IIIII epl EDMONTON PUBLIC LIBRARY

REPORT

Title: Enhancing the User Experience with Single Sign-On

Presented by: Allison DaSilva, Digital Discovery & Access Intern Librarian

Date: April 4, 2014

Introduction

One of the Edmonton Public Library's 2014-2018 strategic goals is to evolve our digital environment by implementing "a single point of discovery for EPL content." To help realize this goal, the Digital Discovery and Access Intern Librarian, in collaboration with the Manager of Digital Literacy Initiatives and Web Services, and the IT Librarian from The Alberta Library (TAL), investigated how to provide customers with a single sign-on (SSO) authentication process using BiblioCommons Advanced SSO solution. This was achieved by corresponding with a BiblioCommons representative and with staff members from Ottawa Public Library (OPL) to learn about their experience implementing BiblioCommons Advanced SSO.

Additionally, other SSO options such as Shibboleth and Central Authentication Service (CAS) were also explored (see Appendix I, p. 7). This was accomplished by reviewing the related literature and web documentation, as well as interviewing Calgary Public Library's (CPL) Manager of Information Technology. CPL was approached because CAS is a feature of their SirsiDynix discovery layer Enterprise.

Single Sign-On

SSO is a user authentication process that allows a customer to provide their library card number or user name and personal identification number (PIN) or password *once* in order to access all systems and applications that require access permission. SSO eliminates the need for future authentication requests – whereby a user would have to enter multiple passwords – when accessing different applications or databases during a particular session, which greatly streamlines access (Lascarides, 2012; The Open Group, 2010).

Spread the words.

Though, one of the challenges in providing SSO authentication with vendor databases is whether or not the vendor can correctly associate a user with the current license for the library. To resolve this, many libraries are using EZproxy as a method for facilitating authentication (Ingham & MacIver, 2012).

EZproxy is software from the Online Computer Library Center (OCLC) that enables access to authentication-required e-content by temporarily changing the user's internet protocol (IP) address to match the library's authorized IP address. Once the library registers their EZproxy server address with their database vendors, the vendor sees a user's "request as coming from an authorized IP address and therefore permits access" (OCLC, 2013).

Methods

To determine the necessary requirements for implementing BiblioCommons' Advanced SSO, the Intern Librarian, in collaboration with the Manager of DLI and Web Services and the IT Librarian from TAL, corresponded with staff from BiblioCommons and OPL via email.

For due diligence, the Intern Librarian also investigated other potentially viable SSO solutions, including CAS. To obtain a better understanding if this SSO product, the Intern Librarian interviewed the Manager of Information Technology from CPL.

Findings

BiblioCommons Advanced SSO

Implementing BiblioCommons Advanced SSO would facilitate unified access to EPL's website, catalogue and licensed databases, ensuring a more integrated and streamlined log-in experience for customers.

In order for EPL to implement BiblioCommons Advanced SSO, EPL will need their:
- Public Stage Application Programming Interface (API)[1] Key,
- Private (Borrowers) Stage API Key, and
- Stage BiblioCommons Catalogue.

EPL would also need their own API keys for production and an EZproxy Ticket

---

[1] An API is a set of commands, functions, and protocols used by programmers when building software applications. APIs ensure all programs using the same API have a similar interface (TechTerms.com, 2014).

EPL EDMONTON PUBLIC LIBRARY

Spread the words.

Secret Key (SHA1), which is generated via EZproxy and can be undertaken by TAL's IT Librarian and EZproxy administrator.

BiblioCommons would also need the following information from EPL:
- The hostname/subdomain the library will be using for the SSO integration testing,
- A subdomain of the site the library wishes to SSO,
- CNAME[2] to BiblioCommons app servers and tell them what the domain name is so they can configure the redirect,
- (Eventually) an Secure Sockets Layer (SSL)[3] certificate for the above domain name, which is particularly useful if HTTPS-only cookies are desired, and
- If using EZproxy, the URL to redirect to for Ticket authentication

BiblioCommons' SSO developer confirmed that SSO "will work with any software that is written against the API," including Drupal 6 (visit BiblioCommons for detailed API documentation). Additionally, BiblioCommons doesn't have an "out-of-the-box SSO module for Drupal" and expects that the library will have to write the code necessary to integrate SSO with the library's website.

It was found that only two other BiblioCommons libraries currently subscribe to their Advanced SSO, one of which is OPL.

Ottawa Public Library & BiblioCommons Advanced SSO

OPL is using BiblioCommons Advanced SSO for single sign-on between their catalogue, EZproxy resources (databases, OverDrive, Freegal etc.) and their website, which is hosted by Drupal 7.

OPL uses EZproxy for all database authentications (not SIP), which "acts as an internal IP that is proxied into after being authenticated against BiblioCommons. Internal users are bypassed by IP range and for ones with accounts the barcode is passed to sync accounts." To restrict access to resources or limit privileges by card holder type (i.e. temporary cards), OPL uses EZproxy groups.

---

[2] CNAME, an abbreviation of Canonical Name, "is a record in the Domain Name System (DNS) database that indicates the true, or canonical, host name of a computer that its aliases are associated with" (Webopedia.com, 2014). "It is essential when running multiple services from a single IP address" (Techopedia.com, 2014).

[3] SSL "is a secure protocol developed for sending information securely over the Internet," protecting users by encrypting the data being transmitted (TechTerms.com, 2014).

