Shibboleth: Improving Access for Library Users

InCommon Library/Shibboleth Project
Holly Eggleston, UC San Diego
Overview

• Overview of electronic resources
• About the Library/Shibboleth Project
• Future directions

Overview of electronic resources
- including how they work now

About the library shibboleth project
- suggested technologies and how they work

Future directions
- activities
- issues needing resolution
- additional participation.
What is a Licensed Electronic Resource?

- Journals, books, encyclopedias, databases, data sets, images, audio
- Indexes and/or full text
- For paid resources, can be a one time payment or ongoing annual subscription
- Subject to use and access restrictions beyond regular copyright

- Indexes or full text – users can move between resources using “link resolver software” such as SFX or Metalib

- How many folks use online resources, such as Safari Tech Books? Good, because they were just added to the InCommon federation.
Most institutions have been working with electronic resources for 10 years, some longer.

Availability of home computing and increase in distance education make electronic resources practical and appealing.

Users expect information to be online and easy to access - they’ve been well trained with web searching.

Typical library licenses hundreds of vendors and publishers, with resources reaching into the thousands when including individual journals.

Resources are expensive, and take up a large portion of most libraries' collections budgets.

Substantial staff time is allocated to ordering, maintaining and troubleshooting these resources.

These resources are predominantly leased, not purchased, which makes them subject to a large number of legal obligations - including who can access and from where, and how they can be used.

Lots of work has been and continues to be done to target at integration of disparate electronic services -- including the rise of Google scholar, link resolver software such as sfx and serials solutions.
Our licenses require defining our access and restricting to particular subsets of users

-Restricted to authorized users
  -Students, staff and faculty
  -Users who are present at the library (walk-ins)
-Restricted to specified locations
  -Restricted campus locations (labs)
  -Full campus
  -Remote access (off-campus)
-Library provides vendor with list of IP addresses

*Issues with providing IP

-Public machines – can be login or no login. In the case of login, walkin users obtain a guest username and password
- IP list is maintained with vendor
- Vendor detects campus IP
- User validated

- Note, if there is personalized functionality, for instance bookmarks, notes or customized alerts, vendor will require additional login.

- Maintaining IP lists with vendors is a chore -- mentioned resources numbering in the hundreds results in mass updates and relying on the vendors to incorporate the changes.
Why change?

For library technical services – IP maintenance.
-- Requires maintenance of list, contacting all vendors, hoping that they have updated the list.
-- This has ongoing concerns for reliability of access for the resource, legal implications in adherence to our licenses.
-- As my IT department likes to remind me, IP addresses aren’t secure and can be easily spoofed

Remote access is one of the primary complaints.
- Service integration that relies on IP address access control doesn't work from home
- Solutions to allow this traditionally rely on user-side configuration
  -- User error
  -- Browser compatibility
  -- Firewalls
  -- And other configuration conflicts

remembering passwords –
- the whole argument for single sign on.
  -- Proxy
  -- Personalized resource
  -- Library account

Admitting this is preaching to the choir, linking into IT initiatives to address these types of problems.
Accessing resources remotely

- Restricted to students, faculty and employees
- Requires user name and password
- Uses authentication software
  - Traditional proxy
  - Rewrite proxy
  - Client VPN
- Similar situation as to the above, with the addition of Proxy or VPN, where the vendor has the IP addresses assigned by the proxy.
Now: Screenshot of Remote access page
Now: Screenshot of proxy prompt
Remote Client Access Challenges

- Requires proxy or client VPN software to assign campus-controlled IP to user machine
- Often requires user to configure their machine
  - User confusion
  - Browser / firewall conflicts
  - Lockdown environments
- Multiple passwords to remember
- Maintenance of IP list at the institution
- Maintenance of IP list at the vendor

- Traditional proxy and regular VPN require users to configure their local machines and is browser dependant
- Both VPN and traditional proxy run into problems with local machine and firewall configurations.
- Also these logins are not single sign on, requiring yet more passwords
- If vendor has personalized functionality, user needs to login to resource in addition to logging in to proxy.
- So we’re interested in getting away from both the need for user side configuration and vendor IP access
In an ideal world ...

• Integrated access to licensed library resources regardless of user location
• Consistent user experience for authentication
• Reduced maintenance overhead for library resources
• Reliable authentication for vendors

- No user configuration of computers
- Use a single password for access to all resources
- No IP’s needed
What is the Library/Shibboleth Project?

