What The Industry Needs

- Ubiquitous, **interoperable**, privacy-respecting, identity layer:
  - Liberty represents all constituencies toward this objective
    - (vendors, enterprise, government, consumers, universities, SME’s, etc.)
  - Must be an open, collaborative system vs. single vendor strategy
  - Identity is important & complex. We must come together OR:
    - industry will become more fractured
    - governments will intervene
- Privacy-compliant practices to exchange identity information
- Standards-based model to …
  - Interoperate in heterogeneous environments
  - Avoid proprietary vendor lock-in
  - Provide flexible foundation for future growth
  - Scale to the WWW
- Consumer & enterprise confidence that security, privacy and data integrity will be maintained.
150 diverse member companies and organizations representing leaders in IT, mobility, government, service provision, system integration and finance working collaboratively to address the technology, business and policy aspects of digital identity management

Who is Liberty Alliance?

Management Board

Members include…
How Do We Get Things Done?

CONSTANT FEEDBACK LOOP

- Regulatory & Policy Considerations
- Standards Review & Convergence
- Technology Development
- Implementation Experience & Interoperability
- Business, Policy & Implementation Guidelines

Market Requirements

Adoption of Market Solutions

Open Public Dialog

Market Requirements Document (Business & Consumer Drivers)
### Who is implementing our standards?

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Version</th>
<th>idP</th>
<th>idP Extended</th>
<th>idP Lite</th>
<th>SP Complete</th>
<th>SP Extended</th>
<th>SP Lite</th>
<th>ECP</th>
<th>Attribute Authority Responder</th>
<th>Attribute Authority Requester</th>
<th>Event Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>SiteMinder®</td>
<td>6.0 SP5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>Entr’ouvert</td>
<td>Lasso</td>
<td>2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>Entrust</td>
<td>Entrust GetAccess™</td>
<td>7.1 SP2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Jul 2006</td>
</tr>
<tr>
<td>Ericsson</td>
<td>EIC</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>Ericsson</td>
<td>EIM SPT</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>HP</td>
<td>OpenView Select Federation</td>
<td>6.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Jul 2006</td>
</tr>
<tr>
<td>NTT</td>
<td>IdLive</td>
<td>4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>NTT Software</td>
<td>TrustBind Federation Manager</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
<tr>
<td>Oracle</td>
<td>Identity Management</td>
<td>10g</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Jul 2006</td>
</tr>
<tr>
<td>Ping Identity Corp.</td>
<td>PingFederate</td>
<td>4.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Jul 2006</td>
</tr>
<tr>
<td>Symlabs</td>
<td>Federated Identity Access Manager (FIAM)</td>
<td>3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dec 2006</td>
</tr>
</tbody>
</table>
More than one billion Liberty-enabled identities and devices in the marketplace today…

The de-facto standard for Identity Federation

Organizations moving from early deployment strategies to mapping ROI

“…authentication integrated into a centralized identity management system is about one fourth the cost.”

“…Liberty Federation has reduced the cost of manual transactions in the Finland Tax Office to approximately 10-50 cents, representing a cost savings of upwards of 95%”

“…T-Online found that ‘each click a user was required to make reduced usage by 10%.’ Federation has reduced the required number of “clicks.”

Who is deploying?: One Billion and Growing
see - http://projectliberty.org/index.php/liberty/adoption
Barriers persist for widespread deployment:
- Standards confusion exists
- Identity selector interoperability
- Inter-organizational “trust” is hard to scale
- Enterprises are struggling to comply with “consent” regulation
- The market is confused
- Enterprise PoC's are non-trivial to stand up

What is Liberty doing to overcome these?...
How to address the new challenges

- Introducing The Concordia Project
  - A new program designed to drive interoperability throughout the Internet Identity Layer
  - Global, cross-initiative collaboration
  - A public call for interop use cases for heterogeneous environments
  - Expansion of Liberty’s interoperability testing to meet new and varied requirements
  - Open source support for relying parties
Concordia Brings Together Disparate Initiatives
Potential Unification Touch Points

**SAML, Liberty Web Services**
- SSO, single logout
- Permission-based attribute sharing
- User-absent use cases
- Optimized for "circles of trust"; interop cert program
- SAML tokens in XML msgs; enterprise security & privacy; smart clients

