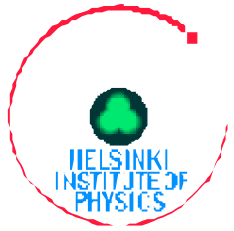
Liberty Alliance

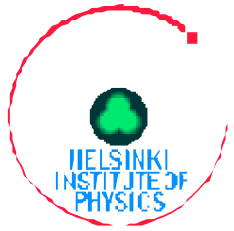


Overview of the Liberty Alliance Architecture

Helsinki Institute of Physics (HIP), May 9th 2003

Mika Silander

Background



- **Liberty Alliance**
  - Formed in September 2001.
  - A large industry driven standardisation organisation, currently 160 collaborating member organisations.
  - Web site: www.projectliberty.org
- **Mission**
  - Create open standards and specifications for identity federation and identity-based services.
  - Favour device neutrality.
  - Access to many services by logging in once (single sign-on).
- **Status**
  - Version 1.1 specifications published.
  - Three groups of specifications.

Liberty objectives

- Enable end users to protect their identity information on the net
- Enable businesses to manage customer relationships without dependence on third-parties
- Create an open single sign-on standard for decentralised authentication and authorization
- Create a network identity infrastructure that supports all current and emerging network devices

The problem and a solution

- **End users obliged to remember numerous Web site accounts and passwords**
- **Personal information**
  - Accounts, names, phone numbers, addresses, credit card numbers.
- **Identity as Liberty Alliance sees it**
  - **Accounts + passwords.**
  - An end user's other personal information**.**

Federated network identity

- **Enables single sign-on**
  - **Allows a user to "link" her different web accounts together but still control what other personal info is given to the individual service providers.**
- **A user account**
  - **The starting point of federation.**
- **An end user's personal info ...**
  - **that, in all or part, can be distributed within a circle of trust.**
  - **whose distribution is completely controled by the end user herself.**

