Liberty Specs Tutorial

WWW.PROJECTLIBERTY.ORG
Tutorial Outline

- Introduction to Liberty Alliance
- Overview & Key Concepts
- Resources
- Architecture and Spec documents
- Phase 1 - ID-FF
  - Federated identity life-cycle
  - Metadata
  - SCR & Interoperability Conformance/Validation
  - Security Mechanisms
- Phase 2 - ID-WSF & ID-SIS
  - Personal profile scenario
- Privacy & Security Guidelines
- Business Guidelines
Identity Needs

- What are your needs for identity management?
- What are your customers’ needs for identity management?
- What are the costs and how long will it take?
What is the Liberty Alliance?

- A **business** alliance, formed in Sept 2001 with the goal of establishing an open standard for federated identity management
- Global membership consists of consumer-facing companies and technology vendors as well as policy and government organizations

**Goals:**

- Provide open standard and business guidelines for federated identity management spanning all network devices
- Provide open and secure standard for SSO with decentralized authentication and open authorization
- Allow consumers/businesses to maintain personal information more securely, and on their terms
Liberty Organizational Structure

Management Board

- 16 founding sponsors
- Responsible for overall governance, legal, finances, and operations
- Final voting authority for specifications

Business Marketing Expert Group

- Develops requirements and use cases
- Responsible for evangelism and public relations
- Develops business templates and guidelines
- Accelerates market creation

Technology Expert Group

- Develops technical architecture
- Develops technical specifications
- Defines interoperability & conformance programs

Public Policy Expert Group

- Advises on privacy, security, and global public policy issues
- Liaison to privacy groups and government agencies
- Develops privacy guidelines and best practices for publication

All members provide feedback on early drafts
Who is the Liberty Alliance today?

Over 160 for-profit, not-for-profit and government organizations, representing a billion customers, are currently Alliance members.

The following represent Liberty’s Board Members and Sponsors
Open Interaction and Participation

Standards Bodies
- IETF
- W3C
- OASIS
- OMA

Other technologies
- MS Passport
- WS-Federation

Utilize & Influence
Co-operate

Develop & Deploy

Liberty Alliance and Members

Government
Lobby Groups
Media
Users

Vendors/Providers
- Sun
- AOL
- HP
- Nokia

Open Source Community
Apache
Key Concepts and Terminology

- Identity
- Simplified Sign-On
- Single Logout
- Network Identity / Federated Identity
- Circle of Trust
  - Principal
  - Identity Provider (IdP)
  - Service Provider (SP)
  - Liberty Enabled Clients or Proxies (LECP)
- Pseudonyms & Anonymity
- Authentication Assertion (SAML)
## Key Concepts

### Network Identity Concepts

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DEFINITION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes:</td>
<td>Traits, profiles, preferences of an identity, device, or business partner</td>
<td>- Personal consumer preferences (e.g., travel, entertainment, dining) - Identity-specific histories (e.g., purchases, medical records, etc.) - Device capabilities information (e.g., text-only, video, etc.)</td>
</tr>
<tr>
<td>Authentication:</td>
<td>A level of security guaranteeing the validity of an identity representation</td>
<td>- Govt issued (Drivers license, social security, Passport) - Biometric (Fingerprint, Retinal Scan, DNA) - Self-selected (PIN number, secret password)</td>
</tr>
<tr>
<td>Authorization:</td>
<td>The provisioning of services or activities based upon an authenticated identity</td>
<td>- Services based on attributes (e.g., Travel, entertainment, dining) - Transaction consummation - Gradient levels of service (e.g., based on employee level)</td>
</tr>
</tbody>
</table>
Simplified Sign-On (aka Single Sign-On)

- Simplified Sign-On allows a user to sign-on once at a Liberty enabled site and to be seamlessly signed-on when navigating to another Liberty-enabled site without the need to authenticate again. Simplified sign-on is supported both within a circle of trust and across circles of trust.
Key Concepts

Single Logout

- **Single Logout** provides synchronized session logout functionality across all sessions that were authenticated by a particular identity provider.
Key Concepts

**Federated Network Identity**

- **Network Identity** is the fusion of network security and authentication, user provisioning and customer management, single sign-on technologies, and Web services delivery.

