Meeting Notes - 2010-12-08 at UC Berkeley

Attendees

(Partial list, please add/edit your names)

Institution	Name
UCB	Dedra Chamberlin, Venu Alla, Ann Geyer, Karl Grose, Jeff McCullough, Sondra Reinman
UCD	Hampton Sublett, Doreen Meyer, David Walker
UCD Health	Monte Ratzlaff, Patrick Flannery
UCM	Brian Koehmstedt, John Kamminga
UCSD	Matt Elder
UCSF	Reba Brindley, Surya Jayanthi
UCSB	
UCLA	Albert Wu, Datta Mahabalagiri
UCSC	Eric Goodman, Idil Sabbagh
UCR (by phone)	Russ Harvey, Andrew Tristan
UCI (by phone)	Chris Peters, Dana Watanabe, Brian Roode
LBNL	Greg Haverkamp, Mike Helm, Dhiva Muruganantham
UCOP	Chet Burgess, Bruce James, Dede Bruno, Partha Chakraborty, Krishna Mohan
CDL	John Ober

Notes:

Campus Updates

UCD: David Walker, Patrick Flannery, Doreen, Curtis, Hampton

- Working on 2 year project to modernize IAM infrastructure
- Project includes health center
- Attempting to integrate role-based access control
- InCommon Silver certification gap analysis

UCLA: Albert Wu, Datta Mahabalagiri

- Moving entire DACS security system into new web-based security tool. Will later move to non-mainframe systems too
- Bringing ASUCLA people into the directory as well as other affiliate populations
- UCSB is moving financial systems to UCLA similar to what Merced currently does
- Will likely face IdM issues including ID matching
- Starting to look at life beyond Sun Directory Server
- Have moved to Shib 2 and will be enabling SAML

UCSF: Surya Jayanthi, Reba Brindley

- Ground work for new IdM system set up several years agao
- Use UCOP mainframe
- Use IBM Tivoli product
- Already do limited RBAC with Tivoli
- Planning to implement Shib as campus SSO

UC Merced: Brian Koehmstedt, John Kamminga

- address engine - custom app for people to enter contact info and sync with Banner
- using "clean address" app to help scrub data (validate addresses)
- Have a new staff person, John, to help with day-to-day operations
- Exploring what to do with Sun product
- Working on feed file for LMS for affiliates

UCOP - Chet Burgess, Bruce James, Krishna Mohan, Partha Chakraborty

- IdM at UCOP cobbled together
- Provide background feeds to third parties, such as recent UC Action
- Question: is UC Action an OP project or a Davis project? Davis thinks it's an OP project.
- UC Action, UC Ready - Both being deployed at IBM hosting service. Looking at system-wide risk management system.
- Chet is setting up initial data provisioning to serve the new UC Action system as well as other future apps
- Moving IdP to shib 2 in first half of calendar year
- Working with some campuses to better handle affiliate records, especially for those people who used to be employees. David Walker said it would be easiest to there was a way LMS could figure out a way to merge records in the LMS system. It would be less costly to figure out how to merge records in LMS than to have every campus solve the ID merge problem. UCOP should press SumTotal to do that work.
- Some campuses have affiliates that need LMS training where it would not be appropriate to gather any data that would generate an identity match
- Albert is concerned that if we can't meet near 100% match with whatever approach we use, that the exceptions will take too much time to deal with. Merging records should happen within the LMS.

CDL - John Ober

- Thanks for contributing to survey and report
- Implications: libraries are better positioned to ask for ID attributes to be released
- He thinks that will happen mostly locally
- Hathi Trust in Michigan - 7 million digitized books, 2 million from UC. There are some cool features, like building your own personal library, only available for people who are shib authenticated
- UCSD has put release of attributes to Hathi Trust into production. Other libraries might come to us to ask the same
- If at some point there is a system-wide library service, John will work with Chet

UCSD: Matt Elder

- recently rolled out LMS
- Allowed affiliate access by pushing affiliate data into system via web services
- They didn't know in advance who would need training
- Somewhat understaffed so migration to Shib 2 delayed
- Only two staff doing IdM work at the moment
- Re-designing front-end for Shib
- At present, they have it set up where user can choose how to authenticate. People are confused and entering wrong passwords

