



SAML V2.0 Executive Overview

Committee Draft 01, 12 April 2005

Document identifier:

sstc-saml-exec-overview-2.0-cd-01

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editors:

Paul Madsen, NTT
Eve Maler, Sun Microsystems

Contributors:

Thomas Wisniewski, Entrust
Tony Nadalin, IBM
Scott Cantor, Internet2
Jeff Hodges, Neustar
Prateek Mishra, Principal Identity

Status:

This is a **Committee Draft** approved by the Security Services Technical Committee on 12 April 2005.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should submit them by filling in the form at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (<http://www.oasis-open.org/committees/security/>).

Executive Overview

The credo "Think globally, act locally" has long provided a helpful principle for guiding effective advocacy efforts. The flip-side, "Think locally, act globally," nicely describes the federated model of identity management, as exemplified by web single sign-on (SSO). In order to access protected resources at a service provider, users authenticate to their identity provider ("thinking locally" because they do not need to authenticate to a remote service provider, just 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 business agreements, cryptographic trust, and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions. Just 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 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 support also appears in major application server products and is commonly found among Web services management and security vendors. SAML V2.0 builds on that success.

Many of these implementations have demonstrated successful 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 U.S. government's General Services Administration (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 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.

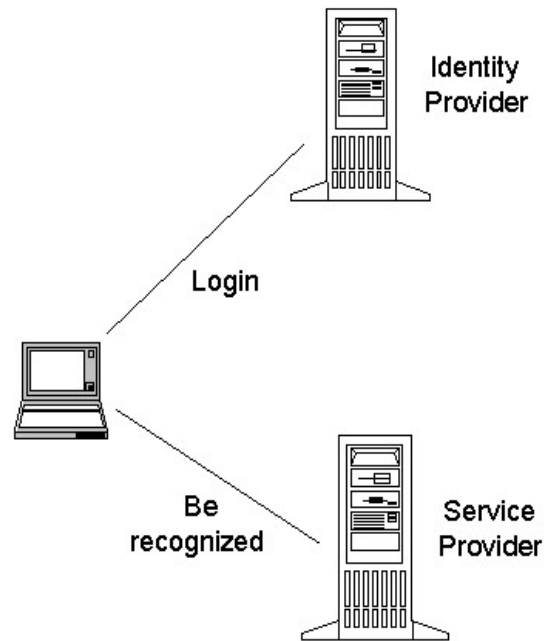
How Is SAML Being Used?

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 Single Sign-On

In web SSO, 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 following diagram. A principal authenticates at the identity provider and is subsequently appropriately recognized (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 was 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 convey security and identity information between actors in web service interactions. The SAML Token Profile produced by the OASIS Web Services Security (WSS) TC specifies how SAML assertions should be used for this purpose with the WS-Security framework. The Liberty Alliance's Identity Web Service Framework (ID-WSF) builds on these specifications to use SAML assertions for enabling secure and privacy-respecting access to web services.

WS-Trust, one component of the private WS-* framework initiative, proposes protocols for the exchange and validation of security tokens used as described within WS-Security. SAML assertions are one such supported security token format.

What Are the Components of SAML?

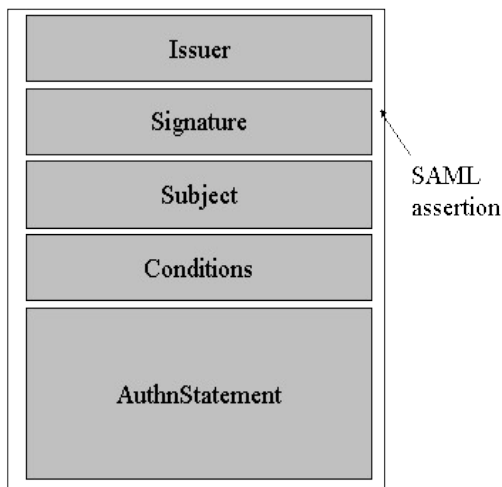
SAML is defined in terms of assertions, protocols, bindings, and profiles.

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?

Building on functionality found in Liberty ID-FF and Shibboleth, this major version introduces a number of major features to SAML:

- **Pseudonyms** – SAML V2.0 defines how an opaque pseudo-random identifier with no discernible 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** – SAML's 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: supports use of UUIDs as attribute names.
 - XACML Attribute Profile: defines 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 user, 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 promoting 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, and intends to use the new version of SAML in concert with its own technical and business guidelines for identity federation going forward

Liberty's Identity Web Services Framework

(ID-WSF), a platform for communicating identity information among web services, continues to be developed within the Liberty Alliance. The latest version of Liberty ID-WSF now uses SAML V2.0 assertions as the security token format for communicating authentication and authorization information amongst web service actors.

Shibboleth

The Shibboleth Project is an initiative of the Internet2 consortium to develop technical and policy frameworks and an open-source software system for controlling access to online resources targeted to the needs of higher education, research, and their partners. Like Liberty, the Shibboleth system has profiled SAML for its particular requirements and has built privacy management into its architecture. Input from the Shibboleth Project's use of SAML 1.x has been fed back into SAML V2.0, and support for SAML V2.0 appears on the near-term roadmap for Shibboleth, as well as for the Internet2 OpenSAML project.

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 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.

WS-*

WS-* is a private initiative proposing a broad set of specifications for different aspects of web services, including security. The security aspects of WS-* are based on the concept of using security tokens as described in WS-Security, and the SAML Token Profile already mentioned specifies the usage of SAML assertions as such a security token.

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.

Resources

For more information, visit these sites:

- **SAML:**
<http://www.oasis-open.org/committees/security/>
- **Liberty Alliance Project:**
<http://www.projectliberty.org>
- **Shibboleth:**
<http://shibboleth.internet2.edu>
- **OpenSAML:**
<http://www.opensaml.org>
- **XACML:**
<http://www.oasis-open.org/committees/xacml/>
- **WS-Security:**
<http://www.oasis-open.org/committees/wss/>

Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website.

Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Copyright © OASIS Open 2005. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.