Meeting Notes - 2009-04-27 at UCSF

Meeting Notes - 2009-04-27 at UCSF

Date and Time: April 27, 2009, 10:00a-3:00p
Location: UCSF Faculty Alumni House

Agenda and logistics

Attendees

Venu Alla Arlene Allen, UCSB Karin Bliman Curtis Bray, UCD Debra Chamberlin, UCB Ann Dobson, UCSF	Matt Elder, UCSD Jannelle Fong, UCSF Greg Haverkamp, LBNL Bruce James, UCOP Randy Jones Julia Koch, UCSF	Datta Mahabalagiri, UCLA Jeff McCullough, UCB Riju Myladumkunnel, UCSF Jocelyn Nakashige, UCSF John Ober, UCOP Javed Shah	Hampton Sublett, UCD David Walker, UCD Albert Wu, UCLA Mukesh Yadav,UCSF

Campus Updates

- UCLA
  - UCLA is looking at compliance with InCommonSilver, and they have found that Silver has requirements to retain records of the identifiers (*e.g.*, driver's license number) of the identification "documents" used to verify someone's identity. David Walker said he'd ask about that requirement. It's not something that is required by UCTrust, and it also requires the creation of a new repository of PII that must be protected.
  - Work is ongoing to implement Grouper for group management.
- UCSF
  - UCSF is using Connexxus in production. It's their first UCTrust application.
  - They are using Shibboleth 2.0. From the discussion, it appears that many campuses are using Shibboleth 2.0 or have plans to migrate.
- UCB
  - Shibboleth support for Connexxus is working fine. They're working on how to assign trip IDs.
  - Deploying Sun Identity Manager; they're currently looking at guest account provisioning and self-service password reset.
  - UCB is currently doing 3-5 year budget planning.
  - UC Ready is being proposed to be one of the Kuali applications.
- UCI
  - UCI is adding student applicants to their identity repository.
  - They plan to deploy a new campus directory this Fall and Shibboleth 2.0 by the end of 2009.
  - Work is proceeding on support for UC Ready.
- UCM
  - SIM is in maintenance mode.
  - They're thinking about role-based permission management and are evaluating Sun Role Manager.
  - Brian recently developed CASShib to smooth the path for CAS-ified applications to become Shibbolized.
- UCOP
  - UCOP plans to deploy Shibboleth 2.0 in August
  - They're running Shibboleth in a redundant VM cluster and will be implementing disaster recovery at UCSD later.
  - They're working with UCSD to integrate the Enterprise Risk Management project's software into UCTrust.
  - There is concern about granting direct access to UCOP's LDAP server for UC Ready.
  - They are now providing identity service for UCLA Spaces.
  - UCOP has implemented a launch page for Shibbolized applications.
  - They're reviewing the InCommon Silver audit requirements.
- LBNL
  - Not certified for UCTrust Basic yet.
  - They're currently running Shibboleth 2.1 for Google Apps and are planning to use it for local SSO.
  - They're looking a a user-friendly multi-factor authentication solution for Shibboleth.
- UCD
  - UCD is currently reimplementing their identity management system using Mural, Sun Identity Manager, and Sun Role Manager.
  - Work is proceeding on UC Ready and Connexxus.
- InCommon
  - David Walker discussed the InCommon Pilot that's being done with the National Institutes of Health (NIH). NIH's Enterprise Research Administration (ERA) application will be made available for institutions certified for InCommon Silver.
  - There's also been some discussion of enhancing the InCommon discovery service (WAYF) with a service that would store a cookie with the user's IdP (as the WAYF already does after its first invocation). This would allow an institution to "pre-load" the WAYF so that end-users do not see the "Where are you from?" screen.
  - Everyone is encouraged to read and comment on the InCommonInCommon Futures document.
- The ITLC wiki
  - These seems to have gone well; the ITLC is actively using the wiki.
  - Attribute release was discussed (again). We really could use an "informed consent" facility in our IdPs.
- UC Grid integration
  - The proposal discussed earlier regarding UCTrust / UC Grid integration has been accepted by the UC Grid community and will be deployed.

