Think globally, act locally” has traditionally been associated with the environmental movement – providing a helpful principle for guiding effective advocacy efforts and making personal lifestyle choices. The flip-side to this well known phrase, namely 'Think locally, act globally' nicely describes the federated model of identity management, as exemplified by Web single sign-on. In order to access protected resources at a service provider, users authenticate to their identity provider (they are 'thinking locally' because they do not need to authenticate to a remote service provider, rather they do so to an identity provider with which they have a closer trust relationship). Based on this authentication, they are then able to access resources at one or many service providers ('acting globally').

Federation is the dominant movement in identity management today. Federation refers to the establishment of some or all of business agreements, cryptographic trust, and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions. As web services promise to enable integration between business partners through loose coupling at the application and messaging layer, federation does so at the identity management layer - insulating each domain from the details of the others' authentication and authorization infrastructure.

Key to this loose coupling at the identity management layer are standardized mechanisms and formats for the communication of identity information between the domains – the standard provides the insulating buffer. The Security Assertion Markup Language (SAML) defines just such a standard.

What Is SAML?

SAML, developed by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS), is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.

SAML is a flexible and extensible protocol designed to be used – and customized if necessary – by other by other standards.The Liberty Alliance, the Internet2 Shibboleth project, and the OASIS Web Services Security (WS-Security) committee have all adopted SAML as a technological underpinning for various purposes.

SAML History

SAML V1.0 became an OASIS standard in November 2002. SAML V1.1 followed in September 2003 and has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. SAML has been broadly implemented by all major Web access management vendors. SAML is also supported in major application server products and SAML support is also common among Web services management and security vendors. SAML V2.0 builds on that success.

Many of these implementations have demonstrated succcessful interoperability at a series of events – the latest of which was held at the 2005 RSA Conference. The OASIS SAML Interoperability Lab, sponsored by the US Government's GSA, used three separate scenarios to demonstrate SAML-based interaction between a government or enterprise portal and sites from typical content or service providers.

SAML V2.0 unifies the building blocks of federated identity in SAML V1.1 with input from both higher education's Shibboleth initiative and the Liberty Alliance's Identity Federation Framework. As such, SAML V2.0 is a critical step towards full convergence for federated identity standards.

What Are the Advantages of SAML?

The benefits of SAML include:

- **Platform neutrality** – SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.
- **Loose coupling of directories** – SAML does not require user information to be maintained and synchronized between directories.
- **Improved online experience for end users** – SAML enables single sign-on by allowing users to authenticate at an identity provider and then

access service providers without additional authentication. In addition, identity federation (linking of multiple identities) with SAML allows for a better-customized user experience at each service while promoting privacy.

- **Reduced administrative costs for service providers** - Using SAML to 'reuse' a single act of authentication (such as logging in with a username and password) multiple times across multiple services can reduce the cost of maintaining account information.This burden is transferred to the identity provider.
- **Risk transference** – SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

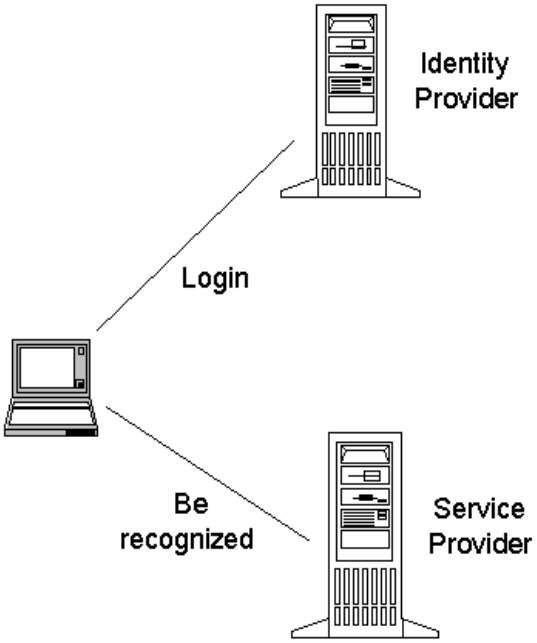
How Is SAML Being Used?

As befits a general framework for communicating security and identity information, SAML is being applied in a number of different ways, the major ones of which are presented here.

Web SSO

In web single sign-on, a user authenticates to one web site and then, without additional authentication, is able to access some personalized or customized resources at another site. SAML enables web SSO through the communication of an authentication assertion from the first site to the second which, if confident of the origin of the assertion, can choose to log in the user as if they had authenticated directly.

The basic SSO model is shown in the diagram below. A principal authenticates at the identity provider and is subsequently appropriately recognized as (and given corresponding access/service) at the service provider.



Attribute-Based Authorization

Similar to the Web SSO scenario, the attribute-based authorization model has one web site communicating identity information about a subject to another web site in support of some transaction. However, the identity information may be some characteristic of the subject (such as a person's role in a B2B scenario) rather than, or in addition to, information about when and how the person wsa authenticated. The attribute-based authorization model is important when the individual's particular identity is either not important, should not be shared (for privacy reasons), or is insufficient on its own.

