Executive Overview of the Security Assertions Markup Language (SAML) v2.0

Working Draft 02, November 01 2004

Document identifier:
sstc-saml-exec-overview-2.0-draft-02

Location:
http://www.oasis-open.org

Editor:
Paul Madsen, Entrust Inc (p.madsen@entrust.com)

Contributors:

Abstract:
This document provides an executive overview of the Security Assertions Markup Language.

Status:

This is boilerplate; to use, fix the hyperlinks:] Committee members should send comments on this specification to the xxx@lists.oasis-open.org list. Others should subscribe to and send comments to the xxx-comment@lists.oasis-open.org list. To subscribe, send an email message to xxx-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

Table of Contents

1 SAML Executive Overview

1.1 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 a local identity provider with which they have a closer relationship). Based on this authentication, they are then able to access resources at the original service provider and others (the '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 between decentralized 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 both domains from the details of the others authentication & authorization infrastructure.

Key to this loose-coupling at the identity management layer are standardized mechanisms and syntax 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.

1.2 What is SAML?

The Security Assertions Markup Language (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, entitlements and attribute information. As its name suggests, SAML will allow business entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, which may be a partner company, another enterprise application etc.

SAML is a flexible and extensible protocol designed to be used by other by other standards.The Liberty Alliance, the Internet2 Shibboleth project, and OASIS Web Services Security (WS-Security) have all adopted SAML as a technological underpinning to varying degrees.

SAML's History

SAML 1.0 became an OASIS standard in November 2002. SAML 1.1 followed in September 2003 and has seen significant success within industry.- gaining momentum in financial services, higher education, government, and other verticals. 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 2.0 builds on that success.

Critically, SAML 2.0 unifies the previous disparate federated identity building blocks of SAML 1.1 with input from both higher education's Shibboleth initiative and the Liberty Alliance's Identity Federation Framework. As such, SAML 2 is a critical step towards full convergence for federated identity standards.

1.3 What benefits does SAML provide?

The benefits of SAML include:

- **Platform neutral** – SAML abstracts the security framework away from particular vendor implementations and architectures.
- **Loose coupling of directories** – SAML does not require user information to be maintained and synchronized between directores.
- **Improved Online Experience for end-users** – SAML authentication assertions enables single sign-on by allowing users to authenticate at an identity provider and then access services/resources at service providers without additional authentication
- **Reduced administrative costs for service providers** - use of SAML for federation between identity domains can reduce the cost of maintaining account information (e.g. username & password).This burden is placed on 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.

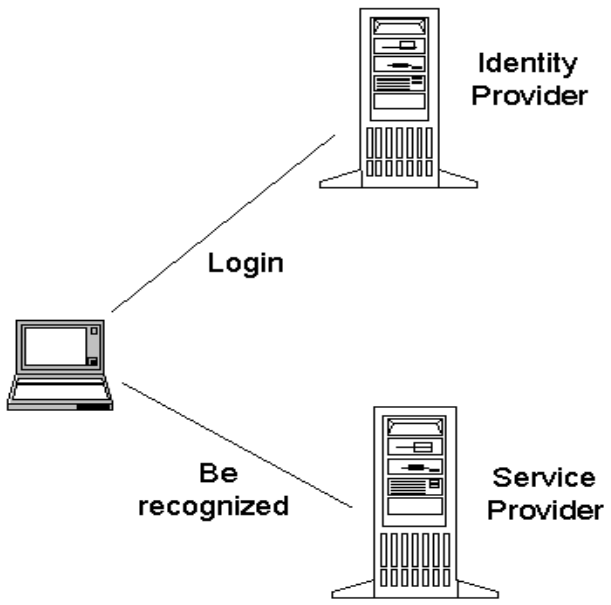
1.4 How is SAML being applied?

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

Web SSO

In Web Single Single-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.



Securing Web Services

SAML Assertions can be used as Security Tokens within SOAP Header blocks 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 packaged into the WS-Security <Security> element in an interoperable manner. The Liberty Alliance's ID-Web Service Framework also uses SAML assertions as the base security token format for enabling secure & privacy respecting access to identity-based web services.

