OASIS Security Services TC Glossary

draft-sstc-glossary-01

Contributors (alphabetically):

Carlisle Adams, Entrust
Zahid Ahmed, CommerceOne
Marlena Erdos, Tivoli
Jeff Hodges, Oblix (editor)
Maryann Hondo, IBM
Hal Lockhart, Entegrity
Prateek Mishra, Netegrity
RL “Bob” Morgan, University of Washington
Eve Maler, Sun
Tim Moses, Entrust
David Orchard, Jamcracker
Darren Platt, Securant
Evan Prodromou, Outlook Technologies
Irving Reid, Balimore

16 July 2001

1. Status of this Document

This document is an OASIS-Draft and is (for the most part) in conformance with relevant OASIS SSTC document standards.

Send overall comments on this document to: security-services@lists.oasis-open.org, though this document, as of this update, been most actively discussed on the security-use@lists.oasis-open.org list and comments to that list about this document are just find, too.

The OASIS Security Services Technical Committee (SSTC) web pages and document repository are available here:

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

1.1. Version History

1.1.1. Document Filenames and Links

This document: **draft-sstc-glossary-01.doc**
draft-sstc-glossary-01.pdf

Prior version of this document: **draft-sstc-glossary-00.doc**

1.1.2. Modification Log

Date	**By Whom**	**What**
21 Jan 2001 v00	Jeff Hodges	Created.
8 Feb 2001 v01	Jeff Hodges	Added various terms supplied by Bob Blakley, and others culled from S2ML 0.8a doc.
9 Feb 2001 v01	Jeff Hodges	Cleaned up refs, added refs, added definitions, enhanced or otherwise mangled others.
30 Mar 2001 v00	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.
Xx Jul 2001 – v01	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.

2. Introduction

This document comprises an overall glossary for the OASIS Security Services Technical Committee (SSTC) and it's subgroups. Individual SSTC documents and/or subgroup documents may either reference this document and/or "import" select subsets of terms.

The sources for the terms and definitions herein are referenced in Appendix A. Please refer to those sources for definitions of terms not explicitly defined here. Where possible and convenient, hypertext links directly to definitions within the aforementioned sources are included. Some definitions are quoted directly from the sources, some are modified to fit the context of the OASIS SSTC (aka SAML) effort.

2.1. Style of use by other SAML documents

Other SAML documents may either or both (a) include copies of definitions herein (define by value), (b) refer to this document and the applicable definitions (define by reference). In the case of (a), editors of those documents should work with the glossary editor in order to normalize the value(s) of the definitions.

3. Notation

Definitions that need to be added (i.e. the entry is presently blank), decisions made about, or otherwise enhanced are marked with a **?.**

Definition senses and/or options – i.e. we need to decide which one(s) to base our usage on -- are denoted by “(a)”, “(b)”, and so on.

Definitions that’ve been specifically agreed to by the Use Case & Requirements (security-use@oasis-open.org) subgroup are denoted by reference to “[33]”.

Entries with a definition of “**?** (xxx)” means that at least the document editor suspects we need to condsider defining this term, and we haven’t yet discussed it and/or no-one’s taken a stab at defining it and/or we might actually not need to define it.

Editorial comments are highlighted like so. Some may also have comments attached at the end of the document.

4. Notes

Clarifications & Musings

It will arguably be reasonable to refer to a system implementing & using SAML as a “A”, “AA”, or “AAA” service – which one depending upon the functionality of the version of SAML being used, what the SSTC decides the functionality of the (potentially) various versions of SAML turn out to be, and so on. Looking ahead, may want to coin a phrase such as “a SAML-based AAA service”, and think about contracting that phrase into a shorter term.

5. The Glossary

Access	To interact with a system entity in order to manipulate, and/or use, and/or 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 (ACI)	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 ACI may be specific to the request itself, others may be associated with the connection via which the request is transmitted, others (e.g. 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, e.g. accessing a resource.
Administrative Domain	An environment or context that is defined by some combination of administrative policies, Internet Domain Name registration(s), civil legal entity(ies) (e.g. individual(s), corporation(s), or other formally organized entity(ies)), 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 (e.g. 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, constituting a declaration of identity, or attribute information, or authorizations.
Asserting Party	Formally, the administrative domain hosting SAML authorities who are issuing assertions. Informally, an instance of a assertion-issuing SAML authority.