LBNL: Greg Haverkamp, MIke Helm, Dhiva Muruganantham

- Shib push. Interfacing with more and more vendors. About 6 at present
- Has had to do a fair amount of one-off work with diff vendors
- Point and Ship, Talio (for recruiting - require min 4 character
- In dealing with vendors, Greg just says SAML, not Shibboleth. Most people have SAML libraries they are using (Burton Ping Federate)
- Rolling out shib as SSO. Using with confluence for now
- Business systems just now pushing to Shibbolize apps. Will be ending direct LDAP authentication.
- David notes that Shibboleth makes it easier in the long run as metadata exchange is then simplified
- Google has gotten in the way as it turns out that it is an IdM nightmare
- Ended up having to become Google migration architect
- Completely rebuilding IdM architecture as they want to be able to certify for LoA 2
- Likely moving to AD as central directory
- MIke Helm (ESNet) - completely different org. Are trying to create more and better access to amazing toys supported by DoE. Also trying to org labs to be Identity Providers. Might try to set up something like UCTrust. Big problem is the lack of identity. It can be hard to get attention unless institution is already going through a major re-org/re-architect effort. DoE likewise not coherent.
  *Deeva

UCSC: Eric Goodman, Idil Sabbagh

- Interface for people to edit their own user data (previously only got data from source systems)
- Using Shib for student facing LMS (sakai). Made daily shib logins move from 10-20/day to 10000.
- PeopleSoft for student now using LDAP for authN and has many thousands of logins per day
  Upcoming:
- Integrating with gmail for students
- 2 factor or some kind of stronger authN
- They currently run Moira - a user and group management system which they now need to retire
- AD/desktop integration
- Major systems updates - They run Sun 7.1 and need to decide if they should upgrade
- Are a few revs behind on Shib software
- Big push for BCDR -

UCB - Dedra Chamberlin, Karl Grose, Jeff McCullough, Venu Alla, Sondra Reinman

- Developing roadmap for IAM framework, post Sun IdM
- Guest access management
- Completing rollout of InCommon Certificate service
- Two-factor authentication pilot with Yubikey
- Seeking resources to contribute to jasig OpenRegistry project
- Have completed report on Group Management options and resource requirements for implementing grouper
- January starting Proof of Concept project to implement ApacheServiceMix ESB to integrate Identity Management System with one downstream app
- Just completed InCommon Silver Certification gap analysis

UCI - Brian Roode (by phone)

- Upgraded our Shibboleth IdP to version 2.1.5 back in June. The upgrade brought to light the potential ongoing compatibility issues we will have between the various versions of Shibboleth components. One of our ongoing challenges has been identifying local supporters for Shibboleth service providers. The risk in not doing so is that we will become the default local supporter. Sharepoint, UCReady/UC Action/UC Tracker and ERMIS are all good examples of this issue.
- UCI is now providing the option for students to use Google Apps for Education for email - there are plans to use Shibboleth/SAML 2.0 to authenticate users to Google. We're currently using local Google accounts and are working on the transition plan.
- Requiring that all our SP's join InCommon has been a bit of a challenge. ALEKS Corporation (math placement testing) was one of them that joined at our request. Standardizing on InCommon has a lot of advantages to us.
- As for core infrastructure; we are working our the final phases of the development of a new campus Identity Management directory system to replace our "Ph/Qi" directory. We are currently running the two directory systems in parallel (read/write) and resolving discrepancies. The new in-house system is written using Ruby, the Rails framework, Active Record, MySQL. We employed much more rigid development standards, review, and testing for this deployment and it serves as a model for how we will develop applications in the future.

UCR - Andrew Tristan and Russ Harvey (by phone)

- We've spent the last few months working on rolling out Exchange and the associated infrastructure including Active Directory. We instantiate user information in AD from our OpenLDAP infrastructure using the LDAP protocol, and passwords get set via an all purpose password changing page.
- We've also been working on single sign on with CAS via SPNEGO. At this point, it's working with MIT Kerberos, but we're also trying to get it working with AD. Among other things, this requires a CAS upgrade, so this effort is in progress as well.
- The Shibboleth upgrade has been postponed until the above work is finished, but we're still planning on doing this in the next few months.
- We've migrated all of our students to Gmail, and still have a few IdM related details to clean up.

