

INFORMATION STANDARDS QUARTERLY

FALL 2014 | VOL 26 | ISSUE 3 | ISSN 1041-0031

ISQ

TOPIC

IDENTITY MANAGEMENT

PRIVACY BY DESIGN
AND THE ONLINE LIBRARY

FROM THE LIBRARY OF CONGRESS
TO THE LIBRARY OF ME

THE INTENTION PUBLISHING ECONOMY:
WHEN PATRONS TAKE CHARGE

A JSON-BASED IDENTITY
PROTOCOL SUITE





Don
Hamparian

From the Library of Congress to the Library of Me

DON HAMPARIAN

OCLC is a worldwide library membership organization that helps libraries work together to connect people and information more efficiently. Founded in 1967 by a small group of library leaders, this non-profit cooperative now consists of thousands of libraries across the globe who actively participate in finding practical solutions for reducing information costs. OCLC's diverse library membership also works to explore trends that shape the future of libraries; to share data, work, and resources; and to magnify the impact of libraries worldwide.

Researchers, students, and other information seekers use our services to obtain abstracts and bibliographic and full-text information. OCLC and its member libraries cooperatively produce and maintain WorldCat®, the world's largest library catalog.

OCLC offers a host of bibliographic services for management and discovery of library collections. Many of our services are hosted at OCLC data centers for our institutions.

The focus of this article is OCLC's Identity Management services and vision and their place in the evolving role of OCLC services in the library community.

The Evolving Role of OCLC Services in the Library Community

Over the years, OCLC's services have been evolving in a variety of ways. A significant part of this evolution is the increasing involvement of the library patron and community as direct users of our services. Today, many of our services include patron self-service functionality, which involves a much larger community of users than even a few years ago. This evolution parallels the library's increasing role as a community hub—a non-partisan place to gather, meet, and exchange ideas and information. OCLC provides services that recognize this community-focused role of libraries. Our Identity Management infrastructure must keep up with this direction.

OCLC's Position of Trust in the Library Community

OCLC is a member-funded and member-governed not-for-profit organization. As such, we are uniquely positioned in the library community to provide identity services and to protect user information consistent with libraries' expectations. OCLC does not resell library user data or have a business model that depends on licensing or sharing this data.

As the range and reach of our services has grown, so has the emphasis on protecting users' privacy. This is a core ethic in the library community: the stewardship of user-related information that allows users to consume library services knowing that their privacy is respected and protected.

E-Content: Discovery to Delivery and OCLC's Vision of Identity Management

One of the primary use cases involving library users is the "Discovery to Delivery" workflow. In years past, this workflow involved searching the card catalog at the library and finding a book on the shelf or working with library staff to request the book from another library. Today, this workflow is handled mostly on users' computing devices and involves discovering an item via a variety of discovery websites (including the local library, OCLC, and many others) and then requesting the item for delivery. A large proportion of the "delivered" items are e-content objects from various publishers and aggregators. Delivering e-content has spawned a variety of tools and infrastructure, including link resolvers, federations, and groups; access and proxy software; and a myriad of administration screens for library staff to enter access information.

This process is frustrating for both library staff who manage the infrastructure and for the end users who can't easily access the materials they want. There are many steps, screens, challenges for credentials, and opportunities for something to go wrong. Usually, the authentication and authorization process uses IP address authentication, which is perceived as easy to administer but has a variety of security and usage limitations.

Related to the areas of access control and identity management, the predominant route to remote access of licensed e-content is through proxy servers. OCLC's EZproxy is one of the leading proxy servers used for this purpose.

Once all the administration and configuration is done, this environment works effectively. However, it still has some limitations, especially with broadband video and e-book borrowing management. Proxying increases network bandwidth consumption and often cannot provide the content provider with sufficient identity information to completely automate the workflow (such as for e-book borrowing).



We run our Identity Management infrastructure in four data centers across the globe in order to segregate our identity data by region. Our data loading, reporting, and management processes are built to maintain this data segregation.

CONTINUED »



We believe we can help libraries take the next step by building virtual communities relevant to the populations they serve.

OCLC's Identity Management Infrastructure and Vision

OCLC's infrastructure is a Shibboleth-compliant facility that provides unique Identity Providers (IdP) for every institution that consumes our WorldShare services. To date, we have configured about 23,000 IdPs for our institutions. We also provide interoperability with external, non-OCLC service providers and support institutions that wish to use their own IdP instead of OCLC's.

We run our Identity Management infrastructure in four data centers across the globe in order to segregate our identity data by region. Our data loading, reporting, and management processes are built to maintain this data segregation.

