# Phase 1 Work

## Work Accomplished in Phase 1

The Phase 1 campuses did some work on the hybrid. Here is a summary of their efforts

---

**UC San Diego**

UC San Diego implemented Shibboleth in 2005 in response to the system-wide UC Trust initiative and requirement for accessing UC internal resources and tools. Shibboleth has been used for many UCSD campus resources since then, including leave balances, travel, finance, Shibboleth enabled campus services, housing and recreation.

**Issues to solve with pilot**

Current methods of remote access have a number of issues that we hoped to address through our work in the Library / Shibboleth pilot.

1. Reduce need for user configuration of computers to provide remote access (user error, firewall/machine conflict, lockdown machines).
2. Reduce need for IP maintenance with vendors
3. Reduce need for manual proxy maintenance
4. Create consistent user experience, using a single user name and password to access both internal campus resources, library services and external library-licensed electronic resources.

**Challenges**

We had a number of initial concerns and scenarios to explore with the pilot:

1. Finding a solution that would work for walk-in users.
2. Minimizing changes in current user experience for on-campus and remote access.
3. Getting familiarity with and implementing EZProxy
4. Compatibility in a consortial environment with shared resources and shared tools.
5. Possibility of integrating Cisco WebVPN as an alternative rewrite proxy solution.

**Lessons learned**

*Questions answered*

1. EZProxy was much easier to implement than originally anticipated.

*Questions raised*

1. **EZProxy variations**: As much of the user experience and general maintenance issues are affected by the EZProxy implementation, we need to know more about best practices for general EZProxy configuration.
2. **Inconsistency with finding login**: The vendor implementations of Shibboleth vary widely. Some resources provide an easy link from all pages to log in using Shibboleth (ScienceDirect); others require a specific URL to provide access to the Shibboleth login option (EBSCO). To provide an easy transition from IP to Shibboleth (and to prevent additional maintenance/updating of access points), getting to a Shibboleth login should be easily accessible from any page on the vendor site.
3. **Inconsistency with WAYF**: Another factor of the varied implementations are the different WAYF pages implemented by different vendors (compare ScienceDirect and JSTOR). The variations in interface, location and selection should be more standardized to prevent user confusion.
4. **Bypassing WAYF:** To permit easier transition of IP based authentication to Shibboleth authentication, more work needs to be done to provide a WAYF-less environment, particularly if the user is already authenticated with Shibboleth in the browser session or is accessing from on-campus (see Shibboleth Enabled Resource - Off Campus above).
5. **Personalized functionality:** One of the primary arguments of why the Shibboleth + EZProxy solution is better than EZProxy alone is the ability to access personalized functionality at the vendor. Very few vendors have implemented this yet.

**Recommendations for others**

1. The biggest surprise for us was the advantage of configuring our access points (catalog, resource database, SFX) in EZProxy - this reduced our setup time and maintenance issues considerably. I'm not sure if this is common practice, but it worked well for us.
2. The JavaScript bookmarklet is great for reinstating proxy access.

---

**University of Chicago**

Issues to solve with pilot:

- Access to licensed library resources and services.
- Access to locally-hosted resources at U. Chicago that must not be accessible by the world.

**Challenges**

- IP-authenticated resources have not required on-campus users to authenticate themselves, and there is a reluctance to inconvenience on-campus users in a Shibboleth environment. How to accommodate this desire is a technical challenge, but changing the experience for on-campus users is a political issue.

The U. Chicago pilot involved migrating from the Squid proxy to EZproxy.

Early Shibboleth testing was done with EBSCOhost, ILLiad was the first production service, and EBSCOhost, ScienceDirect, Scopus, and ARes planned for fall.

Integration: Library-controlled services such as the catalog, AquaBrowser, SFX and Metalib, all are configured to rewrite URLs to all resources to route access through the proxy server. Not all resources require authorization, so if a resource is not in EZproxy's configuration file, the proxy server will forward the browser directly to the remote service, stepping out of the interaction entirely. If a service is in the configuration, EZproxy is configured to first allows IP-based authentication for proxying if the user is on campus. For off-campus users, the proxy requires authentication with a University ID. Given successful authentication, the proxy checks the user's attributes to see whether they are allowed access to a particular resource. As we move resources to Shibboleth, we expect that EZproxy will also step out of the loop, and not proxy access to Shibbolized resources.

Initially, the proxy server was configured to perform LDAP- based authentication. At that time, everyone in LDAP was eligible to use these resources through the Library's licensing; authentication was equivalent to authorization. However, as the University moved to fully integrate the campus ID namespace and include the Hospitals, Laboratory School, and alumni in campus authentication services, the equivalence of authentication and authorization would be broken. We had been planning with this in mind, and EZproxy was configured to authenticate via our Web ISO and use our Shibboleth IdP for authorization. EZproxy checks user attributes against the resource they are accessing, and allows or disallows access accordingly.

---

**University of Washington**

Electronic resources are generally licensed for all three campuses, and access control is based on IP addresses. As a state institution, UW Libraries provides services and resources to community members while they are physically present at the Libraries' facilities. A small number of resources are limited to students, faculty, and staff only; these resources require authenticated access even from campus IP addresses, or are available only in restricted labs.

The Libraries use Innovative Interfaces' Millennium integrated library system; since April 2007, OCLC's WorldCat Local has been the default public catalog. Offcampus access to electronic resources is mainly via EZProxy. OpenURL link resolution is provided by III's WebBridge module, and holdings data for electronic journals is purchased from Serials Solutions. Most library-provided services that require authentication use the campus single sign-on service "pubcookie"; authorization is done via a locally built web service that obtains real time status information on users from the enterprise directories.

