Large scale en masse federation:
An HP IT case study

Anjali Anagol-Subbarao
Chief Architect, IDM, ebusiness HP IT
Agenda

- Overview of HP-IT Identity Management
- Federation Use Cases
- Learnings
HP IT’s IDM system
Objectives/Drivers for IdM at HP

- Enable new business opportunities
- Enable extended enterprise
- Cost Reduction
- Risk Mitigation and Security
- Enable non-interactive principals (e.g. app to app)
- Move toward loosely coupled web services based IdM capabilities
HP’s IDM Verticals

- Customer IdM
- Employee IdM
- Supplier/Partner IdM
- Managed Services IdM
HP Customer Identity Management

It provides a mission critical horizontal process and shared service for hp.com web sites.
Industry Leading Implementation

• One of the largest IDM systems in the industry
  − 21MM users, growth rate of 700,000/month

• One of the highest Available systems in HP
  − SLA of 3 9’s, avoids loss in revenue /minute of $2000

• Decreased cost/user by $10 to < 60 cents

<table>
<thead>
<tr>
<th></th>
<th>Total Site cost of development</th>
<th>Cost of Authentication Dev</th>
<th>HPP Integration (Median)</th>
<th>Cost avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>$2,000,000</td>
<td>$400,000</td>
<td>$55,337</td>
<td>$344,663</td>
</tr>
<tr>
<td>Medium</td>
<td>$1,000,000</td>
<td>$200,000</td>
<td>$47,120</td>
<td>$152,880</td>
</tr>
<tr>
<td>Low</td>
<td>$750,000</td>
<td>$150,000</td>
<td>$20,025</td>
<td>$129,975</td>
</tr>
</tbody>
</table>
Federation Use Cases
Federation architecture
Workings

- Interoperability between different vendors established
- Accounts 1:1 linked between IDP and SP
- User attributes sent in SAML 2.0 assertion
- Authorization by sending group membership through SAML assertion as attributes
- Session management like common and local logout achieved
- Privacy of user – action of federation and shared attributes
Federation Setup

Legend
- IDP apps
- SP apps

Applications protected by SP

Authentication thru Federation

SP

User Id, group membership

Service Provider

SAML 2.0

User Id, group membership

SF Identity Provider in Weblogic app server

IDP

Applications protected by IDP

Oracle Db
Learnings
Federation strategy

• One consistent federation architecture across all 4 verticals
  – Leverage
  – Consistency of architecture
  – One face to customer
Account linking

- 1 to 1 Account linking between IDP and SP users to facilitate
  - Personalization
  - Audit ability
  - Change from many to 1 to relationship- 1 to 1 would be new design
  - If user has a pre-existing account and via a federated relationship binds there pre-existing directory entry to the federation relationship they can’t unbind it.
User parameters

- Bulk federation for existing users
- Auto discovery of new users by SP
- User centric- User in control of attributes
  - Privacy maintained for attributes sharing
  - action of being federated shown to users
Central login server

- HP as an SP uses a central login server so decisions about IDP can be made centrally

  1. Different urls for each IDP
  2. If the user’s IDP cannot be determined show list of IDPs

- Central login server will also serve as IDP site for HP to federate to external parties

- Central login server is more secure as it handles credentials
User Experience considerations

- Clarity for native login users

- Seamless login from IdP to SP
  - If user comes thru federation link from IDP
  - If user comes to SP and needs to be redirected to IDP
  - If IDP of user needs to be determined
Various Flows contd.

- Redirect to central login server
  - Does the user have a SAML assertion from a trusted IDP?
    - No
      - Use Case of user goes to SP site first, without logging into IDP
    - Yes
      - Which IDP? Multiple ways of determining
        - Redirect to IDP
          - IDP authenticates user
            - Use federated link
            - SP session
  - Use Case of user goes to IDP first, then to SP site next using federation link
Details of Use Cases

- Use cases can get complex
- Should analyze, document, test
- May need customized code for some use cases
- Include use cases to allow for future IDP and SP integrations
Future vision

• Move to a complete infrastructure services based architecture
  – Registration services
  – Authentication and Authorization services
  – Federation services

• Use ID-WSF standards for these services
Call to Action

• Use Learnings for your own implementations

• Liberty Alliance specification http://www.projectliberty.org/

• OASIS SAML specification

• SF web site
Thank you