Securing Web Services

SAML assertions can be used within SOAP messages in order to carry security and identity information between actors in web service transactions. The SAML Token Profile of the OASIS WS-Security TC specifies how SAML assertions should be used for this purpose. The Liberty Alliance's Identity Web Service Framework (ID-WSF) also uses SAML assertions as the base security token for enabling secure and privacy-respecting access to web services.

What Are the Components of SAML?

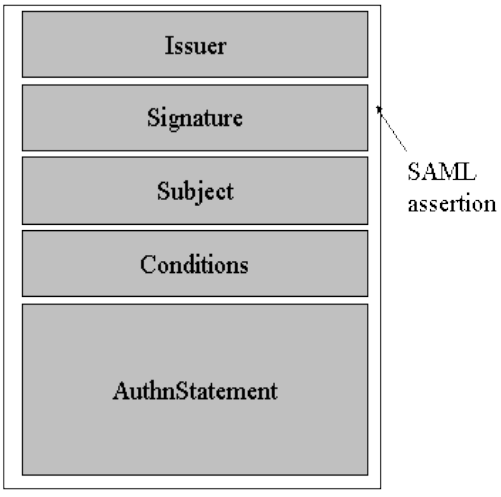
SAML is defined in terms of assertions, protocols, bindings, and profiles.

Assertions

An assertion is a package of information that supplies one or more statements made by a SAML authority. SAML defines three different kinds of assertion statement that can be created by a SAML authority.

- **Authentication:** The specified subject was authenticated by a particular means at a particular time. This kind of statement is typically generated by a SAML authority called an identity provider, which is in charge of authenticating users and keeping track of other information about them.
- **Attribute:** The specified subject is associated with the supplied attributes.
- **Authorization Decision:** A request to allow the specified subject to access the specified resource has been granted or denied.

The outer structure of an assertion is generic, providing information that is common to all of the statements within it. Within an assertion, a series of inner elements describe the authentication, attribute, authorization decision, or user-defined statements containing the specifics. The diagram below illustrates the high-level structure of a typical SAML authentication assertion.



Protocols

SAML defines a number of request/response protocols that allow service providers to:

- Request from a SAML authority one or more assertions (includes a direct request of the desired assertions, as well as querying for assertions that meet particular criteria)
- Request that an identity provider authenticate a principal and return the corresponding assertion
- Request that a name identifier be registered
- Request that the use of an identifier be terminated
- Retrieve a protocol message that has been requested by means of an artifact
- Request a near-simultaneous logout of a collection of related sessions (“single logout”)
- Request a name identifier mapping

Bindings

Mappings from SAML request-response message exchanges into standard messaging or communication protocols are called SAML protocol *bindings*. For instance, the SAML SOAP Binding defines how SAML protocol messages can be communicated within SOAP messages, whilst the HTTP Redirect binding defines how to pass protocol messages through HTTP redirection.

Profiles

Generally, a *profile* of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application – the goal being to enhance interoperability by removing some of the flexibility inevitable in a general-use standard. For instance, the Web Browser SSO Profile specifies how SAML authentication assertions are communicated between an identity provider and service provider to enable single sign-on for a browser user.

The Web SSO Profile details how to use the SAML Authentication Request/Response protocol in conjunction with different combinations of the HTTP Redirect, HTTP POST, HTTP Artifact, and SOAP bindings.

Another type of SAML profile is an attribute profile. – SAML defines a series of attribute profiles to provide specific rules for interpretation of attributes in SAML attribute assertions. An example is the X.500/LDAP profile, describing how to carry X.500/LDAP attributes within SAML attribute assertions.

What's New in SAML V2.0?

SAML V2.0 introduces a number of new features,

including:

- **Pseudonyms** – SAML V2.0 defines how an opaque pseudo-random identifier with no discenible correspondence with meaningful identifiers (for example, emails or account names) can be used between providers to represent principals. Pseudonyms are a key privacy-enabling technology because they inhibit collusion between multiple providers (as would be possible with a global identifier such as an email address),
- **Identifier management** – SAML V2.0 defines how two providers can establish and subsequently manage the pseudonym(s) for the principals for whom they are operating.
- **Metadata** – The metadata specification defines how to express configuration and trust-related data to make deployment of SAML systems easier. In doing this, it identifies the actors involved in the various profiles, such as SSO Identity Provider and Service Provider, and Attribute Authority and Requester.

  The data that must be agreed on between system entities includes supported roles, identifiers, supported profiles, URLs, certificates and keys.
- **Encryption** – SAML V2.0 permits attribute statements, name identifiers, or entire assertions to be encrypted. This feature ensures that end-to-end confidentiality of these elements may be supported as needed.
- **Attribute Profiles** – Attribute profiles simplify the configuration and deployment of systems that exchange attribute data. The attribute profiles include:

  Basic attribute profile: supports string attribute names and attribute values drawn from XML schema primitive type definitions.