- Established 2007
- Six universities + Internet2
- Campus IT, Library IT, Librarians

- Overview of Library/Shibboleth project
- Step by step through proposed user scenarios
- Identifying issues
- Progressively incorporating SSO and other technologies

- Result of discussions in InCommon Shibboleth group with Peter Brantley and Cliff Lynch

- Establishing a group of institutions willing to examine issues and pilot shibboleth solutions for library resources

- participate in biweekly phone calls

- Adding shibboleth to existing library services
Focus of the Library/Shibboleth Project

- Improving access to licensed electronic resources
- Identify user scenarios
- Document business practice and technology issues
- Test proposed solutions

- Current focus is accessing library commercial resources
- Enumerating user scenarios
- Identifying issues both business and technical
- Testing different solutions for proof of concept and eventually best practices.
We’ll go into these with more detail.

Technologies investigated

- Federated Access
  - Shibboleth
- Shibboleth-enabled Rewrite Proxy
  - EZProxy
  - WebVPN
Shibboleth addresses many of these issues:

- The authentication list is maintained locally
- The same login information is used for multiple resources
- It gives the ability to protect user privacy by sending a generic or anonymized identifier while permitting personalized access to resources
- Provides ability to give selective access to resources based on criteria
- It removes the need for IP maintenance and increases authentication reliability on the vendor side
- Open standards assures compatibility with vendor implementations
Federations provide a way for member institutions and vendors to define a standard for how Shibboleth authentication information will be transferred between member institutions. This saves time in the vendor negotiation process, as all attributes are agreed upon by the federation members.
Internal campus resources: leave balances, employee information, student registration information
These are vendors that are enabled for Shibboleth, but may or may not be part of the US federation.

A more comprehensive list of vendors and resources are on the information page at the end of this presentation.
- For the authorized user, this is the ideal scenario.
- User accesses resource directly which invokes call to IdP - either directly or by clicking "login" link
- Allows for one login for both remote and personalized access

- Now this is great for the users that have accounts with the institution, but most libraries also allow for (and in cases of state institutions, are obligated to) provide access for patrons who may not be affiliated with the university, but who are on the premises -- otherwise known as "walk-in's"
Screenshot: ScienceDirect remote access, no IP

Click to login

For the existing users, having to click the WAYF and login on the screens is a change.
Screenshot: ScienceDirect Shibboleth WAYF (where are you from) page

Select institution
Screenshot: UCSD Shibboleth Authentication
For users that do not have a user name/password, such as walk-ins,

- Enter mod_auth_location -- thanks to University of Washington

- At the time of IdP detection, the mod_auth_location Apache model can identify the user's IP and verifies against list of permitted addresses, allowing for login as a "generic user" -- just enough to be able to gain access to library resources while they're on the premises.

- However, this is problematic for authorized users that may be using one of these public machines to access their personalized resources (campus or library), so the user is actually given a choice to login with their personal login or be authenticated as a guest.

- Unfortunately, even in a best case scenario not all resources will be shibboleth enabled, which means we still need a method of authenticating users outside of the campus IP space.
Library concerns with Shibboleth

- Communication with campus IT
- Privacy
  - Privacy with individual vendors
  - Privacy across vendors
  - Session persistence
- User experience is different for on-campus users
- Walk-in users don’t have SSO accounts
- Library patron database integration
- Not all resources will use Shibboleth
- IP is still needed for some resources

With thanks to Cliff Lynch and Peter Brantley

- IT Communication – communicating with libraries and bringing this to their attention

- Privacy - requires meeting campus and possibly federation standards for passing user-identifiable information
  -- How much information do we pass to vendors? As little as we can. However, may need to have user-individuation for allowing personalized functionality.
  -- Proposed “user confirmation of attributes” for IdP v. 2.2 would address this issue.
  -- Also concern about sending consistent identification to multiple vendors – EduPersonTargetedID in Shibboleth 2.0 makes this easier to maintain and generate.
  -- SSO in a public environment can be dangerous because of session persistence. Need to ensure a mechanism to close the browser or reboot the machine.

- User experience is different for on campus users – by default, they do not have automatic access by virtue of their location.

- Walk-in users - we addressed this as part of the scenarios

- Library patron database integration -- less of an issue for electronic resources, but essential if looking at enabling library services such as account management and ILL requests for single sign on.

- And as much work as is being done, there will always be resources that will continue to use IP access.
- A proxy by a different name

- Primarily a library-implemented solution to provide off-campus access to library resources.
  - Inexpensive
- Many libraries already use this for remote access – I’ve had sessions where every hand in the room goes up when I ask who is using EZProxy.
  - Server side proxy that acts as both a virtual server and virtual client by rewriting the resource URL’s.

