Liberty Technical Glossary

Version: v2.0-05

Editors:
Jeff Hodges, NeuStar, Inc.

Contributors:
Robert Aarts, TrustGenix
Carolina Canales-Valenzuela, Ericsson
Peter Davis, NeuStar, Inc.
John Kemp, Nokia
Elisa Korentayer, IEEE-ISTO
John Linn, RSA Security, Inc.
Thomas Wason, IEEE-ISTO

Abstract:
This glossary defines many of the technical terms and phrases used in Liberty Alliance Project specifications and documents.

Filename: draft-liberty-glossary-v2.0-05.pdf
Notice

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

Implementation of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS", and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementors of this Specification are advised to review the Liberty Alliance Project’s website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Copyright © 2006 Adobe Systems; America Online, Inc.; American Express Company; Amsoft Systems Pvt Ltd.; Avatier Corporation; Axalto; Bank of America Corporation; BIPAC; BMC Software, Inc.; Computer Associates International, Inc.; DataPower Technology, Inc.; Diversinet Corp.; Enosis Group LLC; Entrust, Inc.; Epok, Inc.; Ericsson; Fidelity Investments; Forum Systems, Inc.; France Télécom; French Government Agence pour le développement de l’administration électronique (ADAE); Gamefederation; Gsm; General Motors; Giesecke & Devrient GmbH; GSA Office of Governmentwide Policy; Hewlett-Packard Company; IBM Corporation; Intel Corporation; Intuit Inc.; Kantega; Kayak Interactive; MasterCard International; Mobile Telephone Networks (Pty) Ltd; NEC Corporation; Netegrity, Inc.; NeuStar, Inc.; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.; NTT DoCoMo, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation; Reactivity Inc.; Royal Mail Group plc; RSA Security Inc.; SAP AG; Senforce; Sharp Laboratories of America; Sigaba; SmartTrust; Sony Corporation; Sun Microsystems, Inc.; Supremacy Financial Corporation; Symlabs, Inc.; Telecom Italia S.p.A.; Telefónica Móviles, S.A.; Trusted Network Technologies; Trustgenix; UTI; VeriSign, Inc.; Vodafone Group Plc.; Wave Systems Corp. All rights reserved.
### Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1. Introduction</td>
</tr>
<tr>
<td>36</td>
<td>2. Definitions</td>
</tr>
<tr>
<td>37</td>
<td>References</td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
1. Introduction

This document is the Liberty Alliance Project glossary of normative technical terms.

This document is not an exhaustive compendium of all Liberty technical terminology because the Liberty terminology is built upon existing terminology. Thus many terms that are commonly used within this context are not listed. They may be found in the glossaries/documents/specifications referenced in the bibliography. Terms defined here that are not attributed to other glossaries/documents/specifications are being defined here.

This glossary is expected to evolve along with the Liberty Alliance Project specifications.
2. Definitions

Terms

AC
See authentication context.

abstract WSDL
An abstract WSDL service definition is that portion of a WSDL document [WSDLv1.1] — describing said service — comprised of the <wsdl:types>, <wsdl:message>, and <wsdl:portType> elements.

account
A formal business agreement providing for regular dealings and services between a Principal and a service provider [Merriam-Webster].

account linkage
See identity federation.

AD
See Authentication Domain.

affiliation
An affiliation is a set of one or more entities, described by providerID’s, who may perform Liberty interactions as a member of the set. An affiliation is referenced by exactly one affiliationID, and is administered by exactly one entity identified by their providerID. Members of an affiliation may invoke services either as a member of the affiliation (using affiliationID), or individually (using their providerID). Affiliation and affiliation group are equivalent terms.

affiliation group
See affiliation.

Affiliation ID
An Affiliation ID identifies an affiliation. It is schematically represented by the affiliationID attribute of the <AffiliationDescriptor> metadata element [LibertyMetadata].

AP
See Attribute Provider.

AS Consumer
See Authentication Service Consumer.

AS Provider
See Authentication Service Provider.

assertion, SAML assertion
An XML-based data structure defined by SAML. Assertions are collections of one or more statements, made by a SAML authority (also known as an issuer), such as an authentication statement or attribute statement. As used in Liberty, assertions typically concern things such as: an act of authentication performed by a Principal, attribute information about a Principal, or authorization permissions applying to a Principal with respect to a specified resource.

attribute
A distinct, named, characteristic of a Principal or other system entity.
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).

attribute container
a module comprised of a collection of attributes grouped together according to expected use patterns.

