2011

ILLiad, CAS, Shibboleth, and PHP: the road to single sign-on

LeEtta M. Schmidt
University of South Florida, lmschmidt@usf.edu

ILLiad, CAS, Shibboleth, and PHP:

the road to single sign-on[1]

LeEtta M. Schmidt

University of South Florida Tampa Library

[1]

This is an electronic version of an article published in the *Journal of Interlibrary Loan, Document Delivery & Electronic Reserve* [ISSN: 1072-303x] *Journal of Interlibrary Loan, Document Delivery & Electronic Reserve* is available online at:
http://www.tandfonline.com/openurl?genre=article&issn=1540-3572&volume=21&issue=3&spage=149

Abstract

In 2010 the Interlibrary Loan department of the University of South Florida, Tampa, moved to unify its ILLiad sign on practices and align with the University wide objective toward a single sign-on environment. Initial plans to implement authentication with CAS evolved in response to obstacles and system failures and resulted in an ILLiad, Shibboleth, and CAS combination. This article reviews the migration project and its culmination in a successful, and unique, authentication assembly.

ILLiad, CAS, Shibboleth, and PHP:

the road to single sign-on

Password proliferation is fast becoming one of the more difficult challenges in managing identity, business, and finances. Businesses have pinpointed password management for creating an unacceptable loss in productivity and money (Spangler, 2001). People with too many passwords to manage tend to make their passwords too weak or use the same password for many systems which leads to security risks for organizational and personal data (Crosman, 2005). The world of academic library resources and service request management systems adds to this plethora of passwords in a way that is ultimately a disservice to library users. To alleviate the growing problem, in 2010, the University of South Florida (USF) library moved to unify its system sign on practices and align with the University wide objective toward a single sign-on environment.

Single sign-on has been a goal in the corporate world and academic groups for many years. In perfect application it would aggregate "identity data from disparate … directories, letting users access multiple Web sites…with one universal ID and password" (Crosman, 2005). USF Information Technology (IT) had already developed a program to "establish a trusted, global identification system" and "create …single-sign-on systems that will…enhance research" (IAMUSF, 2009). Many applications at USF were already using Shibboleth to authenticate users. Shibboleth, created by the not-for-profit advanced networking consortium, Internet2, was designed to be a solution to single sign-on both "across and within organizational boundaries" (Shibboleth, 2011). The University had also adopted CAS, a central authentication system developed by Yale, to allow users to sign in once and "access all the applications he or she has been authorized to access" (About CAS, 2009). Even though Shibboleth was widely in use at USF, CAS was chosen as the primary authentication method for single sign-on because of its compatibility with more applications (Pierce, 2011). One of the first library systems USF chose for single sign-on with CAS was ILLiad, its interlibrary loan request management system.

Background and planning

The USF libraries were quick to see the potential benefits to a new system developed by Virginia Polytechnic Institute & State University in 1997 to manage patron requests for interlibrary loan materials (Kriz, 1998). The libraries migrated their interlibrary loan operations to the ILLiad request management system in 1999. Four libraries in three cities shared an ILLiad server to manage requests from patrons that would often move between the locations. Later, USF's ILLiad installation was moved to a hosted server managed by Atlas in 2003. At the time of the initial ILLiad implementation there were three authentication, or sign on, methods available: Import Validation, or loading a table of users into ILLiad (now ILLiad Exclusive), LDAP, or referring ILLiad to a pre-existing table of users, and Basic Authentication (Cella, 2011). From the beginning USF had used ILLiad's Basic Authentication method, which relied upon patron initiated registration followed by staff verification of patron credentials. The patron's user account on the ILLiad server was not verified or updated by any external system. This sometimes led to outdated information being stored in the system. The combination of USF's multiple ILLiad sites, for each branch library, serving the same patron community and patron initiated registration also enabled the creation of duplicate patron records on the server that could not always be sorted out by staff who could only view one ILLiad site at a time.

