Liberty’s Architecture

<table>
<thead>
<tr>
<th>Liberty Identity Federation Framework (ID-FF) &amp; Security Assertion Markup Language (SAML) 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liberty Identity Services Interface Specifications (ID-SIS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liberty Identity Web Services Framework (ID-WSF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles</td>
</tr>
</tbody>
</table>

Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)
What is ID-WSF?

- A framework for locating and invoking identity based Web services to provide a simplified & customized online experience

- Identity-based Web services:
  - Are associated with a Principal's Identity (e.g. My Calendar Service)
  - Can be Invoked using a Principal’s Identity

- Permissions-based Attribute Sharing
  - Invoking Services under control of user
  - Service Requestor doing so on behalf (either directly or indirectly) of user.
The State of the World

The Need:
- Dynamic business and personal partnership environment – dynamically and/or statically bound
- Wide variety of Internet web sites providing:
  - Multimedia content services
  - Mobile-specific services (SMS, MMS for example)
  - Personal-computer specific services (Software package management for example)
  - Specialized personal and business application services
- Built on:
  - Multiple access protocols (HTTP+SOAP, SIP and others)
  - Proprietary, closed systems
  - Non-interoperable systems and functions
  - Diverse programming languages and operating platforms
Identity Web Services

Approach

- Create a level of abstraction from disparate software systems and platforms with a Service-Oriented Architecture (SOA)
- Define standard interfaces that MUST be implemented by all solutions to achieve interoperability
- Define frameworks that allow standardized, modular software composition
Why Do Web Services?: A World of Services

WSP = Web Service Provider
WSC = Web Service Consumer

A WSC is an app that uses 1 or more other apps, WSP, to add value. A travel agent WSC could use a flight reservation WSP, a hotel reservation WSP, a calendar WSP.

The WSPs that a WSC uses are run by different businesses. Several businesses can offer the same type of service.

A web site can act as WSC, often on behalf of the visitor - offering personalized service.

A WSP can also act as a WSC to use other WSPs. A map WSP can use a routing WSP and an "attractions" WSP.

Phones, PDAs, PCs and refrigerators can all run WSCs, WSPs (or nothing!)
Web Services Standards

- Standards are needed at many layers of the "web services stack" to enable the service world
- XML, SOAP + WSDL are the building blocks for web services
- SOAP messages may need additional security to that provided by the transport mechanism – "message authentication"
- XML Signature and XML Encryption can be used to protect the integrity of messages
Web Services Frameworks

- What are some of the things you need to access a Web service?
  - Where is this web service?
  - How does the web service know who I am?
  - How does the web service know who we're talking about?
  - How can I ensure privacy, but still get good service?
  - Is this service connection secure?
- Use a framework that specifies these interoperably!
Some Observations

- The success of Web Services depends on (among other things):
  - Standard interfaces – no agreement means no guarantee of interoperability
  - Componentization – ability to create self-contained modular software, and delegate tasks to standard libraries – now, how do these components all work together???
  - Security in an insecure world – ability to secure messages and transactions conducted between parties separated by a network neither owns
  - Identification – the ability for different entities (ie. different businesses) to identify and talk about a "Security Principal" (often a person!)
  - Support for mobile (and other) devices
Real World Use Cases
Mobile: Access Control

- Access control to applications is a fundamental identity service in the mobile space and may be mobile or provide a bridge between mobile and fixed.
- Target Markets
  - Corporate VPNs, Home Banking, Government Portals…
- Possible Formats
  - One-time Password (OTP)
  - Challenge / Response
Mobile: Identity Services

Liberty provides a framework for permission-based and interoperable data services...

1. Where's my closest open bank?
2. Who's this person?
3. What's the Location service for this person?
4. Where's this person?
5. Can My Bank get your location data?
6. Here's your closest bank. Enjoy

Thanks!
E-Gov’t: Finland Board of Taxes

- Allow citizens to file taxes and interact with the Board of Taxes through a browser
  - Supporting e-government in general: State Information society program and NBT IT-strategy
  - Increase productivity and reduce costs of current infrastructure
Finland Board of Taxes: Browser Based Authentication

Welcome TestCompany user!

E-Filing

Please Sign In

Tax Portal

Katso IDP

NetBanks

PKI

MobilePKIs
Finland Board of Taxes: Benefits to the Government

- E-services enables significant cost savings
  - Every transaction made in office costs 20 – 50 euros and an e-transaction 0,1 – 0,5 euro cents
- Simplified processes
  - Reduced 5 phases on e-filing
- New possibilities to arrange e-services
  - E.g. e-filing straight from Pay-roll –system instead of Tax portal web site
- Life-cycle management (e.g. changes in management, users, mergers etc.)
- Reliable roles and authorization (audit-trail)
Finland Board of Taxes: Benefits to Organizations

- Prerequisite to be able to use government e-services
- Secured and faster transactions
- Streamlined process
  - No manual work, no papers, no archiving
  - No need to go to an agency
- Cost savings
  - Use of existing data from pay-roll or accounting system
  - Better return on investments on ERP-system
Use Case: OnStar/Music Store PoC

B2C Use cases:
- Federation
  - Federate
  - De-federate
- Authentication
  - SSO
  - SLO
- Attribute sharing
- Browse
- Buy

High Level Sequence
- User authenticates to MyOnStar
- User authenticates to Music Store via Federation
- Music Favorites are sent using Data Services Template
Use Case: AOL Services
Use Case: Address Book Service

Interacting with a service

- How do I find this service?
- Who are you?
- How do I know you are who you say you are?
- Is this message in response to a message I sent?
Use Case: Address Book Example (cont)

1. Create a connection to Address Book type of service

2. Get the security token and address of the Discovery Service

3. Get the security token and address of Address Book Service

4. Send search requests to Address Book as XML messages

Structured information can be easily utilized in both ends.
Wrap Up: Why Use Identity Web Services?

- Interoperability at the message layer enables loosely-coupled systems
  - Reduce costs and time for integration
  - Simplify maintenance
- Supports service oriented architecture
  - Compose services
  - Substitutable components
- Enables new business models
  - $$$$$
  - Customer Loyalty
  - New partnering possibilities
- Can help address compliance and risk management
Liberty Alliance Position in Web Services

- Focused on business use of *identity-based* web services
- Defines a mechanism for the interchange of privacy-preserving *name identifiers*
- Driven by SAML technology for web-browser SSO, and the exchange of security-related assertions
- Provides a standards framework for identity web services, covering (among other things) the interchange of identity information, authentication, simple message threading, identity web service discovery, user interaction in a web services world
- Offers a chance for business customers to be involved in the development of the standards which will affect the products they want
Thank You