- Two main advantages
  - Server side -- no user configuration needed
    - Can be enabled for single sign on authentication

- UCSD is currently working with the WebVPN rewrite proxy from Cisco that is part of their new VPN client, but this is not as widely used, nor as inexpensive.
- User accesses library web page, clicks on resource
- Directed to EZProxy, which validates to the IdP
- If going to a Shib-enabled resource, user initiated login and WAYF, passed through and persistent identifier is detected, passing additional attributes as necessary
- If going to an IP validated resource, uses proxy to act as permitted IP address
Screenshot: Library Webpage without Proxy authentication
Click bookmarklet or have embedded link on page to login to EZProxy
Screenshot: Shibboleth login for EZProxy
Screenshot: Proxied Library Page

There are some user training issues for those that have not implemented a rewrite proxy:
- Rewrite proxies are dependent on having an explicitly written URL and clicking links from the current page.
- If user manually types a URL or clicks an external link, they need a quick way to get validated (bookmarklet).
- Depending on your configuration, you can create modified URL's in existing links, or (as we've done in our example), included our catalog and SFX as proxied sites, so it automatically provides a passthrough.
- As a rewriting proxy modifies the URL change, it can get tripped up by programming variations outside of the HTTP stream or on different ports.
- Rewriting proxies do not work on “client software” based resources such as Scifinder Scholar. In both of these cases, a VPN is a better choice.

The institutions that have implemented this resource have used a combination of technological solutions and user education to address these issues, but it is a consideration for those libraries that have not adopted a server-side proxy.
Screenshot: UCSD links to resources
Screenshot: Ebsco authenticated with EZProxy SSO Login
Screenshot: Search for article in ScienceDirect
Screenshot: Passthrough to UC Elinks (SFX), using a WAYF-less URL
Screenshot: UCSD Shibboleth Authentication
Screenshot: ScienceDirect authenticated with Shibboleth information provided at EZProxy login.

In the case that a resource is entirely Shibboleth enabled, you can still pass the resource through EZProxy (to maintain the rewrite functionality), but as IP’s are no longer maintained with the vendor, the authentication will occur with the Shibboleth credentials, not the IP address.
An SSO enabled rewrite proxy by itself has a number of advantages

Benefits to our users:
- Single password
- As it’s server side, users don’t need to modify their local machines – a bonus for users in lockdown environments.
- User experience – seamless access, personalization and consistent behavior on and off campus

Benefits to our librarians
- Support – reduction in help tickets

Benefit to library administration
- Local foot traffic log
So if I have a shib-enabled rewrite proxy, why should I take the extra step and access my resources through Shibboleth?

Don’t have to maintain IP’s with Shib resources, if 80% case is handled through Shib, possible to route the rest of the functionality through a router, effectively eliminating the need for IP maintenance.

To recap, what are the benefits that these technologies can provide to the libraries?

Benefits to our users:
- In addition to a single password for remote access, now a single password to also access their personalized features

Benefits to our librarians
- By using Shibboleth for the high traffic resources, can route all traffic through local proxy, reducing the need to maintain large IP lists with the vendor.
- SSO enabled proxy allows for gradual integration of Shibboleth-enabled resources with a minimum of impact to the user – this is not perfect, we’ll be talking about this in a later slide.

Benefits to Vendors
- Authoritative validation – I talked about IT concerns with the security of IP-based access
- Being able to more quickly identify and resolve breach issues is useful for both Vendors and Libraries
- No maintenance of passwords by the vendor

Benefit to library administration
- Depending on your data collection and privacy policies, the proxy provides a central foot traffic log, as does Shibboleth. In addition, Shibboleth can provide additional data to permit summarizing demographic information.
Implemented Shibboleth with the release of 1.0
Initially focused on campus services, currently in production
Currently piloting electronic resource access using hybrid EZProxy solution
  - high use
  - programmatically complex
  - historically problematic
Production rollout for resources for historically problematic populations (biomed)

We are a ILL shop, and are in discussions with them for Shibboleth compatibility with ILS services

Also working on how to integrate this as participants of the larger UC system - some of the solutions implemented by single systems create conflict with our multi-campus cataloging/shared SFX database.

UCSD recently implemented Cisco WebVPN – another rewrite proxy, and are working on integrating Shibboleth login to provide an alternate option for the hybrid environment.

Other participants are further along in their production library implementations such as University of Maryland, who has a production environment using EZProxy, SFX, Shib enabled library services and campus portal.
Performed initial testing with individual SP’s
Tested feasibility of individual solutions
Maryland testing with Ebsco
Chicago / Washington testing Refworks
Basic use cases – entry points

- Connecting from known URL
  - Library A-Z
- Connecting from unknown URL
  - Google Scholar, email link
- Moving between resources
  - SFX
  - Serials Solutions
- Using Federated Search
Basic use cases – configuration

• Walk-in user on library public machine
• Known user on library public machine
• Known user on campus assigned machine
• Known user, off-campus personal machine
• Known user, off-campus lockdown machine
Licensing configuration scenarios

- Restricted to subset of authorized users
- Restricted to subset of locations
Shibboleth has lots of potential for addressing these ongoing problems encountered by libraries. The hybrid solution is necessary for making this work. The current situation is good for beta testing or small pilots, but it’s not ready for production implementation.

