UC Systemwide Library Use Cases for Shibboleth/UCTRUST/InCommon
Draft for Discussion

What: As described by the InCommon Library Service Collaboration (https://spaces.internet2.edu/display/inclibrary/InC-Library) libraries face special situations in making online resources available, including walk-in and remote users, a large number and variety of 3rd party (vended) online information resources, and a growing portfolio of library-based campus services. Additionally, in the UC context, there are systemwide (centralized) applications and services which require coordinated authentication across the campuses, or, more accurately, across the UC community. These include, but are not limited to:

- Systemwide access to scholarly materials licensed for the entire UC community (see, e.g. http://www.cdlib.org/inside/groups/uc-elinks/a2z.html)
- Systemwide (union) Melvyl Catalog with services allowing UC community members to establish profiles, auto-alerts for new materials, etc. (http://melvyl.cdlib.org);
- Interlibrary loan (lending and borrowing of materials between the UC campuses (and other institutions) with components that authenticate a) end-users (e.g. look up the status of a loan request) and b) library-based library staff (e.g. place a request into the system on behalf of a patron);
- Systemwide repository, publishing, and preservation services, such as eScholarship (http://repositories.cdlib.org/escholarship/) and the Web Archiving Service (http://cdlib-s10.cdlib.org/inside/projects/preservation/webatrisk/web_archiving.html).

To date these Systemwide applications and services use a mixture of authentication and authorization technologies, including IP authentication for vended information resources such as e-journals and abstracting & indexing databases (with high overhead for the aggregation of UC IP ranges and delivery of IP information to vendors), home-grown 10-way accommodation of campus-based authentication, or separately constructed ID/password systems.

While several of the separate UC libraries are working with their campus IT/UCTrust partners to shibbolize intra-campus applications and services (see Appendix), the UC library community would like to form appropriate partnerships to analyze and, where appropriate and feasible, apply the advantages of single-sign on and other features of shibboleth to multi-campus and systemwide library service use cases.

Who: The UC library community has several permanent strategic planning and operational working groups with relevant interest and expertise. They include:

- Systemwide Operations and Planning Advisory Group (SOPAG)
- Library Technology Advisory Group – LTAG (http://libraries.universityofcalifornia.edu/sopag)
- Heads of Public Services – HOPS (http://libraries.universityofcalifornia.edu/hops
- Resource Sharing Committee - RSC (http://libraries.universityofcalifornia.edu/rsc)

LTAG has been asked to investigate and report on the background technical status, environment, and next steps for shibboleth authentication to systemwide library services.

Sample Use Cases

1. Access to Tier 1 (all-campus) Licensed Content. A faculty member browses electronic journals from the office with no apparent authentication (transparent IP-based) and would prefer a single-sign on experience from home or while traveling.
   Primary actor: Library patron
   Trigger: Patron attempts to access restricted resource
   Current flow: Vendor web apps check the IP of the incoming traffic against a list of included ranges from UC, including vpn and proxy-based IP assignment. Individualized services require separate vendor-side AuthN/AuthZ (ID/PW pairs).
   Ideal flow: Via web browser, patron attempts to access -protected resource. By virtue of either IP-based access rules (incl. proxy/vpn for walk-in patrons) or successful shibboleth AuthN, access to resource is granted. With permission, additional attributes released for personalized services.
   Alternate workflow(s):
   1. Patron accessing from IP address external to "included" range is routed through university Identity provider for AuthN, AuthZ.
   2. Patron affiliated with InCommon Federation member institution attempts accessing from IP address external to "included" range is routed through home institution/organization's AuthN/AuthZ service, routed to target.
   3. Patron affiliated neither with university nor InCommon member institution/organization denied access.

2. Patron use of Systemwide library services. Example: Interlibrary Loan. After finding a book record in Melvyl, a patron requests an interlibrary loan of the book. He can choose the campus delivery location (e.g. a branch library), and check status, renew, or cancel the loan via “MyILL.”
   Primary actor: library patron
   Precondition: Patron is included in library AuthN/AuthZ group
   Trigger: Patron initiates ILL “request” or “MyILL” session
   Current flow: CDL-based “request” application asks for “Library card/account number” and PIN and checks against UC IdP (usually at the library to account for special or blocked privileges).
   Ideal flow: Via web browser, patron begins Request process of MyIll session. By virtue of shibboleth authorization/SSO, access to service is granted.

3. Library staff member administration of campus-specific portion of systemwide services. Example: As a branch-based interlibrary loan librarian, a library staff member authenticates to the ILL/Request administrative interface and begins processing the queue of incoming loan requests from other campuses.
   Primary actor: library staff member
   Precondition: Included in AuthZ group
   Trigger: Library staff member begins administration/management session
   Current flow: CDL-based “request” application maintains and asks for embedded AuthN/AuthZ info (ID/PW pair).
   Ideal flow: Via web browser, librarian begins admin session. AuthN is established via shibboleth authorization/SSO and handed off to application for AuthZ.

Appendix: Extant or pending UC library UCTrust/Shibboleth projects

Campus	Project/activity	Services	Timing	More info
CDL	Re-specify preference for content vendors to authenticate via Shibboleth	Systemwide licensed content (aka "Tier 1")	in place	"UC's Preferred Solution for Authentication" in Technical Requirements for Vendors (http://www.cdlib.org/vendors/#technical)
UCSD	Pilot EZProxy-Shibboleth integration (part of InCommon-Library pilot group)	remote access to licensed content (JSTOR and ScienceDirect)	pilot ended 8/7/08	https://spaces.internet2.edu/display/inclibrary/University+of+California+-+San+Diego+Profile+and+Project+Update
UCSF	Replace GALEN accounts with "MyAccess" shib-based AuthN	Library Wiki; Podcast@UCSF; Library Wireless; Library Printing; Moodle; CLE+ (new system replacing SOM curriculum management system); SFGH Wireless	8/1/09 – 6/30/10	Ann Dobson, UCSF