Attribute-based Authorization

Similar to the Web SSO scenario, the Attribute-based Authorization model has one web site communicating identity information about a principal to another web site in support of some transaction that principal is attempting to perform there. However, unlike the SSO scenario, the nature of the information is not an authentication assertion (i.e. that the principal authenticated at a certain time) but rather some other characteristic of the principal (e.g. their roles in a B2B scenario). The Attribute-based authorization model is important when the individuals particular identity is either not important or should not be shared (for privacy reasons).

1.5 What is SAML composed of?

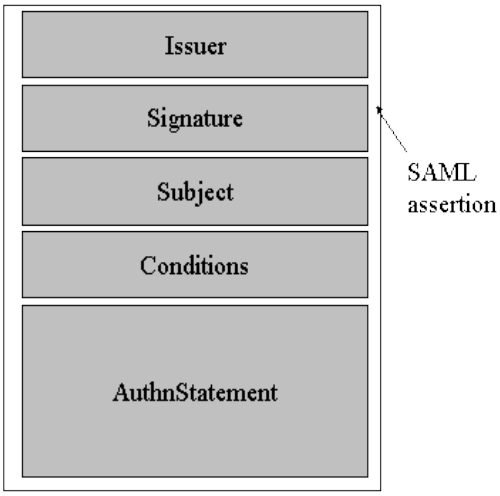
SAML is composed of a number of distinct (but interrelated) components.

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.
- **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 SAML authentication assertion.



Protocols

SAML defines a number of different (generally) request/response protocols, including allowing providers to:

- Request one or more assertions (includes a direct request of the desired assertions, as well as querying for assertions that meet particular criteria)
- Request that a principal be authenticated with the corresponding assertion returned
- Request that a name identifier be registered
- Request that a federation 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

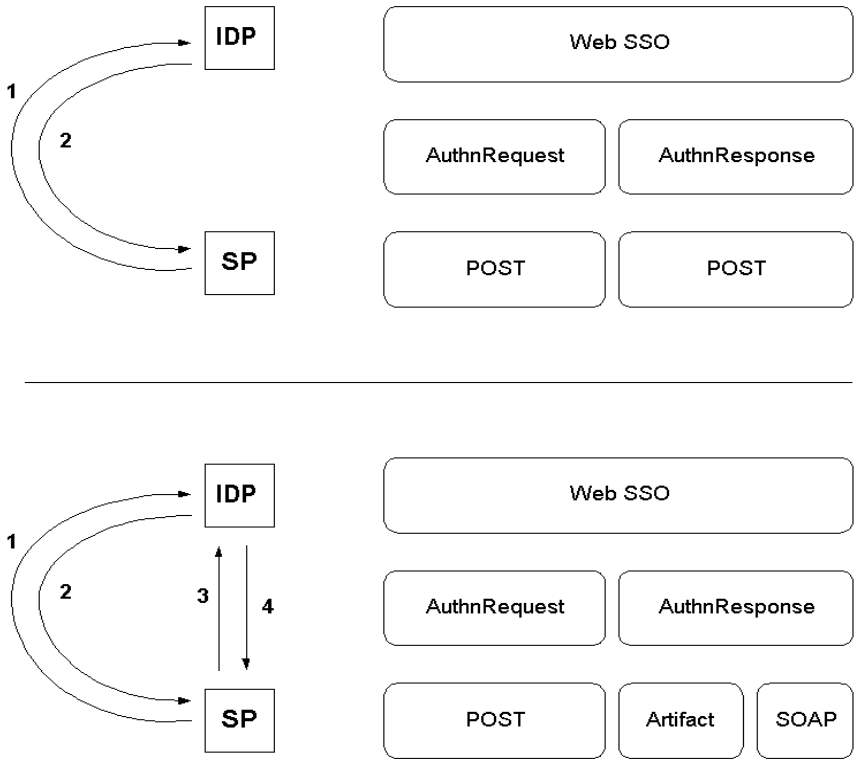
Bindings

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 SAML URI Binding defines how SAML protocol messages can be communicated through URI resolution

Profiles

Generally, a profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application – the goal to enhance interoperability by removing some of the flexibility inevitable in a general usage 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. Two different combinations are shown in the diagram below. In the top diagram, both the AuthnRequest and the subsequent response are sent using the HTTP POST Binding. In the bottom diagram, the AuthnRequest is sent using the HTTP POST Binding, the Response however uses a combination of the HTTP Artifact & SOAP Bindings.