UC Library Use Cases

- John Ober of the California Digital Library led a discussion of the issues described in UC_Systemwide_ Library_Shib_ UseCases.pdf.
- Authorization for library resources can be "volatile." For example, students might lose their right to use inter-library loan, because they have too many overdue books.
- There is a need to bypass authentication for specific workstations (*e.g.*, within library buildings). Shibboleth 2.x has a facility to allow this.
- We will need some way for IdPs to assert common entitlement values to authorize access to specific resources. The rules for granting those entitlements to people, however, may vary from campus to campus.
- Not all library patrons are in the campus identity management systems. There's been some talk at Berkeley, but none of the others at the meeting have done anything. The patrons will need to be included in the campus systems, presumably with the libraries identifying the additional patrons. Also, there are other communities, such as UCDC and alumni that need consideration.
- There are a number of small library vendors that may have trouble joining InCommon. This may not be a major issue for UC, though, once money is involved. The advantages to vendors (large and small) include reduced administration and an enhanced/personalized user experience.
- It was agreed that UCTrust members would participate in a joint group to address these issues with the Library Technical Advisory Group (LTAG) and Heads of Public Services (HOPS).

Quick Items

- Final acceptance of UCTrust Work Group Work Plan - 2009
  - The plan was accepted with one change: the item reading "Permission management, particularly group management" was changed to "Group management."
- Create a subgroup to discuss end-user communication, discovery services, *etc*.?
  - Albert Wu, Eric Goodman, and Matt Elder have agreed to form this group.
- Create a subgroup to discuss federated group management?
  - Albert Wu and David Walker have agreed to form this group.

Provisioning and Non-Web Applications

- Use cases
  - UC Ready
    - UC Ready allows anyone to login via UCTrust. In order to grant some access to a document you have created, however, you must locate them in your campus's LDAP directory. This creates a problem for campuses without LDAP directories, or LDAP directories that do not link back to UCTrust-based identifiers.
  - Berkeley database management system
    - Interest has been expressed at some campuses to use UCB's database management services.
    - UCB's database management group would like a way to map between database accounts and a unique (UCTrust) ID. They would also need notification when a user's status changes.
    - An IdP-provided "preferred" login ID and inter-domain Active Directory trust were also mentioned.
      - Given name space collisions, it's not clear how valuable the preferred login ID would be.
      - It's not clear what inter-domain trust for AD would mean. Bring all participating ADs up to a UCTrust Basic level of assurance? How many such ADs would participate?
  - Kuali Identity Manager (KIM)
    - "Out of the box," KIM stores authorization information for all Kuali-based applications within KIM's own store.
    - Should KIM integration be via provisioning, or through the implementation of "gateways" to/from the campus identity and access management system?
    - For audit reasons, it may be better to implement gateways to centralize authorization information for all applications, not just Kuali applications.
  - Ssh for the Triton cluster at SDSC
    - Triton is a high-performance computing cluster at SDSC that is available to users throughout UC. Ssh is used to login; how can UCTrust help with user account creation and login?
    - UC Grid will provide some integration, once its UCTrust integration is deployed.
    - Perhaps there could be a UCTrust-enabled web application that would assist with the management and distribution of ssh public keys.
- Project proposal to build something?
  - InitialDraftITLCProjectProposalTemplate-UserProvisioning.docwas discussed. The consensus was that it's a good idea to build a common provisioning infrastructure, but that a target completion at the end of 2010 is too soon. It's been submitted to the ITLC as a joint project proposal with the IT Architecture Group (ITAG).
  - Implementation strategies were discussed, including:
    - An enterprise service bus
    - A central repository of identity information that is updated regularly from campus systems
    - An LDAP metadirectory that extracts information "real time" from campus systemsor the Learning Management System

Consistent Identifiers for the Learning Management System

- Bruce James led a discussion of Consistent Identifiersfor the HR learning management system.
  - The learning management people would like a unique identifier for people that is consistent over time. They would also like that identifier to be consistent across campuses, but that is less important.
    - UCnetID does this for employees, and attempts to do it for students, but the algorithm (which is based on SSN and birth date) is only reliable for employees, as birth date is not availble for students.
    - Some campuses, including UCB and UCSF, have business processes that they believe would recognize a returning person at least 50% of the time, as they ask "new" people if they've had a UCB login in the past before creating a new identity for them.
      - A process that could recognize returning people with high reliability for other than employees and, perhaps, students. This is because doing so requires the collection of personal information like the SSN and birthdate that are used for UC netIDs, and it's not appropriate to collect that kind of information, for example, when someone simply registers for a public lecture series that includes personalized access to a web site.

- Bruce will write a proposal for discussion. Assuming a project would come out of that proposal, the ITLC would need to be involved, too.
    - Hope was expressed that we could move away from the "short campus" ID.

Next Meeting

Out next meeting will be May's monthly conference call. Scheduling will begin soon.