# Meeting Notes - 2008-10-23 at UCI

## Meeting Notes - 2008-10-23 at UCI

### Attendees

| | | | |
|---|---|---|---|
| Greg Ackerman, UCIMC<br>Arlene Allen, UCSB<br>Curtis Bray, UCD<br>Chet Burgess, UCOP<br>Dedra Chamberlin, UCB<br>Steve Chen, UCIMC<br>Adam Cohen, UCB | Josh Drummond, UCI<br>Holly Eggleston, UCSD<br>Matt Elder, UCSD<br>Greg Fellin, UCM<br>Declan Fleming, UCSD<br>Jann Fong, UCSF | Eric Goodman, UCSC<br>Brian Koehmstedt, UCM<br>Datta Mahabalagiri, UCLA<br>Neil Matatall, UCI<br>Jeff McCulough, UCB<br>Chris Peters, UCI | Tom Poage, UCD<br>Brian Roode, UCI<br>Hampton Sublett, UCD<br>David Walker, UCD<br>Dana Watanabe, UCI<br>Albert Wu, UCLA |

### Summary of Significant Issues and Action Items

- Updates on Significant Campus Identity Management Activities
  - It was agreed that campuses would post links to their SP documentation, both policy and technology, on the wiki.
  - Campuses should consider making their first InCommon contact be the help desk.
  - Campuses should review their Shibboleth SP and IdP error pages to ensure users are seeing good information.
    - Matt Elder will post the list of customizable Shibboleth pages.
  - The IBM consultants had proposed using electronic mail address as the unique user identifier for the Enterprise Risk Management system. The Work Group recommended ePPN; Chet Burgess will pass this back to the project team.
  - It appears that funding for ERM's UCTrust interface may be cut. The group's consensus was that this should not be done if it would increase campus administrative burden to support some other authentication scheme.
- UC Ready
  - A statement of purpose and vetting for UCTrust Basic assurance should be added to the wiki.
  - We should address some back-end channel for exchanging identity information outside of Shibboleth.
- Recommended List of UCTrust Attributes and Identifiers for Application Developers
  - For discussion at a later meeting, it was agreed that everyone would update their column of UCTrust Attributes and Identifiers.
- Shibboleth 2.0 Planning
  - UCTrust should not fall behind InCommon's requirements for specific versions of Shibboleth implementations.
  - Moving earlier than later is a good idea. As much as practical, new deployments should use 2.x.
  - Emphasis should be placed on upgrading UC's system-wide applications to 2.x to avoid future system-wide coordination issue that might arise.
- Short Items
  - David Walker will convene a conference call of interested parties to discuss format, frequency, and agenda setting for future meetings.
- Permission Management
  - It may be more appropriate to federate entitlements, rather than business roles, leaving the mapping of business roles to entitlements to the campuses.
  - We need multiple interfaces between applications and identity repositories, as Shibboleth functions only for the current user during a session. We need a "back end" channel.
  - We should define a structure for UCTrust-wide groups.
  - Signet provides important functionality. We will need it, or something like it, in the near future.

### Updates on Significant Campus Identity Management Activities

- UCD
  - UCD is currently finalizing the planning for its identity management project, identifying the priorities of and products to support identity "joining" among payroll, student system, *etc*. (Sun MDM, Mural, Initiate), an application provisioning engine (Sun Identity Manager), and permission management (Sun Role Manager or other).
- UCSB
  - UCSB is continuing on their implementation of Sun Identity Manager. They are using it for the identity join.
- UCSD
  - UCSD is expanding their Shibboleth-supported SPs (constantly). They are using Shibboleth 2.x for new deployments.
    - The configure UCSD-only SPs with a "WAYF" of their identity management system to avoid the "Where are you from?" prompt by InCommon.
    - They don't register UCSD-only SPs with InCommon. The SPs, though, do load InCommon metadata for information about IdPs.
  - They're looking at Shibboleth 2 for their IdP, but it will take a while, as they have built a custom data conector that will need some reimplementation.
  - They have a home-grown Java-only SP that they're trying to move away from by having people integrate Apache into their Java environments.
- UCM
  - They are currently cleaning up their processes so they can start asserting UCTrust Basic.
- UCB
  - UCB has gotten the go-ahead to implement Sun Identity Manager. They're trying to get the cost of Role Manager down, but MDM is likely to be too expensive.
  - They're looking at how to distribute authentication and other critical servers around the campus.
- UCOP
  - UCOP is looking at moving to a single repository of identity information.
  - They went live with Connexxus on September 19 and have been running President Yudof's Project Tracker application for a number of months.
  - They have tested their IdP with the SumTotal learning management system, but there is no imminent use right now.