Liberty principals

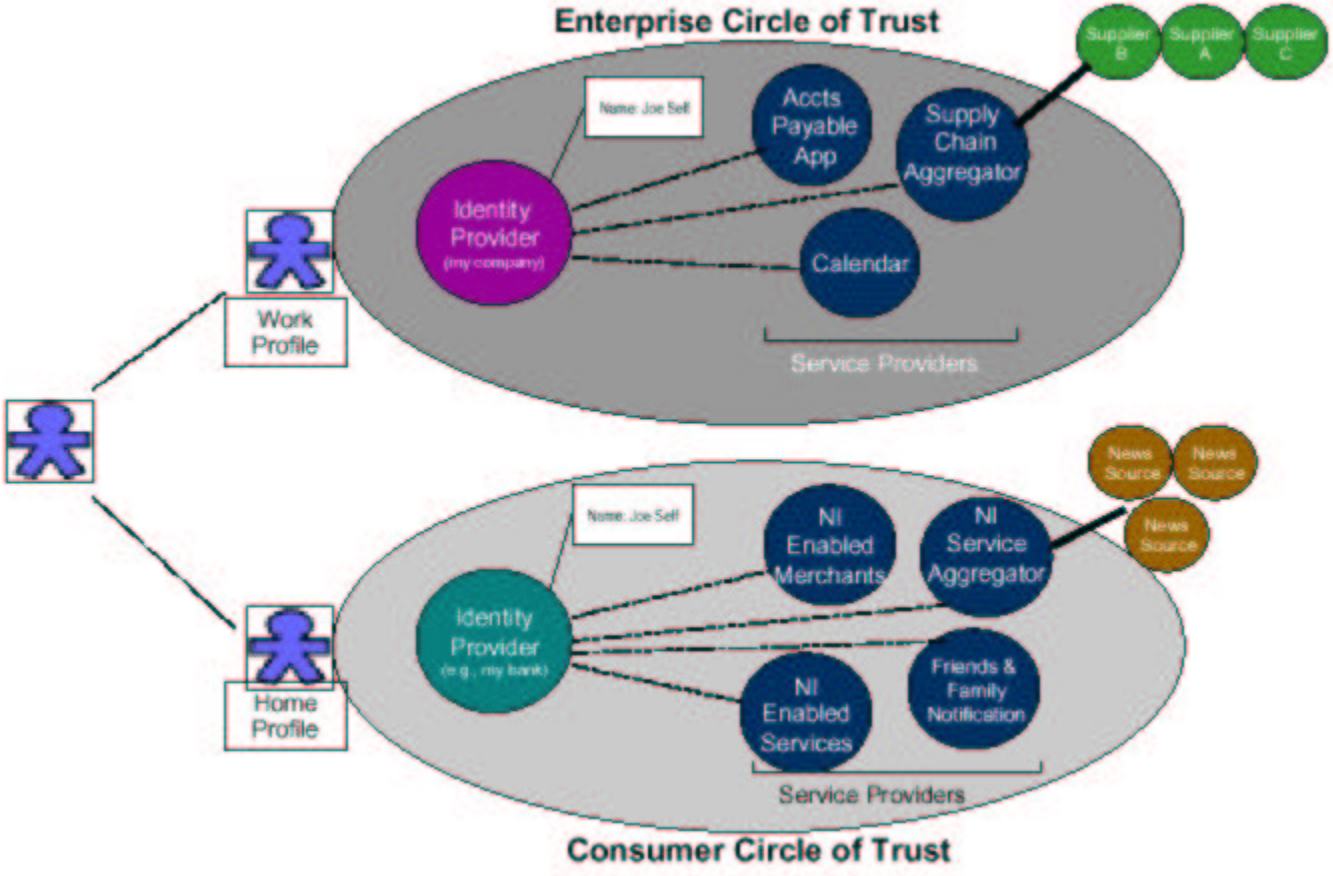


Figure: Federated Identity and Circles of trust

(source: Liberty ID-FF Architecture Overview draft v1.2-03)

Liberty principals & concepts

- **Identity providers (IDPs)**
  - Initiates end user identity federation.
  - Maintain user profile information.
  - Distribute (federate) user identities and profiles.
- **Service providers (SPs)**
  - Affiliate with identity providers.
  - Maintain user profile information.
- **Circles of trust**
  - Communities of IDPs and SPs that share federated identities.
  - Adhere to commonly defined business agreements and procedures.
- **The end user**
  - Controls what info is federated to whom and how.