- A **federated identity** architecture delivers the benefit of simplified sign-on to users by granting rapid access to resources to which they have permission, but it does not require the user's personal information to be stored centrally.
“Circle of Trust” Concept

Network Identity Hub Provider

Partner A
Partner B
Partner C
Partner D
Partner E
Partner F
Partner G
Partner H

External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner
External Federated Partner

A circle of trust is 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.
“Circle of Trust” Model

Identity Service Provider
(e.g. Financial Institution, HR)
- Trusted entity
- Authentication infrastructure
- Maintains Core Identity attributes
- Offers value-added services (optional)

Affiliated Service Providers
- Offer complimentary service
- Don't (necessarily) invest in authentication infrastructure

Circle of Trust
- Business agreements
- SLAs
- Policies/Guidelines/AUP

Network Identity Hub Provider

Partner A
Partner B
Partner C
Partner D
Partner E
Partner F
Partner G
Partner H
Key Concepts

Circle of Trust Participants

• 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.

• An **Identity Provider** (IdP) is 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.

• A **Service Provider** (SP) is an entity that provides services and/or goods to Principals.
Key Concepts

Liberty Enabled Clients or Proxies (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.
Key Concepts

Pseudonyms & Anonymity

- Pseudonyms are arbitrary names 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.

- Anonymity enables a service to request certain attributes without needing to know the user’s identity. For example, in order to provide personalized weather information to a user, a weather service provider can ask for a user’s zip code using anonymous service request without knowing the identity of that user.
An assertion is 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.

SAML is an XML standard for exchanging authentication and authorization data between security systems.

http://www.oasis-open.org/committees/security/#documents
Key Concepts

Authentication Assertion (SAML)

Authentication Assertion
- Assertion ID
- Issuer
- Issue Instant (timestamp)
- Validity time limit
- Audience Restriction

Authentication Statement
- Authentication Method
- Authentication Instant
- User account info (IdP pseudonym)
- User account info (SP pseudonym)

Digital Signature of assertion
Resources

- Liberty Developer Resource Center
  www.projectliberty.org/resources/resources.html
- SAML
  www.oasis-open.org/committees/security
- SOAP
  www.w3.org/2000/xp/Group/
- SSL/TLS
  www.ietf.org/html.charters/tls-charter.html
Phases to Interoperable Federated Identity Services

- **Phase 1**
  - Simplified sign-on and identity federation (ID-FF)
  
- **Phase 2**
  - Web Services Framework (ID-WSF)

- **Future Phases**
  - Enhancements to Federation and Services Infrastructure (ID-SIS)

**INCREASED BUSINESS VALUE**

**INCREASED INTEROPERABILITY**

- **JULY 2002-JANUARY 2003**
- **MID 2003**
- **2003-2004**
Complete Liberty Architecture

Liberty Identity Federation Framework (ID-FF)
Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management.

Liberty Identity Services Interface Specifications (ID-SIS)
Enables interoperable identity services such as personal identity profile service, alert service, calendar service, wallet service, contacts service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)
Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles.

Liberty specifications build on existing standards
Spec Summary

**ID-FF**

- **Liberty ID-FF Architecture Overview** is a non-normative summary description of the Liberty ID-FF architecture, including policy and security guidance.

- **Liberty ID-FF Implementation Guidelines** defines the recommended implementation guidelines and checklists for the Liberty architecture focused on deployments for the service-providing entities: service providers, identity providers, and Liberty-enabled clients or proxies (LECPs).

- **Liberty ID-FF Static Conformance Requirements**

- **Liberty ID-FF Protocols & Schema** defines the abstract protocols and XML schemas for Liberty.

- **Liberty ID-FF Bindings & Profiles** defines concrete transport bindings and usage profiles for the abstract Liberty protocols.

- **Liberty Authentication Context** defines the authentication context schema, which is used to communicate information about an authentication event.

- **Liberty Metadata** describes metadata, protocols for obtaining metadata, and resolution methods for discovering the location of metadata.
Liberty ID-WSF Architecture Overview is a non-normative document intended to provide an overview of the features of the Liberty ID-WSF Version 1.0 Specifications.