    - They're starting to work on interfacing with AYSO and UC Ready.
    - There was some discussion of the new Enterprise Risk Management (ERM) system.
        - The IBM consultants had proposed using electronic mail address as the unique user identifier for the Enterprise Risk Management system. The Work Group recommended ePPN; Chet Burgess will pass this back to the project team. ✅
        - It appears that funding for ERM's UCTrust interface may be cut. The group's consensus was that this should not be done if it would increase campus administrative burden to support some other authentication scheme. ✅
- UCSF
    - UCSF's Tivoli-based identity management system, MyAccess, is up. Mass deployment will start in late October.
    - They're doing a proof of concept with AYSO and are ready to start Connexxus testing. There's been some confusion within the Connexxus project of who UCSF should work with for testing.
    - They asked for documentation for SP administrators/developers from other campuses. It was agreed that campuses would post links to their SP documentation, both policy and technology, on the wiki. ✅
- UCSC
    - UCSC is in the final stages of completing their InCommon membership. Shibboleth should be up very soon.
    - They decided to deploy a new user name / password pair for this project. It will be LDAP-based.
    - They're in the middle of evaluating what they need to do for UCTrust certification. They're using Berkeley's principles.
    - For federated applications, they're focused on UC Ready, the learning management system, and Connexxus.
- UCI
    - UCI is reimplementing their identity management system. It will continue to be a local implementation.
        - This is happening at the same time that they will be adding approximately 50,000 applicants to their old system.
    - They've just implemented Connexxus.
        - There have been some problems of help desk coordination, both within Connexxus and within UCI.
        - The first InCommon contact is the one reported by the default configurations of SP and IdP error pages.
            - Campuses should consider making their first InCommon contact be their help desk. ✅
            - Campuses should review their Shibboleth SP and IdP error pages to ensure users are seeing good information. ✅
            - Matt Elder will post the list of customizable Shibboleth pages on the wiki. ✅
    - UCIMC has integrated their login and building entry registration processes.
- UCLA
    - UCLA is looking at Sun products beyond the directory server.
    - They're deploying Shibboleth for all applications, not just external.
    - They're starting to work with their medical center on identity management.
    - They're starting to look at groups and roles.
    - Albert asked if it would make sense to have a shared knowledge base of UCTrust-related issues. Everyone liked the idea.

## UC Ready

- Adam Cohen distributed a revision of the document he distributed to the UCTrust Work Group a few weeks ago.
    - UCTrust Basic assurance will not be needed.
        - A statement of purpose and vetting for UCTrust Basic assurance should be added to the wiki. ✅
    - They're using ePPN for the user identifier.
    - They're asking for affiliation but are not using it at this time. It may be used in the future for authorization.
        - It was pointed out that the eduPerson *Scoped* Affiliation should be used here.
    - They're asking for UID to support LDAP queries.
        - UCD and other campuses have requested the ability for UC Ready to keep contact up to date within UC Ready documents.
        - There are a number of issues with doing this on a system-wide basis.
            - Not all campuses support LDAP access to identity information.
            - UCTrust hasn't established any standards for local LDAP directories, even when they exist. UC Ready will need to be able to query for different attributes from different campuses.
            - It's not clear what contact information is desired; it may not be supported by the campus.
            - We should address some back-end channel for exchanging identity information outside of Shibboleth. ✅
    - Adam asked what attribute should be used to determine a user's location (*e.g.*, campus) within UC. It was decided that it would be best to use the IdP's InCommon entityID for this purpose. It's a long URN, but it is stable and can be mapped to printable / friendlier names for the campuses.

