

Smooth Sailing for Library Services Through InCommon

Moss Landing, ScienceDirect plumb the depths of federating.

 ScienceDirect, a service of Elsevier, provides full-text and bibliographic information to the world's science, technology, and medical communities.



Moss Landing Marine Laboratories, located on Monterey Bay, provides a Masters of marine science program for a consortium of seven California State University campuses.

The Problem

Moss Landing's students, faculty, and researchers roam the world, from Antarctica to Alaska, and from Chile to the Caribbean. But their lives don't stop while they conduct their studies. Writing and publishing – articles and Masters theses and book chapters – require reference works and journals that just aren't available on the coast of Bimini. With one librarian, plus one FTE position split among several graduate students, managing multiple digital resources can become a whale of a burden.

"The bottom line is that users were demanding remote access to library resources," says Joan Parker, librarian at Moss Landing. "Because all of our resources were IP-authenticated, remote access did not work."

Moss Landing researchers make heavy use of ScienceDirect, which offers a treasure trove of electronic resources. With contracts in place at more than 80 percent of the colleges and universities in the world, the service needs an identity and access management solution that can scale.

"IP-based access is fundamentally simple in that it is generally tied to a physical location – but that's also its limitation," said Ale de Vries, senior product manager at ScienceDirect and Scopus. "It also provides our company with maintenance overhead and causes some security concerns."

The Solution

At the same time Parker was fishing for a solution, the Cal State Chancellor's office began ramping up their use of Shibboleth® Single Sign-on and Federating

Software in preparation to federate some system-wide applications through InCommon.

With InCommon, individuals can use their university-issued credentials for access to ScienceDirect and scores of other federated services. Service providers can leverage an existing identity management system, rather than create a separate user database.

"I was looking for a remote-access solution and the Chancellor's office was looking for a test case," Parker said. "The Chancellor's office came through with the Shibboleth implementation and, as it turns out, even hosting Moss Landing's identity system."

"I rarely hear from users, which means this is a raging success. Users have something they did not have before and it is easy for them to use."

- Joan Parker, Moss Landing Librarian

ScienceDirect knows the advantages of single sign-on. "Managing access to resources has scalability challenges," de Vries says. "We have to generate and maintain user IDs, have a registration process, and have a help service for those who forget their IDs and passwords – on top of managing IP address ranges. Federated authentication replaces technologies that are more cumbersome, more complex, and less secure."

The Result

"I rarely hear from users, which means this is a raging success," Parker says. "Users have something they did not have before and it is easy for them to use. And it doesn't chew into staff resources. Now my frustration is that many major publishers have been slow to federate."

When she does hear from users, it typically takes little time to set things right. "I was in Italy last fall and one of my researchers was in Chile," Parker said. "He was having authentication problems and I could solve it on the spot."

ScienceDirect has a growing number of U.S. customers migrating to federated use of the service. There is an increasing interest in the library community to provide single sign-on support, as database offerings (and the potential for the proliferation of user IDs and passwords) continue to expand.

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.