Liberty Architecture Glossary

Draft Version 1.2-04

14 April 2003

Editor:

Tom Wason, IEEE ISTO

Contributors:

John Linn, RSA Security, Inc.
Carolina Canales-Valenzuela, Ericsson
Elisa Korentayer, IEEE-ISTO

Abstract:

Important terms, abbreviations and acronyms used in the Liberty Alliance specifications.

Notice

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

Revision History

Rev	Date	By Whom	Description
1.2 Draft	14-Mar-03	Tom Wason	Addition of the following terms: access control, AP, authentication, Authentication Domain, authentication quality, delegation, discovery service, ID-PP, identity service, introduction, invocation identity, MEP, PAOS, PDP, PEP, policy, POTS, relying party, recipient, requestor, resource offering, ROI, SAML Authority, service instance, Trusted Authority, TTP, VoIP,
1.2 Draft	21-Mar-03	Tom Wason	Revised the following term: policy
1.2-04	13-Apr-03	Tom Wason	Removed POTS, VOIP
1.2-04	14-Apr-03	Tom Wason	Added: Attribute Broker (AB), Attribute Class, Attribute Provider (AP), Liberty-Enabled Provider, permission, proprietary data, Rights Expression Languages (RELs),

Abstract

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

access control

The act of mediating requested access to a resource based on privilege attributes of the requestor and control attributes of the requested resource.

account

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

account linkage

See identity federation.

AP

The attribute provider (AP) provides ID-PP information. Sometimes called a ID-PP provider, the AP is a ID-WSF web service that hosts the ID-PP.

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.

Attribute Broker (AB)

An entity that serves as a relay for receiving attribute requests and sending attribute responses on behalf of multiple attribute providers. The attribute broker adheres to the business policies of the attribute providers and permissions of the Principal. This arrangement facilitates fewer business relationships/agreements between entities, as attribute providers can benefit from one attribute broker registering with several service providers on their behalf. Only one attribute broker may exist for an attribute class per Principal. If an attribute broker exists for an attribute class for a Principal, all attribute providers who wish to provide service to the Principal must work through the attribute broker.

attribute class

A predefined set of attributes, such as the constituents of a Principal's name (prefix, first name, middle name, last name, and suffix). Liberty entities may standardize such classes.

Attribute Provider (AP)

The attribute provider (AP) provides Identity Personal Profile (ID-PP) information. Sometimes called a ID-PP provider, the AP is a ID-WSF web services that hosts the ID-PP.

authenticated Principal

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

authentication (AuthN)

The process of verifying the ability of a communication party to “talk” in name of a Principal.

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 Domain

An Authentication Domain (AD) is a formal community of Liberty-enabled entities that interact using a set of well-known common rules.

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.

authentication quality

The level of assurance that a service provider can place in an authentication assertion it receives from an identity provider.

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:RFC2828

- 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.

delegation

Enabling a system entity to operate on behalf of a principal to access an identity service.

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.

discovery service

An identity service that allows requesters to discover resource offerings.

DNS (Domain Name System)

A general-purpose distributed, replicated, data query service chiefly used on the Internet for translating hostnames into /search?q=Internet%20addressesInternet 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].

ID-PP

The ID Personal Profile is identity information regarding the principal, be it in private or work capacity.

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.

identity service

an abstract notion of a web service that acts upon some resource to either retrieve information about an identity or identities, update information about an identity or identities, or perform some action for the benefit of some identity or identities.

introduction

A 1-2 sentence definition relative to Working with Multiple IdPs needed.

invocation identity

The subject of SAML assertion, party requesting service when message is processed.

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]ftp://ftp.isi.edu/in-notes/rfc1510.txthttp://www.ietf.org/html.charters/krb-wg-charter.html.

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.

Liberty-Enabled Provider

As used herein, and only herein, LEP may be either an Attribute Provider (AP), Discovery Service (DS), Service provider (SP), Identity Provider (IdP), or Attribute Broker (AB) who collects, transfers, or receives the Personally Identifiable Information (PII) of a Principal.

