1
2
3
4
5
6
7

Liberty Architecture Glossary

8
9
Version 08
15 November 2002
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

26

27 **Document Description:** draft-liberty-tech-glossary-08

28

Notice

30 Copyright © 2002 ActivCard; American Express Travel Related Services; America Online, Inc.; Bank of
31 America; Bell Canada; Cingular Wireless; Cisco Systems, Inc.; Citigroup; Communicator, Inc.; Consignia;
32 Deloitte & Touche LLP; EarthLink, Inc.; Electronic Data Systems, Inc.; Entrust, Inc.; Ericsson; Fidelity
33 Investments; France Telecom; Gemplus; General Motors; Hewlett-Packard Company; i2 Technologies, Inc.;
34 Intuit Inc.; MasterCard International; NEC Corporation; Netegrity; NeuStar; Nextel Communications; Nippon
35 Telegraph and Telephone Company; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OneName
36 Corporation; Openwave Systems Inc.; PricewaterhouseCoopers LLP; Register.com; RSA Security Inc; Sabre
37 Holdings Corporation; SAP AG; SchlumbergerSema; SK Telecom; Sony Corporation; Sun Microsystems,
38 Inc.; United Airlines; VeriSign, Inc.; Visa International; Vodafone Group Plc; Wave Systems. All rights
39 reserved.

40 This specification document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby
41 granted to use the document solely for the purpose of implementing the Specification. No rights are granted to
42 prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this
43 document for other uses must contact the Liberty Alliance to determine whether an appropriate license for
44 such use is available.

45 Implementation of the Specifications may involve the use of one or more of the following United States
46 Patents claimed by AOL Time Warner, Inc.: No.5,774,670, No.6,134,592, No.5,826,242, No. 5,825,890, and
47 No.5,671,279. The Sponsors of the Specification take no position concerning the evidence, validity or scope
48 of the claimed subject matter of the aforementioned patents. Implementation of certain elements of this
49 Specification may also require licenses under third party intellectual property rights other than those identified
50 above, including without limitation, patent rights. The Sponsors of the Specification are not and shall not be
51 held responsible in any manner for identifying or failing to identify any or all such intellectual property rights
52 that may be involved in the implementation of the Specification.

53 **This Specification is provided "AS IS", and no participant in the Liberty Alliance makes any warranty**
54 **of any kind, express or implied, including any implied warranties of merchantability, non-infringement**
55 **or third party intellectual property rights, and fitness for a particular purpose.**

56 Liberty Alliance Project
57 Licensing Administrator
58 c/o IEEE-ISTO
59 445 Hoes Lane, P.O. Box 1331
60 Piscataway, NJ 08855-1331, USA

61

Editors

63   Hank Mauldin, Cisco Systems

64   Tom Wason, IEEE-ISTO

65

Contributors

<div style="columns:2">

ActivCard
American Express Travel Related Services
America Online, Inc.
Bank of America
Bell Canada
Cingular Wireless
Cisco Systems, Inc.
Citigroup
Communicator, Inc.
Consignia
Deloitte & Touche LLP
EarthLink, Inc.
Electronic Data Systems, Inc.
Entrust, Inc.
Ericsson
Fidelity Investments
France Telecom
Gemplus
General Motors
Hewlett-Packard Company
i2 Technologies, Inc.
Intuit Inc.
MasterCard International
NEC Corporation

Netegrity
NeuStar
Nextel Communications
Nippon Telegraph and Telephone Company
Nokia Corporation
Novell, Inc.
NTT DoCoMo, Inc.
OneName Corporation
Openwave Systems Inc.
PricewaterhouseCoopers LLP
Register.com
RSA Security Inc
Sabre Holdings Corporation
SAP AG
SchlumbergerSema
SK Telecom
Sony Corporation
Sun Microsystems, Inc.
United Airlines
VeriSign, Inc.
Visa International
Vodafone Group Plc
Wave Systems