Liberty ID-WSF Security & Privacy Overview is a non-normative document providing an overview of the security and privacy issues in ID-WSF technology and briefly explaining potential security and privacy ramifications of the technology used in ID-WSF.

Liberty ID-WSF Static Conformance Requirements

Liberty ID-WSF Data Services Template provides protocols for the querying and modifying of data attributes when implementing a data service using the Liberty Identity Web Services Framework (ID-WSF).

Liberty ID-WSF Discovery Service describes protocols and schema for the description and discovery of ID-WSF identity services.

Liberty ID-WSF Interaction Service specifies an identity service that allows providers to pose simple questions to a Principal.

Liberty ID-WSF Security Profiles specifies security mechanisms that protect identity services.

Liberty ID-WSF SOAP Binding defines the Liberty Identity Web Services Framework (ID-WSF) SOAP binding. It specifies simple SOAP message correlation, consent claims, and usage directives.

Liberty Reverse HTTP Binding for SOAP specifies a binding that enables HTTP clients to expose services using the SOAP protocol, where a SOAP request is bound to an HTTP response, and a SOAP response is bound to an HTTP request.
Spec Summary

**ID-SIS**

- **Liberty ID-SIS Personal Profile** describes a web service that provides a Principal's basic profile information, such as their contact details, or name.
- **Liberty ID-SIS Employee Profile** offers profile information regarding employee.
Phase 1 - ID-FF

- Federated identity life-cycle
- Metadata
- SCR & Conformance
- Security Mechanisms
Federated Identity Life-Cycle

1. Metadata Exchange
2. Federate
3. Single Sign On (already federated)
   - Name Registration
   - Single Log Out
   - Federation Termination
Metadata specification extensible framework for describing
  - cryptographic keys
  - service endpoints information
  - protocol and profile support in real time

Metadata exchange options:
  - In-band DNS based discovery
  - In-band URI based discovery
  - Out-of-band

Classes of metadata:
  - Entity provider metadata
  - Entity affiliation metadata
  - Entity trust metadata

Origin and document verification through use of signatures
- **Optional** profile

- **Common Domain Cookie**
  - MUST be named `_liberty_idp`
  - MUST be base-64 encoded list of IdP succinct Ids
  - Session or Persistent

- **Common domain established within the identity federation network for use with introduction protocol**
Single Sign On and Federation

**User**
- Login/Authenticate
- Introduction cookie
- Login/Authenticate
- You have a cookie from IDP, federate accounts?
- Yes, federate my accounts
- Redirect to IDP with Authentication Request
- AuthnRequest
- Authentication Assertion Issued
- Redirect to SP
- Here is my SAML Assertion or SOAP endpoint @ IDP
- SOAP

**SP**
- SOAP
- Process Assertion
- Start service
Federating an Identity

Airline, Inc
Welcome to Fly Right Airline Group

Do you want to federate your Car Rental, Inc. account?
Yes Cancel

CarRental, Inc
Fly Right Airline Group

Welcome John12
You’re signed on.

Perform federation

IdP A
Airline, Inc
SP 1
CarRental, Inc

Access after Federation
Account Federation Details (1)

- User connects to IdP and authenticates

Airline, Inc
Fly Right
Airline Group

Login: John
Password: xxx

User goes to IdP of his choosing and authenticates himself. For example, using ID and password.

Enter URL, connect to IdP

Authentication Request

User authentication (e.g., ID and password)

Other authentication methods are possible (e.g., certificate-based, Kerberos, etc.)

Authentication Check

Web page is displayed
Account Federation Details (2)

- User can choose to federate accounts with the IdP

**Welcome, John**

You can link the following accounts

- **Car Rental, Inc**

After authenticating with the IdP other accounts that can be federated are listed.

**Airline, Inc**

Fly Right

Airline Group

User IDP

SP

Identity Provider

Service Provider

User

IDP

SP

Begin Federation

Initial authentication

Authentication Completed

Federation Request

Begin Federation
Federation initiated at the IdP

- Federation requires connecting to the SP and authenticating once.