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.

MEP

A Message Exchange Pattern (MEP) is a template that establishes a pattern for the exchange of messages between SOAP nodes. (Ref: SOAP 1.2).

metadata

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

minimum maximum

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

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.

PAOS

A Reversed HTTP binding for SOAP. The primary difference from the normal HTTP binding for SOAP is that here a SOAP request is bound to a HTTP response and vice versa.

password

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

PDP

Policy decision point

PEP

Policy enforcement point

permission

Privileges granted to each user with respect to what data that the user is allowed to access and what menus options or commands he or she is allowed to use.

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.

policy

A logically defined, executable and testable set of rules of behavior.

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.

proprietary data

Protected data specific to an organization.

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.

relying party

The recipient of a message that relies on a request message and associated assertions to determine whether to provide a requested service.

recipient

An entity which receives a message and acts as the message's ultimate processor.

repudiation

The rejection or renunciation of a duty or obligation.

requestor

Entity which sends a message to a recipient for processing. Commonly, the requestor is also the message's author.

resource offering

The association of a resource and a service instance.

Rights Expression Languages (RELs)

A machine-based language that enables communication about usage directives. RELs allows an information provider to request intended uses of information before the information is exchanged and to designate approved uses for information exchanged during a particular transaction.

ROI

Resource Owner Interaction. The Resource Owner Interaction service is a Liberty identity service that exposes interaction with a resource owner. It allows clients (typically WSPs, that act towards the ROI service as WSC!) to query a resource owner for consent, authorization decisions, etc.

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.

SAML Authority

A party that has applied its signature to a signed SAML assertion, usually a trusted third party.

service instance

The physical instantiation of a particular type of identity service. A service instance is a running web service at a distinct protocol endpoint.

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.

Trusted Authority

In Liberty, a Trusted Third Party (TTP) which issues and vouches for SAML assertions.

TTP

Trusted third party

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 (1997). "Privacy-enhancing Technologies for the Internet." Proc. of IEEE Spring COMPCON.

[RFC1510] Kohl, J., & Neuman, C. (September 1993). "The Kerberos Network Authentication Service (V5)" RFC 1510. Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc1510.txt> [20 December 2002].

[RFC2141] Moats, R. (May 1997). "URN Syntax." RFC 2141. Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2141.txt> [20 December 2002].

[RFC2246] Dierks, T. & Allen, C. (January 1999). "The TLS Protocol" Version 1.0. RFC 2246, Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2246.txt> [20 December 2002].

[RFC2396] Berners-Lee, T., Fielding, R., & Masinter, L. (August 1998). "Uniform Resource Identifiers (URI): Generic Syntax," RFC 2396. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2396.txt> [18 December 2002].

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (June 1999). "Hypertext Transfer Protocol -- HTTP/1.1," RFC 2616. The Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2616.txt> [18 December 2002].

[RFC2693] Ellison, C. Frantz, B., Lampson, B., Rivest, R., Thomas, B., & Ylonen, T. (September 1999). "SPKI Certificate Theory," RFC 2693. Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2693.txt> [20 December 2002].

[RFC2828] Shirey, R. (May 2000). "Internet Security Glossary," RFC 2828. Internet Engineering Task Force, <http://www.rfc-editor.org/rfc/rfc2828.txt> [20 December 2002].

[SAMLGloss] Hodges, J., Maler, E, eds. (05 Nov. 2002). "Glossary for the OASIS Security Assertion Markup Language (SAML)," Version 1.0, OASIS Standard. Organization for the Advancement of Structured Information Standards, <http://www.oasis-open.org/committees/security/#documents> [18 December 2002].

[SOAP1.1] D. Box et al. (May 2000). "Simple Object Access Protocol (SOAP) 1.1," Note. World Wide Web Consortium, <http://www.w3.org/TR/SOAP> [18 December 2002].