



Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0

OASIS Standard, 15 March 2005

Document identifier:

saml-glossary-2.0-os

Location:

<http://docs.oasis-open.org/security/saml/v2.0/>

Editors:

Jeff Hodges, Neustar
Rob Philpott, RSA Security
Eve Maler, Sun Microsystems

SAML V2.0 Contributors:

Conor P. Cahill, AOL
John Hughes, Atos Origin
Hal Lockhart, BEA Systems
Michael Beach, Boeing
Rebekah Metz, Booz Allen Hamilton
Rick Randall, Booz Allen Hamilton
Thomas Wisniewski, Entrust
Irving Reid, Hewlett-Packard
Paula Austel, IBM
Maryann Hondo, IBM
Michael McIntosh, IBM
Tony Nadalin, IBM
Nick Ragouzis, Individual
Scott Cantor, Internet2
RL 'Bob' Morgan, Internet2
Peter C Davis, Neustar
Jeff Hodges, Neustar
Frederick Hirsch, Nokia
John Kemp, Nokia
Paul Madsen, NTT
Steve Anderson, OpenNetwork
Prateek Mishra, Principal Identity
John Linn, RSA Security
Rob Philpott, RSA Security
Jahan Moreh, Sigaba
Anne Anderson, Sun Microsystems
Eve Maler, Sun Microsystems
Ron Monzillo, Sun Microsystems
Greg Whitehead, Trustgenix

45 **Abstract:**

46 This specification defines terms used throughout the OASIS Security Assertion Markup Language
47 (SAML) specifications and related documents.

48 **Status:**

49 This is an **OASIS Standard** document produced by the Security Services Technical Committee. It
50 was approved by the OASIS membership on 1 March 2005.

51 Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)
52 [services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by filling out the web form located
53 at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The
54 committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog
55 of any changes made to this document.

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

60 **Table of Contents**

61 1 Glossary.....4
62 2 References.....13

1 Glossary

63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103

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.

Some definitions have multiple senses provided. They are denoted by (a), (b), and so on. References to terms defined elsewhere in this glossary are italicized.

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

Term

Definition

Access	To interact with a <i>system entity</i> in order to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's <i>resources</i> . [RFC2828]
Access Control	Protection of <i>resources</i> against unauthorized <i>access</i> ; a process by which use of resources is regulated according to a <i>security policy</i> and is permitted by only authorized system entities according to that policy. [RFC2828]
Access Control Information	Any information used for <i>access control</i> purposes, including contextual information [X.812]. 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 a request itself, some may be associated with the connection via which a request is transmitted, and others (for example, time of day) may be "environmental". [RFC2829]
Access Rights	A description of the type of authorized interactions a <i>subject</i> can have with a <i>resource</i> . Examples include read, write, execute, add, modify, and delete. [Taxonomy]
Account	Typically a formal business agreement for providing regular dealings and services between a <i>principal</i> and business service providers.
Account Linkage	A method of relating <i>accounts</i> at two different <i>providers</i> that represent the same <i>principal</i> so that the providers can communicate about the principal. Account linkage can be established through the sharing of <i>attributes</i> or through <i>identity federation</i> .
Active Role	A role that a <i>system entity</i> has donned when performing some operation, for example <i>accessing a resource</i> .