</div>

67

Document History

Rev	Date	By Whom	Description
00	13-Mar-02	Gary Ellison, Sun	Renamed, added MRD/ERD terms
01	2-April-02	Hank Mauldin, Cisco	Added terms from architecture documents, included input from policy/marketing.
02	11-April-02	Hank Mauldin, Cisco	Added LECP
03	12-April-02	Hank Mauldin, Cisco	Corrected an invalid reference
04	25-April-02	Hank Mauldin, Cisco Terry Stone, Bank of America	Add new terms and delete non referenced terms.
05	7-May-02	Hank Mauldin	Changes recommended by tech editor
06	10-May-02	Hank Mauldin	Add new definitions
07	15-May-02	Hank Mauldin	Minor changes and new definition
08	14-Nov.-02	Thomas Wason, ISTO	Addition of "Minimum maximum" Changed SAMLGloss to 1.0

69

1 Introduction

74

75 This document is intended to provide a reference of terms, which ensures that when discussing
76 identity solutions for the Internet and, in particular, the solution defined by the Liberty Alliance, a
77 common understanding of their meaning exists.

78 This document is not intended to be a complete and authoritative compendium of all terms used when
79 discussing network identity, but rather a comprehensive list of definitions for concepts used in the
80 whole Liberty scope. Many terms that are commonly used within this context, but which retain their
81 everyday meaning, are not listed. Furthermore, many terms that are relevant to Liberty typically have
82 a security and/or privacy focus. Therefore, [RFC2828] has been adopted as a foundation to this
83 document so that terms that are not defined here and are described as RECOMMENDED definitions
84 in [RFC2828] shall be considered normative. Note: Certain definitions from [RFC2828] have been
85 included (with attribution) in this document so that the set of Liberty documents has a single glossary
86 of terms that have been identified as needing description for the community.

87 Finally, this glossary is a living document and, therefore, is subject to constant revisions. Comments
88 regarding content and format are welcome, and should be sent to the Liberty Technology Working
89 Group (technology@projectliberty.org).

2 Definitions

account
A formal business agreement for providing regular dealings and services between a Principal and service providers.

account linkage
See identity federation.

artifact, SAML
A small, random number designed to point to full SAML assertions. SAML artifacts are passed between sites by the browser on URL query strings.

assertion
A piece of data produced by a SAML authority regarding an act of authentication performed on a Principal, attribute information about the Principal, or authorization permissions applying to the Principal with respect to a specified resource.

attribute
A distinct characteristic of a Principal. A Principal's attributes are said to describe it.

authenticated Principal
A Principal who has had his identity authenticated by an identity provider.

authentication assertion context (AAC)
In addition to the authentication assertion itself, the information that the service provider may require before it makes an entitlements decision.

authentication (AuthN)
process of verifying the ability of a communication party to "talk" in name of a Principal.

authentication session
The period of time starting after A has authenticated B and until A stops trusting B's identity assertion and requires reauthentication. Also known just as "session," it is the state between a successful login and a successful logout by the Principal.

authorization (AuthZ)
A right or a permission that is granted to a system entity to perform an action.

certificate management
The functions that a digital certificate issuer may perform during the life cycle of a certificate, including the following:

- Acquire and verify data items to bind into the certificate.
- Encode and sign the certificate.
- Store the certificate in a directory or repository.
- Renew, rekey, and update the certificate.
- Revoke the certificate and issue a CRL. [RFC2828]

126 **certificate policy (CP)**
127   A named set of rules indicating the applicability of a certificate to a particular community and/or class
128   of application. For example, a certificate policy might indicate that a particular type of certificate is
129   appropriate for the authentication of participants in a business-to-business transaction within a given
130   price range. The fundamental difference between the certificate practice statement and the certificate
131   policy is that the former is "owned" by the issuing certification authority and the latter by the entities
132   that will use the issued certificates. Certificate users define certificate policies, and certification
133   authorities (with different certificate practice statements) attest that a particular certificate is
134   appropriate for that certificate policy.

135 **certificate practice statement (CPS)**
136   A statement of the practices that a certification authority employs in issuing certificates. A certificate
137   practice statement may take the form of a declaration by the certification authority of the details of its
138   trustworthy systems and the practices it employs in support of its issuance of certificates.

139 **certificate revocation list (CRL)**
140   A data structure that enumerates digital certificates that have been invalidated by their issuer prior to
141   when they were scheduled to expire **[RFC2828]**.

