Glossary for the OASIS Security Assertion Markup Language (SAML)

Document identifier: draft-sstc-glossary-02

Location: http://www.oasis-open.org/committees/security/docs

Publication date: 10 January 2002

Maturity Level: Committee Working draft

Send comments to: security-services-comment@lists.oasis-open.org *unless* you are subscribed to the security-services list for committee members -- send comments there if so. Note: Before sending messages to the security-services-comment list, you must first subscribe. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

Contributors:

Carlisle Adams, Entrust
Zahid Ahmed, CommerceOne
Marlena Erdos, Tivoli
Jeff Hodges, Oblix, editor (jhodges@oblix.com)
Maryann Hondo, IBM
Hal Lockhart, Entegrity
Prateek Mishra, Netegrity
Eve Maler, Sun Microsystems
RL “Bob” Morgan, University of Washington
Tim Moses, Entrust
David Orchard, BEA
Darren Platt, RSA
Evan Prodromou, Securant
Irving Reid, Baltimore

Rev	Date	By Whom	What
00	21 Jan 2001	Jeff Hodges	Created.
01	8 Feb 2001	Jeff Hodges	Added various terms supplied by Bob Blakley, and others culled from S2ML 0.8a doc.
01	9 Feb 2001	Jeff Hodges	Cleaned up refs, added refs, added definitions, enhanced or otherwise mangled others.
00	30 Mar 2001	Jeff Hodges	Aligned terms with draft-sstc-use-domain-02 and discussion thereof in the security-use subgoup’s conference calls. Aligned terms with usage in X.8xx/ISO-10181 series of docs. Added commentary to various definitions where security-use needs to come to consensus and/or make decision(s) on refining said definitions. Deleted various referenceable terms such as HTTP, LDAP, etc. Renamed doc to draft-sstc-glossary-00.
01	Jul 2001	Jeff Hodges	Incorporate extensive comments from Eve Maler Incorp. F2F #2 comments.

			Use Blakley-massaged F2F #3 version as starting point of crafting this version.
02	21 Dec 2001	Eve Maler	Prepared for interim end-of-year release.

1. Introduction

This normative document defines terms used throughout the OASIS Security Assertion Markup Language (SAML) specifications and related documents.

Some definitions are derived directly from external sources (referenced in an appendix), some definitions based on external sources have been substantively modified to fit the SAML context, and some are newly developed for SAML. Please refer to the external sources for definitions of terms not explicitly defined here.

2. Notation

Some definitions are tentative or missing. They are denoted with a question mark (**?**).

Some definitions have multiple senses provided. They are denoted by (a), (b), and so on.

> **Note:** Tentative and missing definitions and multiple senses are currently non-normative and form part of the remaining work of the OASIS Security Services Technical Committee.

Definitions that have been specifically agreed to by the Use Case and Requirements subcommittee are denoted by reference to "[33]".

In this document, references to SAML defined terms in the text are italicized.

3. Glossary

Following are the defined terms used in the SAML specifications and related documents.

Access	To interact with a *system entity* in order to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's *resources*. [4]
Access Control	Protection of *resources* against unauthorized access; a process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy. [4]
Access Control Information	Any information used for access control purposes, including contextual information [10]. Contextual information might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Portions of access control information may be specific to the request itself, some may be associated with the connection via which the request is transmitted, and others (for example, time of day) may be "environmental". [25]
Access Rights	A description of the type of authorized interactions a *subject* can have with a *resource*. Examples include read, write, execute, add, modify, and delete. [8]
Active Role	A role that a *system entity* has donned when performing some operation, for example accessing a *resource*.

