Meeting Notes - 2010-11-15 Conference call

Meeting Notes - 2010-11-15 Conference call

Agenda

Attendees

(Partial list, please add/edit your names)

David Walker, UCD Dedra Chamberlin, UCB Dede Bruno, UCOP Karl Heins, UCSB	Craig, UCI John Ober, UCOP/CDL Frank Templeton, UCM Greg Haverkamp, LBNL	Stephen Hock, UCR Albert Wu, UCLA Datta Mahabalagiri, UCLA Warren Leung, UCLA	Celia Cheung, UCLA (scribe) Chet Burgess, UCOP Arlene Allen, UCSB Patrick Flannery, UCD	Bob Ono, UCD Curtis Bray, UCD Eric Goodman, UCSC Jeff McCollough, UCB	Tom Poage

Notes:

Berkeley December UC Trust meeting:

In person UC Trust meeting in Berkeley on December 8th, 2010 from 10am to 4pm. Location specifics to come. Afterwards, those wishing to discuss the Sun and Oracle contract issues can stay.

Some agenda items:

- Present gap analysis from UCD and UCB for InCommon Silver.
- Review feedback on refining documentation for InCommon Silver.
- Discussing the replacement of IAM components and other options.
- Campus status report (~5 minutes each).
- The engagement of the ITLC with SP's.

User Provisioning Project:

Currently, the high level design has been completed. We are now moving forward with the detailed design, and have a full team dedicated to this now. David Walker says there aren't any technical aspects that have changed since the last call. Albert Wu says that UCLA is volunteering two people to work on the detailed design, as is UC Berkeley. We will start the process in January. There may be a meeting prior to January to go over the background information as well as discussing everyone's roles.

As a quick recap, this project is meant to extend what we have done with federated identity management. We need to take care of data transmission needs besides single sign on. So far every UC Trust application needs this, and we don't have a consistent way of doing it. We need to create a standard protocol, or set of protocols, for exchanging data. Then we need the implementation of the protocol. By the end of the project, we want to deliver a working product that campuses can use. This project is also a result of the ITLC asking the ITAG for a project that would use middleware. It was determined that this would be a good first application to use middleware. The project has already been presented to and accepted by ITLC, and they are aware that we are moving into the detailed design phase. Currently, the timeline for this project depends on people being available at the beginning of next year.

Question: Can we look at core business needs in terms of sharing resources between the different campuses? For example, looking at authentication and not just the user provisioning piece? Would it be possible to add non-web based authentication as another item to work on during this phase?
Answer: It is one of the use cases that was discussed. It was decided that we are not going to build anything to reach into applications. We will just deliver the information in the standard format, and the application will have to take it from there. We will not do non-web logins, but we will provide the information to the application so they can do it themselves.

OID versus human-friendly URNs in SAML 1 and SAML 2:

A useful document on this: https://spaces.ais.ucla.edu/display/uctrustwg/ConfiguringScopedAttributes

This project was discussed in the context of the risk management application run under the Office of Risk Services at UC Davis. It is actually the kind of URN that is the issue at hand. In the early days of Shibboleth, people felt that the attributes should have human friendly names. But now, an OID (object identifier) is used. An OID is an LDAP designation of a string of numbers, like a hierarchical namespace except that everything is numerical. Each org is assigned a certain prefix of numbers so that it is certain that the OID's are unique.

The problem is that there are 20-25 attribute names that are old and valid only for SAML 1.x and not for SAML 2, since SAML 2 requires the OID form of the attribute names. In some cases, there was a release to both SAML 1 and SAML 2, so there were problems with duplicates. The standard has been decided - if the mace dir attribute is defined, then we use human readable names in SAML 1.x. If mace dir is not defined, then use the OID. For SAML 2, OID is always used.

Shibboleth is configurable internally so that it will bring in the correct attribute name depending on whether it is communicating with the SP via SAML 1 or SAML 2. By using this approach, we can avoid any duplicates.

It would be useful for a small group to meet and document the correct configuration and expected behavior of this process. Tom will do a quick documentation of this and allow others to review it; if needed, Chet will schedule a meeting time to discuss. UCSD, UCD and UCLA have volunteered to participate.

InCommon Silver:

A gap analysis is in progress, and the first draft will be out in about two weeks. The key issues haven't really changed since the last call. It will be ready before the UC Trust in person meeting in December. Feedback should be shared with InCommon.

Question: We suggested holding off on any audits until this process is over. Do we need to get in touch with the ITLC?
Answer: Yes, we do need to get back to the ITLC. We told the previously to delay UC Trust audits until we got to a point where we understood what we needed by end of this year. This can be another agenda item for next month's meeting. Most campuses are due for their audits.

In order to meet the requirements for InCommon Silver, UCD is thinking of bringing up a new password. This brings up the question of how to manage the security of passwords. The group that is responsible for the IdP is responsible for knowing the shared secrets being protected. UCD brings up several options - Active Directory, Kerberos, etc. which allow an application to know someone's password. The downside to AD is that it is hard to control.

Question: Is this a requirement? For example, if I have an LDAP server that stores passwords, and people do binds and pullbacks on the directory, do I just need a written policy that says that if you bind, make sure you do it securely?
Answer: This is an open question - it falls under the requirements to control the access and to protect the passwords. We do need to worry about this. Some campuses have top down control of their systems through AD, so they already have the controls in place.

In the future, if we use Shibboleth to authenticate, we can check the logs to see if someone is using AD authentication and tell them to stop.

Replacement of IAM system components:

This is one of the agenda items for next month's meeting. We need to discuss what the alternatives are, the different components of the IAM systems, what we currently do and what we can do in the future. Data integration, guest access, and a variety of other functions and tools that are in use will be covered.