Initial hopes for the single sign-on implementation included:

- Allowing users to sign into one University system and have their credentials automatically transmitted to ILLiad once they decided to make a request
- Allow patrons to utilize the University assigned user IDs (NetIDs) to sign in to ILLiad
- Restrict access to ILLiad for users who are no longer at a status to receive ILL services
- Ensure contact information in ILLiad was more accurate
- Minimize duplication of user records in the ILLiad database
- Maintain an option for the addition of user accounts outside of single sign-on

After talking out the options with University IT and members of Atlas the decision was made to proceed with a migration of the current ILLiad sign on method to single sign-on with CAS during the summer of 2010. Atlas would create the environment for testing and install the ISAPI (Internet Server Application Programming Interface) filter needed to facilitate communication between CAS and ILLiad. The creation of that ISAPI filter and all customizations, maintenance and programming of CAS would be the responsibility of University IT. The USF Tampa ILL department would handle the manual process of merging of pre-existing duplicate usernames, as well as advertising the impending change to patrons.

Several Universities had already laid the groundwork for an ILLiad and CAS marriage. A few notable contributors to the quest for single sign-on were freely providing the building blocks for others to follow in their footsteps. The University of California at Davis's Information Educational Technology department had created an ISAPI filter in 2007, a new version of which was released in 2010, that was being used at other Universities all over the nation. This filter had been extensively modified by the University of Arizona and both filters were on offer for re-use by interested parties (Remote Auth with ILLiad, 2009).

Opportunity

Around the time discussions had been started about how to move ILLiad to a single sign-on environment, the USF Tampa library had acquired Aeon, another Atlas product, to manage Special Collections materials and reading room requests. Operating under the same library wide goal to unify system sign on practices, the Aeon implementation's infancy made it the perfect proving ground for single sign-on with CAS.

Migration of ILLiad was put on hold while University IT and Atlas moved Aeon to single sign-on for its service launch in May 2010. Like the ILLiad implementation, the Aeon implementation at USF would require two separate sign-on methods, one for users in the University global identification system

and one for non-affiliates to self-register. The Aeon installation was set up with a locally modified sample filter provided by the University of Arizona.

Implementation with ILLiad

After the test environment had been constructed to prepare for the ILLiad migration it became apparent that the ISAPI filter used for Aeon would not work on the Windows 2008 64 bit server where ILLiad was located. The 2010 version of the 64 bit ISAPI filter developed by UC Davis was then loaded into ILLiad test and seemed to be the key to realizing the single sign-on project until a more thorough examination of user logins.

The username is the only piece of patron information that ILLiad requires must be unique. While no two people would have the same NetID (USF student, staff, and faculty online usernames), the first initials and last name construction of these usernames made it possible that a non-NetID user could choose the same username that had been assigned to someone else as a NetID.

Each individual library at USF maintained site specific policies and patron groups to whom they provided ILL service. This created user populations that would not have NetIDs. Because of this, the libraries would need to retain a basic sign in method where in patrons chose usernames and passwords outside of the CAS system.

The simple construction of NetIDs and the need to continue providing service to non NetID users could create scenarios where a patron would be given access to another patron's ILLiad account upon sign in. A few simple tests revealed that the UC Davis filter would not be able to pass a secondary attribute (or University ID number; the primary attribute being the NetID) from CAS to ILLiad at login. Writing an ISAPI filter from scratch was deemed prohibitively complex and unlikely with current resources. USF IT had used another filter, written by CCCI, with great success on several other projects with CAS (Pierce, 2011). After installation and brief testing, the libraries were back on track with their migration to single sign-on.

Single sign-on with CAS would not correct pre-existing user data in the ILLiad system or expire/block patrons who were no longer eligible for the service. The username would be the only data passed to ILLiad when a new user registered, and anyone with an active NetID would be able to sign on to ILLiad. Because of this, the USF ILLiad sites retained their pre-existing process of clearing and maintaining patron records.