Administrative Domain	An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations, or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may, and in many cases will, evolve over time. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries.
Administrator	A person who installs or maintains a system (for example, a SAML-based security system) or who uses it to manage *system entities*, users, and/or content (as opposed to application purposes; see also *End User*). An administrator is typically affiliated with a particular *administrative domain* and may be affiliated with more than one administrative domain.
Anonymity	The quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed. [4]
Assertion	A piece of data produced by a *SAML authority* regarding either an act of authentication performed on a *subject*, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified *resource*.
Asserting Party	Formally, the *administrative domain* that hosts one or more *SAML authorities*. Informally, an instance of a *SAML authority*.
Attribute	A distinct characteristic of an object (in SAML, a *subject*). An object’s attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, and so on. Which attributes of an object are salient is decided by the beholder. See also *XML attribute*.
Attribute Authority	A *system entity* that produces *attribute assertions*. [33]
Attribute Assertion	An *assertion* that conveys information about *attributes* of a *subject*.
Authentication	To confirm a *system entity*’s asserted *principal identity* with a specified, or understood, level of confidence. [7] [33]
Authentication Assertion	An *assertion* that conveys information about a successful act of *authentication* that took place for a *subject*.
Authentication Authority	A *system entity* that produces *authentication assertions*. [33]
Authorization	The process of determining, by evaluating applicable *access control information*, whether a *subject* is allowed to have the specified types of *access* to a particular *resource*. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access. [8]
Authorization Decision	The result of an act of authorization. The result may be negative, that is, it may indicate that the *subject* is not allowed any access to the *resource*.
Authorization Decision Assertion	An *assertion* that conveys information about an *authorization decision*.
Binding, Protocol Binding	An instance of mapping SAML request-response message exchanges into a specific protocol. Each binding is given a name in the pattern “SAML xxx binding”.

Credentials	Data that is transferred to establish a claimed principal identity. [9] [33]
End User	A natural person who makes use of resources for application purposes (as opposed to system management purposes; see Administrator, User).
Identifier	A representation (for example, a string) mapped to a *system entity* that uniquely refers to it.
Login, Logon, Sign-On	The process whereby a *user* presents *credentials* to an *authentication authority*, establishes a *simple session*, and optionally establishes a *rich session*.
Logout, Logoff, Sign-Off	The process whereby a *user* signifies desire to terminate a *simple session* or *rich session*.
Keep-alive	**?**
Markup Language	A set of *XML elements* and *XML attributes* to be applied to the structure of an XML document for a specific purpose. A markup language is typically defined by means of a set of *XML schemas* and accompanying documentation. For example, the *Security Assertion Markup Language* (SAML) is defined by two schemas and the set of normative SAML specification text.
Party	Informally, one or more *principals* participating in some process or communication, such as receiving an *assertion* or accessing a *resource*.
Policy Decision Point (PDP)	A *system entity* that makes *authorization decisions* for itself or for other system entities that request such decisions. [31] For example, a SAML PDP consumes authorization decision requests, and produces *authorization decision assertions* in response. A PDP is an “authorization decision authority”.
Policy Enforcement Point (PEP)	A *system entity* that requests and subsequently enforces *authorization decisions*. [31] For example, a SAML PEP sends *authorization decision* requests to a PDP, and consumes the *authorization decision assertions* sent in response.
Principal	A *system entity* whose identity can be authenticated. [34]
Principal Identity	A representation of a principal’s identity, typically an *identifier*.
Profile	A set of rules describing how to embed *assertions* into and extract them from a framework or protocol. Each profile is given a name in the pattern “xxx profile for SAML”.
Proxy	a) An entity authorized to act for another. b) Authority or power to act for another. c) A document giving such authority. [28]
Proxy Server	A computer process that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. [4]
Pull	To actively request information from a *system entity*.
Push	To provide information to a *system entity* that did not actively request it.
Relying Party	A *system entity* that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving *assertions* from an *asserting party* (a *SAML authority*) about a *subject*.

