OASIS Security Services TC Glossary

draft-sstc-ftf3-glossary-00.doc

Incorporates draft-sstc-glossary-00.doc

20 June 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-00.doc**
draft-sstc-glossary-00.html
draft-sstc-glossary-00.pdf

Prior version of this document: **draft-sstc-hodges-glossary-01.html**

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.

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.

Candidates for removal

These are term that the editor thought more folks than just himself ought to think about removing.

AAA Server	- synonymous with a PDP?
Access Control Factors	- synonymous with access control information?
Actor	- synonymous with principal?
Authc	- synonymous with authn?
Clearance	- specific to Multilevel Security (MLS)
Label	- specific to Multilevel Security (MLS)
Policy Decision	- essentially synonymous with Access Control Decision.
Receiving Site	- synonymous with Relying party.

77 # 5. The Glossary

AA or AAA	"Authentication and Authorization", or "Authentication, Authorization, and Accounting (or Auditing)" – each of the "A"s being a *general class* of security mechanism. These mechanisms are key building blocks for implementing security architectures and security services.
ACI	See Access Control Information.
ADF	See Access Control Decision Function.
ADI	See Access Control Decision Information.
AEF	See Access Control Enforcement Function.
AP	See Asserting Party.
AAA Administrative Component	An AAA system component whose users are typically administrators and whose function is mangement of various aspects of a AAA system deployment.
AAA Service	A network service providing AAA or AA functionality. AAA services typically implement portions of security policies, and are implemented by security mechanisms. AAA services are essentially a subset of security services, but the terms are sometimes informally used synonymously.
AAA Server	A system entity that is also an AAA system component whose function is to make policy decisions on behalf of requesters. It accepts and answers queries via some network protocol (TBD). It may or may not rely on information stored in a (external) repository, e.g. in a directory service, or a RDBMS, etc. [23]
AAA System	A set of AAA system components delivering a AAA service.
AAA System Component	**?** A system entity that is one of the identifiable components of embodiments of AAA systems.
AAA System Deployment	An instance of a deployed AAA system. An AAA System Deployment is typically hosted within, and delivers security services to, a given administrative domain, It also may be utilized to provide such services to other administrative domains.
Access	The ability and means to communicate with, or otherwise interact with, a system entity in order to manipulate, and/or use, and/or gain knowledge of, some (or all) of a system entity's system resources. [4]
Access Control	1. Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized system entities (users, programs, processes, or other systems) according to that policy. [4] 2. The prevention of unauthorized access of a resource, including the prevention of use of a resource in an unauthorized manner. [9]
Access Control Decision	**?** The decision arrived at as a result of evaluating the requester's identity, the requested operation, and the requested resource in light of applicable security policy. (surprisingly enough, not explicitly defined in [10])

Access Control Decision Function	A specialized function that makes access control decisions by applying access control policy rules to an access request, access control decision information (of initiators, targets, access requests, or that retained from prior decisions), and the context in which the access request is made [10].
Access Control Decision Information	The portion (possibly all) of the Access Control Information made available to the Access Decision Function in making a particular access control decision [10].
Access Control Enforcement Function	A specialized function that is part of the access path between an initiator and a target on each access request and enforces the decision made by the Access Control Decision Function [10].
Access Control Information	Any information used for access control purposes, including contextual information [10].
Access Control Factors	A request, when being processed by a server, may be associated with a wide variety of security-related *factors* (e.g. section 4.2 of [17]). The server uses these factors to determine whether and how to process the request. These are called *access control factors* (ACFs). They might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Some factors 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 Control Policy	The set of rules that define the conditions under which an access may take place [10].
Access Control Policy Rules	**?** Security policy rules concerning the provision of the access control service [10].
Access Path	**?** (haven't been able to find a concise def for this with a modicum of looking**)**
Access Permissions	**?** (xxx)
Access Privileges	**?** (xxx)
Access Rights	**?** (xxx)
Access Request	The operations and operands that form part of an attempted access of a system resource. An access request may be communicated between parties via a request. [10]
Active Role	**?** A role that an actor has donned when performing some operation, e.g. accessing a resource.
Actor	**?** From [2]: A computational entity [i.e. system entity] utilizing security services. Examples of actors include application servers, application programs, security services (?), transport and message-level interceptors etc. Perhaps actor is effectively synonymous with system entity.

