Survey of ID mgrs - library issues

As discussed at the 6/21/2010 UCTrust Conference Call, UC Trust principal contacts are . Refer to UC Trust - UC Libraries ad hoc working group -- Request for Info from UCTrust for context.

Background Info

1. What is your campus' single sign on solution?

UCB: CAS
UCD: CAS
UCI: Home grown WebAuth software on top of Kerberos.
UCM:
UCR: CAS
UCLA: We use Shibboleth natively as our SSO solution.
UCSD: We use Shibboleth natively as our SSO solution.
UCSF: Shibboleth
UCSB: Currently, the WAM is Netpoint. It will become OpenSSO this fall. There is no current plan to use intra-campus Shibb technology.
UCSC: We are using Shibboleth natively as our SSO solution.

2. At your campus, should the library use the contact listed in http://www.ucop.edu/irc/itlc/uctrust/contacts.html for IdP questions?
a. Is there a campus mailing list for service issues and questions?

UCB: Yes, or calnet-idm@lists.berkeley.edu
UCD: Yes, shibadmin at ucdavis dot edu
UCI: Contact OIT@UCI.EDU since contacting a single person may be unfortunate if they or unavailable.
UCM:
UCR: Yes
UCLA: Yes, or contact iamucla@ucla.edu.
UCSD:Yes. a) we use shibsupport@ucsd.edu.
UCSF: Yes, we have a mailing list. The contact for UCSF should be Surya Narayana (surya.narayana@ucsf.edu)
UCSB:Yes.Identity problems are directed to directoryhelp@isc.ucsb.edu. This is not a list.
UCSC:Yes (there are alternates if necessary). We generally intake questions through help@ucsc.edu, which populates a trouble ticket that should be escalated to our group.

3. What attributes does your campus commonly release via Shibboleth?

UCB: At present, the following: ucnetid, uctrustcampusidshort, edupersonscopedaffiliation, edupersonprincipalname, givenname, displayname, mail. In the future, we will add uctrustassurance, targetedID, and others by request.
UCD: ePPN,displayName,mail,ucNetID,ucBasicAssurance,ucCampusShortID,cn,sn,givenName. Others available, depending on needs.
UCI: ePPN commonly, other local attributes on request
UCM:
UCR: In general, ePPN plus whatever the service requires.
UCLA: UCLA by default releases targetedID. Everything else is subject to data steward approval. We can assert name, basic contact info, eduPersonAffiliation, UC Trust attributes, and by agreement, eduPersonEntitlement vallues.
UCSD:targetedID, affiliation and scopedAffiliation, mail, name attributes. We have a lot of ucsd specific attributes we release internally as well, which can sometimes be mapped to standard attributes.
UCSF:ePPN, sn, givenname, mail
UCSB:None yet. The design is for what I believe are the minimums mandated: ucnetid, uctrustcampusidshort, uctrustassurance, ucemployeeid, edupersonscopedaffiliation, edupersonprincipalname, sn, givenname, displayname, mail.
UCSC:We have on occasion released ePAffiliation (unscoped), ePPN, sn, givenname, mail, uctrustcampusidshort. We have other attributes available, but notable ones we do NOT have are: targetedID, entitlement management.

4. At your campus, how do we add new vendors to the Shibboleth list?
a. Is there a formal process to request a new SP be registered as the recipient of ID information via shibboleth?
i. Is there a form, and if so what is its location/URL?
ii. Does the process accommodate both campus service providers and external service providers (e.g. that the library sponsors or brokers)?
iii. How does the process accommodate requests for attributes not otherwise/previously released (e.g. the InCommon-Lib recommended use of eduPersonEntitlement, see below)