142 **circle of trust**
143   A federation of service providers and identity providers that have business relationships based on
144   Liberty architecture and operational agreements and with whom users can transact business in a secure
145   and apparently seamless environment.

146 **cookie**
147   A collection of information, usually including a username and the current date and time, stored on the
148   local computer of a person using the Web and used chiefly by Websites to identify users who have
149   previously registered or visited the site.

150 **credentials**
151   Known data attesting to the truth of certain stated facts.

152 **a**
153   Any information that a Principal provides to an identity provider or a service provider.

154 **defederate identity**
155   To eliminate linkage between Principal's accounts at an identity provider and a service provider, such
156   that the identity provider no longer provides user identity to the service provider, and the service
157   provider will no longer accept user identity from the identity provider.

158 **digital certificate**
159   A digitally signed assertion. The same Principal that issued the underlying assertion must sign the
160   certificate.

161 **digital signature**
162   A data structure that strongly depends on a private key and the contents of the message being signed.
163   Digital signatures should be uniquely verified with the corresponding public key. Note: Digital
164   signatures are not equivalent to hand-written signatures in most respects. Note: In an international

165　　　legislation context, the definition of digital signature differs broadly. See also public-key
166　　　cryptography.

DNS (Domain Name System)
168　　　A general-purpose distributed, replicated, data query service chiefly used on the Internet for
169　　　translating hostnames into /search?q=Internet%20addressesInternet addresses.

ECML (Electronic Commerce Modeling Language)
171　　　A set of hierarchical payment-oriented data structures that will enable automated software, including
172　　　electronic wallets, from multiple vendors to supply needed data in a more uniform manner.

entity-provided data
174　　　Any data directly provided by an entity to a member of a Liberty circle of trust.

federate
176　　　To link or bind two or more entities together.

federated architecture (authentication)
178　　　An architecture that supports multiple entities provisioning ncipals among peers within the
179　　　Liberty circle of trust.

federation
181　　　An association comprising any number of service providers and identity providers.

HTTP (Hypertext Transport Protocol)
183　　　An application-level protocol for distributed, collaborative, hypermedia information systems
184　　　[**RFC2616**].

identity
186　　　The essence of an entity and often described by its characteristics.

Identity federation
188　　　Associating, connecting, or binding multiple accounts for a given Principal at various Liberty Alliance
189　　　entities within a circle of trust.

identity provider (IdP)
191　　　A Liberty-enabled entity that creates, maintains, and manages identity information for Principals and
192　　　provides Principal authentication to other service providers within a circle of trust.

IPsec (Internet Protocol Security)
194　　　A framework of open standards for ensuring confidentiality, integrity, and authenticity of data
195　　　communications across a public network.

Kerberos
197　　　A trusted third-party authentication protocol. [RFC1510]ftp://ftp.isi.edu/in-
198　　　notes/rfc1510.txthttp://www.ietf.org/html.charters/krb-wg-charter.html.

erty Alliance guidelines
200　　　Policies defined by the Liberty Alliance and recommended to be followed for maximizing the
201　　　implementation of Liberty specifications.

202 **Liberty Alliance principles**
203   The commitments that an identity provider or service provider must contractually agree to (if any) to
204   be Liberty-compliant.

205 **Liberty architecture**
206   An architecture that supports the technical programs and specifications to provide a single sign-on
207   with federated identities.

208 **Liberty-enabled client or proxy (LECP)**
209   A Liberty-enabled client is a client that has, or knows how to obtain, knowledge about the identity
210   provider that the Principal wishes to use with the service provider. A Liberty-enabled proxy is an
211   HTTP proxy (typically a WAP gateway) that emulates a Liberty-enabled client.

212 **login**
213   The act of a Principal gaining access to a session in which the Principal can use system resources
214   [RFC2828].

215 **logout**
216   The termination of a session.

217 **metadata**
218   Definitional data that provides information about or documentation of other data managed within an
219   application or environment.

220 **minimum maximum**
221   The smallest maximum value or size for a field that is to be supported. For example, if a URL has a
222   minimum maximum of 256 characters, then any system that supports that field must support at least
223   256 characters. It may support more.