Liberty architecture

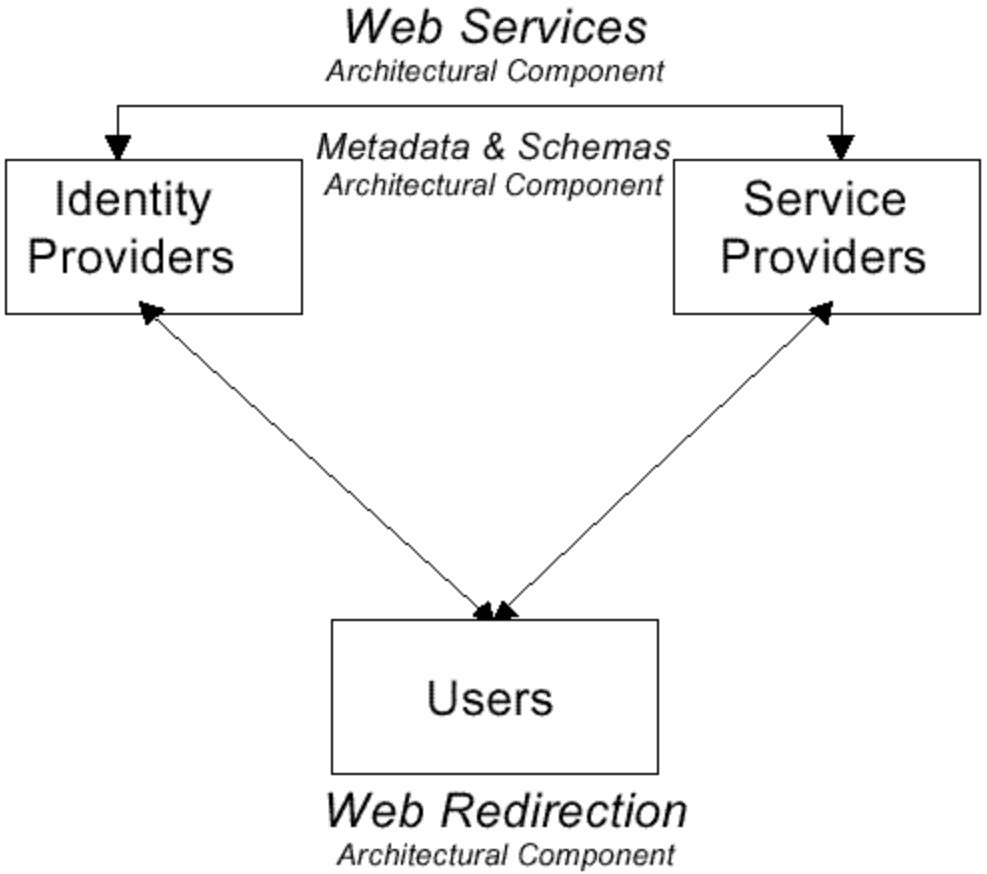