  X.500/LDAP attribute profile: supports canonical X.500/LDAP attribute names and values.

  UUID Attribute Profile: Use of UUIDs as attribute names.

  XACML Attribute Profile: formats suitable for processing by XACML.
- **Session management** – The single logout protocol in SAML V2.0 provides a protocol by which all sessions provided by a particular session authority can be near-simultaneously terminated. As an example, if a principal, after authenticating at an identity provider, achieved single sign-on to multiple service providers, they could be automatically logged out of all of those service providers at the request of the identity provider.
- **Devices** – SAML V2.0 introduces new support for the mobile world – addressing both the challenges introduced by device and bandwidth constraints and the opportunities made possible by emerging smart or active devices.
- **Privacy Mechanisms** – SAML V2.0 includes mechanisms that allow providers to communicate privacy policy and settings. For instance, SAML makes it possible to obtain and express a principal's consent to some operation being performed.
- **Identity provider discovery –** In deployments having more than one identity provider, service providers need a means to discover which identity provider(s) a principal uses. The identity provider discovery profile relies on a cookie written in a common domain between identity and service providers.

How Does SAML Relate to Other Standards and Initiatives?

SAML is used by several other standards groups to provide a security and identity underpinning for their work.

Liberty Alliance

The Liberty Alliance is an industry consortium defining standards for federated identity – including enabling simplified sign-on through federated network identification using current and emerging network access devices, as well as supporting and promoteing permission-based attribute sharing to enable a user's choice and control over the use and disclosure of his/her personal identification.

Liberty had defined its Identity Federation Framework (ID-FF) on the base provided by SAML V1.x, layering additional functionality on top. Recognizing the value of a single standard for federated SSO, the Alliance submitted ID-FF V1.2 back into the OASIS Security Services Technical Committee as input for SAML V2.0.

Liberty's Identity Web Services Framework (ID-WSF), a platform for securing identity-based web services, continues to evolve within the Liberty Alliance. Liberty ID-WSF uses SAML assertions as the security token format by which the authentication and authorization information associated with the various web service actors are communicated amongst them.

Shibboleth

Shibboleth is a project within the Internet2 higher-education consortium to develop technical and policy frameworks and an open software system for the sharing of online resources among researchers, professors, and students, . Like Liberty, Shibboleth profiled SAML for its particular requirements and, also like Liberty, built privacy management into its architecture. Shibboleth's input has been fed back into SAML V2.0.

XACML

XACML (eXtensible Access Control Markup Language) is an XML-based language for access control that has been standardized in OASIS. XACML describes both an access control policy language and a request/response language. The policy language is used to express access control policies ('who can do what when'). The request/response language expresses queries about whether a particular access should be allowed (requests) and describes answers to those queries (responses). The newest versions of XACML and SAML have been designed to complement each other; for example, an XACML policy can specify what a provider should do when it receives a SAML assertion, and XACML-based attributes can be expressed in SAML.

WS-Security

WS-Security is an OASIS standard that specifies how SOAP messages can have their integrity and confidentiality ensured. WS-Security defines a *framework* for securing SOAP messages, with the specifics being defined in profiles determined by the nature of the security token used to carry identity information. So, for instance, there are different profiles of WS-Security for various different security token formats such as X.509 certificates and Kerberos tickets. As already noted in the Securing Web Services section above, there is also a SAML token profile of WS-Security that specifies how SAML assertions can be used to provide message security.

Additionally, SAML itself points to WS-Security as an approved mechanism for securing SOAP messages carrying SAML protocol messages and assertions.

Summary

A federated identity is one that is both *portable* and *potable*, that is, it can be transported and consumed across autonomous domains or business boundaries. Effective identity federation benefits both users and enterprises - providing principals with a smooth, cross-domain browsing experience through SSO and allowing enterprises to make available its resources to a class of users without the associated administrative costs.

SAML has emerged as the gold standard for federated identity. By defining standardized mechanisms for the communication of security and identity information between business partners, SAML makes federated identity, and the cross-domain transactions that it enables, a reality. Importantly, with SAML V2.0, the industry has taken a key step towards convergence in the federated identity management standards space.

Revision History

#	Date	By Whom	What
00	18 Jun 2004	Paul Madsen	Initial draft.
01	30 Jun 2004	Paul Madsen	Expanded on What is SAML section, Added Benefits section, New Stack diagram, New 'Whats new in SAML2' section, removed section on federation models
02	01 Nov, 2004	Paul Madsen	Expanded 'Other Standards' section, removed web services stack diagram, filled in 'What's New' section
03	18 Jan 2005	Paul Madsen	Moved into two column format , removed boilerplate etc
04	1 Feb 2005	Paul Madsen	Added text from Prateek and Eve, Tom, and Scottt
05	17 Feb 2005	Paul Madsen	'assertions' -> assertion in SAML expansion
06	Mar 10, 2005	Eve Maler	Editorial cleanup