104	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.
105		
106		
107		
108		
109		
110		
111		
112		
113		
114		
115		
116		
117	Administrator	A person who installs or maintains a system (for example, a SAML-based security system) or who uses it to manage <i>system entities</i> , users, and/or content (as opposed to application purposes; see also <i>End User</i>). An administrator is typically affiliated with a particular <i>administrative domain</i> and may be affiliated with more than one administrative domain.
118		
119		
120		
121		
122		
123	Affiliation, Affiliation Group	A set of <i>system entities</i> that share a single <i>namespace</i> (in the federated sense) of <i>identifiers</i> for <i>principals</i> .
124		
125	Anonymity	The quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed. [RFC2828]
126		
127		
128	Artifact	See SAML Artifact.
129	Assertion	A piece of data produced by a <i>SAML authority</i> regarding either an act of <i>authentication</i> performed on a <i>subject</i> , <i>attribute</i> information about the subject, or <i>authorization</i> data applying to the subject with respect to a specified <i>resource</i> .
130		
131		
132		
133	Asserting Party	Formally, the <i>administrative domain</i> that hosts one or more <i>SAML authorities</i> . Informally, an instance of a <i>SAML authority</i> .
134		
135	Attribute	A distinct characteristic of an object (in SAML, of a <i>subject</i>). An object's <i>attributes</i> 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. Attributes are often represented as pairs of "attribute name" and "attribute value(s)", e.g. "foo" has the value "bar", "count" has the value 1, "gizmo" has the values "frob" and "2", etc. Often, these are referred to as "attribute value pairs". Note that <i>Identifiers</i> are essentially "distinguished attributes". See also Identifier and XML attribute.
136		
137		
138		
139		
140		
141		
142		
143		
144		
145		
146	Attribute Authority	A <i>system entity</i> that produces <i>attribute assertions</i> . [SAMLAgree]
147	Attribute Assertion	An <i>assertion</i> that conveys information about <i>attributes</i> of a <i>subject</i> .
148		
149	Authentication	To confirm a <i>system entity's</i> asserted <i>principal identity</i> with a specified, or understood, level of confidence. [CyberTrust] [SAMLAgree]
150		
151		

152	Authentication Assertion	An <i>assertion</i> that conveys information about a successful act of <i>authentication</i> that took place for a <i>subject</i> .
153		
154	Authentication Authority	A <i>system entity</i> that produces <i>authentication assertions</i> .
155		[SAMLAgree]
156	Authorization	The process of determining, by evaluating applicable <i>access control information</i> , whether a <i>subject</i> is allowed to have the specified types of <i>access</i> to a particular <i>resource</i> . Usually, authorization is in the context of <i>authentication</i> . Once a subject is authenticated, it may be authorized to perform different types of access. [Taxonomy]
157		
158		
159		
160		
161		
162	Authorization Decision	The result of an act of <i>authorization</i> . The result may be negative, that is, it may indicate that the <i>subject</i> is not allowed any <i>access</i> to the <i>resource</i> .
163		
164		
165	Authorization Decision Assertion	An <i>assertion</i> that conveys information about an <i>authorization decision</i> .
166		
167	Back Channel	Back channel refers to direct communications between two <i>system entities</i> without “redirecting” messages through another system entity such as an HTTP client (e.g. A user agent). See also <i>front channel</i> .
168		
169		
170		
171	Binding, Protocol Binding	Generically, a specification of the mapping of some given protocol's messages, and perhaps message exchange patterns, onto another protocol, in a concrete fashion. For example, the mapping of the SAML <AuthnRequest> message onto HTTP is one example of a binding. The mapping of that same SAML message onto SOAP is another binding. In the SAML context, each binding is given a name in the pattern “SAML xxx binding”.
172		
173		
174		
175		
176		
177		
178	Credentials	Data that is transferred to establish a claimed <i>principal identity</i> .
179		[X.800] [SAMLAgree]
180	End User	A natural person who makes use of resources for application purposes (as opposed to system management purposes; see <i>Administrator, User</i>).
181		
182		
183	Federated Identity	A <i>principal's identity</i> is said to be <i>federated</i> between a set of <i>Providers</i> when there is an agreement between the providers on a set of <i>identifiers</i> and/or <i>attributes</i> to use to refer to the Principal
184		
185		
186		
187	Federate	To link or bind two or more entities together [Merriam].
188	Federation	This term is used in two senses in SAML: <ul style="list-style-type: none"> a) The act of establishing a relationship between two entities [Merriam]. b) An association comprising any number of <i>service providers</i> and <i>identity providers</i>.
189	Front Channel	Front channel refers to the “communications channel” that can be effected between two HTTP-speaking servers by employing “HTTP redirect” messages and thus passing messages to each other via a user agent, e.g. a web browser, or any other HTTP client [RFC2616]. See also <i>back channel</i> .
190		
191		
192		
193		