Attribute Provider (AP)
An attribute provider (AP) provides Identity Personal Profile (ID-PP) information. Sometimes referred to as an ID-PP provider.

authenticated identity
An identity, representing a system entity, which often is a Principal, that is asserted to have been the subject of a successful authentication.

authenticated Principal
A Principal who has had his identity authenticated by an Identity Provider.

authenticating authority
Synonymous with authenticating identity provider or authenticating IdP. An identity provider that authenticated a Principal (see also authentication). In [LibertyAuthnContext], the authenticating authority is identified by the first occurring <AuthenticatingAuthority> element instance.

authenticating entity
A system entity that engages in the process of authenticating itself to another system entity, the latter typically being an Identity Provider (see also authentication). More formally, an authenticating system entity.

authentication assertion
A SAML-based assertion that, in the Liberty specification suite, contains a <lib:AuthenticationStatement>.
Note that the foregoing element is defined in a Liberty namespace. Also known as Liberty authentication assertion and ID-FF authentication assertion.

Liberty authentication assertions are formal XML extensions of SAML assertions [SAMLCore11].
Semantically, an assertion issuer is stating that the subject of the assertion authenticated with it (the issuer) at some point in time. Assertions are typically time-limited.

authentication authority
A system entity that produces authentication assertions [SAMLGloss]. In the Liberty architecture, it is typically an Identity Provider.

authentication context (AC)
Authentication Context is an extensible XML-based "schematic" description of authentication event characteristics [LibertyAuthnContext].

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

authentication exchange
See authentication protocol exchange.
authentication mechanism

An authentication mechanism is a particular, identifiable, process or technique that results in a confirmation of a system entity’s asserted identity with a specified, or understood, level of confidence. See also SASL mechanism. An authentication mechanism may be employed in the process of generating security tokens attesting to the authenticated identity of an authenticating entity. The ID-WSF Authentication Protocol specifies such a process [LibertyAuthn].

authentication protocol exchange

Authentication protocol exchange is the term used in [RFC2222] to refer to the sequence of messages exchanged between the client and server as specified and governed by the particular SASL mechanism being employed to effect an act of authentication.

authentication quality

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

authentication server

The precise, specific role played by a server in the protocol message exchanges defined in the ID-WSF Authentication Protocol.

Authentication Service Consumer (AS Consumer)

A Web Service Consumer (WSC) implementing the client-side of the ID-WSF Authentication Service [LibertyAuthn].

Authentication Service Provider (AS Provider)

A Web Service Provider (WSP) implementing the server-side of the ID-WSF Authentication Service [LibertyAuthn].

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 simply as a session, it is the state between a successful login and a successful logout by a Principal.

authorization (authz)

The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access [SAMLGloss].

bearer token

A bearer token is a form of security token having the property of connoting some attribute(s) to its holder, or bearer. In [LibertySecMech], bearer tokens connote identity and they consist essentially of credentials of some form, e.g. SAML assertions [wss-saml].

bootstrap

See discovery bootstrap.

Circle of Trust (CoT)

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. Also known as a Trust Circle.

client

A role assumed by a system entity who makes a request of another system entity, often termed a server [RFC2828]. A client is at varying times a sender or a receiver.
A concrete WSDL document (which includes at least the `<wsdl:binding>`, `<wsdl:service>`, and `<wsdl:port>` elements) that contains the protocol endpoint information necessary for a client to communicate with a particular service instance.

CoT

See circle of trust.

credentials

Data that is transferred or presented to establish either a claimed identity or the authorizations of a system entity.

defederate, defederate identity

To eliminate linkage between a Principal’s accounts at an identity provider and a service provider.

delegation

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

discoverable

A discoverable "in principle" service is one having an service type URI assigned (this is typically in done in the specification defining the service). A discoverable "in practice" service is one that is registered in some discovery service instance.