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, maintains, and/or makes use of the resources of a AAA System Deployment for system management and/or user management and/or content management purposes (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. See also deployer.
Anonymity	The quality or state of being anonymous.
Anonymous	The condition of having a name [or identity] that is unknown or concealed. [4]
Application Server	A software system run on a host that provides an execution environment for higher-level applications, for example business-oriented apps.
Assertion	(a) A piece of data constituting a declaration of identity or authorizations. See also: credential. **?** (b) "Data that is transferred to establish the claimed identity of an entity." [9]
Asserting Party	**?** An issuer of assertions.
Attack	An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. [4]
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, address, phone number, 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. Attributes are of various types, and are often represented by an attribute name along with one or more attribute values. See also Attribute Value Assertion, entry. [11] [17]
Attribute Authority	**?** (a) A system entity that produces Attribute assertions, based upon TBD inputs. [33] (b) An authority which assigns privileges by issuing attribute certificates. [32]
Attribute Assertion	**?** An assertion about attributes of a principal.

Attribute Name	The human-palatable name associated with a particular attribute type.
Attribute List	A data structure consisting of lists of attribute value assertions (aka name-value pairs). [12]
Attribute Type	An attribute type typically governs whether an attribute is single- or multi-valued, the syntax to which the values must conform, the kinds of matching which can be performed on values of that attribute, and other functions. [17]
Attribute Value	An attribute value is one or more pieces of data, encoded according to the syntax of the attribute's type. [17]
Attribute Value Assertion	An Attribute Value Assertion is an assertion with the general abstract form of "attribute type IS attribute value". [17]
Audit	Independent review and examination of records and activities to determine compliance with established usage policies and to detect possible inadequacies in product technical security policies of their enforcement. [8]
Audit Identity	An identity attribute containing an identity used only for accountability purposes. [13]
Authc	See Authentication
Authn	See Authentication
Authz	See Authorization
Authenticate	**?** (a) To verify (i.e., establish the truth of) an identity claimed by or for a system entity. [4] [8] (b) "to authenticate" – the act of presenting one's credentials in order to become authenticated.
Authentication	**?** (a) Authentication is the process of confirming a system entity's asserted principal identity with a specified, or understood, level of confidence. [7] [33] (b) The process of verifying a principal identity claimed by or for a system entity. [12] [33]
Authentication Assertion	Data vouching for the occurrence of an authentication of a principal at a particular time using a particular authentication mechanism. Synonym(s): name assertion.
Authentication Authority	A system entity that verifies credentials and produces authentication assertions. [33]

Authentication Mechanism	**?** *Examples*.. • Simple username & password. • Kerberos • Client-side (and server-side) authn via the TLS/SSL "handshake protocol" during TLS/SSL session establishment. • Any SASL mechanism. JeffH hasn't yet found a concise and referenceable def for this term.
Authority	An identified computer-based entity implementing a security service (e.g. creation of assertions, credentials, PACs, and so on). [12]
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 Assertion	**?** In concept, an authorization assertion is a statement of policy about a resource, such as: The user "noodles" is granted "execute" privileges on the resource "/usr/bin/guitar." Should this be Authorization Decision?
Authorization Attribute	Attributes about a principal which may be useful in an authorization decision (group, role, title, contract code,...). [33]
Authorization Data	A data structure that contains Authentication Assertions and Authorization attributes.
Authorization Identity	**?** An authorization identity is one kind of access control factor. It is the name of the user or other entity that requests that operations be performed. Access control policies are often expressed in terms of authorization identities; e.g., entity X can perform operation Y on resource Z. [25] The transmitted authorization identity may be different than the identity in the client's authentication credentials. This permits agents such as proxy servers to authenticate using their own credentials, yet request the access privileges of the identity for which they are proxying. [27]
Authorized	A system entity or actor is "authorized" if it is granted a right or a permission or a capability to access a system resource. See also authorization.
Capability	A token that gives its holder the right to access a system resource. Possession of the token is accepted by the access control mechanism as proof that the holder has been authorized to access the resource named or indicated by the token. [12]