194	Identifier	This term is used in two senses in SAML: <ul style="list-style-type: none"> c) One that identifies [Merriam]. d) A data object (for example, a string) mapped to a <i>system entity</i> that uniquely refers to the system entity. A system entity may have multiple distinct identifiers referring to it. An identifier is essentially a "distinguished attribute" of an entity. See also <i>Attribute</i>.
195 196 197	Identity	The essence of an entity [Merriam]. One's identity is often described by one's characteristics, among which may be any number of identifiers. See also <i>Identifier</i> , <i>Attribute</i> .
198 199	Identity Defederation	The action occurring when <i>Providers</i> agree to stop referring to a <i>Principal</i> via a certain set of <i>identifiers</i> and/or <i>attributes</i> .
200	Identity Federation	The act of creating a <i>federated identity</i> on behalf of a <i>Principal</i> .
201 202 203 204	Identity Provider	A kind of <i>service provider</i> that creates, maintains, and manages identity information for <i>principals</i> and provides principal authentication to other <i>service providers</i> within a <i>federation</i> , such as with web browser <i>profiles</i> .
205 206	Initial SOAP Sender	The SOAP sender that originates a SOAP message at the starting point of a SOAP message path. [WSGloss]
207 208 209	Login, Logon, Sign-On	The process whereby a <i>user</i> presents <i>credentials</i> to an <i>authentication authority</i> , establishes a <i>simple session</i> , and optionally establishes a <i>rich session</i> .
210 211	Logout, Logoff, Sign-Off	The process whereby a <i>user</i> signifies desire to terminate a <i>simple session</i> or <i>rich session</i> .
212 213 214 215 216 217	Markup Language	A set of <i>XML elements</i> and <i>XML attributes</i> 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 <i>XML schemas</i> and accompanying documentation. For example, the <i>Security Assertion Markup Language</i> (SAML) is defined by two schemas and a set of normative SAML specification text.
218 219 220	Name Qualifier	A string that disambiguates an <i>identifier</i> that may be used in more than one <i>namespace</i> (in the federated sense) to represent different <i>principals</i> .
221	Namespace	This term is used in several senses in SAML: <ul style="list-style-type: none"> e) (In discussing federated names) A domain in which an identifier is unique in representing a single principal. f) (With respect to authorization decision actions) A URI that identifies the set of action values from which the supplied action comes. g) (In XML) See <i>XML namespace</i>.
222 223 224	Party	Informally, one or more <i>principals</i> participating in some process or communication, such as receiving an <i>assertion</i> or accessing a <i>resource</i> .

225	Persistent Pseudonym	A privacy-preserving name <i>identifier</i> assigned by a <i>provider</i> to identify a <i>principal</i> to a given <i>relying party</i> for an extended period of time that spans multiple <i>sessions</i> ; can be used to represent an <i>identity federation</i> .
226		
227		
228		
229	Policy Decision Point (PDP)	A <i>system entity</i> that makes <i>authorization decisions</i> for itself or for other system entities that request such decisions. [PolicyTerm]
230		For example, a SAML PDP consumes authorization decision requests, and produces <i>authorization decision assertions</i> in response. A PDP is an “authorization decision authority”.
231		
232		
233		
234	Policy Enforcement Point (PEP)	A <i>system entity</i> that requests and subsequently enforces <i>authorization decisions</i> . [PolicyTerm] For example, a SAML PEP sends <i>authorization decision</i> requests to a PDP, and consumes the <i>authorization decision assertions</i> sent in response.
235		
236		
237		
238	Principal	A <i>system entity</i> whose identity can be authenticated. [X.811]
239	Principal Identity	A representation of a principal’s identity, typically an <i>identifier</i> .
240	Profile	A set of rules for one of several purposes; each set is given a name in the pattern “xxx profile of SAML” or “xxx SAML profile”.
241		<ul style="list-style-type: none"> a) Rules for how to embed <i>assertions</i> into and extract them from a protocol or other context of use. b) Rules for using SAML protocol messages in a particular context of use. c) Rules for mapping attributes expressed in SAML to another attribute representation system. Such a set of rules is known as an “attribute profile”.
242	Provider	A generic way to refer to both <i>identity providers</i> and <i>service providers</i> .
243		
244	Proxy	An entity authorized to act for another. <ul style="list-style-type: none"> a) Authority or power to act for another. b) A document giving such authority. [Merriam]
245	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. [RFC2828]
246		
247		
248	Pull	To actively request information from a <i>system entity</i> .
249	Push	To provide information to a <i>system entity</i> that did not actively request it.
250		
251	Relying Party	A <i>system entity</i> that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving <i>assertions</i> from an <i>asserting party</i> (a <i>SAML authority</i>) about a <i>subject</i> .
252		
253		
254		