The UW Libraries' interest in a Shibboleth pilot stemmed from our dissatisfaction with location-based access control, a particularly bad fit given our geographically distributed user base. We also wanted to extend our user's single sign-on experience to include remote resources. Our main concern was identifying targets that wouldn't negatively affect the users but would give us some operational experience with Shibboleth.

**RefWorks**

In early 2008, UW logins to RefWorks began using Shibboleth and trust metadata provided by the InCommon federation. The UW IdP's attribute release policy sends eduPersonScopedAffiliation and privacy-preserving eduPersonTargetedID values to RefWorks for eligibility verification and record keeping.

Prior to converting to Shibboleth access, users had to create an account that included a username and password. When offcampus, users were required to access RefWorks via EZProxy. Users could create multiple accounts; these secondary accounts provide a way for instructors to share bibliographies with a class, for example. Relatively few users have multiple accounts.

Post-Shibboleth, UW changed its advertised RefWorks URL to avoid the WAYF and take users directly to the UW weblogin service. The RefWorks login page (http://www.refworks.com/Refworks/login.asp?WNCLang=false) added a "Login through your institution" link for Shibbolized access, and UW-specific information was added to the customizable portion of that page.

Users with existing RefWorks accounts were offered the option of Shibbolizing them on initial login. It was not possible to use EZProxy with the Shibbolized accounts, so EZProxy was configured to not proxy any RefWorks access. Only one account per user could be Shibbolized; users with secondary accounts had to continue using RefWorks native authentication with those accounts. Because EZProxy was not proxying RefWorks, those secondary accounts can now only be used from campus IP addresses. RefWorks is looking at how best to support secondary accounts in the Shibbolith environment.

**Accommodating Walk-Up Users with Location-Based Authentication**

Summary: In some situations it is useful to authenticate user sessions based on location (meaning network address) instead of the more usual credentials (e.g. username and password). An Apache module, mod_auth_location, is available for this purpose.

Most modern application sign-on scenarios operate via credentials associated with and provided by a user: a username and password, Kerberos ticket, X.509 certificate, etc. Use of such credentials permits a user to sign on to a system or service regardless of where the user happens to be. Many institutional systems have worked hard to eliminate the practice of basing access based on location (meaning client machine network address, usually), for various reasons: lack of personal accountability, disconnect with policy, etc.

In one use case, access based on location is exactly what policy calls for. Traditionally, licenses for use of physical library materials have granted access to members of the institution, or any others physically present in the library. As access has moved online it is necessary to continue to support this access policy. Terminals (kiosks) are placed in the library to support both institutional user and library walk-in access.

Many remote vendor-provided licensed resources have had access control set up by location. Typically the licensee institution provides the licensor with its network address ranges, and resources may be accessed from machines in those ranges. Walk-in user access fits in easily with this method. As resources move to using user authentication for access, steps must be taken to preserve walk-in user access. There are a variety of approaches to this, complete discussion of which is out of scope in this document.

From the resource provider point of view, especially for new resources which have never used location-based access, configuring resources for location-based access just to deal with walk-in users is onerous. It is desirable to hide this complexity from the resource provider, and instead handle location-based access as an authentication mechanism at the identity provider (ie the licensee institution).

mod_auth_location from the University of Washington is an extension to the Apache httpd web server for this purpose. It can be configured ...

In an environment using the SAML web browser signon profile (as supported by the Shibboleth system among many other implementations) this permits a location-based walk-in user to appear to a resource provider just as a user-authenticated user does, simplifying resource access setup.

**University of Maryland**

**Conclusions**
The goal of this experiment was twofold: 1) to test a method for providing seamless authentication to library-licensed online resources, and 2) to test that this method would integrate with existing library technology and allow relatively easy creation of authenticated URLs to library-licensed online resource. In both cases, this experiment was successful.

Using EBSCO online resources as an example, we were able to take a user from an OpenURL resolver or online gateway directly to the resource without ever asking the user to identify where they were from or ask the user to log in more than once. And, so we were able to provide seamless authentication to resources.
For the second part of the goal, we tested SFX and Metalib as existing library technology. SFX and Metalib are not unique in their category of software in that they are aware of ezproxy, and that they can act according to a user's location. Very little, if any, configuration needed to be done to the existing library software in order to provide access to EBSCO online resources.

In terms of ease of URL creation, a user, say a faculty member, could take a known URL for an online resource, and simply tack an ezproxy prefix (ex. http://biblos.umd.edu:2048/login?url=) to the beginning of the known URL.

**Recommendations**

For Resource Providers:

- Implement SessionInitiators to avoid the WAYF when at all possible
- If a resource provider is going to provide multiple forms of authentication, specifically IP and Shibboleth based authentication, there should be a single URL syntax that works for both methods.
  For Library Software Admins:
- Use ezproxy as single point for directing URLs that require some sort of authentication.
- For ease of URL generation, configure ezproxy to make decisions regarding how to handle on and off campus traffic.
- Use ezproxy's SPUEdit directives to redirect traffic to shib-enabled resources through SessionInitiators provided by Resource Providers
- For resources that allow both IP and shib authentication, take advantage of SPUEdit IP directives (-ExcludeIP, -IncludeIP, -AutoLoginIP) to redirect on campus traffic to the original URL, so as to bypass forcing on campus users to log in.

Shibboleth implementation can be done in two phases - enabling Shibboleth login to access the rewrite proxy, as well as providing access to individual vendors using Shibboleth.