Clearance	Initiator-bound ACI that can be compared with security labels of targets [10].
Client	A system entity that requests and uses a service provided by another system entity, called a "server". [4]
Context	**?** See Contextual Information. (we may actually want to use a much more general, commonplace definition of context – i.e. what we mean when we're waving our hands and saying something like "that all depends upon the context". This because contextual information is defined narrowly.
Contextual Information	Information about or derived from the context in which an access request is made (e.g. time of day). [10]. Effectively synonymous with access control factors.
Control Attribute	**?** Attributes, associated with a security object that, when matched against the privilege attributes of a security subject, are used to grant or deny access to the security object. [19]
Credential	**?** (a) Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity. (See also: assertion, authentication information, capability, ticket.) [4] (b) Data that is transferred to establish a claimed principal identity. [9] [33] --- We need to decide between (a) and (b).
Decision	The response of an Access Control Decision Function to a decision request [12], using terminology from [10]. See also access control decision.
Decision Request	The message an Access Control Enforcement Function sends to an Access Decision Function to ask it whether a particular access request should be granted or denied [12] , using terminology from [10].
Deployer	An administrator in the act of, and/or (sometimes) primarily responsible for deploying a particular system or systems in an administrative domain's network infrastructure. This may involve configuring the system or systems to interact with systems of other administrative domains.
Deployment Time	The time at which a system is actually configured, tested, and/or put to use, as opposed to its being in the vendor's development pipeline or in transit between the vendor and a customer. See also site-specific.
DMZ	"DMZ" is from the military term for an area between two opponents where fighting is prevented. See also [6] and DMZ network.
DMZ network	DMZ network is a commonly-used, equivalent term for (see also) perimeter network.
End User	An entity, usually a human individual, that makes use of resources for application purposes (as opposed to system management purposes. See Administrator).
End User's Computer	A host that an end user makes use of for general computational, application, and communication purposes.

End User Profile	Various attributes and attribute values, mapped to a given end user. User attributes are stored in the profile, e.g. identifier(s), name(s), contact information, organizational information, computing infrastructure information, etc. Profiles are often implemented as directory entries.
End User System	Typically the combination of: an End User, plus the End User's computer, plus the browser running on that computer. End User system is (often? sometimes?) used, in place of the terms "client" or "user" because there are often many components that act as clients of other components, and which may not be directly and/or actively controlled by a user.
Entitlement	**?** (a) A data structure containing Access Control Decision Information and/or access control policy rule information in a form usable by applications to, for example, customize their behavior based on access control policy or to make access control decisions in their own code [12] , using terminology from [10]. (b) a digitally signed XML assertion consisting of a "portable" package of authorization data created by an issuing authority concerning an authenticated subject. [2]
Entity	See System Entity.
EU System	See End User System.
EUS	See End User System.
External Network(s)	Networks outside one's administrative domain and (in typical usage of the term) with which one's networks are connected.
Extranet	The part of a company or organization's computer network which is available to outside users, for example, information services for customers and/or suppliers. [14] See also extranet in [6].
Firewall	A firewall is a device that gives an administrative domain a means to control how their internal network(s) interact with external networks.
Firewall boundary	A commonly-used term referring to a security perimeter that is largely defined by the presence of one or more firewalls.
Host	A computer that is attached to a communication subnetwork or internetwork and can use services provided by the network to exchange data with other attached systems. A host is distinguished from other similarly connected and addressable devices on the network, e.g. routers, in that it doesn't forward Internet Protocol packets that are not addressed to it. A host may be either an end user's computer or a server. [8]
Identity	A representation (e.g. a string) uniquely mapped to a system entity (e.g. an end user, an administrator, a host, or some process, or some network device).
Initiator	An entity (e.g. human user or computer-based entity) that *attempts to access* other entities [10].