Car Rental, Inc
Fly Right
Airline Group

ID: [ ]
Password: [ ]

☑ Federate with Airline, Inc

OK

User
IDP
SP

Redirect to SP for federation

User authentication

SP login and federation opt-in

Authentication Check

Federation Processing
User handles (name identifiers)
– Eliminates need for global ID
– Prevents collusion between SP1 and SP2
Instead of the SP directly authenticating the user, the SP queries the IdP and the IdP issues an authentication assertion.
- User connects to IdP and authenticates

**Identity Provider**

User goes to IdP of his choosing and authenticates himself. For example, using ID and password.
- User chooses an SP

- **Airline, Inc**
  - Fly Right
  - Airline Group
- **Welcome, John**
- **Federated SPs**
  - Car Rental, Inc
  - Hotels, Inc

- **User is connected to the SP he chooses**

- **Identity Provider**

- **Service Provider**

- **User**
  - Choose SP or enter URL
  - IdP web page is displayed

- **IDP**

- **SP**
  - Authentication Request
- User redirected to IdP based on authentication request from SP

User authentication request results in redirect to IdP

SP can specify the authentication level it requires
IdP issues an authentication assertion

- Assertion is generated if user is authenticated and identity at the SP is federated.
- If user is not already authenticated at IdP then initial authentication is performed.

IdP: Identity Provider
SP: Service Provider
User
Authentication Request (redirect)
Authentication Assertion Issued
Airline Inc
Fly Right
Airline Group
Login: [ ]
Password: [ ]
Single Sign-On (5)

- Authentication assertion sent from IdP to Sp

- Secure communication channel (SSL) is required

- Only Browser Post profile

- In Browser-artifact profile the IdP and SP would exchange the authentication assertion between themselves (back-channel)

- Authentication assertion sent (SOAP)
- SP checks the authentication assertion and allows access to service

User

Check authentication assertion

Start service

IDP

Car Rental.inc

Fly Right

Airline Group

Welcome, John123

[Authenticated]

Service Provider

Check authentication assertion

Identity Provider

Service started
Available profiles:
- Browser Artifact
- Browser POST
- LECP
Browser Artifact Single Sign-On Profile

1. GET <inter-site transfer service host name and path>?RelayState=<resource URL>

2. Obtain IdP

3: 302; Location: <IdP Single Sign-On Service>?<AuthnRequest>()

4: GET <IdP Single Sign-On Service>?<AuthnRequest>()

5. Process AuthnRequest

6: 302; Location: <SP Assertion Consumer URL>?RelayState=<resource URL>&SAMLart=<...>

7: GET <SP Assertion Consumer URL>?RelayState=<resource URL>&SAMLart=<...>

8. SOAP POST: <samlp:Request>()

9: 200 OK SOAP: <samlp:Response>()

10. Process Assertion

11: 200 OK: <resource URL>()
Browser POST Single Sign-On Profile

1. GET <inter-site transfer service host name and path>?RelayState=<resource URL>
2. Obtain IdP
3. 302; Location: <IDP Single Sign-On Service><AuthnRequest>
4. GET <IDP Single Sign-On Service>?<AuthnRequest>
5. Process AuthnRequest
6. HTTP 200; FORM; METHOD=POST; ACTION=<SP assertion consumer URL>; LARES=<AuthnResponse>
7. POST <SP assertion consumer URL>; LARES=<AuthnResponse>
8. SOAP POST: <samlp:Request>
9. 200 OK SOAP: <samlp:Response>
10. Process Assertion
11. 200 OK: <resource URL>
LECP Single Sign-On Profile

1. HTTP Request; Liberty-Enabled Header()

2. Obtain IdP

3: 200 OK <AuthnRequestEnvelope>; Liberty-Enabled Header

4: SOAP POST: <AuthnRequest>; Liberty-Enabled Header()

6: 200 OK SOAP: <AuthnResponseEnvelope>; Liberty-Enabled Header()

7: POST <SP Assertion Consumer URL; LRES=<AuthnResponse>; Liberty-Enabled Header

8. SOAP POST: <sampl:Request>()

9: 200 OK SOAP: <sampl:Response>()

5. Process AuthnRequest

10. Process Assertion

11. HTTP Response; Liberty-Enabled Header()
Single logout initiated at the IdP

- **Airline, Inc**
  - **Fly Right**
  - **Airline Group**

  - Do you want to logout?
  - Yes

  - **Logout from all Service Providers**

  - The IdP can offer to logout the user from all sessions that were authenticated by this IdP