224 **namespace**
225   A set of names in which all names are unique.

226 **network identity**
227   The abstraction of the global set of attributes composed from all of a Principal's existing accounts.

228 **nonce**
229   A nonce is a value used no more than once for the same purpose.. A nonce can be a time stamp, a visit
230   counter on a Web page, or a special marker intended to limit or prevent the unauthorized replay or
231   reproduction of a file.

232 **nonrepudiation**
233   The inability of a Principal to legally repudiate its involvement with an action or a piece of
234   information.

235 **opaque handle**
236   A string that has meaning only in the context between a specific identity provider and specific service
237   provider.

238 **password**
239   A secret data value, usually a character string, that is used as authentication information **[RFC2828]**.

240 **sonally identifiable information (PII)**
241   Any data that identifies or locates a particular person, consisting primarily of name, address, telephone
242   number, e-mail address, bank accounts, or other unique identifiers such as Social Security numbers.

243 **PIN (personal identification number)**
244   See [RFC2828]. Essentially the same thing as a password. It typically is restricted in size and content
245   to a few characters and/or numbers.

246 **Principal**
247   A Principal is an entity that can acquire a federated identity, that is capable of making decisions, and
248   to which authenticated actions are done on its behalf. Examples of principals include an individual
249   user, a group of individuals, a corporation, other legal entities, or a component of the Liberty
250   architecture.

251 **privacy**
252   Proper handling of personal information throughout its life cycle, consistent with the preferences of
253   the subject.

254
255 **profile**
256   Data comprising the broad set of attributes that may be maintained for an identity, over and beyond its
257   identifiers and the data required to authenticate under that identity. At least some of those attributes
258   (for example, addresses, preferences, card numbers) are provided by the Principal.

259 **proxy**
260   An entity authorized to act for another.

261 **pseudonym**
262   An arbitrary name assigned by the identity or service provider to identify a Principal to a given relying
263   party so that the name has meaning only in the context of the relationship between the relying parties.

264 **public-key infrastructure (PKI)**
265   A system of certificate authorities (and, optionally, registration authorities and other supporting
266   servers and agents) that perform some set of certificate management, archive management, key
267   management, and token management functions for a community of Principals in an application of
268   asymmetric cryptography [RFC2828].

269 **public-key cryptography**
270   Set of cryptographic techniques that uses two keys: The first key is always kept secret by an entity;
271   and the second key, which is uniquely bound to the first one, is made public. Messages created with
272   the first key (the *private key*) can be uniquely verified with the second key (the *public key*) in a
273   "strong" way, where the strength of the verification is so high that the messages are called *digital*
274   *signatures*. Finally, messages created using the public key can be deciphered only with the
275   corresponding private key. See digital signature.

276 **repudiation**
277   The rejection or renunciation of a duty or obligation.

278 **RPC (Remote Procedure Call Protocol)**
279   A protocol that allows a program running on one host to cause code to be executed on another host
280   without the programmer needing to explicitly code for this action.

281 **SAML (Security Assertion Markup Language)**
282   An XML standard for exchanging authentication and authorization data between security systems. See
283   http://www.oasis-open.org/committees/security/#documents.

284 **service provider (SP)**
285   An entity that provides services and/or goods to Principals.

286 **single sign-on (SSO)**
287   The ability to use proof of an existing authentication session with identity provider A to create a new
288   authentication session with identity provider B.

289 **smartcards**
290   A tamper-resistant credit-card sized device containing one or more integrated circuit chips, which
291   perform the functions of a computer's central processor, memory, and input/output interface.

292 **SOAP (Simple Object Access Protocol)**
293   An XML envelope and data encoding technology used to communicate information and requests
294   across the Web. It is typically considered the protocol used by Web services. It is actually an envelope
295   encapsulation format that can be used with lower level Web protocols such as HTTP and FTP. See
296   [SOAP].

297 **SSL (Secure Sockets Layer Protocol)**
298   An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-
299   oriented end-to-end encryption to provide data confidentiality service and data integrity service for
300   traffic between a client (often a Web browser) and a server and that can optionally provide peer entity
301   authentication between the client and the server. See Transport Layer Security. [RFC2828].