ID-WSF services are by definition discoverable in principle because such services are assigned a service type URI facilitating their registration in Discovery Service instances. Once so registered, they are discoverable in practice.

discovery bootstrap

A SAML (see [SAMLCore2]) `<Attribute>` element defined such that an Endpoint Reference (EPR) for the discovery service itself—an ID-WSF EPR—can be conveyed via SAML assertions. Upon authentication or SSO, such a "discovery bootstrap" is conveyed to the authenticating (aka relying) party as a part of the Principal’s security token. The relying party is thus able to query the Principal’s discovery service for references to the Principal’s other identity services.

Discovery Service (DS)

An ID-WSF service facilitating the registration, and subsequent discovery of, ID-WSF service instances [LibertyDisco], as indexed by Principal identity. See also discoverable.

Discovery Service Provider (DS Provider)

A Web Service Provider (WSP) implementing the server-side of the ID-WSF Discovery Service [LibertyDisco].

endpoint

A term used in [WSDLv1.1] — it is the short form of protocol endpoint — and which itself means an identified entity, at the current level of abstraction, to which a protocol message, of the same level of abstraction, may be sent. For example, at the Internet Protocol (IP) layer, an endpoint is represented by an IP address, and one may send an IP datagram (AKA a “message”) to said endpoint. In contrast, at the HTTP layer, an endpoint is represented by a URL, in conjunction perhaps with other information included in the so-called "HTTP header".

See also ID-WSF Endpoint Reference

federate

To link or bind two or more entities together.
federation
(1) The act of establishing a relationship between two entities.
(2) An association comprising any number of service providers and identity providers.

final SASL response
The final <SASLResponse> message sent from the server to the client in an authentication exchange [LibertyAuthn].

gWS
See generic web service.

gWSP
See generic Web Service Provider.

generic web service (gWS)
A generic web service is defined by sense (1) of the web service definition.

generic Web Service Provider (gWSP)
A generic Web Service Provider (gWSP) an entity providing generic web services.

header, header block, header element
See SOAP header block.

ID-*
A shorthand designator referring to the Liberty ID-WSF, ID-FF, and ID-SIS specification sets. For example, one might say that the former specification sets are all part of the Liberty ID-* specification suite.

ID-* fault message
An ID-* fault message is a SOAP [SOAPv1.1] <S:Fault> element containing a <Status> element, with the attributes and attribute values of both elements configured as specified herein, or as specified in other specification(s) in the ID-WSF or ID-SIS specification sets.

ID-* header block
One of the header blocks defined in this specification, or defined in any of the other Liberty ID-* specification suite.

ID-* message
Equivalent to ordinary ID-* message.

ID-FF
The Identity Federation Framework (ID-FF) is the title for a subset of the Liberty specification suite which defines largely HTTP-based protocols for web single sign-on and identity federation [LibertyProtSchema].

ID-FF authentication assertion
See authentication assertion.

ID-PP
The "ID Personal Profile" is an ID-SIS -based service which can provide profile information regarding Principals, typically subject to policy established by said Principals [LibertyIDPP].

ID-SIS
Liberty Identity Service Interface specification set.

ID-SIS service
See ID-SIS-based service.
ID-SIS-based service

*ID-SIS-based services* are *identity services* typically built on *ID-WSF* — i.e. they are essentially *ID-WSF-based services* — and are often also built on the [LibertyDST] specification. [LibertyIDEP] and [LibertyIDPP] are examples of ID-SIS service specifications.

**ID-WSF**

Liberty Identity Web Services Framework specification set.

**ID-WSF Endpoint Reference**

An *ID-WSF Endpoint Reference* (ID-WSF EPR) is a reference to a *service instance*. It contains the address, security context, and other metadata necessary for contacting the identified service instance. The underlying structure of an ID-WSF EPR is based on *wsa:EndpointReference* [WSAv1.0-SOAP] [WSAv1.0], and conceptually is similar to the *Resource Offering* from earlier versions of the Discovery Service specification.

**ID-WSF EPR**

See *ID-WSF Endpoint Reference*.

**ID-WSF service**

See *ID-WSF-based service*.

**ID-WSF-based service**

An *ID-WSF-based service* is an *identity service* that is at least *discoverable* in principle, and is based on [LibertySOAPBinding] and [LibertySecMech].

**identity**

The essence of an entity. One’s *identity* is often described by one’s characteristics, among which may be any number of identifiers.

A *Principal* may wield one or more identities. See also *Principal identity*.

**Identity federation**

Creating associations between a given system entity’s identifiers or accounts.

