Identity Trust Requirements at the University of California

David Walker
Office of the President
University of California
David.Walker @ ucop.edu
Overview

- Example Trust Frameworks
- Criteria for Selecting Trust Frameworks
- Example Applications
Example Trust Frameworks

- **OpenID**
  - Identities and identity providers are self-declared

- **InCommon Bronze / UCTrust Campus**
  - Identity providers self-declared (by US universities)
  - Identity management is documented

- **InCommon Silver / UCTrust Basic**
  - Identity providers vetted
  - Minimum requirements for identity management
Criteria for Choosing Trust Frameworks

- Risk
  - What is the impact of incorrect identity information?

- Target Community
  - What is the target user community?
  - What trust frameworks are feasible?

- Cost
  - What is the cost of bringing the target community into a trust framework?
Example Applications - Melvyl

- The UC libraries' union catalog
- Available to all Internet users
- No need to identify individuals
- Users can, at their choice, store preferences
- UCTrust Campus or OpenID
  - User choice?
Example Applications – Employee Training

- Available to employees and others who require training
- Need to identify individuals for compliance
- Low risk
- UCTrust Campus
Example Applications – Connexxus

- The (future) UC travel system
- Available to employees and others who travel
- Need to identify individuals to deliver services
- Authorization to expend University money
- Audit
- Medium risk
- UCTrust Basic