Liberty Architecture Glossary

Version 1.0

11 July 2002

Document Description: liberty-tech-glossary-v1.0

Notice

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

Editor

Hank Mauldin, Cisco Systems, Inc.

Contributors

The following Liberty Alliance Project Sponsor companies contributed to the development of this specification:

ActivCard
American Express Travel Related Services
America Online, Inc.
Bank of America
Bell Canada
Catavault
Cingular Wireless
Cisco Systems, Inc.
Citigroup
Cyberun Corporation
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
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
Sony Corporation
Sun Microsystems, Inc.
United Airlines
VeriSign, Inc.
Visa International
Vodafone Group Plc
Wave Systems

Table of Contents

1 Introduction

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

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

Finally, this glossary is a living document and, therefore, is subject to constant revisions. Comments regarding content and format are welcome, and should be sent to the Liberty Technology Working 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)
The 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]

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

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

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

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

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

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

data
Any information that a Principal provides to an identity provider or a service provider.

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

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

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

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

DNS (Domain Name System)
A general-purpose distributed, replicated, data query service chiefly used on the Internet for translating hostnames into Internet addresses.

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

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

federate
To link or bind two or more entities together.

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

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

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

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

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

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

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

Kerberos
A trusted third-party authentication protocol. [RFC1510].

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

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

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

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

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

logout
The termination of a session.

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

namespace
A set of names in which all names are unique.

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

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

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

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

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

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

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

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

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

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

proxy
An entity authorized to act for another.

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

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

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

repudiation
The rejection or renunciation of a duty or obligation.

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

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

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

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

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

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

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

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

trust circle
See circle of trust.

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

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

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

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

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

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

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

Web service
A service that uses Internet protocols to provide a service designed to be used by programs.

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

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

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

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

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/draft-sstc-glossary-02.pdf, OASIS, December 2001.

[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/.