Federated Identity: Evolving Past Industry Strife

Brett McDowell, Liberty Alliance
Eve Maler, Sun Microsystems
02/09/07 - EXP-403
Federated = Distributed

• Federated Identity management provides benefits broadly:
  — New business opportunities
  — Cost savings
  — Flexibility
  — Social networking

• Distributing identity tasks and information across domains provides:
  — Opportunities
  — Risks and challenges
Opportunities

• People:
  — Authentication
  — Personalization
  — Privacy control

• Services and applications:
  — Delegation
  — Unification
  — Access control

• Organizations:
  — Secure outsourcing
  — Reduce costs

“We believe that federation is going to become a mandatory part of doing business on the Web. For the consumer, it makes their life so much easier by reducing the need for multiple IDs and passwords. Federation is also attractive because it provides a way to maintain privacy and secure identity. With all the problems around ID theft, this is very important.”

--GM, John Jackson, Director of Software Technology
Risks and challenges

• Loss of privacy
• Compliance regulations
• Unifying disparate models
• Lack of interoperability
• Integrating with legacy systems

...all of which can be mitigated by

— Open technology standards
— Deployment policy guidance
— Independent 3rd-party certification
The Liberty Alliance

- An open consortium of ~150 businesses, government agencies, & .org’s
- Since 2001, its mission has been to foster a ubiquitous, interoperable, privacy-respecting federated identity layer for web applications and services
- Leadership of the Alliance:
Proactive cross-industry coordination

- Founded on the principle of “leverage and extend” vs. “re-invent the wheel”
- Actively working with these organizations and many more
Delivering solutions to real problems
Liberty technology deliverables to date

Liberty Web Services
Optimized for application-to-application interaction

Identity-attesting entities

Advanced Clients
“ID-aware”

Identity-wielding entities

Identity-relying entities

Liberty Federation (SAML2)
Optimized for human-to-application interaction
A sampling of vendor adoption

<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 2008</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 2008</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 2008</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 2008</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 2008</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 2008</td>
</tr>
<tr>
<td>NTT</td>
<td>I-dLive</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 2008</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 2008</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 2008</td>
</tr>
<tr>
<td>Ping Identity Corporation</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 2008</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 2008</td>
</tr>
</tbody>
</table>
A sampling of deployment case studies

Panel Q and A - Moderator

Deploying Liberty Federation

T-Online (slide 4 from PDF attached)

Identity Management solution for the online mass market.
“Netzausweis” Enabling services for simplified Internet usage - more than just Single Login/SignOn.

Overview

Single Login / SignOn

Data Vault

Age Verification

Account aggregation and starting point for traffic

Easy and secure login into web based forms

With one Login, everything is just a mouseclick away!

Federation Setup

SSO for a central service platform

Orange provides a technical framework:
- Context adaptation
- Mobile & web portal
- Access to Orange mobiles (SIM, MMS, location, etc.
- Billing integration

Orange provides some branded services:
- Communication services
- Business services

Liberty SSO for partner services integration

MDM is the Orange UMMI

Internal SSO for internal components
So where's the industry strife today?

- New identity-related technologies are entering the market
- The development of generic web services standards has lagged behind identity web services standards
- Participation in open dialog between leaders followed “silo” development
- Despite recent convergence trends, only Liberty technologies have a certification program
Liberty's recipe for evolving past industry strife

• Throwing open the doors to collaboration
  — Opening up meetings
  — Opening up public forums & lists
  — Growing liaison relationships with many new communities
  — Publishing a huge inventory of previously confidential material

• The Concordia Program™
  — Issuing a public call for interop use cases for heterogeneous environments
  — Expand certification program to meet the requirements
Technology evolution

Eve Maler, Sun Microsystems, Inc.
A closer look at SAML

• XML-based framework for:
  — Marshaling security and identity information
  — Exchanging it across domain boundaries

• Out-of-the-box profiles for:
  — Human-to-application interaction
  — Single sign-on, single logout, account linking...