  - User
    - IdP logout web page is displayed
    - Single logout request
      - * Only SOAP/HTTP-based profile.** With HTTP Redirect and HTTP GET profiles the user agent contacts each SP directly
      - Single logout confirmed
    - Single logout request
    - Single logout response

  - **Identity Provider**
    - Logout Request Sent
    - Service Provider
      - Process logout
      - Authentication Completed
Single Logout

- Can be initiated at either the IdP or SP
- Available profiles
  - HTTP-Based
    - For IdP-initiated: HTTP-Redirect or HTTP GET
    - For SP-initiated: HTTP-Redirect
  - SOAP/HTTP-based
IdP-initiated Single Logout
SOAP/HTTP-based
• Can be initiated at either the IdP or SP
• Available profiles
  – HTTP-Redirect-Based
  – SOAP/HTTP-based
IdP-initiated Federation Termination Notification

HTTP-Redirect

1. HTTP Request()

2. 302: Location: <Federation Termination service at SP>?<FederationTerminationNotification>

3. GET: <Federation Termination service at SP>?<FederationTerminationNotification>

4. Process Request

5. 302: Location: <Return URL at Identity Provider>()

6. GET: <Return URL at Identity Provider>()

7. 200 OK: <Confirmation Message>()
IdP-initiated Federation Termination Notification

SOAP/HTTP-based

1. GET <Federation Termination service host name and path>()
2. SOAP POST: <lib:FederationTerminationNotification>()
3. Process Request
4: 204 OK:()
5: 200 OK: <Confirmation Message>()
Static Conformance Requirements

- SCR (ID-FF 1.1) describes four profiles and the specific features (required or optional) for each profile
  - IDP
  - SP Basic
  - SP Complete
  - LECP
<table>
<thead>
<tr>
<th>Feature</th>
<th>IDP Profile</th>
<th>SP Basic</th>
<th>SP Complete</th>
<th>LECP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-On using Artifact Profile</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Sign-On using Browser POST Profile</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Sign-On using LECP Profile</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Register Name Identifier (IdP Initiated) - HTTP Redirect</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Register Name Identifier (IdP Initiated) - SOAP/HTTP</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Register Name Identifier (SP Initiated) - HTTP Redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Register Name Identifier (SP Initiated) - SOAP/HTTP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Federation Termination Notification (IdP Initiated) - HTTP Redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Federation Termination Notification (IdP Initiated) - SOAP/HTTP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Federation Termination Notification (SP Initiated) - HTTP Redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Federation Termination Notification (SP Initiated) - SOAP/HTTP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Logout (IdP Initiated) - HTTP Redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Logout (IdP Initiated) - HTTP GET</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Logout (IdP Initiated) - SOAP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Logout (SP Initiated) - HTTP Redirect</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Single Logout (SP Initiated) - SOAP</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>MUST</td>
<td></td>
</tr>
<tr>
<td>Identity Provider Introduction</td>
<td>MUST</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>57</td>
</tr>
</tbody>
</table>
Interoperability Validation

- A vendor becomes eligible to be licensed to use the “Liberty Interoperable” Logo by asserting compliance against one or more Liberty Alliance SCR conformance profiles and then participating in a Liberty Alliance InterOp event to validate the assertion(s).
Security Mechanisms

### Channel Security
- SPs authenticate IdPs using IdP server-side certificates
- Mutual authorization: SPs configured with list of authorized IdPs and IdPs configured with list of authorized SPs
- Before user presents personal authentication data to IdP, the authenticated identity of IdP must be presented to the user

### Message Security
- Digital signatures should use key pairs distinct from those used for TLS and SSL, also suitable for long-term
- Request protected against replay and responses checked for correct correspondence with issued requests
Not all SAML assertions ‘are created equally’
  – Different Authorities will issue SAML assertions of different quality
How will a consumer of these assertions discriminate?
Authentication Context is the information *extra* to the SAML assertion itself that describes:
  – Identification, e.g. Physical verification
  – Physical Protection, e.g. Private Key in hardware
  – Operational Protection, e.g. N of M controls
  – Authentication Mechanisms e.g. Smartcard with PIN
Gives a consumer of a SAML assertion the information they need in order to determine how much assurance to place in the assertion
Liberty defined an XML Schema by which the Authority can assert the context of the SAML assertions it issues.