**Identity Provider (IdP)**

A Liberty-enabled system entity that manages *identity* information on behalf of Principals and provides assertions of Principal *authentication* to other providers.

**identity service**

See *identity web service*.

**identity token**

*identity tokens* [LibertySecMech20SAML][LibertySecMech] are a means for conveying the *identity* of a *Principal* involved in an ID-WSF interaction, by means of stipulating one of the Principal’s identifiers, as well as (typically) an ID-WSF EPR denoting the Principal’s Discovery Service.

**identity web service**

A type of web service whose operations are indexed by *identity*. Such services maintain information about, or on behalf of, Principals — as represented by their *identities* — and/or perform actions on behalf of Principals. They are also sometimes referred to as simply *identity services*.

In Liberty ID-WSF, such services are both mapped on a per-principal basis and *discoverable* — meaning that once a Principal authenticates, the authenticating party possesses a reference to the Principal’s Discovery Service instance, which it may use to discover the Principal’s other identity services. See also “discoverable”.

See also *Discovery Service*, *discoverable*, *web service* (2), and [LibertyDisco].
initial response

A [RFC2222] term referring to authentication exchange data sent by the client in the initial SASL request. It is used by a subset of SASL mechanisms. See Section 5.1 of [RFC2222].

initial SASL request

The initial <SASLRequest> message sent from the client to the server in an authentication exchange [LibertyAuthn].

IdP

See Identity Provider.

invocation identity

The identity of the system entity invoking a service.

LEC

See Liberty-Enabled Client.

LECP

See Liberty-Enabled Client or Proxy.

LEP

See Liberty-Enabled Proxy.

Liberty authentication assertion

See authentication assertion.

Liberty-enabled client (LEC)

An entity that has, or knows how to obtain, knowledge about the identity provider that the Principal wishes to use with the service provider.

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

An umbrella term referring to any Provider offering any ID-FF-, ID-WSF-, or ID-SIS-based services.

Liberty-Enabled Client and Proxy Profile

This profile specifies interactions between Liberty-enabled clients and/or proxies, service providers, and identity providers [LibertyBindProf].

Liberty-enabled Proxy (LEP)

A Liberty-enabled proxy is an HTTP proxy (typically a WAP gateway) that emulates a Liberty-enabled client.

Liberty-enabled User Agent or Device (LUAD)

A user agent or device that has specific support for one or more profiles of the Liberty specifications. It should be noted that although a standard web browser can be used in many Liberty-specified scenarios, it does not provide specific support for the Liberty protocols, and thus is not a LUAD.

No particular claims of specific functionality should be implied about a system entity solely based on its definition as a LUAD. Rather, a LUAD may perform one or more Liberty system entity roles as defined by the Liberty specifications it implements. For example, a LUAD-LECP is a user agent or device that supports the Liberty LEC profile, and a LUAD-DS would define a user agent or device offering a Liberty ID-WSF Discovery Service.
In the Liberty context, this term refers to a notion of session state "local" to, i.e. maintained by, a provider, with respect to an interaction with another system entity, typically a user agent. Note that the concrete techniques used to maintain session state vary; cookies [RFC2965], so-called "URL re-writing", and so-called "hidden form fields" are the most viable techniques in the HTTP, aka "web", world.

The act of a Principal proving their identity to a system entity, which typically establishes a session.

The termination of a session.

See Liberty-enabled User Agent or Device.

A Web Service Consumer (WSC), that may or may not also be a Liberty-enabled User Agent or Device.

A process or technique for achieving a result [Merriam-Webster].

see Message Exchange Pattern.

A term, borrowed from [SOAPv1.2], for the overall notion of various patterns of message exchange between SOAP nodes. For example, request-reply and one-way are two MEPs used in this specification.

A message thread is a synchronous exchange of messages in a request-response MEP between two SOAP nodes. All the messages of a given message thread are "linked" via each message’s <wsa:RelatesTo> header block value being set, by the sender, from the previous successfully received message’s <wsa:MessageID> header block value.

Definitional data that provides information about other data or system entities managed within an application or environment. In Liberty, metadata is Provider information that is necessary for interacting with Providers [LibertyMetadata].

An abstraction, consisting of a Principal’s global set of attributes, which is composed from a "union" of the Principal’s accounts. See also identity.

the ability to act for another entity based on Trusted Authority Policy. The capability is non-transferable.