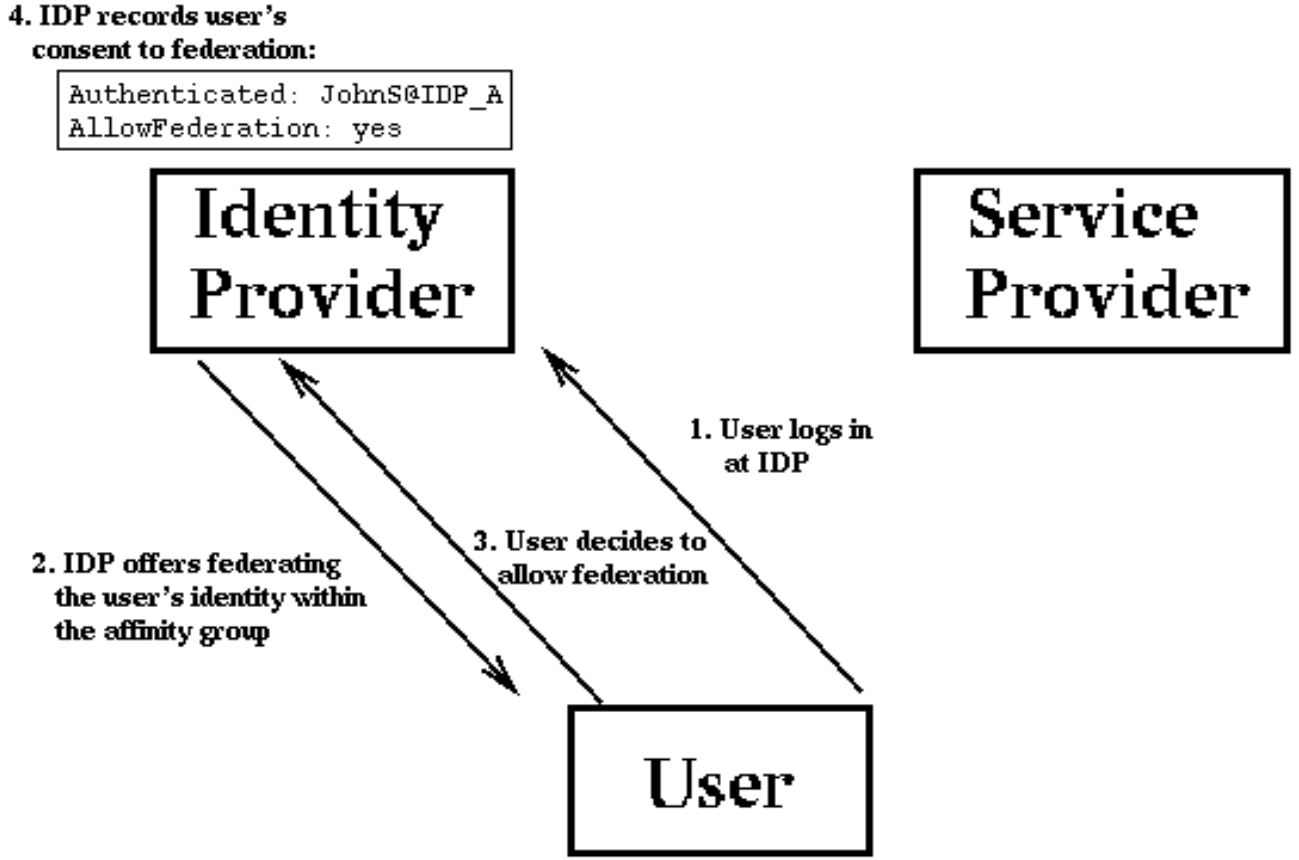
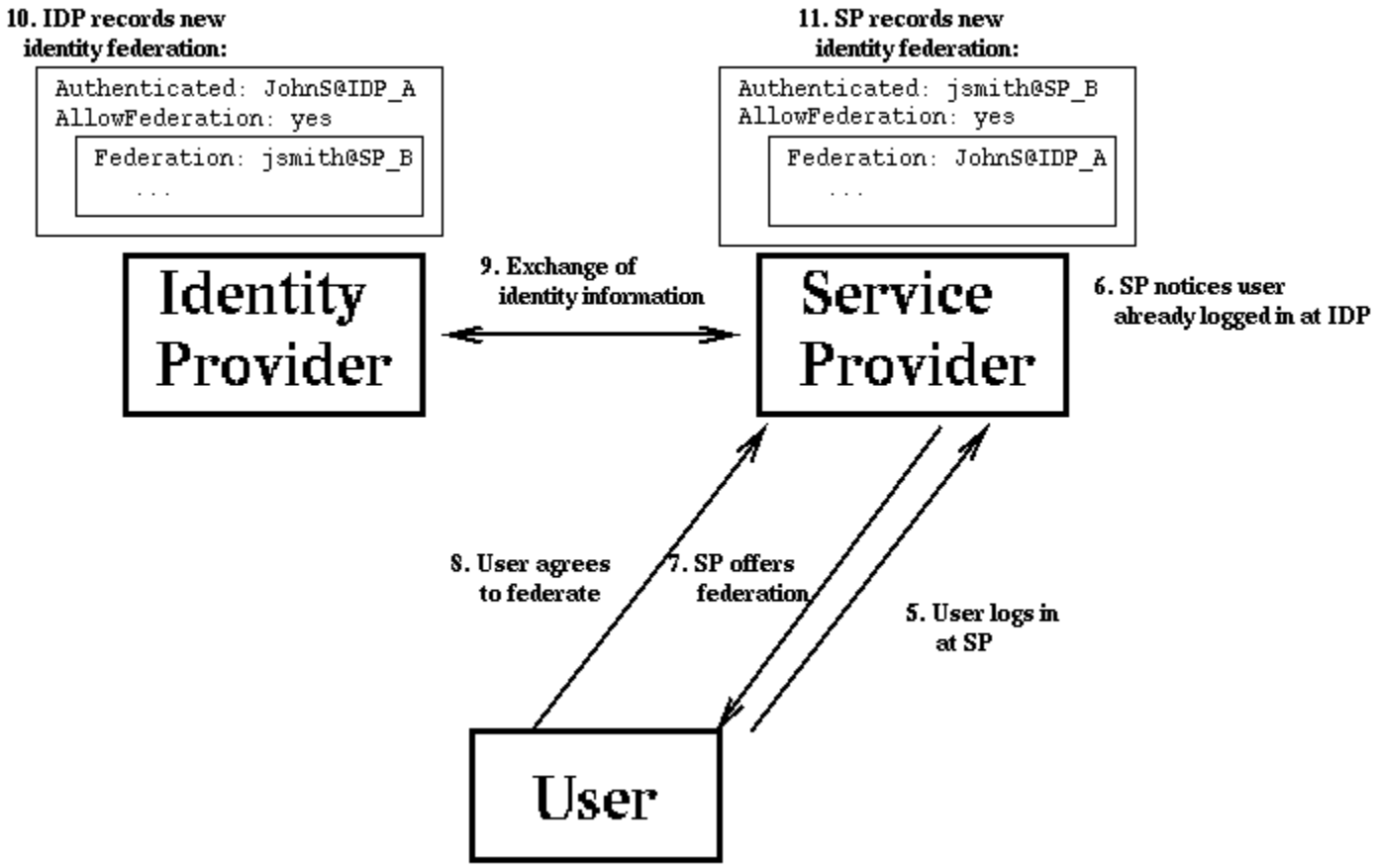