Another distinct type of SAML profile are the Attribute profiles – definitions of specific rules for the allowed names and syntax of attributes passed within SAML attribute assertions. An example of such an attribute profile is the X.500/LDAP profile, describing how to carry X.500/LDAP attributes within SAML attribute assertions.

1.6 What's new in SAML 2?

SAML 2 introduces a number of new features, including.

- **Pseudonyms** – SAML2 defines how an opaque pseudo-random identifier with no discenible correspondence with meaningful identifiers (e.g. 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)
- **Federation management** – SAML2 defines how two providers can establish and subsequently manage the pseudonym(s) for the principals for whom they are operating.
- **Session management** - The single logout protocol in SAML2 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, was SSO'd to multiple service providers, they could be automatically logged out of all of those service providers at the request of the identity provider.
- **Mobile** – SAML 2 introduces new support for the mobile world– both addressing the challenges introduced by device and bandwidth constraints as well as the opportunities made possible by emerging smart or active devices.
- **Privacy Mechanisms** - SAML 2 includes mechanisms that allow providers to communicate privacy policy/settings from one to the other. For instance, a principal's consent to some operation being performed, fundamental to privacy, can be obtained at one provider and this fact can be communicated

to another provider through the SAML assertions and protocols.

1.7 How does SAML relate to other standards/initiatives?

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, and (ii) support and promote 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 ID-Federation Framework on the base provided by SAML 1, layering additional functionality on top. Recognizing the value of a single standard for federated SSO, the Alliance submitted v1.2 of the ID-FF into the SAML TC as input for SAML 2.

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

Shibboleth

Shibboleth is an Internet2 initiative for sharing of resources for researchers, graduate students, etc between higher education institutes. Like Liberty, Shibboleth profiled SAML for their particular requirements and, also like Liberty, built privacy management in. Shibboleth's input has been fed back into SAML2.

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). XACML and SAML complement each other nicely (despite some protocol overlap); an XACML policy can specify what a provider should do when it receives a SAML assertion.

WS-Security

WS-Security is a OASIS standard that specifies SOAP security extensions providing data integrity and confidentiality. WS-Security defines a framework for securing SOAP messages- the specifics 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 the different security token formats of X.509 certificates, Kerberos tickets, and SAML assertions.

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

1.8 Summary

A federated identity is one that is both *portable* and *potable*, ie it can be used and understood across autonomous domains or business boundaries. Effective identity federation can 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 & identity information between business partners, SAML makes federated identity, and the cross-domain transactions that it enables, a reality. Importantly, with SAML 2, the industry has taken a key step towards convergence in the federated identity standards space.

With SAML,

A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS SSTC Technical Committee, whose voting members at the time of publication were:

- Conor P. Cahill, AOL, Inc.
- Hal Lockhart, BEA
- Gavenraj Sodhi, Computer Associates
- Tim Alsop, CyberSafe
- John Hughes, Entegrity Solutions
- Paul Madsen, Entrust (editor)
- Miguel Pallares, Ericsson
- Irving Reid, Hewlett-Packard Company
- Paula Austel, IBM
- Maryann Hondo, IBM
- Michael McIntosh, IBM
- Anthony Nadalin, IBM
- Scott Cantor, Individual
- Bob Morgan, Individual
- Prateek Mishra, Netegrity (co-chair)
- Peter Davis, Neustar
- Frederick Hirsch, Nokia
- John Kemp, Nokia
- Nicholas Sauriol, Nortel
- Charles Knouse, Oblix
- Steve Anderson, OpenNetwork
- Darren Platt, Ping Identity
- Jim Lien, RSA Security
- John Linn, RSA Security
- Rob Philpott, RSA Security (co-chair)
- Dipak Chopra, SAP
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Jeff Hodges, Sun Microsystems
- Eve Maler, Sun Microsystems
- Ron Monzillo, Sun Microsystems
- Mike Beach, The Boeing Company
- Greg Whitehead, Trustgenix

B. Revision History

Rev	Date	By Whom	What
00	18 Jun 2004	Paul Madsen	Initial draft.
01	30 Jun 2004	Paul Madsen	Exapnded on What is SAML section, Added Benefits section, New Stack diagram, New 'Whats new in SAML 2' section, removed section on federation models
02	01 November	Paul Madsen	Expanded 'Other Standards' section, removed web services stack diagram, filled in 'What's New' section

C. 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.