Identity Governance Framework

Privacy In Perspective Series
Liberty Alliance Webcast
April 23, 2008
The following is intended to outline our general direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The following information is based on information publicly available from Project Liberty. Specifications shown are published at www.openLiberty.org under Apache 2.0 license and are considered draft specifications only. Specifications are subject to change pending publication from Liberty Alliance.

The development, release, and timing of any features or functionality described for openLiberty or Liberty Alliance remains at the discretion of openLiberty and Liberty Alliance.
Current use of personal information is highly unstructured, unmonitored, and in many cases, poorly governed. Legislation, privacy breaches, liability suits, and press exposure are highlighting the need for proper governance and management of personal information.

With proper governance, the sharing of personal information can reduce information collection, improve privacy, reduce liability, and improve business accuracy, workflow, and profitability.
Many Types of Silos

- Built for specific purposes
- Multiple organizations:
  - Producers, Refiners, Distributors

Source: commons.wikimedia.org
Enterprise Identity Silos

- Healthcare & Benefits
- Travel & Other Services
- Telecom
- Employees, Contractors
- Professional
- HR Systems
- CRM / Sales
- E-Mail
- Financial & Purchasing Systems
- Employees,
  Contractors
Transportation & Provisioning

Meta-Directory
Uber-directory approach to synchronizing silos
Provisioning
Bus approach provisions & sync’s silos

Sometimes silos are used to build more silos!

Source: commons.wikimedia.org
Consumer Identity Silos

- Healthcare
- Professional
- Web Vendor
- Search/Readers
- Consumers
- Employers
- E-Mail
- Financial
- Telecom

LIBERTY ALLIANCE PROJECT
Risks Exist

- Size of the silo
- Information accuracy
- Accidental loss
- Distributing copies
- Loss of control
- Unencrypted backups
- Unintended use
- Legislation

Uncontrolled release of information

Source: commons.wikimedia.org
Pythia, the priestess presiding over the Oracle of Apollo at Delphi
Where Are We Now?

- Silo Protocols
  - LDAP, Database, etc

- User-centric Federation Protocols
  - ID-WSF & SAML 2.0
  - InfoCards and WS-Fed
Opportunities

- Federation - identity networking
  - Improved information accuracy
  - Less liability through minimization
  - Less ‘bulk’ distribution
  - Better information controls
  - User-consented exchange
  - Contextual controls
  - Improved legislative compliance
  - Ability to audit
What is the Identity Governance Framework?
Identity Governance

- A set of declarative policies that document and govern exchange of identity-related data between consumers and providers.

Web Applications ➔ Attributes Required and Usage Assertions “CARML” + WS-Policy

Attribute use-policies “AAPML”/XACML ➔ Attribute Authorities
### Assurance
- Liberty IAF
- PCI
- Audit Standards?

<table>
<thead>
<tr>
<th>What</th>
<th>quality is the data being transferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>NIST Level?</td>
</tr>
</tbody>
</table>

### Governance
- Liberty IGF (CARML)
- XACML (AAPML)
- WS-Policy
- Privacy Legislation

<table>
<thead>
<tr>
<th>Why</th>
<th>should information be transferred, collected, or updated?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who</td>
<td>gets to do what?</td>
</tr>
<tr>
<td>Where</td>
<td>will the be used or held?</td>
</tr>
</tbody>
</table>

### Protocol
- LDAP
- SAML2, ID-WSF
- WS-Trust / WS-Policy

<table>
<thead>
<tr>
<th>How</th>
<th>should information be exchanged?</th>
</tr>
</thead>
<tbody>
<tr>
<td>What</td>
<td>security mechanisms?</td>
</tr>
</tbody>
</table>
Initial announcement in November 2006
- Led by Oracle, support from CA, Layer 7, HP, Novell, Ping Identity, Securent, Sun Microsystems
- Released key draft specifications for review
  - CARML and AAPML draft specifications
  - Sample CARML API
Liberty Alliance work began in February 2007
- Creation of MRD - Use-cases, Scenarios, End-to-End Examples
  - Computer Associates, France Telecom/Orange, Fugen, HP, Intel, NEC, New Zealand, NTT, Oracle
  - MRD document released July 2007
- TEG Work started fall 2007
Current Status

- Two Track Approach
  - Development of open source components at www.openliberty.org
    - Core components based upon Apache 2.0 license
      - Broadly embeddable developer API and tools, IDEs
    - Start with Java and expansion to other languages (future)
    - Aligned with open source ecosystem (Higgins)
      - Re-use existing components wherever possible
    - Simultaneous with creation of Liberty final specification drafts

- Technical work – specifications and profiles – ongoing at Liberty Alliance TEG
  - Builds on IGF Market Requirements Document and CARML, AAPML draft specifications
IGF Walk-through

1. **igf-CARML (Compile-Time)**
   - Schema Interaction Defns
   - WS-Policy

2. **Client Application Server**

3. **Web App/Svc**

4. **Identity Provider / Attribute Authority**

5. **Reporting/Audit**

6. **Privacy Impact Assessment**

7. **Reporting/Audit**

8. **User-Agent (optional)**
- Schema
  - Attributes
  - Predicates
  - Roles
  - Filters
- Interactions
  - Declarations of transactional operations
  - Find, Search, Compare, Read, Add, Modify, Delete
IGF Walk-through

- **igf-DeployIdPolicy** (Deploy-Time)
  - Requirements
  - Declarative Assertions

- **igf-CARML** (Compile-Time)
  - Schema
  - Interaction Defns
  - WS-Policy

- **igf-AppIdPolicy** (Compile-Time)
  - Requirements
  - Declarative Assertions

- **Privacy Impact Assessment**

- **Reporting/Audit**

- **User-Agent** (optional)

- **Identity Provider / Attribute Authority**

- **Web App/Svc**
WS-Policy Assertions

- Compile-Time Assertions by Developer
  - Purpose
  - Retention
    - Duration & Archive Policy
    - Caching
  - Data Display Mask
  - Value Transfer Mask
  - Propagation Partner Service URIs
WS-Policy Assertions

- Deployment time assertions
  - Purpose
  - Propagation Hosts
  - Data Loss or Breach Policy
  - Contractual URI
Transaction Metadata

- WS-Policy like assertions
  - Not protocol specific
- Request Assertions
  - AppId
  - ActiveUser
  - RelatedSubject
  - InteractionId
- Response Assertions
  - ValueNotDefined
  - ValueDefaults
  - ValueDerived
  - ValueAssurance
  - DataConstraint
  - UndefinedException
  - ConsentException
  - PolicyException
Implementing IGF

- Existing Applications
  - CARML declaration passed offline to attribute authorities
  - Minimal or no transactional IGF assertions

- New Applications
  - New CARML declarative API
  - Push protocol & deployment complexity down-the-stack
  - Multi-protocol support
  - Deployment time configuration vs. compile time
IGF Summary

- Standards
  - CARML - Data and transaction definitions
  - WS-Policy - Privacy assertions
  - AAPML - Attribute Authority Policy
  - Protocol Profiles - How IGF is Applied to Protocols

- Open Source
  - An open reference implementation of IGF
Learn More

- http://www.openliberty.org

- Inquiries to
  - phil.hunt@oracle.com
  - prateek.mishra@oracle.com

- Blogs:
  - http://independentid.com - Phil
  - http://blogs.oracle.com/identityprivacy - Prateek