Intermediary	? An entity which, after receiving an access request from an initiator, issues another access request on that initiator's behalf [12]. This is a narrow definition of intermediary and is essentially the same a "proxy". We need to carefully think about our use of this term and carefully define it and associated terms.
Internal Network	See Intranet.
Intranet	A local area network which may or may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's web documents. [14] See also intranet in [6].
Issuer	? A system entity that issues stuff, e.g. an issuer of assertions. [2]
Label	A marking that is bound to a protected resource and that names or designates the security-relevant attributes of that resource (derived from [9]).
Network-based security	The notion of controlling network access and usage, and consequently protecting hosts from attack, via network routing configuration and filtering, the use of firewalls and similar devices, or some combination thereof. See also [5].
Network Device or Network Element	For the purposes of this document, one of routers, bridges, repeaters, hubs, switches, etc.
Network Service	Work performed (or offered) by a server over a network. This may mean simply serving simple requests for data to be sent or stored (as with web servers); or it may be more complex work, such as that of print servers, distributed file servers, X Windows servers, AAA servers, or application servers. (definition largely from [6])
Network Topology	A configuration of network devices and hosts, and their interconnections.
Operation	The action that an initiator's access request asks to have performed on a protected resource [12].
Origin Server	The server on which a given resource resides or is to be created. [16]
Origin Site, Originating Site	? The site where the origin server resides.
PAC	See Privilege Attribute Certificate.
PDP	See Policy Decision Point.
PEP	See Policy Enforcement Point.
Package	= assertions [+ entitlements] + payload ?
Party	? An actor or actors (principal or principals) participating in some process or communication, such as accessing a resource. See also: access request, system entity, user.
Passive Role	? A role that a resource effectively dons when it is the *object* of some operation.

Payload	The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination. Note that what constitutes the payload may depend on the point-of-view. To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include the part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end user (or whatever entity) at the destination. [26]
Perimeter Network	A network between external networks and internal networks whose explicit role is to facilitate creation and management of additional layer(s) of security (as compared to not having a perimeter network). Also sometimes called a DMZ network. See also [5].
Perimeter Security	Network-based security applied at the perimeter of one's security domain. See also [5].
Policy, Policies	**?** Concisely, a policy is a mapping of user credentials with authority to act [8]. Policies are often essentially access control *lists*. [8]
Policy Decision	**?** essentially synonymous with Access Control Decision.
Policy Decision Point	**?** (a) A [system] entity that makes policy decisions for itself or for other system entities that request such decisions. [31] (b) Synonymous with Access Control Decision Function. [10] (c) Synonymous with AAA Server. --- JeffH feels that (a) and (b) are essentially equivalent and we need to decide whether.. 1. we use (a) "as is", or, 2. we use (b) "as is" (this would mean moving the def for Access Control Decision Function to this location), or, 3. we use (c) "as is", or, 4. we blend the three definitions together Selecting any of the above options involves deleting the entries for Access Control Decision Function and AAA Server from this doc, and updating all definitions using those terms to use the new terms.