Delay delay delay

While ISAPI filter testing was tried and tried again in the test environment, interlibrary loan staff at the Tampa library was sorting through the glut of duplicate patron records among all the USF ILLiad sites. Each duplicate had to be manually merged to its currently in use patron record to minimize patron inconvenience during the process. Nearly eleven years of retained patron and request data made this task quite a bit larger than initially projected, and by the time they were finished ILL staff at the Tampa library had merged over 1500 duplicate records in a combined total of more than sixty hours. More delay was caused by the fact that no extra staff were brought in to handle the extra work required for the single sign-on migration.

The projected migration day was carefully chosen with regard to the work still under way and the goal to have single sign-on for ILLiad before the beginning of the fall semester. Advertisements to users began, a month in advance of the July 27th migration day, to alert them of the impending change. However, confusion regarding the number of patron duplicates and the previously unforeseen need of a new sign in page for OpenURL links required a new migration date, one week later, be chosen. Preparing the ILLiad web pages to accept two different methods of sign in created two different OpenURL sign in pages. One would direct the user to the CAS supported University sign in page and the other would direct non NetID users to an ILLiad supported sign in page. Databases and indexes use one link to transfer citation information. A re-directional web page, maintained on University servers,

would need to be established to allow two different patron communities to make use of the OpenURL capabilities.

Aeon's previous migration to single sign-on had used a php redirect to shuffle the OpenURL connections from the USF catalog to the Aeon web forms via two sign in methods. The pages had been originally developed by the University of Chicago for their implementation of Aeon with Shibboleth within the library catalog, and seemed to need little alteration to be used for ILLiad as well.
This re-directional page created a new challenge for the project. Every USF subscribed database and index that utilized OpenURL connections to ILLiad needed to be updated with the new php page address. Many of these systems allowed staff at subscribing libraries to log in and update information directly. For these, the challenge was simply workload. Requests were submitted to all the others, and all but two of the OpenURL connections were changed on migration day.

Problems always show up after the sigh of relief

Migration day on Wednesday, August 4th, 2010, began with a flurry of activity by ILL and technical services staff, changing all the OpenURL connections immediately after the system had been taken off line. After some final patron record problems were cleared up, staff began drafting emails to heavy users to remind them of the migration. After only eight hours ILLiad was back up and available for patron use.

It took twenty four hours for reports to reach ILL staff that some OpenURL connections were not reaching the re-directional page, or were not successfully connecting to ILLiad through the page. A week of gathering and testing OpenURL links from all the databases revealed that the original php script, written by the University of Chicago to handle links from the library catalog only, was not allowing for the wide variety of OpenURL links generated by the library's database subscriptions. After heavy editing of the php script, the problem was fixed.

The USF ILLiad database was moved to a new SQL Server by Atlas approximately one month after migration as a part of standard maintenance. This event was only made significant by the errors that began to occur approximately one week afterwards.

Patrons were attempting to sign in via the CAS enabled log in page and were either seeing a blank screen that did not advance to the ILLiad pages or were being referred back to the Interlibrary loan services page (the normal destination for those who logged out of the system). Initially the problem seemed to be resolved by restarting the web service. The login problem resurfaced the next day, but could not be fixed by restarting the web service or rebooting the server all together. A week of investigatory trial and error yielded a simple solution in a change to a single line of code.

Four days later the system was down again. The cache file that the ISAPI filter was using during patron login had been locking itself. Discussions between the library, University IT and Atlas landed on the hypothesis that the specific combination of ISAPI filter, passing a secondary attribute in the CAS ticket, and the 64-bit environment was causing a kind of perfect storm. University IT proposed inserting Shibboleth, designed from the beginning to support additional attribute release and successfully paired with the same ISAPI filter in other campus implementations, between CAS and ILLiad in the USF implementation. Retaining the CAS enabled log in pages would allow all students, staff and faculty to access all University applications with just one login (Pierce, 2011).