Figure: Liberty Alliance architecture
(source Liberty ID-FF Architecture Overview draft v1.2-03)

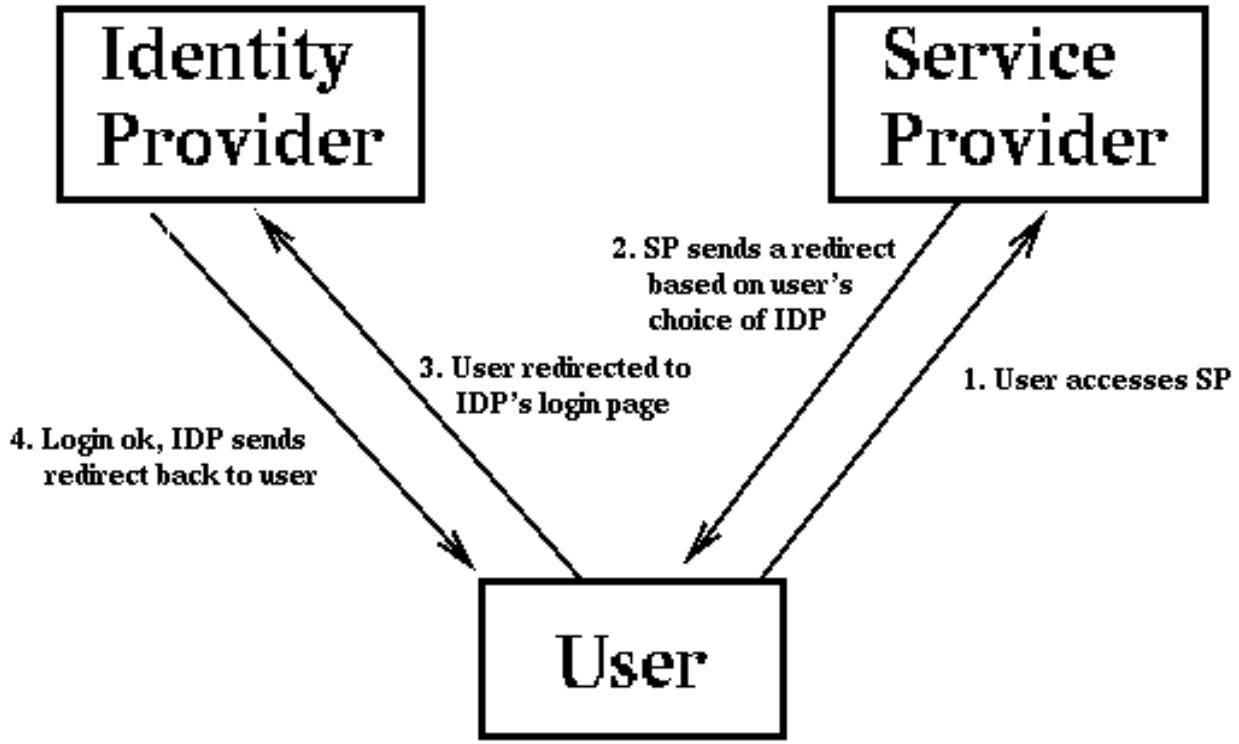
Federating an identity



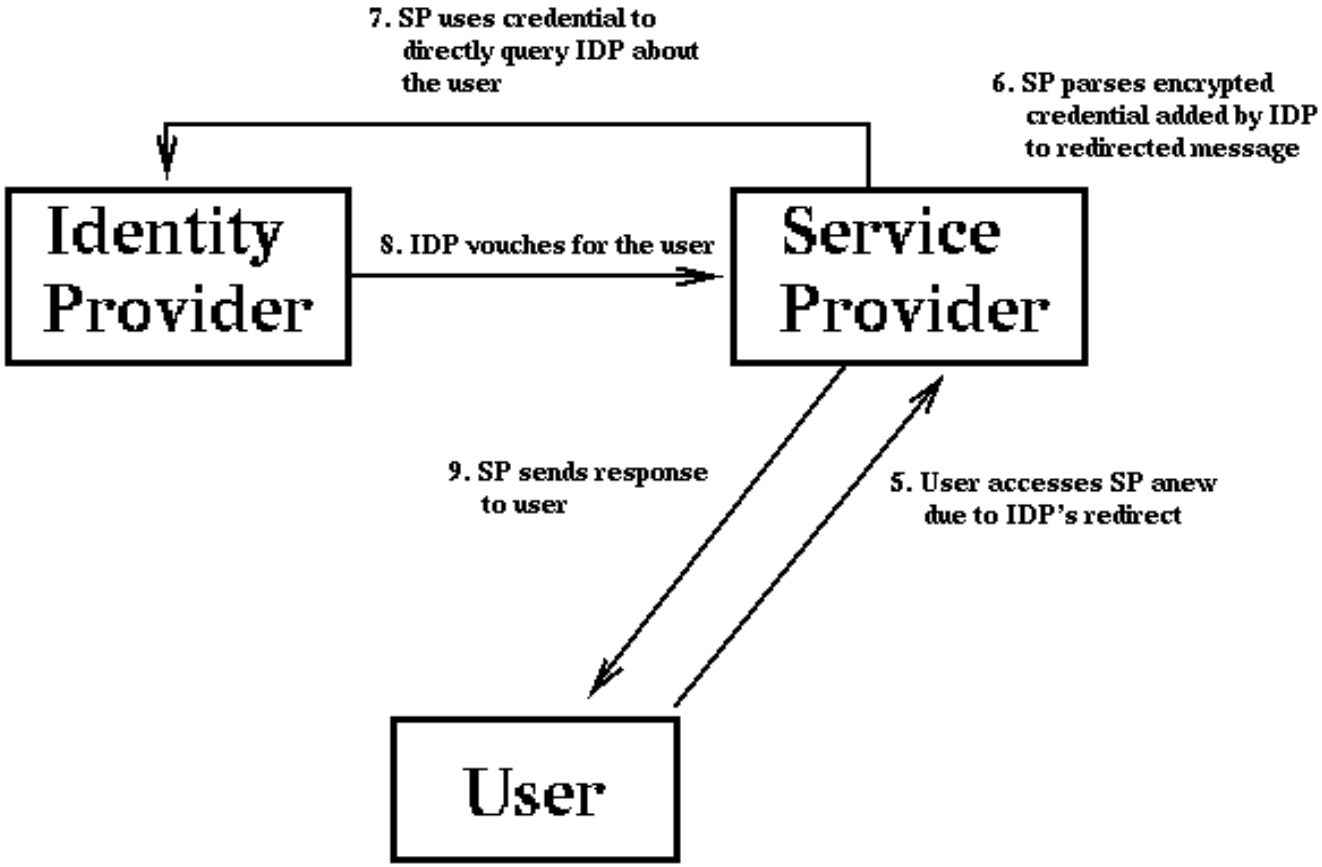
Federating an identity (cont.)