Liberty also defined Authentication Context ‘classes’ – patterns against which an IdP can claim conformance.

Classes are designed to be representative of today's (and future) authentication technologies, for instance:
- Password over SSL
- Smartcard
- Pre-paid Mobile Login
- Biometric
SPs have a means to say
- I require that the User be authenticated with:
  • Smart card with private key’,
  • ’Password or better’,
  • ‘Any mechanism, you decide, I trust your opinion’
- The assertion you previously sent is insufficient for my current transaction, authenticate the user again

IDPs have a means to indicate to the SP the specific details
- Password policy requires 8 characters minimum, e.g.
- The User was physically present at registration
Phase 2 - Terms & Concepts

- **Discovery Service** enables various entities (e.g. Service Providers) to dynamically discover a Principle’s registered identity services.

- **Interaction Service** protocols provide an identity service the means to obtain permission from a user.

- **Attribute Provider** hosts a data service - such as ID-Personal Profile.
**Identity Service** is an abstract notion of a web service that acts upon some resource to either retrieve information about an identity, update such information, or perform some action on behalf of the identity.

**Web Services Client (WSC):** typically, the invoker/consumer of an identity service.

**Web Services Provider (WSP):** typically, the provider of an identity service.

**Data Services Template (DST):** provides an extensible framework to produce new Identity Services above the protocol stack, allowing interoperability eg: ID-Personal Profile and ID-Employee Profile.
In many cases, these two entities are co-located, i.e., Disco is the part of IDP. In this scenario, IS is provided with a redirect profile and thus, strictly speaking, IS is not an entity, i.e., IS is one of the functions of AP.
Liberty Identity Federation Framework (ID-FF)

Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management.

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, alert service, calendar service, wallet service, contacts service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles.

Liberty specifications build on existing standards
ID-WSF Security & Privacy Overview
– An overview of the security and privacy issues in ID-WSF technology and briefly explains potential security and privacy ramifications of the technology used in ID-WSF

Privacy and Security Best Practices
– Highlights certain national privacy laws, fair information practices and implementation guidance for organizations using the Liberty Alliance specifications.
Federated Identity cannot be successful based on technology alone

Address business issues that need to be considered when implementing circles of trust and enabling federated network identity

- Mutual confidence
- Risk
- Liability
- Compliance
Business Guidelines
Sample Download Statistics

- **SourceID** enables Liberty federation and SSO and is a good indicator of Liberty interest. Download statistics below*
  - More than 1,000 downloads in 100 days
  - Majority of downloads are by global 1000 corporations
  - Approximately 40% are from companies outside the U.S. Germany (9%) and Japan (8.5%) have highest percentage
  - 72.85% are from companies *not* members of the Alliance
  - 22.8% of the downloads are from governmental or academic institutions
  - Telecommunications/wireless, financial services and manufacturing sectors have highest number of downloads

- **Immediate interest in Liberty’s Phase 2 specifications**
  - Approximately 5,000 downloads of specification-related documents from Liberty’s website three weeks following launch
  - 800 downloads of Liberty’s Privacy Best Practices document from Liberty’s website three weeks following launch

*SourceID sponsored by Liberty member Ping Identity Corporation
Liberty-enabled products & services

Communicator (available)
Computer Associates (Q4*)
DataKey (available)
DigiGan (Q3*)
Ericsson (Q4)
Entrust (Q1 2004)
France Telecom (Q4 2003)
Fujitsu Invia (available)
Gemplus (TBD)
HP (available)
July Systems (available)
Netegrity (2004)
NeuStar (available)
Nokia (2004)
Novell (available)

NTT (TBD)
NTT Software (available)
Oblix (2004)
PeopleSoft (available)
Phaos Technology (available)
Ping Identity (available)
PostX (available)
RSA (Q4)
Salesforce.com (TBD)
Sigaba (available)
Sun Microsystems (available)
Trustgenix (available)
Ubisecure (available)
Verisign (Q4*)
Vodafone (2004)
WaveSet (available)

*Delivery dates being confirmed
For more information…

WWW.PROJECTLIBERTY.ORG