An identifier that has meaning only in the context between a specific identity provider and specific service provider.
ordinary ID-* message

An ordinary ID-* message is a Liberty Identity Web Services Framework (ID-WSF) or Service Interface Specification (ID-SIS) message as defined in the [LibertyDST], [LibertyDisco], and [LibertyIDPP] specifications and others. It is "ordinary" as opposed to being a ID-* fault message.

It has the characteristics of being designed to be conveyed by essentially any transport or transfer protocol, notably SOAP [SOAPv1.1]. It is also known among the ID-* specifications as a service request, or an ID-WSF (service) request, or an ID-SIS (service) request.

PAOS

A Reversed HTTP binding for SOAP [SOAPv1.1] 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. "PAOS" is "SOAP" spelled backwards (pun intended).

PDP

See Policy Decision Point

PEP

See Policy Enforcement Point

permission

Privileges granted to a system entity with respect to operations that may be performed on some resource.

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.

PII

See personally identifiable information.

policy

A logically defined, enforceable, and testable set of rules.

Policy Decision Point

A system entity that evaluates decision requests in light of applicable policy and information describing the requesting entity or entities and renders an authorization decision.

Policy Enforcement Point

A system entity that performs access control by making decision requests and enforcing authorization decisions. If the authorization decision is pushed to the PEP there will be no need for it to create a request.

Principal

Succinctly, a principal is a system entity whose identity can be authenticated. In Liberty usage, the term Principal is often synonymous with "natural person" or "user". A Principal’s identity may be federated. Examples of Principals include individual users, groups of individuals, organizational entities e.g. corporations, or a component of the Liberty architecture.

Principal identity

An identity being wielded by a Principal, or that is mapped to a Principal in some fashion.

privacy

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

processing context

A processing context is the collection of specific circumstances under which a particular processing step or set of steps take place.
A processing context facet is an identified aspect, inherent or additive, of a processing context.

Profile is used in two distinct senses in Liberty specifications:

1. Data comprising the broad set of attributes that may be maintained on behalf of a system entity (typically a Principal), over and beyond the entity’s various identifiers. At least some of this information (for example, addresses, preferences, and card numbers) is typically provided by the Principal.


A communication point from which data may be sent or received.

See also endpoint, ID-WSF Endpoint Reference.

A provider is a Liberty-enabled entity that performs one or more of the provider roles in the Liberty architecture, for example Service Provider or Identity Provider. Providers are identified in Liberty protocol interactions by their Provider IDs or optionally their Affiliation ID if they are a member of an affiliation(s) and are acting in that capacity.

A Provider ID identifies an entity known as a provider. It is schematically represented by the providerID attribute of the <EntityDescriptor> metadata element [LibertyMetadata].

(1) An entity authorized to act for another [Merriam-Webster].

(2) A system entity whose authenticated identity, according to the recipient, differs from that of the system entity making the invocation under consideration.

An arbitrary identifier 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 parties.

An entity that receives a message and acts as the message’s ultimate processor.

See Rights Expression Languages.

A role taken by a system entity when it receives a message sent by another system entity. See also SOAP receiver in [SOAPv1.2].

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

A system entity which sends a service request to a provider.
Resource is one of those terribly overloaded terms in the computer science and distributed systems realms. As used in various Liberty specifications, it has (at least) two definitions, depending on whether one is using the term in an identity-based context (1) or not (2):

1. Resource refers to either data related to some identity or identities, or a service acting on behalf of some identity or group of identities. An example of an identity-based resource is a Principal’s calendar service.

2. A resource is whatever might be identified with a URI, although often there is a connotation that one might be able to obtain information of some sort from said "resource".

Rights Expression Language (REL)

A Rights Expression Language facilitates the expression of who are the "rights holders" for a resource, who is authorized to use a resource and their applicable permissions, and any constraints or conditions imposed on such permissions. They also may express "rights entities" and "rights transactions".

Security token

In Liberty, a security token is a collection of security-related information that is used to represent and substantiate a claim [LibertyIDWSFSecurityPrivacyGuidelines] [LibertySecMech]. Outside of Liberty, the term "security token" often refers to hardware-based devices, e.g. so-called "token cards". One should not confuse the latter and the former definitions. However, it is possible for some given authentication mechanism to employ token cards in the process of authentication.