255 256 257 258 259 260 261	Requester, SAML Requester	A <i>system entity</i> that utilizes the SAML protocol to request services from another system entity (a <i>SAML authority</i> , a <i>responder</i>). The term “client” for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the <i>initial SOAP sender</i> .
262 263	Resource	Data contained in an information system (for example, in the form of files, information in memory, etc), as well as: <ul style="list-style-type: none"> a) A service provided by a system. b) An item of system equipment (in other words, a system component such as hardware, firmware, software, or documentation). c) A facility that houses system operations and equipment. [RFC2828]
264 265		SAML uses <i>resource</i> in the first two senses, and refers to resources by means of <i>URI references</i> .
266 267 268 269 270 271 272	Responder, SAML Responder	A <i>system entity</i> (a <i>SAML authority</i>) that utilizes the SAML protocol to respond to a request for services from another system entity (a <i>requester</i>). The term “server” for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the <i>ultimate SOAP receiver</i> .
273 274 275 276 277	Role	Dictionaries define a role as “a character or part played by a performer” or “a function or position.” <i>System entities</i> 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.
278 279 280	SAML Authority	An abstract <i>system entity</i> in the SAML domain model that issues <i>assertions</i> . See also <i>attribute authority</i> , <i>authentication authority</i> , and <i>policy decision point (PDP)</i> .
281 282 283 284 285 286	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. [CyberTrust]
287 288 289 290 291 292 293 294 295 296 297 298 299	Security Architecture	A plan and set of principles for an <i>administrative domain</i> 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. [RFC2828]

300 301	Security Assertion	An <i>assertion</i> that is scrutinized in the context of a security architecture.
302 303 304 305 306 307	Security Assertion Markup Language(SAML)	The set of specifications describing <i>security assertions</i> that are encoded in <i>XML</i> , <i>profiles</i> for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and <i>bindings</i> of this protocol to various transfer protocols (for example, SOAP and HTTP).
308 309 310 311 312 313 314 315 316 317 318 319 320 321	SAML Artifact	A small, fixed-size, structured data object pointing to a typically larger, variably-sized SAML protocol message. SAML artifacts are designed to be embedded in URLs and conveyed in HTTP messages, such as HTTP response messages with "3xx Redirection" status codes, and subsequent HTTP GET messages. In this way, a service provider may indirectly, via a user agent, convey a SAML artifact to another provider, who may subsequently dereference the SAML artifact via a direct interaction with the supplying provider, and obtain the SAML protocol message. Various characteristics of the HTTP protocol and user agent implementations provided the impetus for concocting this approach. The HTTP Artifact binding section of [SAMLBind] defines both the SAML Artifact format and the SAML HTTP protocol binding incorporating it.
322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337	Security Context	<p>With respect to an individual SAML protocol message, the message's security context is the semantic union of the message's security header blocks (if any) along with other security mechanisms that may be employed in the message's delivery to a recipient. With respect to the latter, an examples are security mechanisms employed at lower network stack layers such as HTTP, TLS/SSL, IPSEC, etc.</p> <p>With respect to a system entity, "Alice", interacting with another system entity, "Bob", a security context is nominally the semantic union of all employed security mechanisms across all network connections between Alice and Bob. Alice and Bob may each individually be, for example, a provider or a user agent. This notion of security context is similar to the notion of "security contexts" as employed in [RFC2743], and in the Distributed Computing Environment [DCE], for example.</p>
338 339 340 341 342 343	Security Domain	An environment or context that is defined by security models and a <i>security architecture</i> , including a set of <i>resources</i> and set of <i>system entities</i> that are authorized to access the resources. One or more security domains may reside in a single <i>administrative domain</i> . The traits defining a given security domain typically evolve over time. [Taxonomy]
344 345 346 347 348 349	Security Policy	A set of rules and practices that specify or regulate how a system or organization provides <i>security services</i> to protect <i>resources</i> . Security policies are components of <i>security architectures</i> . Significant portions of security policies are implemented via security services, using <i>security policy expressions</i> . [RFC2828] [Taxonomy]
350 351 352	Security Policy Expression	A mapping of <i>principal identities</i> and/or <i>attributes</i> thereof with allowable actions. Security policy expressions are often essentially <i>access control</i> lists. [Taxonomy]