Policy Enforcement Point	**?** (a) A [system] entity that [requests and subsequently] enforces policy decisions. [31] (b) Synonymous with Access Control Enforcement Function. [10] --- JeffH feels that (a) and (b) are essentially equivalent and we need to decide whether.. 1. we use (a) "as is", or, 2. we use (b) "as is" (this would mean moving the def for Access Control Enforcement Function to this location), or, 3. we blend the two definitions together. Selecting any of the above options involves deleting the entry for Access Control Enforcement Function itself from this doc, and updating all definitions using those terms to use the new terms.
Principal Principal Identity	**?** (a) AAA Service clients are sometimes called *principals* in order to distinguish them from clients of other services, and perhaps their own clients, if they are themselves servers. Note that a AAA service principal may be any form of system entity. [29] (b) An instantiation of a system entity within the security domain. [33] (c) An entity whose identity can be authenticated. [34]
Privilege Attribute	An attribute associated with an initiator that, when matched against control attributes of a protected resource is used to grant or deny access to that protected resource (derived from ECMA TR/46 definition). [19]
Privilege Attribute Certificate	A data structure containing privilege attributes. May be signed by the authority which generated it [12].
Protected Resource	A target, access to which is restricted by an access control policy [12].
Protected Web Resources	Web resources whose availability to requesters is being managed, i.e. protected, via some access control mechanism.
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	**?** (xxx)
Push	**?** (xxx)
RP	See Relying Party.
Receiving Site	**?** A site that receives, interprets, and acts according to security assertions. Essentially synonymous to relying party.

Relying Party	? One who is making a decision contingent upon information or advice from another entity. E.g. an entity that is *relying* upon various security assertions about some other party(ies), made by yet another party(ies).
Resource	? Synonymous in this document for System Resource. JeffH feel's that we need to decide whether we use the term "resource" or "system resource" in this and other SAML docs. We need to choose one and use it consistently.
Request	? What clients make to servers. (need to enhance this ;)
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.
Risk	(a) In the computer system and networking sense: An *expectation of loss* expressed as the probability that a particular threat (or set of threats) will exploit a particular vulnerability (or set of vulnerabilities) with a particular harmful result(s). [8] (b) In general, the level of risk in a given context is inversely proportional to the level of trust the relationships within the context are accorded. [30] (c) More generally: possibility of loss or injury. [28]
Risk Analysis	Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of your risks, then ranking those risks by level of severity. For example, see the Risk Assessment section of Chapter 2 in [22].
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.
Scrutinize	To examine or observe with great care; inspect critically. [28]
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 Domain	An environment or context that is defined by security policies, *security models*, and a security architecture, including a set of system 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 Mechanism	The logic or algorithm that implements a particular security-enforcing or security-relevant function in hardware and software. [8]
Security Object	A system entity in a passive role to which a security policy applies. [19]
Security Package	**?** one or more security assertions or credentials combined into a single overall, for example, MIME-encoded data structure, or package.
Security Perimeter	The boundary of a security domain. [8]
Security Policy	A set of rules and practices specifying the "who, what, when, why, where, and how" of access to system resources by system entities (often, but not always, involving or acting on behalf of *people*). Significant portions of security policies are implemented via security services. Security policies are components of security architectures. [8]
Security Requirements	The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy [given the results of a risk analysis]. [8]
Security Service	A processing or communication service that is provided by a system to give a specific kind of protection to system 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. [8]
Security Subject	An entity in an active role to which a security policy applies. [19]
Server	A process or set of processes running on a host that provide a network service. See also Server Host. [8]
Server Host	A host on which a network service is being run. For example, the host upon which a web server is being run is one kind of a server host, referred to in this glossary as a web server host. Hosts regarded as server hosts are *typically not used simultaneously* as end users' computers, *but may be*.
Service	See Network Service.
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.
Site-specific	A thing or a thing's deployment configuration that is tailored on a site-by-site basis. For example, *how* a site configures and performs load balancing of incoming HTTP requests to web server hosts *is site-specific*. From a vendor's perspective, site-specific decisions are usually made at deployment time.