Requester	A *system entity* that utilizes a protocol to request services from another system entity. The term "client" for this notion is not used because many system entities simultaneously or serially act as both clients and servers.
Resource	a) Data contained in an information system (for example, in the form of files, information in memory, etc). b) A service provided by a system. c) An item of system equipment (in other words, a system component such as hardware, firmware, software, or documentation). d) A facility that houses system operations and equipment. [4] **?** Should this definition mention the relationship to URI references? We probably only want the (a) and (b) senses.
Rich session	**?**
Role	**?** Dictionaries define a role as "a character or part played by a performer" or "a function or position." Principals don various types of roles serially and/or simultaneously, for example, active roles and passive roles. The notion of an Administrator is often an example of a role.
SAML Authority	An abstract *system entity* in the SAML domain model that issues *assertions*. See also *attribute authority*, *authentication authority*, and *policy decision point (PDP)*.
Security	A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity, and availability. It is intended to ensure that a system resists potentially correlated attacks. [7]
Security Architecture	A plan and set of principles for an *administrative domain* and its *security domains* that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment. A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security, and physical security, and prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain's evolution. [4]
Security Assertion	An *assertion* that is scrutinized in the context of a security architecture.
Security Assertion Markup Language (SAML)	The set of specifications describing *security assertions* that are encoded in *XML*, *profiles* for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and *bindings* of this protocol to various transfer protocols (for example, SOAP and HTTP).
Security Domain	An environment or context that is defined by security models and a *security architecture*, including a set of *resources* and set of *system entities* that are authorized to access the resources. One or more security domains may reside in a single *administrative domain*. The traits defining a given security domain typically evolve over time. [8]

Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect *resources*. Security policies are components of *security architectures*. Significant portions of security policies are implemented via *security services*, using *security policy expressions*. [4] [8]
Security Policy Expression	A mapping of *principal identities* and/or *attributes* thereof with allowable actions. [8] Security policy expressions are often essentially access control lists. [8]
Security Service	A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKI-based document attribution and authentication service. A security service is a superset of AAA services. Security services typically implement portions of *security policies* and are implemented via security mechanisms. [4] [8]
Session	A lasting interaction between system entities, often involving a user, typified by the maintenance of some state of the interaction for the duration of the interaction.
Site	An informal term for an *administrative domain* in geographical or DNS name sense. It may refer to a particular geographical or topological portion of an administrative domain, or it may encompass multiple administrative domains, as may be the case at an ASP site.
Subject	A *principal* in the context of a *security domain*. SAML assertions make declarations about subjects.
System Entity	An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality. [4] [33]
Time-In	**?**
Time-Out	A period of time after which some condition becomes true if some event has not occurred. For example, a *session* that is terminated because its state has been inactive for a specified period of time is said to “time out”.
User	A natural person who makes use of a system and its resources for any purpose [33]
Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical *resource*. [37] [21] URIs are the universal addressing mechanism for resources on the World Wide Web. Uniform Resource Locators (URLs) are a subset of URIs that use an addressing scheme tied to the resource’s primary access mechanism, for example, their network “location”.
URI Reference	A URI that is allowed to have an appended number sign (#) and fragment identifier. [37] [21] Fragment identifiers address particular locations or regions within the identified resource.
XML	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. [36]
XML Attribute	An XML data structure that is embedded in the start-tag of an XML element and that has a name and a value. For example, the italicized portion below is an instance of an XML attribute: <Address *AddressID=”A12345”*>…</Address> See also *attribute*.

XML Element

An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a start-tag and end-tag or an empty tag. For example:

```
<Address AddressID=”A12345”>
    <Street>105 Main Street</Street>
    <City>Springfield</City>
    <StateOrProvince>
        <Full>Massachusetts</Full>
        <Abbrev>MA</Abbrev>
    </StateOrProvince>
    <Post Code=”567890”/>
</Address>
```

XML Namespace

A collection of names, identified by a *URI reference*, which are used in XML documents as element types and attribute names. An XML namespace is often associated with an *XML schema*. For example, SAML defines two schemas, and each has a unique XML namespace.

XML Schema

The format developed by the World Wide Web Consortium (W3C) for describing rules for a *markup language* to be used a set of XML documents. In the lowercase, a “schema” or “XML schema” is an individual instance of this format. For example, SAML defines two schemas, one containing the rules for XML documents that encode security assertions and one containing the rules for XML documents that encode request/response protocol messages. Schemas define not only XML elements and XML attributes, but also datatypes that apply to these constructs.

Appendix A. 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.

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.