Attribute	A distinct characteristic of an object. An object's attributes are said to describe the object. Objects' attributes are often specified in terms of their 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, etc. Which attributes of an object are salient is decided by the beholder.
Attribute Authority	A system entity that produces SAML attribute assertions. [33]
Attribute Assertion	An assertion 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 authenticates a subject.
Authentication Authority	A system entity that produces SAML authentication assertions. [33]
Authorization	The process of determining which types of activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated an entity, the entity may be authorized different types of access or activity. [8] <rough>The "act of authorization" is when an AEF acts upon information received from an ADF.</rough> The (act of) granting of access rights to a subject (for example, a user, or program). [12]
Authorization Decision	The result of evaluating, against applicable security policy expressions, a request to access a resource.
Authorization Decision Assertion	An assertion that conveys an authorization decision.
Credential	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 (e.g. a string) uniquely mapped to a system entity, thus identifying it. See Principal Identity.
Login Logon Signon	The process of presenting credentials to an authentication authority, establishing a simple session, and optionally establishing a rich session.
Logout Logoff Signoff	The process whereby a user signifies their desire to terminate their simple session or rich session.
Keep-alive	
Party	Informally a principal or principals participating in some process or communication, such as receiving a SAML assertion, or accessing a resource. See Asserting Party.

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-based PDP consumes Authorization Decision Assertion Requests, and produces Authorization Decision Assertions in response.
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions. [31] For example, a SAML-based PEP sends Authorization Decision Assertion 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.
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 actively provide information to a system entity, who did not explicitly request it.
Relying Party	A system entity who is making a decision contingent upon information or advice from another system entity. E.g. a system entity that is relying upon various SAML assertions about some other party(ies), made by yet other party(ies).
Requester	As in "service requester", or "requester of resources". A system entity that is utilizing a protocol to request services from a service. Essentially functionally equivalent to the term client, but often used rather than "client" because many system entities simultaneously and/or serially act as both clients and servers.
Resource	(a) Data contained in an information system (e.g. in the form of files, information in memory, etc); or a service provided by a system; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment. [4]
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, e.g. active roles and passive roles. The notion of an Administrator is often an example of a role.
SAML Authority	One of the set of abstract authorities defined in the SAML domain model.
Security	Security refers to a collection of safeguards that ensure the confidentiality of information, protect the system(s) or network(s) used to process it, and control access to it (them). Security typically encompasses the concepts/topics/themes 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 (a) the security services that a system is required to provide to meet the needs of its users, (b) the system elements required to implement the services, and (c) the performance levels required in the elements to deal with the threat environment. A complete system security architecture addresses administrative security, communication security, computer security, emanations security, personnel security, and physical security. It prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental kinds of 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 typically scrutinized in the context of a security policy.
Security Assertion Markup Language (SAML)	SAML is the name for a specification describing set of security assertions that are encoded using XML, the request/response protocols used to obtain the security assertions, and the bindings of these protocols to various transfer protocls (e.g. SOAP, BEEP, HTTP, etc.).
Security Domain	An environment or context that is defined by security policies, security models, and a security architecture, including a set of resources and set of system entities that are authorized to access the resources. An administrative domain may contain one or more security domains. 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	Concisely, a security policy expression is a mapping of principal identities, and/or attributes thereof, with authority to act [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. E.g. an authentication service, a PKI-based document attribution & authentication service. Security Service describes 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 iinteraction.
Site	A term commonly used to refer to an administrative domain in geographical and/or DNS name sense. Thus *site* may refer to a particular geographical and/or topological subportion of an administrative domain, or, a site may contain multiple administrative domains, as may be the case at an ASP site.
Subject	A principal, in the context of a security domain, about which a given assertion makes a statement.
System Entity	An active element of a computer/network system--e.g., an automated process or set of processes, a subsystem, a person or group of persons--that incorporates a distinct set of functionality. [4] [33]

Timein	
Timeout	A period of time after which some condition becomes true if some event has not occurred. For example, A session whose state has been inactive for a specified period of time is said to “timeout”.
User	A natural person that makes use of a system and its resources for any purpose [33] See also Administrator, End User.
Uniform Resource Identifier	A compact string of characters for identifying an abstract or physical resource. See [37] [21].
Uniform Resource Locator (URL)	Defined as “a compact string representation for a resource available via the Internet.” URLs are a subset of URI. See [37] [21].
XML (Extensible Markup Language)	Extensible Markup Language, abbreviated XML [36], describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language [ISO 8879]

Appendix A. 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. Jamcraker 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.
On-line 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

References are continued on the next page…

[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

[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 on-line 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

References are continued on the next page…

[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

[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