Beginning to enumerate issues and possible useful functionality, anticipate that this will happen as pilot testing continues.

Implementing at campuses
  - Communication with IT
  - Available technological expertise / technical overhead
Streamlining activation process
  - ensuring that institutions have all the information they need to activate with SP’s

SP membership in federation
  - continuing to work with SP’s for membership

SP functionality
  - SP’s have taken the big step to adopt the technology, but the implementations vary widely between vendors. To make this compelling and easy for users, the experience needs to be consistent and intuitive.

Next slide
Step for us: Where do we want to focus our efforts. Identifying the common licensed library vendors (probably 15-18) that represent 80-90 percent of the traffic for most libraries. Determining whether those vendors are Shib-enabled (many probably are through the UK federation), working with those vendors to join InCommon, and promoting federating among these vendors and libraries.

Advocating to service providers about the basic technology of federating and providing the use cases to support this.

Advocating to service providers on standards needed to federate to make it easy for users.

Adam Chandler reported that NISO (National Information Standards Organization) has been exploring something similar. He and Oliver Pesch of NISO are drafting a work item for NISO in this area. As well, we’re communicating with the UK federation for sharing ideas and open issues.
Features and functionality - Shibboleth

- Improvements with the unique identifier
- Movement of users between IdP
- Customized / consented release of attributes
- Known IP override
- WAYF-less interface for existing logins

The question – should be focus on creating solutions with supporting technology to make this work, or are there features that shibboleth can/should implement to make the real-life solution easier?

Are these problems that shibboleth can address?

Movement of users between IdP’s – as faculty and students move between institutions, how can they maintain access to resources that provide personalized services such as alerts, bookmarks, markup? This is addressed via an external management solution by the Swiss federation, are there other ways this can be implemented?

Consented release of attributes – mentioned as a possible feature for 2.2.

WAYF-less interface addressed by use of the WAYF-less URL – will this address our concerns for the use cases?

This is just the emphasis that the conversations need to happen at a more technical level – we have the issues, but need to identify where it is most appropriate to be addressed.
Communicate features and functionality
- continue to develop functionality requests lists and identify appropriate venues for promotion and communication

Identifying the common licensed library vendors (probably 15-18) that represent 80-90 percent of the traffic for most libraries. Determining whether those vendors are Shib-enabled (many probably are through the UK federation), working with those vendors to join InCommon, and promoting federating among these vendors and libraries.

Continue outreach to librarian groups, write up case studies, white papers on hybrid solution and creating public web page

Opening the group to additional participants and establishing a wider affiliation
- actively partner with UK federation to share our mutual experiences
- opportunities for national level collaboration – EDUCAUSE, NISO, CNI
- library organizations

Outline the remaining questions related to proposed solutions and conduct tests to determine answers
- More functional testing
- Expand technologies and vendors tested

Expand pilot efforts to include concurrent shibboleth related projects and interested institutions.
Future steps - Outreach

- Continued outreach to librarian groups
- Case studies
- White papers and other documents on hybrid solution
- Public web page

- Developing information (such as white papers, use cases or other documents) on the hybrid Shibboleth/EZProxy solution to library access.
- Sharing case studies, documenting what works and what doesn’t.
- Mapping the presentations (which are on the wiki) into more generic reports, suggestions and recommendations.
- Public web page
Future steps – Group configuration

• Opening group to additional participants
• Establishing wider affiliation
  • International federations
  • EDUCAUSE, NISO, CNI
  • Library organizations

- Determining whether to open this group to a wider audience and, if so, when and how.
- Monitoring email lists of other groups
- Making contacts with peers in Europe to share experiences and use cases.

There are a number of email lists which may help identify likely candidates. It may be useful for members of this working group to monitor those email lists, gathering information about general trends and identifying people with whom we might collaborate.
We’ve done a lot of component testing, but it's down to how it all works together for the users.

Continuing to identify questions and test solutions

Testing other technologies, SP’s

Enabling more service providers

Opening the pilot to a wider group

JISC
CIC Digital Repository
NJEdge
Ohiolink
NCMC (North Carolina) – k-20 initiatives

the University of Chicago is moving forward. Applications in production (using Shibboleth and EZProxy) include RefWorks and Elsevier (Scopus and Science Direct).
Getting involved

• Informal
  • EZProxy users, use Shibboleth for EZProxy authentication

• Formal
  • Contact us
Contact

- http://www.incommon.org/library