**OpenID**
- Can do authn with URI-based IDs; authn-method agnostic
- Supports user control/empowerment models
- Distributed authentication and simple attribute sharing with URI-based IDs; low-trust scenarios; explicitly no need for preconfigured trust
- Solutions for consistent user experience

**CardSpace**
- Phishing-resistant authentication and attribute sharing though client; "card" paradigm; requires WS-Trust; can front-end various SSO systems

Eve Maler, Sun Microsystems
Liberty’s Identity Web Services

**ID-WSF**
Identity web services
application framework standard – focuses on interoperability, security, identity, permission, and privacy – applies to non-identity services as well

**WS-***
Generic web services
framework – broad feature set beyond security, identity, and trust – focuses on modularization and composability

Messaging model based on SOAP/WSDL;
message addressing model based on WS-Addressing;
message security model based on WS-Security;
shared usage of SAML Token Profile
Concordia Components

- Open Wiki: [http://www.projectconcordia.org](http://www.projectconcordia.org)
- Events
  - IOS, IIW, Catalyst, DIDW, etc.
- Use case definitions
  - More than 20 submissions, including detailed use cases from AOL, Boeing, GM, Government of British Columbia, and the US GSA
- Future Interop Event(s)
- Specification work to be done in appropriate standards bodies
- Future Certification Program Support from Liberty Alliance
Liberty helps organizations build a foundation for trust -- critical for the overall success of identity-based services and efficiencies.
Identity Assurance Expert Group

- Newly formed Identity Assurance Expert Group (IAEG) designed to foster adoption of identity assurance services
- Initial contributions from EAP and U.S. E-Authentication Federation
- Objective is to create a framework of baseline policies, business rules and commercial terms against which identity assurance services can be assessed and certified
- Goal is to facilitate trusted identity federation to promote uniformity and interoperability amongst identity service providers
IAEG Trust Framework

- Utilizes EAP Trust Framework and US e-Authentication Federation Credential Assessment Framework as a baseline
- Harmonized, best-of-breed industry identity assurance standard
- Framework supporting mutual acceptance, validation and lifecycle maintenance across identity federations
- Framework consists of:
  - Business Rules
  - Assurance Levels
  - Service Assessment Criteria
  - Accreditation and Certification Model
IAEG Certification Model

- Program for auditors to execute certification/accreditation process
- Provide Identity Assurance service providers with guidelines for certifying to Liberty Alliance IAEG
- Federations certifying their members for the benefit of inter-federation and streamlining the certification process for the industry
- Liberty Alliance IAEG to provide governance over certification process

- Phase 1 = Identity Providers
- Phase 2 & 3 = Relying Parties and Federation Operators
IGF to help industry meet regulation

- Increasing legal and regulatory concern about access to identity-related data about users
  - Privacy concerns: HIPAA, SB 1386, theft of user data
  - Compliance: SOX, GLB, EU legislation
  - Who has access to my social security number or account number, and, under what conditions?

- Effective business applications require flexible access to data about users
  - Value of data held by enterprise lies in its use!
  - Application developers should focus on business requirements not on protocols or identity stores

- CHALLENGE: Need an enterprise-wide framework for managing access to identity-related data provided by multiple sources
Identity Governance Framework

- **CARML** – Defines application identity requirements
  - what identity information an application needs and how the application will use it.

- **AAPML** – Defines identity use policies (XACML)
  - Constraints on user and application access to personal data
  - obligations and conditions under which data is to be released

- **Attribute Service** – Links applications to identity data

- **Developer APIs/Tools** – Developers can express identity requirements at a business level at development time
  - Key to IGF adoption/use
Moving the Industry Forward

**Figure 1: Projecting Federated-Identity Adoption**

- **2004—2005:** Pairwise federations
  - Leveraging existing relationships, legal agreements
  - Extranets, Web SSO
  - SAML 1.x, Liberty ID-FF
  - Early communities

- **2006—2007:** Community federations
  - Industry-specific federations
  - Limited trust, industry-specific agreements
  - SAML 2.0, WS-*
  - P2P experiments

- **2008—2010:** Dynamic federations
  - Across industries
  - Built-in federation tools
  - Standardized trust fabrics, agreements
  - Identity networks
  - Reputation systems, ad hoc federations

Increasing market complexity, value
Questions

Contact: Brett McDowell, Executive Director, brett@projectliberty.org (+1.413.662.2744)