Appendix B. References

Many of the definitions in this glossary are based on those found in the references below: [1], [2], [3], [4], [5] (page 102), [6], [7] (Appendix K *Glossary*), [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], ,

[1] **Authentication Markup Language – AuthXML**. Evan Prodromou, Darren Platt, Robert L. Grzywinski, Eric Olden, Third Draft - Version 0.3 - 12/14/2000.
Available at: http://www.oasis-open.org/committees/security/docs/draft-authxml-v2.pdf

[2] **Security Services Markup Language (S2ML)**. P. Mishra, P. Hallam-Baker, Zahid Ahmed, Alex Ceponkus, Marc Chanliau, Jeremy Epstein, Chris Ferris, David Jablon, Eve Maler, David Orchard. Rev 0.8a, 8-Jan-2001.
Available at: http://www.s2ml.org/downloads/S2MLV08a.pdf

[3] ITML MESSAGE AND PROTOCOL SPECIFICATION WORKING DRAFT. Dave Orchard et al. Jamcracker 22-Nov-2000, version 0.8.
available at: http://www.oasis-open.org/committees/security/docs/draft-orchard-itml-messaging-00.pdf

[4] **Internet Security Glossary**. Robert W. Shirey, RFC 2828, May 2000.
Available at: http://www.ietf.org/rfc/rfc2828.txt

[5] **Building Internet Firewalls, 2nd Ed**. D. Brent Chapman & Elizabeth D. Zwicky, O'Reilly, ISBN 1-56592-871-7, June 2000.
Available at: http://www.oreilly.com/catalog/fire2/

[6] **Free On-Line Dictionary of Computing**. Denis Howe, on-going.
Available at: http://foldoc.doc.ic.ac.uk/foldoc/

[7] **Trust in Cyberspace**. Committee on Information Systems Trustworthiness, Fred B. Schneider - Editor, National Research Council, ISBN 0-309-06558-5, 1999.
Online copy and ordering information available at: http://www.nap.edu/readingroom/books/trust/
Glossary: http://www.nap.edu/readingroom/books/trust/trustapk.htm

[8] **Security Taxonomy and Glossary**. Lynn Wheeler, on-going.
Available at: http://www.garlic.com/~lynn/secure.htm; see http://www.garlic.com/~lynn/ for the list of sources.

[9] **Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture**. ISO 7498-2:1989, ITU-T Recommendation X.800 (1991).
Available at: http://www.itu.int/itudoc/itu-t/rec/x/x500up/x800.html

[10] **Security frameworks for open systems: Access control framework**. ITU-T Recommendation X.812 (1995 E), ISO/IEC 10181-3: 1996 (E)
Available at: http://www.itu.int/itudoc/itu-t/rec/x/x500up/x812.html

[11] **Understanding and Deploying LDAP Directory Services**. Tim Howes, Mark Smith, and Gordon Good, Macmillan Technical Publishing & Netscape Communications Corporation, 1999, ISBN: 1578700701.
Description at: http://www.informit.com/product/1578700701/

[12] **Authorization (AZN) API**. Open Group Technical Standard, C908, ISBN 1-85912-266-3, January 2000.
Available at: http://www.opengroup.org/publications/catalog/c908.htm

[13] **Authentication and Privilege Attribute Security Application with related Key Distribution Functions - Part 1, 2 and 3**. Standard ECMA-219, 2nd edition (March 1996).
Available at: http://www.ecma.ch/ecma1/STAND/ECMA-219.HTM

[14] **Computer Currents High-Tech Dictionary**. On-going
Available at: http://www.currents.net/resources/dictionary/

[15] **Hypertext Transfer Protocol -- HTTP/1.0**. T. Berners-Lee, R. Fielding, H. Frystyk, RFC1945, May 1996.
Available at: http://www.normos.org/ietf/rfc/rfc1945.txt

References are continued on the next page…

[16] **Hypertext Transfer Protocol -- HTTP/1.1**. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee, RFC2616, June 1999.
Available at: http://www.normos.org/ietf/rfc/rfc2616.txt

[17] **Lightweight Directory Access Protocol (v3).** M. Wahl, T. Howes, S. Kille, RFC2251, December 1997.
Available at: http://www.normos.org/ietf/rfc/rfc2251.txt

[18] **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies**. N. Freed, N. Borenstein, RFC2045, November 1996.
Available at: http://www.normos.org/ietf/rfc/rfc2045.txt