353	Security Service	A processing or communication service that is provided by a system to give a specific kind of protection to <i>resources</i> , where said resources may reside with said system or reside with other systems, for example, an <i>authentication</i> 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 <i>security policies</i> and are implemented via security mechanisms. [RFC2828] [Taxonomy]
354		
355		
356		
357		
358		
359		
360		
361	Service Provider	A <i>role</i> donned by a <i>system entity</i> where the system entity provides services to <i>principals</i> or other system entities.
362		
363	Session	A lasting interaction between <i>system entities</i> , often involving a <i>Principal</i> , typified by the maintenance of some state of the interaction for the duration of the interaction.
364		
365		
366	Session Authority	A <i>role</i> donned by a <i>system entity</i> when it maintains state related to <i>sessions</i> . <i>Identity providers</i> often fulfill this role.
367		
368	Session Participant	A <i>role</i> donned by a <i>system entity</i> when it participates in a <i>session</i> with at least a <i>session authority</i> .
369		
370	Site	An informal term for an <i>administrative domain</i> 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.
371		
372		
373		
374		
375	Subject	A <i>principal</i> in the context of a <i>security domain</i> . SAML assertions make declarations about <i>subjects</i> .
376		
377	System Entity, 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. [RFC2828] [SAMLAgree]
378		
379		
380		
381	Time-Out	A period of time after which some condition becomes true if some event has not occurred. For example, a <i>session</i> that is terminated because its state has been inactive for a specified period of time is said to “time out”.
382		
383		
384		
385	Transient Pseudonym	A privacy-preserving <i>identifier</i> assigned by an <i>identity provider</i> to identify a <i>principal</i> to a given <i>relying party</i> for a relatively short period of time that need not span multiple <i>sessions</i> .
386		
387		
388	Ultimate SOAP Receiver	The SOAP receiver that is a final destination of a SOAP message. It is responsible for processing the contents of the SOAP body and any SOAP header blocks targeted at it. In some circumstances, a SOAP message might not reach an ultimate SOAP receiver, for example because of a problem at a SOAP intermediary. An ultimate SOAP receiver cannot also be a SOAP intermediary for the same SOAP message. [WSGloss]
389		
390		
391		
392		
393		
394		
395	User	A natural person who makes use of a system and its resources for any purpose [SAMLAgree]
396		

397 398 399 400 401 402	Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical <i>resource</i> . [RFC2396] 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".
403 404 405	URI Reference	A <i>URI</i> that is allowed to have an appended number sign (#) and fragment identifier. [RFC2396] Fragment identifiers address particular locations or regions within the identified resource.
406 407 408 409	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. [XML]
410 411 412 413 414	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: <pre><Address AddressID="A12345">...</Address></pre> See also <i>attribute</i> .
415 416 417 418 419 420 421 422 423 424 425 426	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: <pre><Address AddressID="A12345"> <Street>105 Main Street</Street> <City>Springfield</City> <StateOrProvince> <Full>Massachusetts</Full> <Abbrev>MA</Abbrev> </StateOrProvince> <Post Code="56789"/> </Address></pre>
427 428 429 430 431	XML Namespace	A collection of names, identified by a <i>URI reference</i> , which are used in XML documents as element types and attribute names. An XML namespace is often associated with an <i>XML schema</i> . For example, SAML defines two schemas, and each has a unique XML namespace.
432 433 434 435 436 437 438 439 440	XML Schema	The format developed by the World Wide Web Consortium (W3C) for describing rules for a <i>markup language</i> to be used in 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.