Our vision for Identity Management is to "lower the barrier of access to content and services while protecting licensed content and user privacy." We are accomplishing this vision by implementing the following:

1 A standards-based interoperable infrastructure

Our infrastructure is natively a SAML 2.0 infrastructure with interoperability support with existing Shibboleth-based federations. Today we support operating with external institution-based Identity Provider and Service Provider components. We also support SAML 2.0 compliant Central Authentication Service (CAS) Identity Providers and can access institution LDAP or Active Directory servers as an alternative user/password database to our own.

2 Single sign-on between OCLC services and institution facilities

Our infrastructure supports single sign-on with CAS and Shibboleth components. We also provide this support with our integration with LDAP and Active Directory since

Service Providers see a standard Shibboleth Identity Provider with our integration.

3 Integration points between e-content management and access control

This area remains to be significantly built out. Today, we integrate with EZproxy and OCLC's discovery services, but need to expand this integration to e-content providers and aggregators. This area will be our focus in the next few years.

4 Identity management infrastructure for libraries who don't have the technical expertise to build it themselves

As noted, we have provisioned approximately 23,000 Identity Providers as part of our initial institution activation work. These Identity Providers are used for providing access to a variety of our services. By default, these Identity Providers start with identities defined for library staff. When a library uses WorldShare Circulation services, we also load all patron identities into our system unless the institution is using their own Identity Provider. We are considering offering other services to populate the Identity provider so that institutions can use them with both OCLC and non-OCLC service providers.

5 A global solution compliant with regional laws and library expectations of privacy

We have to accommodate expectations of privacy from both legal and library perspectives. In both of these cases, the expectation and requirements of privacy vary by region. In the case of library expectations of privacy, these expectations can also vary by the type of library (for example, public, academic, school). Our implementation is built to provide strict segregation and protection of data by region and institution.

Solving the E-Content Access Problem

Solving the e-content access problem requires a reduction in the management/administration overhead required to provide access, the development of a standard method to provide appropriate identity data to e-content providers, and a reduction in the number of login challenges and authentication credentials the user needs to enter or remember. We believe that using a SAML-based infrastructure, such as Shibboleth, is a leading way to reduce our dependence on IP proxying and to provide true interoperability between libraries, content providers, and identity providers (such as OCLC). However, technology is only part of this solution. There are legal, cultural, and regional challenges to solving this problem. Also, we need to provide a solution for both browser and non-browser (mobile application) environments.

Using Identity Management to Build the Library Community

Libraries are natural organizations to build region-based communities. They are already popular gathering spots for people in the community and provide a non-partisan setting for community groups to gather. We believe we can help libraries take the next step by building virtual communities relevant to the populations they serve. In order to do this, Identity Management services can be used to determine that the community members are in fact affiliated with the library or the local region. This is a logical extension to the Identity Management services that OCLC provides.

Conclusion

Identity Management infrastructure has grown and evolved so far that the next generation of e-content access can be defined and implemented. The technology is mature and in wide use in academic institutions. Our remaining technical challenge is providing hosted and deployed solutions that are practical for smaller academic institutions and public libraries that don't have the technical support that larger academic institutions have. It is vital that our solution extends across all library types and sizes and can be easily implemented by both small and large content providers.

Technology is only part of the solution. No one organization will be able to completely solve the e-content access problem. We also have to continue to build the partnerships and trust between the institutions, identity providers, and content providers. Importantly, we have to

Libraries are natural organizations to build region-based communities. They are already popular gathering spots for people in the community and provide a non-partisan setting for community groups to gather.

extend this trust and technical services to public libraries and smaller academic institutions. These institutions don't have the legal and technical support required to participate in today's Identity Federations.

Is a SAML-based infrastructure a cost-effective and easier to manage alternative to IP authentication, proxy, and multiple sets of credentials required to access e-content? We know that a SAML-based identity management infrastructure will provide more flexible and granular access to content, the ability to implement additional e-content based borrowing services, and allow widespread use of broadband content. Our challenge is to provide a set of affordable solutions that can be implemented by all ranges of libraries, institutions, and content providers. We believe our community is ready to meet that challenge.

|| IP | doi:10.3789/isqv26no3.2014.03

DON HAMPARIAN (hamparid@oclc.org) is Sr. Product Manager Identity Management at OCLC.

OCLC

<http://www.oclc.org/>

EZproxy

<http://www.oclc.org/en-US/ezproxy.html>

Security Assertion Markup Language (SAML) v2.0

<https://www.oasis-open.org/standards#samlv2.0>

Shibboleth

<http://shibboleth.net/>

WorldCat

<http://www.oclc.org/en-US/worldcat.html>

WorldShare

<http://www.oclc.org/en-US/worldshare.html>



RELEVANT
LINKS