Meeting Notes - 2008-03-26 at UCSB

Meeting Notes - 2008-03-26 at UCSB

Attendees

Arlene Allen, UCSB Curtis Bray, UCD Chet Burgess, UCOP Dedra Chamberlin, UCB Matt Elder, UCSD Greg Fellin, UCM Eric Goodman, UCSC Karl Heins, UCOP Steve Hock, UCR Bruce James, UCOP	Mike Kennedy, UCR Datta Mahabalagiri, UCLA Jeff Mccullough, UCB Chris Peters, UCI Brian Roode, UCI Heidi Schmidt, UCSF Adam Stone, LBNL Hampton Sublett, UCD Andrew Tristan, UCR

Significant Campus Activities

- UCR
  - UCR recently brought AYSO up in production. They plan a campus rollout in April.
  - The HR LMS is also in production.
- UCB
  - UCB just certified for UCTrust.
  - They are working with Infosys to to implement Sun Identity Manager
- LBNL
  - LBNL is working on completing their UCTrust certification.
- UCSF
  - UCSF is working on an implementation of the Tivoli identity and access manager.
- UCM
  - UCM uses Sun Identity Manager for most applications.
- UCOP
  - UCOP has an IdP running, using Active Directory for authentication, and is ready to integrate with the HR LMS.
  - They are working on UCTrust certification.
- UCR
  - UCR is working on two-factor authentication using Safeword. (Presentation later in the meeting.)
  - They are rolling Kerberos out for system administration. It is provisioned from their identity management system.
- UCI
  - AYSO is in production, as is the HR LMS.
  - They are reimplementing their identity and access management systems, which date back to the '90s ('80s?). The new system will be developed locally.
  - UCI would like the ability to add student IDs to PPS.
    - So would everyone else. This will be proposed to the ITLC.
    - There was also discussion of assigning UCnetIDs to students. There are some issues with the business process that may preclude this. UCSC and UCSB have "fuzzy" algorithms for uniquely identifying students that work pretty well (~30 mismatches /quarter for UCSB, 0.7%-0.9% for UCSC).
- UCSB
  - UCSB is using the Sun JES identity suite and is hiring Sun to do the implementation.
- UCSC
  - UCSC is using the Sun JES product, contracting Aegis for implementation.
    - They're managing only identities, not authentication.
  - The issue of implementing a single login has become a sticking point for them. Many legacy applications don't want shared userids and passwords.
- UCLA
  - UCLA has had Shibboleth 1.3 in production for over a year and plan to migrate campus applications to Shibboleth over the next 6-12 months.
- UCD
  - UCD is implementing CAS in a high-availability configuration and is upgrading their Kerberos service.
  - They're looking at the right model for integrating with their medical center.
    - This is a common issue for all medical center campuses. For now, medical centers are part of the campus identity management service, but often also have one of their own; UCSF, however, is integrated.
- UCSD
  - UCSD just went live with AYSO.
  - They're implementing access for non-student / non-employee members of their community.
- Internal Audit
  - Karl Heins recently had a discussion with PWC about auditing identity management services, both for UCtrust and InCommon. The goal is to identify what controls and procedures need testing, as well as identifying (and, possibly, certifying) who should do such audits.

Updates

- AYSO
  - Bruce James presented a few slides showing AYSO use via UCTrust to date.
  - UCD, UCI, UCR, and UCSD are enabled for UCTrust access to AYSO. UCI and UCSD have rolled it out to their communities.

    - The usage statistics show that there is no strong preference among AYSO users regarding the option to continue to prompt for the AYSO password at the start of a session. It appears that giving users the choice was the right thing to do. It did create some minor confusion at UCI about the difference between the AYSO password and the UCInetID password.
- Connexxus
    - David Walker discussed the two documents that were distributed with the agenda, SystemIssues-2008-03-20.doc and Re: Trondent Standard Profile fields.
    - Connexxus's UCTrust interface will use eduPersonPrincipleName to identify the user and will require *UCTrust Basic* assurance.
    - There will be two versions of the profile feeds. Version 1 will address the first two locations' needs (UCR and UCSD), and Version 2 will address all locations' needs. Version 1 should be final very soon.
- HR LMS (aka UC Learning Center)
    - The UC Learning Center's UCTrust interface is in production and is starting to see use from the campuses.
- Recent InCommon Level of Assurance discussions
    - The registration requirements for UCTrust, InCommon Silver, and eAuthentication level 2 are still difficult for campuses, particularly for remote users.
        - There is at least one service that can call a telephone and "speak" some information. Such a service could be used to "... confirm existing records of the registrant's electronic mail address, telephone number, or postal address," as described in UCTrust's remote registration requirements.
        - Notary Publics were also suggested to support remote registration processes.