Group affirmation:

- Requests to UCTrust for things like attribute release, data provisioning, etc, should come through a UCTrust representative at an institution (not from a vendor, for example)
- We should add something on the public wiki where all the IdM reps are listed that informs vendors and others that they should contact a specific UCTrust rep who will in turn take a request to the larger UCTrust group.
- Requests to UCTrust members should be given with as much advanced warning as possible

User Provisioning Project

- See slides from David Walker
- ITAG asked to propose the first "middleware" project
- User provisioning for UC-wide services a historic pain point
- A service provider needs ID info. IdPs release ID info at start of session. **But** apps need to know about users **before** the start of a session
- David thought we could just have providers implement provisioning on demand at first login, but there are some times when the system needs to know about a person first
- User provisioning project has four proposed data integration approaches: snapshot, event-driven, changelog and SSO
- snapshots are simple, but get out of date right away. High overhead as you pull in everyone every time
- Subscription - event driven not deployed at most campuses
- None of our IdM systems can generate transactions now, but a goal is to develop that functionality
- Berkeley and UCLA contributing people to work on the detailed design for the project. UCOP project manager is Dede Bruno.
- Will try to leverage as much of SAML as possible
- Detailed design phase starting in January
- Need to make sure we have defined common attributes that might need to be shared.
- We need to start thinking about access management in a different way. Right now, authorization is an afterthought.
- All campuses would enable all elements of the proposed common interface (see David's slides)
- The frequency of updates for each interface may vary depending on local implementations (eg event-driven interface might exist, but if source systems only update daily, changes will only be published daily)
- UC CIO Shel Waggener joined the conversation. He said this project is critical for sharing resources across campuses. He said we shouldn't be shy about asking for necessary resources. Make sure requests are clear. ITLC may have some "jump start" funding.
- This effort is in alignment with Regents directive to share services where possible
- Hampton: Could ITLC resources be used to create a mobile taskforce to implement work at multiple schools? Yes
- Define strategic partnerships
- Detailed design team will interview each school. We will keep design work transparent It would be great to have strong engagement from throughout the system on this project.
- Shel - list sub-initiatives at other campus that depend on this effort
- Need to make sure we work in parallel (can't take forever to get there)
- David noted that this work might inform other federation efforts such as the I2 project COmanageco-manage - try to set up our project as a model.
- Eduroam - possibly incorporate into federation
- Shel is chair elect of ITLC and this is one of top 5 activities
- UCB Infrastructure Services Manager Walt Hagmaier noted that UCB is working hard to sell services to other campus. Our current approach only works well on a small scale as we have to add users to our IdM stores. We don't have an easy way to provide access to other schools on a large scale.
- Blaine from the UCB Enterprise Windows team describes cloud services offering. Creating accounts for people at other UC schools does not scale well
- Why don't we have a master IdP for the system?
- David Walker and Albert argue that a central credential service is not a great solution as it just makes the environment even more complicated (users have more credentials and getting those credentials provisioned and deprovisioned is complicated).
- Mike Helm commented that trying to come up with a central credential would be very hard. Might also weaken security in some areas.
- We agreed that we need to have a better understanding of what non web-based services campuses want to share and how people authenticate to them. Then we can try to figure out the user provisioning project can facilitate sharing those resources.

IAM Components

- The group reviewed the list of IAM functions included in the survey Hampton sent out.
- We identified four priority areas for further discussion and research:
    - Provisioning to target systems
    - Group management
    - Role management
    - Two-factor authentication
- We set up small groups for each topic. Those groups will come up with a set of key questions/functional requirements for that area by the end of January so that we can discuss them on our Feb UCTrust conf call
- Then the groups will do some research/exploration of different technologies that would meet those requirements, most likely starting with open source solutions and where those don't exist or don't meet requirements, exploring commercial options
- The groups will ask for input from campuses that have already conducted RFPs for commercial IdM products as those RFPs should contain useful questions/requirements
- Dedra asks how this relates to Regent directive to share solutions where possible. Is there pressure in the UC system to adopt a standard ERP solution? If so, that should influence our direction with IdM, too.
- UCTrust should claim ownership for setting direction on IdM efforts. Dedra and David will send ITLC an update to let them know we are going to investigate options for IdM solutions and will get back to them with recommendations
- Do we think we will get pressure to adopt a particular solution, or to choose commercial product vs. an open source one? We will be likely to get pressure to use a product suite with formal support, even if we don't go with a commercial product