• At SAML's core: assertions about subjects
  — About identity, authentication, attribute, and entitlement
  — Reused in many other specs

• SAML2 + business guidelines + certification = Liberty Federation
Evolution to date in identity federation standards

- **2002**: Liberty “Phase 1”
  - SAML 1
  - Liberty bases new federation standard on emerging SAML standard

- **2003**: Liberty ID-FF 1.1, 1.2
  - SAML 1.1
  - Shibboleth 1.0, 1.1
  - Liberty tracks SAML evolution; Internet2 Shibboleth bases its solutions on SAML also

- **2004**: Liberty contributes ID-FF to OASIS for SAML2 convergence; Shibboleth also takes part
  - Shibboleth 1.2
  - Liberty endorses SAML2 as its identity federation solution and provides interop and conformance testing; Shibboleth is working on new SAML2 based APIs

- **2005**: Liberty Federation
  - SAML2
A closer look at Liberty Web Services

- Building on the value of identity federation with **application-to-application** interaction
  - Avoids browser limitations
  - Allows transactions where a human can't (or doesn't want to) be present
  - Allows services in multiple domains to cooperate securely, with user privacy

- **Out-of-the-box services** for:
  - Personal profile, employee profile, geolocation, social networking...
Zooming in on key framework features

- **Standards-based** framework
- Rich **web services identity** model
- **Bootstrapping** from SSO to kick off transactions from human authentication
- Service **discovery** for dynamic lookup
- Access based on user **policy, consent**, and even **interaction**
- End-to-end **privacy**
- Optimizations to handle all **network devices**
- **Social networking services**

TCP/IP, UDP, SSL/TLS, HTTP, SOAP 1.1, SAML assertions
Evolution to date in identity web services standards

- 2003: WS-Security, SAML TP 1.0
- 2004: ID-WSF 1.0
  - Liberty ID-WSF uses WS-Security before the ink is dry
- 2005: ID-WSF 1.1
  - ID-WSF revision takes into account new versions of underlying standards
- 2006: ID-WSF 2.0
  - Incorporates WS-Addressing once standardized
SAML, Liberty

- Allows for user-absent scenarios; supports arbitrary user interaction paradigms
- Broader protocol framework; SAML tokens; XML messaging; enterprise-level security and privacy; ID-aware clients

OpenID

- Can use URLs and XRIs as identifiers; IdP- and RP-initiated flows
- Supports user control and empowerment
- Focuses on consistent user experience
- SSO with URI as identifier; web page ownership for authn; low-sensitivity uses (e.g. blog comments)

CardSpace

- Based on WS-Trust; card paradigm; blocks phishing
Coverage touchpoints: OpenID with SAML and Liberty...

- Protocol designers have been working on this proposition since Oct 2006:
  - How to move from incompatibility (divergence)
    - ...to equivalence (mappings)
    - ...to compatibility (protocol gateways)
    - ...to convergence (unified solution)?

- Efforts under way:
  - OpenID-SAML Profile based on iSSO and Lightweight SSO specs, covering simultaneous attribute exchange
  - Bootstrapping from OpenID authentication into ID-WSF
  - SAML Authentication Context descriptors for OpenID “assertion quality”

- Efforts being considered:
  - OpenID-based identity services, such as the People Service, and unified open source implementations that make this exploration easier
• We heard announcements this week from Microsoft regarding OpenID:
  — Support in products for OpenID
  — Collaboration on use of CardSpace with OpenID

• CardSpace is proving to be an authentication method that integrates easily with existing federated identity systems
  — Martin Gee of ICSynergy last month announced development of a CardSpace AuthModule for with Sun’s OpenSSO
• SAML tokens already in use (the universal solvent of identity data)
• Being considered: CardSpace-to-ID-WSF bootstrapping
• More opportunities for integration – as Kim Cameron said in an interview in Feb 2006:

  “[InfoCard] is not positioned against Liberty. I am an admirer of Liberty. Liberty has done a lot of great things around policy, leadership on federation. This is something that a Liberty-enabled site can use for interacting with their customers.

  “Now, in terms of WS standards and Liberty, currently Liberty runs on the SAML (Security Assertion Markup Language) protocol [sic], and WS standards are slightly different, although they share components. We're also working to try and align those things. But those things don't impact InfoCard.”
...and between identity web services and generic web services
Next Actions

Brett McDowell, Liberty Alliance
Goal: Ubiquitous, interoperable, privacy-respecting layer for network identity

Liberty’s open call for next actions

• Subscribe to Concordia Forum
  projectliberty.org/index.php/liberty/public_community/forums

• Subscribe to News RSS feed for breaking news
  projectliberty.org/rss/feed/events

• Attend Brussels IOS event April 26-27

• Join Liberty Alliance (optional but recommended)
Questions?