Sender

(1) A role donned by a system entity when it constructs and sends a message to another system entity. See also SOAP sender in [SOAPv1.2].

(1a) an initial SOAP sender. A sender is a proxy when its identity differs from the invocation identity.
server
A role donned by a system entity that provides a service in response to requests from other system entities called clients [RFC2828]. Note that in order to provide a service to clients; a server will often be both a sender and a receiver.

service
(1) A collection of endpoints designed to offer some service or to provide information [WSDLv1.1].
(2) Short form of ID-WSF Service or ID-WSF-based Service.

service discovery
The act of looking up a service(s) in the Discovery Service.

service instance
The physical instantiation of a service. A service instance is a web service at a distinct endpoint.

service instance address
An address of a service instance, typically expressed in URI syntax [RFC3622].

Service Provider (SP)
(1) A role donned by system entities. In the Liberty architecture, Service Providers interact with other system entities primarily via vanilla HTTP.
(2) From a Principal’s perspective, a Service Provider is typically a website providing services and/or goods.

service request
A service request is another term for an ordinary ID-* message sent by a client. Service request is also loosely equivalent to a "SOAP-bound (ordinary) ID-* message".

Service Type URI
ID-WSF-based services are assigned a Service Type URI as a part of each service’s definition. The Service Type URI is a factor in service discovery [LibertyDisco].

session
[Merriam-Webster] defines session (in its sixth sense [sic]) as: "a meeting or period devoted to a particular activity" [as in "an Irish drinking session", Ed.]. Thus, a given interaction between some set of system entities may involve a notion of session, especially if one or more of the system entities maintain session state.

session state
If an interaction between system entities involves one or more of the system entities maintaining information pertaining to the interaction itself — such as who the other involved system entity(ies) are, when the interaction began, etc. — then there likely is an explicit notion of session and thus this information is termed session state information.

Simple Authentication and Security Layer (SASL)
SASL [RFC2222] is an approach to modularizing protocol design such that the security design components, e.g. authentication and security layer mechanisms, are reduced to a uniform abstract interface. This facilitates a protocol’s use of an open-ended set of security mechanisms, as well as a so-called “late binding” between implementations of the protocol and the security mechanisms’ implementations. This late binding can occur at implementation- and/or deployment-time. The SASL specification also defines how one packages authentication and security layer mechanisms to fit into the SASL framework, where they are known as SASL mechanisms, as well as register them with the Internet Assigned Numbers Authority [IANA] for reuse.
single sign-on (SSO)

From a Principal’s perspective, single sign-on encompasses the capability to authenticate with some system entity — in the Liberty context, an Identity Provider — and have that authentication honored by other system entities, termed Service Providers in the Liberty context.

Note that upon authenticating with an Identity Provider, the Identity Provider typically establishes and maintains some notion of local session state between itself and the Principal’s user agent. Service Providers may also maintain their own distinct local session state with a Principal’s user agent.

Single Sign-On Service (SSO Service, SSOS)

An ID-WSF-based service providing WSCs a means of obtaining ID-FF authentication assertions [LibertyAuthn].

Single Sign-On Service Consumer (SSO Service Consumer, SSOS Consumer)

A Web Service Consumer (WSC) implementing the client-side of the ID-WSF Single Sign-On Service [LibertyAuthn].

Single Sign-On Service Provider (SSO Service Provider, SSOS Provider)

A Web Service Provider (WSP) implementing the server-side of the ID-WSF Single Sign-On Service [LibertyAuthn].

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 [SOAPv1.1] and [SOAPv1.2].

SOAPO-bound ID-* message

A SOAP message conveying ID-WSF and perhaps ID-SIS header blocks and conveying either an ordinary ID-* message or an ID-* fault message. After being bound to SOAP, the resultant composite messages are referred to as an Ordinary SOAP-bound ID-* Message and a SOAP-bound ID-* Fault Message, respectively.

SOAP header block

A [SOAPv1.2] term meaning: An [element] used to delimit data that logically constitutes a single computational unit within the SOAP header. In [SOAPv1.1] these are known as simply SOAP headers, or simply headers. Liberty specifications borrow the SOAPv1.2 terminology.

