Meeting Notes - 2010-10-15 Conference call

Meeting Notes - 2010-10-15 Conference call

Agenda

Attendees (Partial List)

Chris Peters, UCI Chet Burgess, UCOP Arlene Allen, UCSB Carl Heins, UCSB	David Walker, UCD Surya Narayana, UCSF Datta Mahabalagiri, UCLA Albert Wu, UCLA	Celia Cheung, UCLA (scribe) Greg Haverkamp, LBNL Dedra Chamberlin, UCB Jeff McCollough, UCB	Matt Elder, UCSD

Notes

User Provisioning Project

- A presentation to the ITLC was made by Mary Doyle on September 28, 2010. The slides can be found here. Our task is to propose a project that would serve as a pilot for this, and lay out the resources needed.

Question: Are we still using Kuali Rice for middleware?
Answer: It should be considered. The investigation of middleware that ITAG did was an evaluation of Rice. Now it has become bigger - it makes sense to have a common middleware for intercampus use at the UC level, but there hasn't been a firm decision that Rice is the right thing. In some way it makes the most sense because a number of campuses are deploying applications that use it, but it is less mature than other options out there.

- Most applications need some information to be sent before the first login. This project proposal is for sending UC Trust information and having that data available at other times; this differs from Shibboleth, which only sends data during a session.

Question: Why do we include the snapshot request? Isn't it very resource intensive?
Answer: You must have at least one snapshot to get started. Obviously, we encourage applications to avoid using too many of them, but when you first bring up a new application you must take a snapshot. We presume that SP's will be reasonable with their usage of snapshots. We should provide some expectations and guidelines of appropriate use of these requests. One use of snapshots is if you ever lose transactions, a snapshot allows you to go back to that point in time to get missing transactions. Snapshots also satisfy one-off vendors.

- The model is like Shibboleth. We want to reuse what we can - Shibboleth interface code,have it running on same platform as Shibboleth, etc. to make things easier. We stop short of provisioning (creating user records in applications); we deliver identity info in standard format and it is up to the application to take that standard format and create user records in the application.

- Right now for UC Trust, there are 5-6 attributes defined. If we move forward with this project, there should be a tremendous increase in the attribute information that we have. We are assuming that the identity management people are the gateway to all of those attributes, in order to create a common interface. But if you don't want to pull from the database that your group maintains and pull from something else, that is up to you. The idea is that each campus will have their own common interface. The intent is that the federation can treat the information as authoritative. However, we are not the authoritative owners of the data; we have to ask for the owners to release data. We do not have the authority to do that.

- One concern is that it leaves all the identity management to the SP. The issue here is that different applications will want to do things differently. For example, many applications won't want to match up the same person from two different campuses. For those that do, we have the same issues trying to match up people across UC's. We do a pretty good job with employees because we ask for strongly protected information, but to extend that to people arbitrarily feels inappropriate.

- Another concern: SP's are getting requests and they want unique ID's and authentication that they can use for system access, database access, etc. but we have no way of reconciling identities across applications.

- We are thinking that getting everyone to install Grouper would be a good idea. This would allow us to have a common way of managing groups. If someone was on two different campuses, this would allow us to put them in different groups on the different campuses based on their roles there. Every campus needs to have some way of managing groups. We want to be able to assign ownership of a group to someone at another campus. This way, the identity information could flow over from campus to campus, group to group. It would be easier to do this if we had the same group management system. Also, implementing group management at the same time with other campus will make things easier. A standard format for group management is what is needed, not necessarily a standard implementation.

Question: Now that this proposal has been presented to ITLC, do people feel like we can meet this proposal timeline?
Answer: The timeline begins when the project starts. Reusing Shibboleth foundations will make things easier, but the project is not without effort. However, even though it is a good amount of work, in the medium or long term it will be less work than continuing to do ad hoc provisioning.

- Another concern is that it may be difficult to move on with this until we are all on Shibboleth 2.0. Since some campuses are still on Shibboleth 1.3, this may be a limiting factor. However, there should still be time to upgrade before this project begins.

- Arlene says that this project is not monolithic; it is broken down into phases. We also still have the detailed design phase and a checkpoint with the ITLC before the project is approved. We have been tasked with laying out the detailed design. Phase One includes detailed planning and detailed design of architecture. During Phase Two, we have a year to select the actual technology to be used, write documentation, do testing, QA, and so forth. After that, Phase Three is done at each campus - to implement group management, see targetedID implemented (as the unique ID that never changes in these provisioning streams), and establish relationships around campus for the likely source of these attributes. We will get a common implementation of the interface with the IAM and we need to integrate that with our local systems. Another point is that Phase Three doesn't have to be done on a campus until that campus needs the capability.

Question: If an SP is handling data, do we ask that SP to follow the same guidelines to handle data that InCommon uses?
Answer: If an SP is using Shibboleth, then they have to join InCommon. If they are not using Shibboleth but are using provisioning streams, they would still go through the same process even if it is internal to UC Trust. The main thing is that they need to have an entityID assigned to them that is unique.

Question: What was the response of the ITLC?
Answer: It was positive, and they asked us to continue to look at more detailed design. There were general questions, etc. at the meeting but there was no hesitance. ITAG is being charged to identify resources to do the detailed design, and suggest what resources are needed. Funding has been slated by ITLC - they have agreed to cover up to $30,000 for the detailed design phase. ITAG is going to make a proposition to say how these resources will be allocated, and ITLC will review this and decide whether or not to move forward. The real question for this project is not "Is it a good idea?" but "Can we find the resources to do it?" It will mean spending money now, but saving money later.

InCommon Silver

- Bob Ono from UC Davis and others had a meeting discussing InCommon Silver. They are starting a depth analysis, and have identified some significant gaps. They want to do more research to fill in those gaps.
- At UC Davis, there are a few areas of work that need to be completed to comply with InCommon Silver. They are working how to better control application access to passwords. They also have a system at their medical center that can manage diverse passwords for non-web systems. They want to increase their documentation, and also brought up the point that there is the InCommon requirement of record retention for seven years after a person is no longer affiliated with your institution. They might want the UC's to lobby for some change from InCommon regarding this policy.
- There will be another meeting between UC Davis and UC Berkeley in the next few weeks, and the goal is to have a written gap analysis within a month. This will be on the agenda for the in-person meeting to be held in December between UC Davis and UC Berkeley. This joint meeting will hash out what needs to be done in order to comply with InCommon Silver. There are a few possible dates in the first two weeks of December being suggested for the meeting; each campus is requested to coordinate availability and report back as soon as possible.