## Recommended List of UCTrust Attributes and Identifiers for Application Developers

- (The discussion was cut short for this item, as earlier agenda items took longer than expected.)
- For discussion at a later meeting, it was agreed that everyone would update their column of UCTrust Attributes and Identifiers. ✅ The goal is to synthesize a set of recommendations that can be given to application developers through the use of the following codes:
    - The supported population is described by one-letter codes that indicate the supported eduPerson affiliation:
        - **F**aculty
        - **S**tudent
        - S**T**aff
        - A**L**um
        - **M**ember
        - **A**ffiliate
        - **E**mployee
        - **L**ibrary-walk-in
        - An **X** indicates support for all affiliations.
    - The currency of the information is described by a code that indicates the number of **H**ours, **D**ays, **W**eeks, or **M**onths that the information may be out of date. For example, "10H" indicates ten seconds, and "2M" indicates two months. **N** indicates that there is no currency standard for this attribute (*e.g.*, it is managed by the user).
    - If further explanation is needed, an asterisk ("*") is linked to a separate page that is named after the campus.
    - Examples:
        - An attribute that is always up to date for all users: **X**

        - An attribute that is made current for employees once a week, but has no currency standard for other affiliations.  There are some exceptions that need explanation, however:  FTE 1W *

## Shibboleth 2.0 Planning

- Right now, Google is the main driver to implement the Shibboleth 2.x IdP.
- UC Ready is using the Shibboleth 2.x SP code.
- There is a difference in how server clustering works between 1.x and 2.x.
- There was consensus that: ✅
    - UCTrust should not fall behind InCommon's requirements for specific versions of Shibboleth implementations.
    - Moving earlier than later is a good idea.  As much as practical, new deployments should use 2.x.
    - Emphasis should be placed on upgrading UC's system-wide applications to 2.x to avoid future system-wide coordination issue that might arise.

## Short Items

- Agenda setting for future meetings
    - The broader issue of meeting format and frequency was raised in light of recent budget woes.  Perhaps we should reduce our face-to-face meetings to two per year.
    - David Walker will convene a conference call of interested parties to discuss format, frequency, and agenda setting for future meetings. ✅
- Relationship with the UC Sun Idm Collaborative Workgroup
    - This will be addressed further in the later meeting of this group.
    - Issues of interoperability among UC locations will be brought to the UCTrust Work Group, if they arise in the UC Sun Idm Collaborative Workgroup.
- An additional UCTrust Metadata Initiator
    - Matt Elder volunteered to take this role.
- UCTrust Campus assurance - do we need it?
    - We will consider the need for this as InCommon implements its Bronze and Silver assurance profiles.

## Permission Management

- David Walker gave a short slide presentation ( AuthZ-2008-10-23.ppt) and reviewed past meetings on this topic ( Notes from the 3/30/2006 Identity Management Meeting at UCSD, Notes from the 6/8/2006 UCTrust Identity Management Meeting at UC Merced, and Notes from the 8/10 /2006 UCTrust Meeting at UC Berkeley ).
    - CO-Manage's implementation of Virtual Organizations (VO) might be a good model for shared applications within UCTrust.
    - It was noted that the word "role" is used a number of different ways in this context, sometimes to indicate a person's purpose for or with the institution, and sometimes to indicate a grouping of permissions within an application (*i.e.*, more of an entitlement in the eduPerson context).  It was decided that "business role" and "application role" would be better terms for these.  [Since the meeting, it has occurred to me that "job function" might be better than "business role." - DHW]
- Curtis Bray reviewed permission management within Kuali Identity Manager (KIM)
    - Kuali's "roles" are more of the "application role" type.
- The following goals were established for permission management:
    - Provisioning and de-provisioning
    - Business orientation
    - Audit and compliance
- Identifying approval points for processes can help to structure business role definitions.
- Greg Ackerman observed that UCIMC has seen that leaving authorization decisions to local administrators tends to grant more access than is needed, as doing so tends to reduce trouble calls.
- UCIMC is addressing permission management to access medical images for HIPAA compliance.
- UCLA permission management
    - Albert Wu presented a few scenarios for permission management (Managing Groups and Roles for a VO in Multiple Collaboration Tools ManageRolesWithGrouperShibboleth, User-Select Attribute Release, and Provisioning Access Using Shibboleth-delivered Role Data).
    - UCLA sees Signet (or something like Signet) as important for applications that require central auditability.  Otherwise global groups with distributed administration within departments will suffice.
- Outcomes from the discussion of permission management: ✅
    - It may be more appropriate to federate entitlements, rather than business roles, leaving the mapping of business roles to entitlements to the campuses.
    - We need multiple interfaces between applications and identity repositories, as Shibboleth functions only for the current user during a session.  We need a "back end" channel.
    - We should define a structure for UCTrust-wide groups.
    - Signet provides important functionality.  We will need it, or something like it, in the near future.

## Next Meeting

The timing of the next meeting will be determined by the forthcoming conference call to discuss future meetings.  UCSF and UCSC are portential venues.