InCommon Silver

- UCD and UCB have completed gap analysis. Some of key questions are the same. Berkeley shared the proposed task list for filling gaps. These documents may be made available on protected portion of UCTrust workgroup page
- Some of UCD key questions:
    - scope - for UCD looking at all staff
    - what authN method will they use for InCommon Silver? Are there remediation measures they should apply to existing credential, or would it be better to have separate LoA2 credential, or to add multi-factor authN?
    - You will need to have the LoA data in your IAM systems that apps that need to can query and verify
    - InCommon Silver terminology is very gruesome and inconsistent.
- David says UCTrust basic was intended to meet LoA 2. But there are some big diffs between UCTrust Basic and InC Silver, namely that InC has stricter retention requirements and requires an external auditor.
- NIST 800-63 not clear on requirement for external audit

David's update from InC - TAC subgroup

- CIC produced report with some concerns.
- Those were combined with UCTrust concerns into a shared spreadsheet
- One of the main concerns was around specific implementation suggestions made in the InC Silver requirements which are likely to be removed as they are not required in the more recent federal government documentation
- InC wants to make sure it's not creating new requirements beyond what is required in government documentation without good cause
- NIST 800-63, the basis for InCommon Silver and UCTrust Basic, is in the process of being revisedThere is some rumor NIST requirements will change, but not clear when that might happen
- InC Silver came out of period of time when national government was working on eAuthentication framework.
- Newer framework is the TF-PAP andfrom ICAM
- The TF-PAP is less specific than the eAuthentication documentation, so the subgroup is looking at the InC Silver requirements and comparing to the TF-PAP and taking things out of the InC Silver requirements where no longer necessary
- From the federation's point of view, the IdP is the whole organization, not the IdMS operations group (see David's slide). Part of identity vetting iscan be done by hiring organization. IS-11 explicitly says each campus will have a designated IdM group and that group will decide what is acceptable.
- What about situations where departments outside the IdMS have access to the "verifier", as in applications can see the campus credential? Could be an argument for adding a second credential for LoA 2 apps or tightening requirements for use of standard campus credential.
- The InC subgroup is reviewing periodic re-certification requirements, which will hopefully be limited to a campus asserting that nothing has changed. There will likely not be a requirement that campuses actually go through a full re-certification process. It may be that InCommon can request re-certification and give campuses enough time to do that.
- The new InC Silver doc will no longer require as much documentationstatement of practices, but most campus IdMS groups will want to document their practices to facilitatepass their audit
- Auditors will essentially confirm that a campus is following the practices cited in their InCommon Silver certification documentation. InCommon will, in some capacity, determine whether or not those practices are acceptable.
- Retention requirements - We are required to report on who had access to what when. Requirement is 7 1/2 years after a person has left the institution. Some concern about the risk involved in keeping that kind of sensitive data for that length of time. The InC subgroup will be asking if these requirements can be changed to match retention requirements for the I-9 process, as that process is how ID will be vetted in many cases initially.
- At the end, these proposed changes will be reviewed by ICAM to confirm they meet fed requirements
  *InCommon is not going to specify how requirements should be implemented, but there is an intention to have campuses who go through the certification process document how the met the requirements - a kind of best practices resource
- InCommon already has an effort ongoing to indicate IdM best practices
- Issues around verifying addresses of record? Probably won't be explicit in requirements, but as long as info is transmitted to some address of record, will likely be deemed acceptable.
- Security questions for passphrase reset is not specifically allowed in documentation. You could consider the answers to them similar to a new passphrase. Eric said he had researched this approach and it did seem like it would be acceptable per passphrase entropy requirements.
- What about using two-factor to get to LoA 2 if you feel existing credential is not strong enough? It is definitely OK to use LoA 3 to meet LoA 2, but if the stronger authentication you use does not actually meet LoA 3, it may also not meet LoA 2 in conjunction with another credential that does not meet LoA 2.
- AD and LoA 2. David talked to MS rep. Couple areas where AD has problems - AD may not use strong enough encryption of passwords, it's hard to control apps outside the IdMS that ask for the username/passwd.
- The MS rep felt you could use configure AD for LoA 2, but that would break more universal uses of AD credential for things like workstation login.

- He essentially suggested a second AD credential that would be run in a way that did not allow use of credential outside AD, configured to use strong enough encryption
- He is hoping to get MS to produce a security template for implementing this
- Davis is thinking about adding a second credential that is run more tightly at UCD, rather than trying to clean up the existing practices for their standard credential.
- David will share with the group the new proposed InCommon Silver certification requirements once they are drafted