InCommon®

www.incommon.org
incommon-info@incommon.org

Libraries Combine to Develop Shibboleth-EZproxy Hybrid

Combination means a move away from IP authentication; provides greater control

Libraries face one of the most complex situations on campus, when it comes to providing access to protected resources. They typically work with a large number of vendors and have a variety of user situations to accommodate.

That's why several college and university IT professionals came together in the InCommon Library Collaboration. The goals included:

- Moving away from IP-based authentication.
- Leveraging the main campus identity infrastructure.
- Gaining fine-grain control over access to accommodate users with different levels of access or access to different materials.
- Encouraging as many vendors as possible to participate in single sign-on, providing increased security and an improved user experience.

The Problem

Libraries subscribe to dozens of online journals and databases and work with many different resource providers. Many vendors have preferred making authorization decisions based on the IP addresses from which the request originates. This makes remote access difficult, given that a user at home or at a coffee shop will not be connecting from an IP addresses controlled by the institution.

The situation is made more complex because many libraries provide services to patrons that are not part of the campus community (and, thus, not part of the identity management infrastructure). For instance:

- The catalog may be open to all who enter the building.
- Specialized databases may be open to anyone physically in the library.
- Databases may be open to those with university credentials regardless of their physical location.
- Some resources may be open only to students and faculty in a certain field (such as the law school or medical school).

The Solution

The collaboration group developed a hybrid of two popular software packages: Shibboleth and EZproxy.

Shibboleth (developed by the Internet2 Middleware Initiative) is the SAML-based, open-source federating and single sign-on software. Shibboleth is adept at managing the interaction between the library, the campus identity system and the resource provider (or vendor).

EZproxy (a product of OCLC) is middleware that authenticates library users and provides remote access to licensed content. EZproxy is widely deployed among libraries, but does not offer the fine-grain access control that can be achieved using Shibboleth to leverage the campus identity system.

This hybrid solution offers benefits to:

Users – providing single sign-on convenience.

Librarians – reducing expenses and support needs, with far less IP and proxy maintenance. It also permits the use of additional federated resources while keeping the user experience consistent.

Library administration – making central usage statistics available.

Vendors – eliminating the need to maintain IDs and passwords, since Shibboleth leverages the university's identity management system, provides the necessary authentication, and allows for quick breach investigation.

Other Resources

The collaboration group also developed a number of helpful documents, including use cases, best practices for service providers and libraries, and short case studies from campuses outlining their experiences with the hybrid. Members have also made numerous presentations and conducted an informative webinar on their work (see www.incommon.org).

The group also approached a number of library resource providers, focusing on those with membership in the federation in the United Kingdom, but not InCommon. Several have joined InCommon as a result of these efforts. As a side benefit, other collaboration groups could mirror this approach to encouraging service providers to join the federation.

You can read more about InCommon on the back of this page. Visit www.incommon.org.

InCommon®

What is the InCommon Federation?

Providing a framework of trust for the safe sharing of online resources

What is InCommon?

Increasingly, far-flung faculty members, universities and service providers work together online. Collaboration groups require user IDs and passwords for their protected online resources. As passwords proliferate, users fill notebooks or add more and more sticky notes around their computer monitors to remember which credentials go with which resource. Security and intellectual property nightmares ensue.

As off-campus resource accounts proliferate, so does personal identity data, which is retained by a multitude of service partners, increasing the likelihood of data spills and misuse that cannot be controlled by campus policies. Furthermore, service providers are forced to provision and maintain large user account systems instead of focusing on their real mission: providing online resources.

InCommon eliminates this need for multiple, password-protected accounts and simplifies access for the end user, minimizing support calls for everyone. Online service providers no longer need to maintain their own databases of identity information for access control.

And best of all, federated access scales. Once an institution or higher-education partner is a participating member, setting up a new relationship can take as little as a few minutes.

How Does it Work?

InCommon's value is based on federated identity management. A user of a resource clicks on a service partner's resource. Once the user is authenticated by his or her home institution, the campus infrastructure releases only enough identity data to allow the service partner to make an access decision.

The user's institution takes responsibility for authentication and controls the release of personal information. The service partner uses the minimal identity information to control access to its resources. End users simply use their campus user ID and password to access off-campus online resources.

InCommon's role in this is simple: It provides a framework of shared policies, trust-establishing processes, and technology standards for universities and service partners to follow. This greatly streamlines collaboration with multiple organizations. For example, institutions and service providers could spend time establishing operating principles, technology hooks, and agreed-upon data exchange elements with each partner, or they could do it once by joining InCommon and then leveraging these common elements for many relationships.

InCommon Benefits

- InCommon supports Web-based distributed authentication and authorization services, such as controlled access to protected content resources.
- Participants exchange information in a standardized format, reducing or removing the need to repeat integration work for each new resource.
- Access decisions and user privacy controls are decided on a case by case basis for each resource, providing higher security and more granular control.
- Institutions experience reduced account management overhead by eliminating the need for separate accounts to access particular resources.
- Campus and company IT professionals provide protected content to multiple organizations using a single authentication framework.
- The home institution controls when an identity is disclosed, and how much information is revealed.

Who can join InCommon?

Any accredited two-and four-year higher education institution can join InCommon. Additionally, higher education participants can sponsor their online service providers that make resources available to individuals or groups. For more information, and a list of participants, see www.incommon.org.

2010-10-INC-LIIBRARY