IdM-Based Architecture

- *[Note: The version of the survey distributed with the agenda was incorrect. Arlene Allen distributed the correct version was distributed during the meeting.]*
- Arlene Allen discussed the proposed survey. The idea is to focus on identity information flows within *processes*, rather than specific *systems*.
- It was the consensus that the survey's scope was very broad. We will limit it by focusing on the system-wide process flows for the following systems:
    - Employee systems (payroll, benefits)
    - Student systems (Pathways)
    - Selected Corporate Data Warehouse systems
    - System-wide applications, specifically UC Learning Center and Connexxus

The UCTrust Work Group Wiki

- The new UCTrust Work Group Wiki was presented by David Walker. Thanks to UCLA for hosting it on their Confluence server.
- It was agreed that anyone would be allowed to read the information on the wiki, except for a specific section that restricts access to authorized members of the UCTrust Work Group.
    - This same group of authorized members will be able to modify any of the pages on the wiki.
    - Campuses will provide the list of their authorized members to David Walker, who will work with UCLA to provide the access rights.
- UCLA's Confluence server requires the release of eduPersonPrincipleName to be used via Shibboleth. email and displayName are also used to populate Confluence's electronic mail and name fields, if they're available, the first time a user connects to the server. After that, the Confluence user interface can be used to set electronic mail address and name.
- Assertion Consumer Service and Single Sign-On URLs will be added to the (retricted access) table of IdPs and SPs.

Identity Management at UCSB

- Arlene Allen presented UCSB's identity management infrastructure and plans.

UCTrust Metadata Management

- We have a new list of initiators and certifiers for the UCTrust metadata. David Walker is the initator, and Tom Poage and Andrew Tristan are the certifiers; we plan to add Arlene Allen as an alternate initiator soon.
- We will soon modify the certification process to ask new locations to send a scanned copy of their certification electronically to UCTrust-L@ucop.edu, as well as on paper to the AVP, Information Resources and Communications.
- Campuses agreed to put the URLs of their public postings of InCommon Participant Operating Practices (POPs) into the table of IdPs and SPs on the wiki.

Criteria Used to Allow an Application Access to an IdP

- Eric Goodman presented some slides as a companion to his earlier electronic mail.
- While the use of a single user name and password for multiple applications does not create a security issue for the identity management service, it may for other applications. On the other hand, people tend to use the same passwords, even when the user name and application are different, so the security threat may remain.
- During the discussion, it was mentioned that it appears that Shibboleth will reveal successful authentication within InCommon, even if it reveals no attributes. Chris Peters of UCI will investigate further and report back to the group.

UC Riverside's Safeword Implementation

- Steve Hock demonstrated UCR's implementation of two-factor authentication, using Safeword hardware tokens, CAS, and OpenLDAP. The requirement for two-factor authentication is based on affiliations, policies, and roles. Steve's slides are available.

Planning for Shibboleth 2.0

- Shibboleth 2.0 shows promise to help with some UCTrust issues.
  - Better tools to integrate UCTrust metadata
  - Potential for a UCTrust Discovery Services (WAYF) that links with the InCommon WAYF
  - Better management for targetID
  - Logout processing
- David and San Diego are starting to look at Shibboleth 2.0, and the AYSO group has committed to implementing logout processing as part of a Shibboleth 2.0 migration.
- We'll create a sub-space of the wiki for Shibboleth 2.0 activities.

UCTrust Presentation and UCCSC

- David Walker, Albert Wu, and Warren Leung will be giving a presentation at this Summer's UCCSC about how to integrate UCTrust functionality into an application. Others who would like to participate should contact David Walker.

Next Meeting

- Our next meeting will be at UC Davis in the June / July time frame.