

# UCLA Identity Management System Updates

Updates at  
the February 2007 UCTrust Meeting

# Background

- Launched enterprise-wide identity management project in 2004:
  - Single logon ID
  - Web single sign-on
  - Federated authentication
- A secure and coherent delivery mechanism for contact and authorization support data
- A stepping stone to enterprise scale, coordinated authorization management

# EDIMI Project Plan

- Phase I
  - Release Basic Directory Server
  - Revamp Campus White-Page directory
  - Create/Manage UCLA Logon ID
  - Supports UC Federated Authentication Project (logging into UCFY and other UCOP applications using UCLA credential)

# Phase I Status

- Release Basic Directory Server
  - Done
- Revamped Campus White-Page directory
  - Almost...
- Create/Manage UCLA Logon ID
  - Consolidated UID/PIN and BOL ID to UCLA Logon ID
  - Now exploring support for UCLA affiliates (parents, visiting scholars, etc.)
- Supports UC Federated Authentication Project (UCTrust)
  - Shibboleth servers in production
  - Need to work out UCNID transmission issues

# On the Horizon

- Forming Management Oversight Group to tackle challenges encountered during Phase I
- Adding more attribute data to ED
- Disaster Recovery – Replicate environment at remote data center
- Begin Migrating ISIS enabled applications to the Shibboleth interface
  - UCLA will be adopting Shibboleth for intra-campus single sign-on
- Engage trial projects to collect detailed requirements for an enterprise permission management system
  - Grouper/Signet

# Challenges

- Data
  - Multiple data owners for common demographic data.
  - Need a more rational and scalable process to manage the appropriate release of data
  - Need an ongoing body to review/confirm definitions of data being introduced into the Enterprise Directory.

# Challenges

- Support
  - UCLA has decentralized help desk topology. Need better coordination.
  - A “user-centric” view is probably better than a “function-centric” view.
  - Need to provide tools to support the help desks
  - The “affiliate” population...

# Challenges

- Others
  - Single Sign-on for non-web systems
  - Ongoing policy management
  - ...

# System Details

- Enterprise Directory
  - 2 Sun Directory Server on Redhat Linux
  - Configured in a hot stand-by mode
  - No direct updates to the directory other than Middleware controlled processes.
- Registry Service/Data Transformation
  - Leverage campus data warehouse: MS SQL Server; Informatica
  - Additional real-time and batch DTS processes written in Java.

# System Details

- Shibboleth
  - 2 Apache/Tomcat servers on Windows 2003
  - Load balanced via content service switch
- ISIS (WebSSO)
  - 2 IIS/ASP.NET servers running on Windows 2003
  - Load balanced via content service switch

