Liberty Alliance Project

Chris Hankin
SUN

Sep. 2002
Establish an open standard for federated network identity through open technical specifications that will:

- Support a broad range of identity-based products and services

- Allow for consumer choice of identity provider(s), the ability to link accounts through account federation, and the convenience of single sign-on, when using any network of connected services and devices

- Enable commercial and non-commercial organizations to realize new revenue and cost saving opportunities that economically leverage their relationships with customers, business partners, and employees

- Improve ease of use for e-commerce consumers
• **Simplified Sign-On:** Provide an open simplified sign-on specification that includes federated authentication from multiple providers operating independently, simplified access across multiple accounts within a trust community, and portable on-line identity

• **Enhance Constituent Relationships:** Enable commercial and non-commercial organizations to control, maintain and enhance relationships with constituents

• **Support All Devices:** Create a network identity infrastructure that supports all current and emerging network access devices

• **Enable Consumer Privacy:** Enable commercial and non-commercial organizations to protect consumer privacy

• **Support Interoperability:** Provide a mechanism supporting interoperability with existing systems, standards, and protocols
Centralized Model

- Network identity and user information in single repository
- Centralized control
- Single point of failure
- Links similar systems

Open Federated Model

- Network identity and user information in various locations
- No centralized control
- No single point of failure
- Links similar and disparate systems
Separate Cards with Each Bank

Linked Cards within Bank Networks

Seamless Access Across all Networks

Individual Accounts with Many Web Sites

Federated Accounts within Trust Domain

Linkage of Trust Domains
Examples of Trust Domains

B2C – Travel Industry

Airline  Car Rental  Hotel  Partner Airlines  Cruise Line  Livery

B2E – Employee Intranet

Company Intranet  401k  3d Party Providers  Employee Purchase Plans  Health Insurance  Dental Insurance

B2B – Financial Services

Treasury  Debt  Equity  Commercial Banking  Clearing House  Credit

B2B – Automotive

Suppliers  Dealers  Manufacturers  Fleet  Financing  Transport Agencies
Specifications: A Phased Approach

Approach Drivers

- Support rapid acceptance and deployment
- Easy incremental adoption

Version 1.0

Federated network identity
Opt-in account linking and simplified sign-on within an authentication domain created by business agreements
Security built across all the features and specifications

Future Versions

Permissions-based attribute sharing
Schema/protocols for core identity profile service
Simplified sign-on across authentication domains created in version 1.0 by business agreements
Delegation of authority to federate identities/accounts
Federated Network Identity and Authentication Sharing

- **Enhance “Affinity” Relationships:** Enable organizations to enhance business relationships by mutually recognizing user authentication across service offerings.

- **Simplify User Experience:** Enable users to login at an organization’s site and then go to a linked site without having to re-authenticate or re-establish identity.

- **Enhance Intra-Enterprise Relationships:** Enable organizations to consolidate identities within their own extended enterprises, enabling customers or employees to move seamlessly from one service to another without having to re-establish their identity or re-authenticate at every site.
Federated Network Identity and Authentication Sharing

- **Enhance “Affinity” Relationships:** Enable organizations to enhance business relationships by mutually recognizing user authentication across service offerings.

- **Simplify User Experience:** Enable users to login at an organization’s site and then go to a linked site without having to re-authenticate or re-establish identity.

- **Enhance Intra-Enterprise Relationships:** Enable organizations to consolidate identities within their own extended enterprises, enabling customers or employees to move seamlessly from one service to another without having to re-establish their identity or re-authenticate at every site.
- Opt-in account linking mechanism
  - Federated network identity and authentication sharing mechanism that is easy to use and interoperable with existing identification systems

- Simplified sign-on
  - For linked accounts

- Improved consumer confidence
  - Extend the best available security measures to identity sharing
  - Provide organizations with guidance about how to provide consumers with permission controls for federated network identity and authentication sharing
• Decentralized approach
  • A fully federated architecture, enabling greater user security and a choice of identity providers
  • Accelerated time to market for identity based services

• Open
  • Open, platform and technology neutral specification

• Interoperability
  • Will seek to ensure interoperability with existing systems, standards, and protocols
Sample Version 1.0 User Experience

1. User Logs on to abc.com
   - User Name: jsmith
   - Password: *****

2. User Hits Link to xyz.com

3. User Asked if Wants to Link Accounts
   - Would you like to link your xyz.com account with your abc.com account?

4. User Logs on to xyz.com
   - User Name: johnsmith
   - Password: ***

5. User Informed Accounts Linked
   - Your accounts at xyz.com and abc.com are now linked!

Next Time User Logs on to abc.com:

1. User Logs on to abc.com
   - User Name: jsmith
   - Password: *****

2. User Hits Link to xyz.com

3. User Given Direct Access to Account at xyz.com
   - Welcome to Your Account at xyz.com, John Smith!
- **Opt-in account linking** – Users can link their accounts with different service providers within “circles of trust”

- **Simplified sign-on for linked accounts** – Once users’ accounts are federated, they log-in, authenticate at one linked account and navigate to another linked account, without having to log-in again

- **Authentication context** – Companies linking accounts communicate the type of authentication that should be used when the user logs-in

- **Global log-out** – Once users log-out of the site where they initially logged in, the users can be automatically logged-out of all of the other sites to which they were linked

- **Liberty Alliance client feature** – Implemented on client solutions in fixed and wireless devices to facilitate use of Liberty version 1.0 specification
- 45 sponsors
- Affiliate and associate memberships opened May 29, 2002
## Membership Levels

### Sponsors
- Full participation and voting in any or all Expert Groups
- Can run to fill Management Board vacancies
- Representatives can be officers in Expert Groups

### Associates
- Can view and comment on draft specifications prior to public release
- Access to alliance member web site
- Can attend semi-annual "All Participants" meetings

### Affiliates
- For government agencies, educational institutions, and non-profit organizations only
- Have same privileges as Associate members
Liberty Alliance Project