2 References

441

- 442 **[CyberTrust]** Fred B. Schneider, editor. *Trust in Cyberspace*. Committee on Information
443 Systems Trustworthiness, National Research Council, ISBN 0-309-06558-5,
444 1999. See <http://www.nap.edu/readingroom/books/trust/> and glossary at
445 <http://www.nap.edu/readingroom/books/trust/trustapk.htm>.
- 446 **[DCE]** *DCE 1.2.2 Introduction to OSF DCE*. The Open Group, Catalog number F201,
447 ISBN 1-85912-182-9, Nov 1997. See
448 <http://www.opengroup.org/pubs/catalog/f201.htm>.
- 449 **[Merriam]** *Merriam-Webster Collegiate Dictionary*. CDROM Version 2.5, 2000. An online
450 version is available at <http://www.m-w.com>.
- 451 **[PolicyTerm]** A. Westerinen et al. *Terminology for Policy-Based Management*. IETF RFC 3198,
452 November 2001. See <http://www.ietf.org/rfc/rfc3198.txt>.
- 453 **[RFC2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax*. IETF
454 RFC 2396, August 1998. See <http://www.ietf.org/rfc/rfc2396.txt>.
- 455 **[RFC2616]** R. Fielding et al. *Hypertext Transfer Protocol – HTTP/1.1*. IETF RFC 2616, June
456 1999. See <http://www.ietf.org/rfc/rfc2616.txt>.
- 457 **[RFC2743]** J. Linn. *Generic Security Service Application Program Interface Version 2,
458 Update 1*, IETF RFC 2743, January 2000. See <http://www.ietf.org/rfc/rfc2743.txt>.
- 459 **[RFC2828]** R. Shirey. *Internet Security Glossary*. IETF RFC 2828, May 2000. See
460 <http://www.ietf.org/rfc/rfc2828.txt>.
- 461 **[RFC2829]** M. Wahl et al. *Authentication Methods for LDAP*. IETF RFC 2829, May 2000. See
462 <http://www.rfc-editor.org/rfc/rfc2829.txt>.
- 463 **[SAMLAgree]** *OASIS Security Services TC Use Case and Requirements Conference Call
464 Consensus*. Consensus on the wording for this item occurred during one or more
465 conference calls of the SAML Use Cases and Requirements subcommittee.
466 Meeting minutes are available at <http://lists.oasis-open.org/archives/security-use/>.
- 467 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
468 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os.
469 See <http://www.oasis-open.org/committees/security/>.
- 470 **[Taxonomy]** *Security Taxonomy and Glossary*. Lynn Wheeler, ongoing. See
471 <http://www.garlic.com/~lynn/secure.htm>. See <http://www.garlic.com/~lynn/> for the
472 list of sources.
- 473 **[X.800]** *Information processing systems – Open Systems Interconnection – Basic
474 Reference Model – Part 2: Security Architecture*. ISO 7498-2:1989, ITU-T
475 Recommendation X.800 (1991). See [http://www.itu.int/itudoc/itu-
476 t/rec/x/x500up/x800.html](http://www.itu.int/itudoc/itu-t/rec/x/x500up/x800.html).
- 477 **[X.811]** *Security Frameworks for Open Systems: Authentication Framework*. ITU-T
478 Recommendation X.811 (1995 E), ISO/IEC 10181-2:1996(E). See
479 <http://www.itu.int/itudoc/itu-t/rec/x/x500up/x811.html>.
- 480 **[X.812]** *Security frameworks for open systems: Access control framework*. ITU-T
481 Recommendation X.812 (1995 E), ISO/IEC 10181-3:1996(E). See
482 <http://www.itu.int/itudoc/itu-t/rec/x/x500up/x812.html>.
- 483 **[XML]** T. Bray et al. *Extensible Markup Language (XML) 1.0 (Third Edition)*. World Wide
484 Web Consortium Recommendation, February 2004. See
485 <http://www.w3.org/TR/2004/REC-xml-20040204>.
- 486 **[WSGloss]** H. Haas et al. *Web Services Glossary*, World Wide Web Consortium Note,
487 February 2004. See <http://www.w3.org/TR/ws-gloss/>.