302 **TLS (Transport Layer Security Protocol)**
303   An evolution of the SSL protocol. The TLS protocol provides communications privacy over the
304   Internet. The protocol allows client/server applications to communicate in a way that is designed to
305   prevent eavesdropping, tampering, or message forgery. See **[RFC2246]**.

306 **trust circle**
307   See circle of trust.

308 **URI (Uniform Resource Identifier)**
309   A compact string of characters for identifying an abstract or physical resource. [RFC2396] defines the
310   generic syntax of URI, including both absolute and relative forms, and guidelines for their use.

311 **URL (Uniform Resource Locator)**
312   The subset of URI. URLs identify resources via a representation of their primary access mechanism
313   (e.g., their network location) rather than identifying the resource by name or by some other attributes
314   of that resource. **[RFC2396]**

315 **URN (Uniform Resource Names)**
316   Names intended to serve as persistent, location-independent, resource identifiers and designed to make
317   it easy to map other namespaces (which share the properties of URNs) into URN-space. See
318   [RFC2141].

319 **user agent**
320   Any software that retrieves and renders Web content for users.

321 **user interface**
322   The controls (such as menus, buttons, prompts, etc.) and mechanisms (such as selection and focus)
323   provided by the user agent.

324 **VPN (Virtual Private Network)**
325   A network that can be run over the public Internet while still giving privacy and/or authentication to
326   each user of the network.

327 **WAP (Wireless Application Protocol)**
328   An open, international specification that empowers mobile users with wireless devices to easily access
329   and interact with information and services.

330 **b service**
331   A service that uses Internet protocols to provide a service designed to be used by programs.

332 **WML (Wireless Markup Language)**
333   A markup language based on XML and intended for use in specifying content and user interface for
334   narrowband devices, including cellular phones and pagers.

335 **WSDL (Web Services Description Language)**
336   A popular technology for describing the interface of a Web service. See http://www.w3.org/TR/wsdl/.

337 **XML (eXtensible Markup Language)**
338   A W3C technology for encoding information and documents for exchange over the Web. See
339   http://www.w3.org/XML/.

340 **ZIC (Zero Install Client)**
341   A commonly used HTTP-based user agent having no Liberty-specific extensions. For example,
342   standard Web browsers are ZICs.

343

344

345

3 References and Recommended Reading

[COMP97]   I. Goldberg, D. Wagner, E. Brewer. Privacy-enhancing Technologies for the Internet. Proc. of IEEE Spring COMPCON, 1997.

[RFC1510]   J. Kohl, C Neuman. The Kerberos Network Authentication Service (V5). Request For Comments (RFC) 1510, Internet Engineering Task Force, September 1993.

[RFC2141]   R. Moats. URN Syntax. Request for Comments (RFC) 2141, Internet Engineering Task Force, May 1997.

[RFC2246]   T. Dierks, C. Allen. The TLS Protocol Version 1.0. Request for Comments (RFC) 2246, Internet Engineering Task Force, January 1999.

[RFC2396]   T. Berners-Lee, R. Fielding, L. Masinter. Uniform Resource Identifiers (URI): Generic Syntax. Request for Comments (RFC) 2396, Internet Engineering Task Force, August 1998.

[RFC2616]   R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol -- HTTP/1.1. Request For Comments (RFC) 2616, Internet Engineering Task Force, June 1999.

[RFC2693]   C. Ellison, B Frantz, B Lampson, R Rivest, B Thomas, T. Ylonen. SPKI Certificate Theory. Request for Comments (RFC) 2693, Internet Engineering Task Force, September 1999.

[RFC2828]   R. Shirey. Internet Security Glossary. Request for Comments (RFC) 2828, Internet Engineering Task Force, May 2000.

[SAMLGloss]   J. Hodges et al., *Glossary for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/docs/cs-sstc-glossary-01.pdf, OASIS, May 2002.

[SOAP]   W3C Note: SOAP 1.1: http://www.w3.org/TR/SOAP/, W3C: SOAP 1.2: http://www.w3.org/TR/2001/WD-soap12-20010709/, W3 Note: SOAP Messages with Attachments: http://www.w3.org/TR/SOAP-attachments/.