UCB: At present, these requests are handled ad hoc. The CalNet team is the main point of contact and coordination (calnet-idm@lists.berkeley.edu) for InCommon registration, metadata updates, getting approval from data proprietors, etc. There is a formal process for requesting release of information not public in our directory. The vendor must respond to the same set of questions we use for privileged LDAP binds (see http://wikihub.berkeley.edu/x/WIJ)
UCD: Requests are generally received via email, or through meetings and phone calls from/with sponsors (the desire for a more formalized process has been expressed by some). Requests involving new attributes may be sent through administrative review for prioritization and scheduling, and sensitive /protected attributes may require assurance of ongoing protection.
UCI: There is a process being formalized. External SPs need campus sponsors. Additional attributes depend on their existence, ease of relay, and who is in charge of making decisions about them.
UCM:
UCR: Requests are currently handled on an ad hoc basis. A process is currently being defined and proposed.
UCLA: A vendor must be sponsored by a campus department. If the vendor is a member of InCommon, it's a matter of us releasing attributes. If the vendor isn't an InCommon vendor, the IAMUCLA team needs to register its metadata in our IDP. To get started, contact iamucla@ucla.edu.
UCSD:An email to shibsupport@ucsd.edu will get things started. Local SPs can use a form at https://a4.ucsd.edu/shibreg/docs. If we decide that we can and should release a new attribute we take the time to implement it.
UCSF:We don't have a form yet. We have a process of getting approval for attribute release from the data owners; same goes for new attributes as well.
UCSB:There is no plan for local SPs. Special attribute requests will be handled by a committee.
UCSC:There is a form, but a request though our trouble ticket system is sufficient to initiate the process (help@ucsc.edu). Yes, we can accommodate external SPs; requires approval. Release of otherwise unreleased attributes is the same as release of existing, request is made, approval granted or not granted. Complexity of approval depends on sensitivity of the data and how it will be used.

b. How much lead time is needed to add a new SP - if only currently available attributes are needed? if new attributes are needed?

UCB: Usually 1-2 weeks for available attributes that do not need separate approval from data proprietors. If approval is needed, it can take up to a month.
UCD: If the SP is already configured, IdP mods can be done in as little as a couple of hours with currently available attributes. Registration with InCommon takes a day or two, depending how much back and forth is required with the SP owner. New attributes usually require a degree of research and policy validation. If they can be computed from existing attributes, it might take a day or more to prototype and test. If an attribute is completely de novo, it may take multiple weeks to a few months, depending on required infrastructure changes, priority and workload.
UCI: In an ideal case, lead time is two weeks. However, this is really completely dependent on the level of involvement from the SP as much as it is our own workloads, difficulties in setting up additional attributes and other Layer 8 issues.
UCM:
UCR: One week or less, after organizational approval. If new attributes are needed, it could be much longer.
UCLA: We recommend allowing for 2 weeks to 30 days for new SP registration. Attribute release aside, we have found that handshake testing takes time.
UCSD:Generally less than 24 hours if no special attribute requirements. Otherwise it could take weeks to implement a new attribute.
UCSF:A week and three weeks respectively.
UCSB:N/A. We assume all SPs will come to us from a UC system wide perspective rather than a local one.
UCSC:Generally a week or two to load a new SP with currently released attributes. Developing new attributes (not just unreleased ones, but ones we don't currently populate) depends entirely upon the requirements and prioritization.

Content vendors and InCommon*-Library Best Practices*
(assumes that the campus library or the CDL is the sponsoring agent for content vendors as 3rd party Service Providers)

5. Can you currently support an Attribute Release Policy that includes eduPersonScopedAffiliation?

UCB: Yes.
UCD: Yes.
UCI: Yes.
UCM:
UCR: Yes.
UCLA: Yes.
UCSD:Yes, although we don't currently assign anyone student@ucsd.edu. member, staff, and employee work.
UCSF:Yes. We currently only have "staff" "student" and "affiliate" only.
UCSB:Yes when it goes live.
UCSC:Yes, though we do not currently populate the "member" value.

6. If your library provides a list of IP addresses for terminals/workstations available for "walk-in" use, can you implement the IPAddress authentication "handler" and assign a time-limited affiliation of "library-walk-in" for any authentication request from that terminal (see https://spaces.internet2.edu/display/SHIB2/IdPAuthIP)?

UCB:
UCD: This handler is not currently supported, so would take a bit of work to prototype/implement in the context of existing priorities. We'd also want an SLA cf. who maintains CIDR blocks, expected response time to changes, etc.
UCI: Possible, but would take some work on both technical and political ends of that.
UCM:
UCR: Not without a substantial amount of work.
UCLA: Not today, but we'd like to engage in that conversation to make it happen.
UCSD:Yes, we could probably implement this.
UCSF:Will require some work to get this going, but yes.
UCSB:We currently use IP address verification through a proxy server. It is assumed that the proxy server will remain active until all Library vendors have converted to federating processes.
UCSC:We are planning to implement this in support of a local library application, so this should be fine. - update: we need to do some shib maintenance before we are able to support this function, and that maintenance can't take place before September. So we still expect to support this (hopefully by year's end), but are unable to at this time.

7. Can you currently support an Attribute Release Policy that includes eduPersonEntitlement with a value of urn:mace:dir:entitlement:common-lib-terms for all faculty, staff, students, and library-walk-ins?
a. If not, please note the timing and conditions necessary in order to support eduPersonEntitlement.
b. Are you able to assert eduPersonEntitlement selectively for individuals or groups of individuals?