SSL/TCP/IP	A shorthand notation denoting a protocol stack consisting of the SSL session layer running over the TCP/IP layers. An application layer protocol, e.g. LDAP or HTTP, is typically run on top of the SSL layer (which in turn is running on top of TCP/IP), and uses that layer (SSL) for end-to-end connection security.
Subject	**?** An identifiable entity. See also security subject. We will likely be describing a subject in terms of a principal, e.g. a subject of a PK certificate identifies the principal the certificate binds the PK to.
System	(a) A specific IT installation, with a particular purpose and operational environment. (b) An assembly of computer and/or communications hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting, receiving, storing, and retrieving data, with the purpose of supporting users. (c) IT products assembled together - either directly or with additional computer hardware, software, and/or firmware - configured to perform a particular function within a particular operational environment. [35] by way of [8]
System Entity	An active element of a system--e.g., an automated process or set of processes, a subsystem, a person or group of persons--that incorporates a specific set of capabilities. [4] [33] JeffH wonders if we shouldn't use a phrase other than "specific set of capabilities here because the latter might be confused with capabilities in the access control mechanism sense rather than generic capabilities something like a system entity might have or embody.
System 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 a system capability, such as processing power or communication bandwidth; 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] (b) Anything used or consumed while performing a function. [8] (c) Data contained in a system entity (e.g. in the form of files, information in memory, etc); or a service provided by a system entity; --- JeffH feels that (a) and (b) are essentially equivalent and we need to decide whether.. 1. we use (a) "as is", or, 2. we use (b) "as is", or, 3. we create another definition, perhaps based upon (a) &| (b), e.g. (c), and use that.

Target	? (a) An entity to which access may be attempted [10]. (b) A resource an entity attempts to access. JeffH suspects sense (b) is the one we should use.
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado). [4] See especially [8].
TCP or TCP/IP	See Transmission Control Protocol.
Ticket	? Aka a token. Specific example: Kerberos Tickets. See [RFC1510]. A ticket *may* be considered a credential.
Token	? See ticket.
Unauthorized	The opposite of a system entity or requester being authorized.
URL	See Uniform Resource Locator.
User	(a) A corporeal human making use of network services and/or application(s) inhabiting a given administrative domain(s), *as a means* rather than as an end. (based on “user” from [6]). See also Administrator, End User. (b) A human individual that makes use of resources for application purposes [33] --- JeffH feels that (a) and (b) are essentially equivalent and we need to decide whether.. 1. we use (a) “as is”, or, 2. we use (b) “as is”, or, 3. we blend the two definitions together.
User Profile or User’s Profile	See End User Profile.
User Session	A “container” for the authentication and attribute assertions that apply to a given system entity through the principals incarnated by that entity. The purpose is to maintain the relationship of the assertions to the initiating entity. [33]
Uniform Resource Locator	Defined as “a compact string representation for a resource available via the Internet.” See [21].
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. [4]

Web-based Service	A network service where requesters are typically web browsers being wielded by end-users, and where the content delivered to the end-users' browsers via the web servers is the network service's primary end-user interface.
Web Browser	A software application used to locate and display web pages.
Web Resource	Any object (e.g. a file (e.g. a web page), a program, or any other system resource) that is being made available to requesters via a web server. Also known as "web-accessible resource". The implication here is that one may make reference to, and access, a web resource via a URL.
Web Server	A server process running on a server host and answering HTTP requests (at least),and often also several other protocols (e.g. FTP, Gopher). See also HTTP Server in [6]. A web server is typically used to implement a web-based service.
Web Server Host	A host running a web server that is in turn providing some or all of the web resources accessible via the web server.
Web Service	See Web-based service.
Web Site	A web site is a site and/or administrative domain providing at least HTTP- (and often FTP-based) network services (sometimes called web services) to some set of users, with perhaps additional services offered based on yet other protocols such as LDAP . The distinguishing characteristic of a web site is that its users may make use of URLs to make reference to, and also to access, the web site's services and web resources.

78

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]

[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.