Can't we all just get along? Achieving Federated Identity Management at the University of California

David Walker
Jacqueline Craig
Office of the President
University of California

© Copyright Regents of the University of California 2005. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the authors.
The University of California

• Ten campuses, three national labs, five medical centers

• Most operational responsibilities on campuses
  – Payroll, Student Information, *etc.*
  – Each campus does its own identity management

• A few services are central
  – Employee self-service and benefits central
  – Most licensed library materials
  – Multi-campus collaborations
Identity Management at UC

- Separate identity management at each campus
- In general, authentication is per-service
- Campuses are starting to develop common authentication
  - UCB: Kerberos
  - UCI: Kerberos
  - UCLA: Home grown
  - UCSD: Home grown
- All four have home-grown identity management
What is the problem?

• How can services of one UC campus be accessed by users of another UC campus?

• Moving toward a new business environment
  – UC employee self-service and benefits
  – access to any UC campus library system
  – Inter-campus access to course management systems
  – collaboration within the Academic Senate
  – administrative applications
Federations

- Federations authenticate locally, share identity information globally
  - Sharing is controlled by policy
  - Good fit for UC

- Other Structures
  - Public Key Infrastructure (PKI)
    - We tried it.
  - Active Directory and LDAP-based structures
  - UC is not hierarchical; one size doesn’t fit all
What are we building?

- Trustworthy exchange of identity attributes
- Trustworthy identity attributes
- Create a trust environment
  - Services trust campuses to provide correct identity information
  - Campuses trust services not to misuse information they receive
  - Participants trust campuses not to reveal information in appropriately and application snot to misuse that information
InCommon

- Defines technology for trustworthy exchange of identity attributes.
- Defines common identity attributes
- Emphasis is on broad membership.
  - Specific agreements (e.g., requirements for identity management) are pairwise.
UCEX

- Establishes global requirements to facilitate system-wide agreements.
- Creates trust in identity attributes through policy.
  - Policy controls the release of information
  - Technology enforces that policy
  - Technology ensures secure transit of identity attributes
- Extends InCommon
UCTrust

• Pilot project with three campuses
  – UC San Diego
  – UC Los Angeles
  – UC Irvine

• UCOP applications
  – Your Benefits Online
  – California Digital Library
InCommon Requirements

- InCommon criteria
  - IdM systems “fall under the purview of organization’s executive management
  - Appropriate risk management practices for issuing end-user credentials
  - Must be documented

- UCTrust requires greater assurance in identity management practices for conformance with existing UC policies
UCTrust Requirements

• Campuses must provide authoritative and accurate attribute assertions

• Campuses must have practices that meet minimum standards
  – establishing electronic credentials and
  – maintaining individual identity information

• Providers receiving individual identity attributes must ensure its protection and respect privacy constraints defined by the campus
Governance

• UCTrust Task Force
  - Composed of campus Identity Providers, Service Providers, UCTrust Administration, UCOP
  - Manages operational policies and procedures
  - Oversight and conflict resolution provided by UC’s Information Technology Leadership Council, the group of UC’s CIOs.
Administration

- UCTrust Federation Administration
  - Provides operational coordination, when needed
  - Maintains documentation repository
  - Not a major resource drain; technology and end-user support is with the Identity and Service Providers.
Identity Provider Responsibilities

- Identification, registration, and authentication processes
  - Accuracy and timeliness of identity information; tools to update
  - Availability of access to enterprise directory, authentication, *etc.*
  - Audit logs to enable investigation
  - Support for end-users, service providers and UCTrust Administration

- Dissemination of policy and best practices
Service Provider Responsibilities

• Secure operation of services
  – Awareness of Identity Provider service levels
  – Audit logs to enable investigations
  – Compliance with Identity Provider standards and best practices
  – Support for end-users, identity providers, and UCTrust administration
Community Member Responsibilities

- Community members are the individuals who have officially established an affiliation with a campus

- Community members are responsible for
  - assurance that their credentials are not given to others
  - compliance with Identity Provider standards and best practices
Current State of UCTrust

• Vetting with various UC constituencies
  – Campus CIOs
  – Controllers
  – Vice Chancellors of Administration
  – Academic Senate IT Committee
• External review for Your Benefits Online
• We expect official creation by campus CIOs in late May
Interesting Issues – Risk Analysis

Potential Risks

– **Identification**: Is correct identification supplied when individual is hired?

– **Registration**: Can someone else’s credential be provided during registration? Can an unauthorized individual obtain a credential? What about legacy information on individuals?

– **Authentication**: Can exchange of user name and password be intercepted or passwords be guessed? What about unattended sessions?
Interesting Issues – Risk Analysis

General Risks

- unauthorized release of campus identity information
- Failure of the identity management infrastructure
- Employees uses same credential (password, private key, token, etc.) with less secure system
Interesting Issues – Recommended Practices

• UI issues
  – Guiding users through multiple browser redirects

• Multifactor authentication
  – If asking for multiple pieces of information, only one should be a password; others should be well-known to the end-user.

• Synchronization with repositories of record
  – Payroll
  – Student Information System
Interesting Issues – Liability

• Who is liable when something goes wrong?
  – *E.g.*, whose budget is impacted?
    • Retirement fund represents a large sum of money, even for only one retiree.

• Intra-institutional liability and trust
  – Not legal liability
  – UC is legally a single entity
Interesting Issues – End-User Options

• When the Service Provider is protecting resources that are really the end-user’s (e.g., benefits), let the end-user choose the appropriate level of protection.
  – Campus-assigned credentials?
  – Separate credentials for the benefits system?
  – Both sets of credentials?

• This was a key issue for us.
Interesting Issues - Dual Campus Authorities

• Two identity authorities for different, but overlapping, subcommunities
• Became an excuse to resolve intra-campus politics
Interesting Issues – Log Retention

- Logs are required for forensic purposes
  - So, keep them as long as practical.
- Logs contain private information.
  - So, don’t keep them.
- Three to six months seems about right.
Interesting Issues – Attribute Naming

- Created name spaces for each Identity Provider.
- Also created a global name space for UCTrust.