User login


Identity Provider
Service Provider
2. SP sends a redirect based on user's choice of IDP
3. User redirected to IDP's login page
1. User accesses SP
4. Login ok, IDP sends redirect back to user
User

User login (cont.)



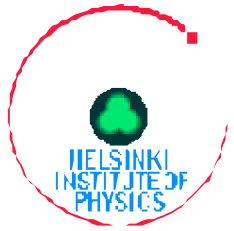
Liberty security features

- Authentication only.
- Authorisation based on access rights tied to the local account.
- Accounting and billing internal to every service provider.
- Single logout.
- Mutual authentication using certifates and secured communication channels required for IDP <-> SP interactions, but weaker methods allowed for user authentication.
- Standards: SAML, various WS security standards, SSL, TLS, PKI.

Security features in grids

- **PKI solutions.**
- **Authentication handled, authorisation management tools with grid-wide scope being developed.**
- **Accounting and billing not yet available.**
- **Web services related security technologies are being adopted.**

Comparisons & conclusions

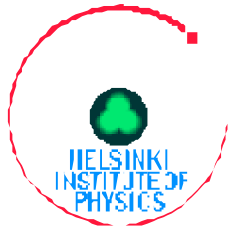


- **Liberty**
  - Security architecture more limited in scope.
  - Security mechanisms a mixed bag of established and evolving technologies and standards.
  - Reliance on redirection.
  - Allows service tailoring based on user profiles.
  - Needs more adopters.
  - Apparently device and software neutral but in practise geared towards browser centred usage and devices.
- **Grids**
  - Security goals more ambitious, extend beyond just simple authentication.
- **Grid and Liberty interoperability**
  - Various levels of iop and options: turning grid services to Liberty service providers, using grid certs transparently for Liberty auth etc

Software

- SourceId
  - Open source solutions for Liberty Alliance identity management.
  - www.sourceid.org
- Sun One Identity Server
- Novell eDirectory's Identity provider
- PingId
  - Provider of Liberty Alliance integration services and interoperability testing.
  - www.pingid.com
- Other 3rd party authentication solutions
  - .NET/Passport
  - Ping ID
  - 3-D Secure
  - Shibboleth

References



1. Liberty ID-FF Architecture Overview draft v1.2-03, J.Hodges & T.Wason, 2003
2. Grid and Liberty Alliance Framework: Goals, Architectures and Feasibility Study for Integration, H.Mikkonen & T.Nissi, Helsinki Institute of Physics, 2003
3. Introduction to the Liberty Alliance Identity Architecture, rev. 1.0, Liberty Alliance, 2003
4. Identity Systems and Liberty Specification Version 1.1 Interoperability, Technical White Paper, Liberty Alliance, 2003
5. Liberty ID-FF Protocols & Schema Specification v1.2-08, S.Cantor & J.Kemp, 2003