OPL generously provided EPL with a library card number and PIN, which allowed us to explore their website, catalogue and licensed databases, and experience SSO from the end-user perspective. Through OPL's SSO we were able to register for events, access and check out an e-book from OverDrive and e-music from Freegal, and submit a request for interlibrary loan (ILL). Unfortunately, OPL doesn't have some of the same databases as EPL, including Freading, Hoopla, IndieFlix, One Click Digital, Press Display and Treehouse; therefore it wasn't possible to verify their SSO authentication. And while OPL also has Zinio, it wasn't accessible through SSO. According to OPL, Zinio doesn't offer SSO with EZproxy at this time, but they will by the end of 2014.

Calgary Public Library & CAS SSO

While SirsiDynix states that their Enterprise/Portfolio 4.2.1 discovery products include CAS SSO (SirsiDynix, 2013), CPL, who uses Enterprise, actually doesn't offer SSO like OPL at this time. It was found that CPL will be upgrading their discovery tool and implementing eResource Central (eRC), an electronic resource management solution from SirsiDynix. Through partnerships with OverDrive, Recorded Books and EBSCO eBooks, among others, eRC enables electronic resources to be integrated into the catalogue discovery layer, allowing users to access *most* resources through SSO. CPL is currently preparing their test environment and can provide us with more information by the end of May 2014.

Conclusion

BiblioCommons Advanced SSO is the best solution for EPL at this time. As demonstrated by OPL, with BiblioCommons Advanced SSO, customers would be able to access My EPL, check out an eBook from OverDrive and register for events, only having to enter their library card number and password once during their session. This provides a more convenient, integrated and streamlined mode of access, greatly improving the customer's digital discovery experience.

epl EDMONTON PUBLIC LIBRARY

Spread the words.

References

API (Application Programming Interface). (2014). In *TechTerms*. Retrieved March 12, 2014 from http://www.techterms.com/definition/api

Canonical Name (CNAME). (2014). In *Techopedia*. Retrieved March 12, 2014 from http://www.techopedia.com/definition/1321/canonical-name-cname

CNAME (Canonical Name). (2014). In *Webopedia*. Retrieved March 12, 2014 from http://www.webopedia.com/TERM/C/CNAME.html

Drupal. (2006). *CAS*. Retrieved March 10, 2014 from https://drupal.org/project/cas

Drupal. (2014). *Central Authentication Service*. Retrieved March 10, 2014 from https://drupal.org/node/1084302

Ingham, A., & MacIver, D. (2012). Using ESPREeSSO to Streamline SSO Access. *The Serials Librarian, 62*,196-199. DOI:0.1080/0361526X.2012.652932

Internet2. (2014). *Shibboleth*. Retrieved February 27, 2014 from http://www.internet2.edu/products-services/trust-identity-middleware/shibboleth/

Jasig. (2009). *Central Authentication Service (CAS)*. Retrieved March 6, 2014 from http://www.jasig.org/cas

Jasig. (2010). *Central Authentication Service (CAS)* [Brochure PDF]. Retrieved March 6, 2014 from http://www.jasig.org/cas

Lascarides, Michael. (2012). *Next-Gen Library Redesign*. Retrieved from Google Books.

OCLC. (2013). *EZproxy for authenticated access to you library's e-content* [Fact Sheet PDF]. Retrieved February 7, 2014 from http://www.oclc.org/ezproxy.en.html

Open Group, The. (2010). *Single Sign-On*. Retrieved January 17, 2014 from http://www.opengroup.org/security/sso/

SirsiDynix. (2013). *SirsiDynix Newsroom: Post-Search Sorting and "Text it to me"*
Added to Enterprise/Portfolio 4.2.1 [2012]. Retrieved March 12, 2014 from
http://www.sirsidynix.com/press/post-search-sorting-and-text-it-to-me-added-
to-enterpriseportfolio-421

SSL (Secure Sockets Layer). (2014). In *TechTerms*. Retrieved March 12, 2014 from
http://www.techterms.com/definition/ssl

Urban Libraries Council. (n.d.). *One-Stop Login (Single Sign On) for Library Online*
Services [2012 Top Innovator, Ottawa Public Library]. Retrieved February 26,
2014 from http://www.urbanlibraries.org/one-stop-login--single-sign-on--for-
library-online-services-innovation-88.php?page_id=38

Appendix I: Other SSO Options

Shibboleth

- Shibboleth is a "standards-based, open-source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner" (Internet2, 2014).

- It began as an Internet2 Middleware activity in 2000 and later partnered with the OASIS Security Assertion Markup Language (SAML) Working Group. SALM is an XML-based protocol used for exchanging authentication and authorized data between an identity provider and a service provider.

CAS

- CAS (central authentication service) was originally developed by Yale University to provide a centralized and convenient log-in experience (Jasig, 2009). CAS "is written purely in Java and does not rely on the features of specific application containers," allowing it to be "portable across many server environments" (Jasig, 2010).

- Since 2004, CAS has been managed by Jasig, "a non-profit consortium of educational institutions and commercial affiliates that sponsors open source software projects for higher education," and CAS "has quickly become the most popular single sign-on solution for universities" (Jasig, 2010; Drupal, 2006).

- Platforms with available CAS client software include Drupal (which also supports CAS out-of-the-box) and SirsiDynix Enterprise/Portfolio 4.2.1 (Jasig, 2010; SirsiDynix, 2013).

- Drupal allows SSO with CAS using phpCAS library: "In its most simple use (CAS can also proxy single sign-on), CAS authenticates users and sends the user to the requested application with a ticket. The application is then responsible for authenticating the ticket (behind the scenes, with a tool like cURL), and automatically logging the user in if the ticket is valid" (Drupal, 2006).

- The CAS module relies on third party library phpCAS, which has to be installed and configured, as well as on a working CAS server.