[19] **Security in Open Systems - A Security Framework**. ECMA Technical Report TR/46, July 1988.
Available at: http://www.ecma.ch/ecma1/TECHREP/E-TR-046.HTM

[20] **SSL 3.0 Specification**. Alan O. Freier, Philip Karlton, Paul C. Kocher, Netscape Communications Corp., 1996.
Available at: http://www.netscape.com/eng/ssl3/

[21] **Uniform Resource Locators (URL).** T. Berners-Lee, L. Masinter, M. McCahill, RFC1738, December 1994.
Available at: http://www.rfc-editor.org/rfc/rfc1738.txt

[22] **Practical Unix & Internet Security, 2nd Edition**. Simson Garfinkel & Gene Spafford, O'Reilly, ISBN 1-56592-148-8, April 1996.
Available at: http://www.oreilly.com/catalog/puis/

23 **AAA Authorization Framework**. J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence. RFC 2904, August 2000.
Available at: http://www.rfc-editor.org/rfc/rfc2904.txt

[24] **Uniform Resource Identifiers (URI): Generic Syntax**. T. Berners-Lee, R. Fielding, L. Masinter. RFC 2396, August 1998.
Available at: http://www.rfc-editor.org/rfc/rfc2396.txt

[25] **Authentication Methods for LDAP**. M. Wahl, H. Alvestrand, J. Hodges, R. Morgan. RFC 2829, May 2000.
Available at: http://www.rfc-editor.org/rfc/rfc2829.txt

[26] **Whatis: IT-specific encyclopedia**. On-going.
Available at: http://whatis.techtarget.com/

[27] **Simple Authentication and Security Layer (SASL)**. J. Myers, RFC 2222, October 1997.
Available at: http://www.rfc-editor.org/rfc/rfc2222.txt

[28] **Merriam-Webster Collegiate Dictionary**. CDROM version 2.5, 2000.
An online version is available at: http://www.m-w.com/

[29] **Kerberos: An Authentication Service for Open Network Systems**. J.G. Steiner, C. Neumann, and J.I. Schiller, USENIX, Winter 1988.
Available at: http://sunsite.utk.edu/net/security/kerberos/usenix.PS

[30] **Risk Management is Where the Money Is**. Daniel Geer, 3-Nov-1998 presentation to Digital Commerce Society of Boston, as reprinted in Risks Digest, Wed, 11 Nov 1998 22:20:09 –0500.
Available at: http://catless.ncl.ac.uk/Risks/20.06.html#subj1.1

[31] **Policy Terminology**. Westerinen et al. Work-in-progress INTERNET-DRAFT, draft-ietf-policy-terminology-02.txt.
Available at: http://www.ietf.org/internet-drafts/draft-ietf-policy-terminology-02.txt

[32] **X.509 4th Edition 2001: PUBLIC-KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS**. ITU-T, COM 7-250-E Revision 1, Feb 23, 2001.
Available at: http://www.itu.int/itudoc/itu-t/rec/x/x500up/x509.html

References are continued on the next page…

[33] **OASIS Security Services TC Use Case and Requirements Conference Call Consensus**. Consensus on the wording for this item occurred during one or more conference calls of the SSTC Use Case and Requirments subgroup. See minutes of the conference calls in the security-use email distribution list archives for details.

Available at: http://lists.oasis-open.org/archives/security-use/

[34] **Security Frameworks for Open Systems: Authentication Framework**. ITU-T Recommendation X.811 (1995 E), ISO/IEC 10181-2: 1996 (E).

Available at: http://www.itu.int/itudoc/itu-t/rec/x/x500up/x811.html

[35] **Information Security An Integrated Collection of Essays**. M. Abrams, S. Jajodia, and H. Podell, eds. IEEE Computer Society Press, January 1995.

[36] Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation 6 October 2000.
Available at: http://www.w3.org/TR/2000/REC-xml-20001006

[37] Uniform Resource Identifiers (URI): Generic Syntax. T. Berners-Lee, R. Fielding, L. Masinter. August 1998.
Available at: http://www.rfc-editor.org/rfc/rfc2396.txt