Appendix A. Acknowledgments

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

- 491 • Conor Cahill, AOL
- 492 • John Hughes, Atos Origin
- 493 • Hal Lockhart, BEA Systems
- 494 • Mike Beach, Boeing
- 495 • Rebekah Metz, Booz Allen Hamilton
- 496 • Rick Randall, Booz Allen Hamilton
- 497 • Ronald Jacobson, Computer Associates
- 498 • Gavenraj Sodhi, Computer Associates
- 499 • Thomas Wisniewski, Entrust
- 500 • Carolina Canales-Valenzuela, Ericsson
- 501 • Dana Kaufman, Forum Systems
- 502 • Irving Reid, Hewlett-Packard
- 503 • Guy Denton, IBM
- 504 • Heather Hinton, IBM
- 505 • Maryann Hondo, IBM
- 506 • Michael McIntosh, IBM
- 507 • Anthony Nadalin, IBM
- 508 • Nick Ragouzis, Individual
- 509 • Scott Cantor, Internet2
- 510 • Bob Morgan, Internet2
- 511 • Peter Davis, Neustar
- 512 • Jeff Hodges, Neustar
- 513 • Frederick Hirsch, Nokia
- 514 • Senthil Sengodan, Nokia
- 515 • Abbie Barbir, Nortel Networks
- 516 • Scott Kiestler, Novell
- 517 • Cameron Morris, Novell
- 518 • Paul Madsen, NTT
- 519 • Steve Anderson, OpenNetwork
- 520 • Ari Kermaier, Oracle
- 521 • Vamsi Motukuru, Oracle
- 522 • Darren Platt, Ping Identity
- 523 • Prateek Mishra, Principal Identity
- 524 • Jim Lien, RSA Security
- 525 • John Linn, RSA Security
- 526 • Rob Philpott, RSA Security
- 527 • Dipak Chopra, SAP
- 528 • Jahan Moreh, Sigaba
- 529 • Bhavna Bhatnagar, Sun Microsystems
- 530 • Eve Maler, Sun Microsystems
- 531 • Ronald Monzillo, Sun Microsystems

- 532 • Emily Xu, Sun Microsystems
- 533 • Greg Whitehead, Trustgenix

534

535 The editors also would like to acknowledge the following former SSTC members for their contributions to
536 this or previous versions of the OASIS Security Assertions Markup Language Standard:

- 537 • Stephen Farrell, Baltimore Technologies
- 538 • David Orchard, BEA Systems
- 539 • Krishna Sankar, Cisco Systems
- 540 • Zahid Ahmed, CommerceOne
- 541 • Tim Alsop, CyberSafe Limited
- 542 • Carlisle Adams, Entrust
- 543 • Tim Moses, Entrust
- 544 • Nigel Edwards, Hewlett-Packard
- 545 • Joe Pato, Hewlett-Packard
- 546 • Bob Blakley, IBM
- 547 • Marlena Erdos, IBM
- 548 • Marc Chanliau, Netegrity
- 549 • Chris McLaren, Netegrity
- 550 • Lynne Rosenthal, NIST
- 551 • Mark Skall, NIST
- 552 • Charles Knouse, Oblix
- 553 • Simon Godik, Overxeer
- 554 • Charles Norwood, SAIC
- 555 • Evan Prodromou, Securant
- 556 • Robert Griffin, RSA Security (former editor)
- 557 • Sai Allarvarpu, Sun Microsystems
- 558 • Gary Ellison, Sun Microsystems
- 559 • Chris Ferris, Sun Microsystems
- 560 • Mike Myers, Traceroute Security
- 561 • Phillip Hallam-Baker, VeriSign (former editor)
- 562 • James Vanderbeek, Vodafone
- 563 • Mark O'Neill, Vordel
- 564 • Tony Palmer, Vordel

565

566 Finally, the editors wish to acknowledge the following people for their contributions of material used as
567 input to the OASIS Security Assertions Markup Language specifications:

- 568 • Thomas Gross, IBM
- 569 • Birgit Pfitzmann, IBM

Appendix B. Notices

571 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
572 might be claimed to pertain to the implementation or use of the technology described in this document or
573 the extent to which any license under such rights might or might not be available; neither does it represent
574 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
575 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
576 available for publication and any assurances of licenses to be made available, or the result of an attempt
577 made to obtain a general license or permission for the use of such proprietary rights by implementors or
578 users of this specification, can be obtained from the OASIS Executive Director.

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

582 **Copyright © OASIS Open 2005. All Rights Reserved.**

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

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

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