Final solution October 20th, 2010

A test environment was created by Atlas to vet the Shibboleth hypothesis, and another migration, two months after the first, successfully ended USF ILLiad's switch to single sign-on. Now, when patrons sign in to ILLiad they are directed to USF's Web Authentication page that is powered by CAS. They log in with their University appointed NetID and password. At login their University number is pulled from the University authenticating server by Shibboleth and passed to ILLiad as the ILLiad username. Only the University number, as the username, is passed to ILLiad. ILLiad does not store the

NetID username or password; it only gives access after authentication. Patron's log in credentials are saved by CAS during an active session and applied to other USF databases and applications that they access so that they do not have to sign in multiple times. No other log in or system errors have been discovered since the final migration.

Benefits received:

- Allow users to sign into one University system and have their credentials automatically transmitted to ILLiad once they decide to make a request
- Allow patrons to utilize the University assigned user IDs (NetIDs) to sign in to ILLiad
- Minimize duplication of user records in the ILLiad database
- Maintain an option for the addition of user accounts outside of single sign-on

An additional, unintentional, benefit was the ability for patrons to get password help twenty four/seven from the IT help desk. Although most of the patron record verification and maintenance remained the same for interlibrary loan staff, the ten to fifteen telephone calls or emails per week for password assistance disappeared. The overdue billing process was beneficially affected as well. Now that the University number was recorded as the patron username, reports on overdue returns no longer had to be checked against a third system before the billing process could begin.

Single sign-on for ILLiad not only relieved patrons of the need to remember an additional login for interlibrary loan services, but directed the application to access login information at a single location controlled by University IT. The process of migrating ILLiad's sign in method to a single sign-on environment was wholly successful because of the cooperation of three separate groups, USF Tampa Library's interlibrary loan department, USF Information Technology Department, and Atlas systems. The project was undertaken with the goal of providing the greatest benefit to students, staff, and faculty at the University by minimizing the need for multiple IDs and passwords across University contracted systems. Although it seemed to be a bumpy road to project completion at times, the generous patience

of USF ILL patrons and the dedication of the project members to a final product that was an error free realization of the project goals made for a sensational triumph.

References

About CAS. (2009) *CAS |Jasig Community Retrieved* April 18, 2011 from http://www.jasig.org/cas/about

Cella, Jennifer. Email Interview. March 15, 2011.

Crosman, Penny Lunt. (2005) ID Keepers: a broadly accepted standard has given federated identity management a push into the mainstream. *IT Architect.* 65(Sept). Retrieved March 14, 2011 from Gale General OneFile, Gale.

Download and Install the CAS ISAPI Filter. (2010) *CAS ISAPI Client.* UCDAVIS University of California. Retrieved March 11 2011 from https://confluence.ucdavis.edu/confluence/display/IETP/CAS+ISAPI+Client#CASISAPIClient-DownloadandInstalltheCASISAPIFilter

IAMUSF: Program Summary. (2009) *University of South Florida Information Technology. Retrieved* March 11, 2011 from http://www.it.usf.edu/standards/security/iamusf

Kriz, H., Glover, J., & Ford, K. (1998) ILLiad: Customer-focused Interlibrary Loan Automation. *Journal of Interlibrary Loan, Document Delivery & Information Supply.* 8(4), 31-47.

Pierce, Eric. Email Interview. January 28, 2011.

RemoteAuth for Illiad. (2009) *Services.* University of Arizona, University Libraries. Retrieved Mar 11, 2011 from http://www.library.arizona.edu/isapi/

Shibboleth (2011) *Internet2 Middleware Initiative*. Internet2. Retrieved April 18, 2011 from http://shibboleth.internet2.edu/

Spangler, Todd. (2001) The Password Plague. *Interactive Week.* 8 ,47.

UC Davis Identity Management Architecture Overview. (2009) *UC Davis Information Educational Technology.* Retrieved April 18, 2011 from http://vpiet.ucdavis.edu/init_identity.cfm