Secure Identity Provisioning for Liberty Advanced Clients

Greg Whitehead
Senior Software Architect - Select Federation
HP Software
Evolution of Liberty Clients

- **Passive Client (Web Browser)**
  1. User authenticates to IdP over network
  2. IdP delivers authentication assertions to relying parties

- **Active Client (Client Application)**
  1. Client authenticates to IdP over network on behalf of user
  2. IdP delivers authentication assertions to client
  3. Client delivers assertions to relying parties

- **Advanced Client (Trusted Module)**
  1. User authenticates to trusted module
  2. Trusted module authenticates user to relying parties on behalf of IdP

Must be provisioned by IdP!
Active and Advanced Clients are built on Liberty Identity Web Services Framework (ID-WSF)

ID-WSF is a set of specifications to build secure identity based web services over SOAP

Includes several framework services:
- Authentication Service (AS) - Used by Active Clients to authenticate to an IdP and obtain a bootstrap reference and security token for a Discovery Service
- Discovery Service (DS) - Used to locate and obtain security tokens for other ID-WSF services
  - Security tokens contain federated pseudonym-based name identifiers (protecting privacy of users that use many services)

Advanced Client work defining several new services, including
- Provisioning Service (ProvS) which HP will be demonstrating
**Registration Application** used to provision a new Advanced Client capable device

1. User making request from client device is authenticated by IdP
2. **Registration Service** called to create **Provisioning Data** for user’s device and store it with **Provisioning Service**
3. **Provisioning Handle** returned to client device (references **Provisioning Data** stored in **Provisioning Service**)
4. Provisioning Handle is de-referenced to obtain Provisioning Data and initialize Advanced Client

**Note:**
- Advanced Client software could be pre-installed on device or downloaded on demand
- Registration Application could run on client device
Standards-based integration of identity systems across company boundaries
  - Secure exchange of user data with external partners through Web SSO and Web Services
  - Support for all major federation protocols
  - Lower helpdesk and admin costs for external users
End-user focused Privacy Management
  - Privacy-controlled data sharing
  - User controlled privacy preferences with Opt-in/Opt-out policies
Architected for business continuity, scale and growth
  - 100% J2EE architecture
Audit & Compliance
  - Integrated with Select Audit to track user activity across provisioning, access and federation infrastructures
  - Avoid liabilities and audit costs of storing external user data in your IT infrastructure
HP Select Federation Architecture

- Privacy Manager
- Admin Console
- Access Management Adaptor
- Protocol Responder
- Interaction Service
- Unified Management Core
  - Privacy Policy Engine
  - Protocol Engine
  - Security Context
    - Session Info
    - Group Info
    - Fed Info
    - Attrib Info
- Access Management System (e.g. SA)
- Web Service (e.g. Prov Svc)

- Federation Policy & Session Info
- User Stores

Protocols

- ID-FF 1.1
- ID-FF 1.2
- SAML 1.0
- SAML 1.1
- SAML 2.0
- ID-WSF 1.0
- ID-WSF 1.2
- ID-WSF 2.0
- WS-Fed
- other

Liberty Alliance Project
An existing BT customer subscribes to BT’s WiFi service from a wired notebook PC in their home and then uses the instantly provisioned credentials to access BT’s wireless service.