SOAP-bound ID-* message

A SOAP message conveying ID-WSF and perhaps ID-SIS header blocks and conveying either an ordinary ID-* message or an ID-* fault message. After being bound to SOAP, the resultant composite messages are referred to as an Ordinary SOAP-bound ID-* Message and a SOAP-bound ID-* Fault Message, respectively.

SOAP node

A [SOAPv1.2] term describing system entities who are parties to SOAP-based message exchanges that are, for purposes of this specification, also the ultimate destination of the exchanged messages, i.e. SOAP endpoints. In [SOAPv1.1], SOAP nodes are referred to as SOAP endpoints, or simply endpoints. The Liberty specifications borrow the SOAPv1.2 terminology.

SP

See Service Provider.

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].
Liberty Alliance Project:  
Liberty Technical Glossary

580  SSO  
581  See single sign-on.

582  SSOS, SSO Service  
583  See Single Sign-On Service.

584  SSOS Provider, SSO Service Provider  
585  See Single Sign-On Service Provider.

586  system entity  
587  An active element of a computer/network system. For example, an automated process or set of processes, a  
588  subsystem, a person or group of persons that incorporates a distinct set of functionality [SAMLGloss].

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

593  token  
594  See security token.

595  trust circle  
596  See Circle of Trust.

597  Trusted Authority  
598  In Liberty, a Trusted Third Party (TTP) which issues and vouches for assertions, otherwise known as an  
599  Identity Provider.

600  Trusted Third Party  
601  In general, a security authority or its agent, trusted by other entities with respect to security-related activities.  
602  In the context of Liberty, these other entities are, for example, Principals and Service Providers, and the  
603  trusted third party is typically the Identity Provider(s) involved in the particular interaction of interest.

604  TTP  
605  See Trusted Third Party

606  URI (Uniform Resource Identifier)  
607  A compact string of characters for identifying an abstract or physical resource. [RFC3986] defines the generic  
608  syntax of URIs. URNs and URLs are proper subsets of URIs.

609  URL (Uniform Resource Locator)  
610  URLs identify resources via a representation of their primary access mechanism (e.g., their network location)  
611  rather than identifying the resource by name or by some other attributes of that resource [RFC3986]. URLs  
612  are a proper subset of URIs.

613  URN (Uniform Resource Name)  
614  Persistent, location-independent, resource names with delegatable sub-namespaces, termed Uniform Re-  
615  source Name (URN) Namespaces [RFC2141]. Liberty’s URN Namespace is defined in [RFC3622]. URNs  
616  are a proper subset of URIs.

617  user agent  
618  Software that a “natural person” interacts with directly. A user agent typically implements a user interface.  
619  A typical user agent is a web browser. A more specialized sort of user agent is the Liberty-enabled User  
620  Agent or Device (LUAD).

Liberty Alliance Project
The controls (such as menus, buttons, prompts, etc.) and mechanisms (such as selection and focus) provided by, e.g., a user agent.

A generic web service (gWS) may be defined in various standardized and/or proprietary contexts. Various organizations, formal or ad-hoc, have their own particular definitions for this term. For example, the W3C’s definition (see http://www.w3.org/TR/ws-gloss/) is:

There are many things that might be called "Web services" in the world at large. However, for the purpose of this Working Group and this architecture, and without prejudice toward other definitions, we will use the following definition:

A Web service is a software system designed to support interoperable machine-to-machine inter-action over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

(2) As specifically used in Liberty specifications, usually in terms of WSCs and WSPs, it means a web service that’s defined in terms of the ID-* "stack", and thus utilizes [LibertySOAPBinding], [LibertySecMech], and is "discoverable" [LibertyDisco]. See also identity web service.

Note that Liberty Identity Web Services also meets the W3C definition.

A role donned by a system entity when it makes a request to a web service.

A means to describe the interface of a Web service. See [WSDLv1.1].

A role donned by a system entity when it provides a web service.

A markup language based on XML and intended for use in specifying content and user interface for narrowband devices, including cellular phones and pagers.

See Web Service Consumer.

See Web Services Description Language.

See Web Service Provider.

A X.509 token is a type of security token containing an X.509 public key certificate.

A W3C technology for encoding information and documents for exchange over the Web. See [XML], [XMLCanon], [XMLDsig], [xmlenc-core], [Schema1] and [Schema2]
References

Normative


Informative