UCB:
UCD: Similar as item 6 above. If entitlement can be computed from existing attributes, it should not be difficult to implement. If entitlement is required to be fine-grained, e.g. asserted for arbitrary individuals, we would have to design/implement a fair chunk of infrastructure to support it.
UCI: We could, but will have to work out the issues with walk-ins.
UCM:
UCR: We do not currently support an ARP that include eduPersonEntitlement. We could possibly implement this by the end of the calendar year (given support of upper management).
UCLA: We could, but we'd have to work out how to assert the value for walk-in's.
UCSD:We could for everyone except library walk ins at the moment. If we implement the previously mentioned IP address authentication, then walk ins would be okay.
UCSF:We could, once we have the "walk ins" configured.
UCSB:We do not have edupersonentitlement implemented. It would imply large scale deployment of custom processes for the delegated implementation that is appropriate to such a set of values. We have no funding for inventing those.
UCSC:We do not have such a value. We could probably implement the catch-all circumstance (all faculty, staff, students and library-walk-ins) using shib filters or some other process. We plan to support selective entitlement management in the future, but nothing is likely before the end of the year.

8. What information would you need about a content vendor or other 3rd party SP beyond what would be available in their InCommon certification?

UCB: As mentioned above, they would need to respond to specific questions if they are requesting release of attributes not publicly available.
UCD: Depends on application at hand cf. attribute sensitivity, and how they address (de)provisioning, SLA.
UCI: It depends on the specifics of the request, but we may like some other contact information.
UCM:
UCR: We would want assurances from the vendor on data security and data use practices.
UCLA: We may at some point ask for information on the vendor's security and data use practices, particularly as it pertains to the data we release to the vendor.
UCSD:It depends on what attributes they want. If they want attributes we don't feel giving out to verdors, I'm not sure what sort of information or contract we would expect of them. If they want basic stuff, we might not ask for much at all, especially if the company is well known.
UCSF: Contact information
UCSB:Unknown.
UCSC:As UCSD. We would expect a campus (or UC) sponsor to make the request. We would probably be happier if the vendor had signed Appendix DS.

HathiTrust* as a test case (refer to* http://www.hathitrust.org/shibboleth*)* (http://www.hathitrust.org/shibboleth*)*

9. Can you currently support HathiTrust's Attribute Release Policy that includes eduPersonScopedAffiliation, eduPersonTargetedID, and optionally, Display Name?

UCB: eduPersonTargetedID is not currently implemented at UCB.
UCD: eduPersonTargetedID not currently implemented at UCD, eduPersonScopedAffiliation is.
UCI: Affiliation and DisplayName, yes, but we do not currently support eduPersonTargetedID; that would take more lead time
UCM:
UCR: Yes.
UCLA:Yes
UCSD:Yes.
UCSF:Requires some work, but yes.
UCSB:No plan to at the moment. I would like to see the technical specs for a targetedid implementation and that every UC campus used the same spec. If not, we will probably avoid it.
UCSC:eduPersonTargetedID is not currently implemented at UCSC. Assuming release of ePPN was approved (would take some time to get the okay to do this) I believe we would be able to support the service.

10. As a specific case of question #6 above, what would you need from your campus library or the CDL to register HathiTrust as a SP?

UCB: Same as UCLA.
UCD: Ditto cf. UCLA.
UCI: To register the SP we would need Campus Contact information, or more formal signatures if we've gotten along farther in our formalization process. For the IP Address configuration, we would need to set up a system for that.
UCM:
UCR: A request from the vendor and the CDL would be enough to get the ball rolling.
UCLA: We need official contact/endorsement from the UCLA library or CDL. We'll need the sponsoring party to submit a request for data release (which the IDM team can facilitate). Of course, technical contact info from HathiTrust so we can coordinate handshake testing efforts.
UCSD:Probably just need to know that they want it. An email would probably suffice.
UCSF:Once we get over the "atttribute release" hurdle, we should be fine with just having contact info.
UCSB:Again. I see SPs as a UC issue, not a UCSB issue.
UCSC:A request from a UCSC/UC sponsor would be best.

11. Is there anything about the implementation of HathiTrust as a SP that you would find useful to track in order to inform future requests from library-sponsored SPs?

UCB: No.
UCD: No.
UCI: Probably not.
UCM:
UCR: Nope.
UCLA: not particularly.
UCSD:Probably not.
UCSF:HathiTrust implementation should point the way to streamline other library-sponsored SPs/implementations from a process perspective.
UCSB:No. I want other than UCSB to take responsibility for SPs.
UCSC:Not immediately.