

Federation Not Small Stuff for Small Colleges

Lafayette federates several applications; Carleton on the way.

The benefits of federation are not limited to research universities with large IT staffs. Using InCommon and federating software, small colleges can also extend their reach and the services they provide.

LAFAYETTE Lafayette College has several federated applications, allowing for both on- and off-campus access to protected resources, including library applications JSTOR and RefWorks, the open-source course management system Moodle, an internally developed DHCP application, and University Tickets.

Carleton College Carleton College has federated a career services application from Symplicity and is looking at federating with a library database vendor and an emergency services provider.

The Problem

Lafayette continues to add online services at the behest of stakeholders, including the library, as well as faculty wishing to collaborate with their colleagues from other institutions. Providing additional services, however, could lead to a proliferation of user IDs and passwords. John O’Keefe, Lafayette’s director of academic technology and network services, also wanted an uncomplicated way to provide off-campus access to services, using single sign-on technology.

Carleton College faced a similar situation when considering NACELink, a career services resource from Symplicity, as well as other online resources. Joel Cooper, director of information technology services, says, “We have other systems where students have silo passwords and there are multiple resources that require new credentials.” Cooper wanted to continue to provide access to multiple protected resources without growing the number of IDs and passwords that users need to maintain.

The Solution

Lafayette used its InCommon membership and Shibboleth® Single Sign-on and Federating Software to provide access to protected resources. With this solution, the college was able to offer single sign-on convenience for its users and provide off-campus access to third-party applications. In the case of

Moodle, this solution also allows access for appropriate outside users.

InCommon membership allowed Carleton to federate career services resource NACELink. “Our IT staff member was looking for a career services resource compatible with our architecture and he had installed Shibboleth,” Cooper said. “NACELink had all of the tools the career center wanted.”

The Result

Lafayette’s O’Keefe said, “[Shibboleth] has become our de-facto application to solve authentication issues with third-party apps, as well as internally hosted apps. Everyone is pleased that campus network IDs can be used to access more resources.”

At Carleton, federating NACELink has simplified things for users — college IDs provide access to the resource. This success has caused Carleton to consider federating other protected resources. “We’re actively looking at others, particularly library resources,” Cooper said. “We are looking to use Shib for internal web authorization, as well.”

"InCommon provides a way for us to expand our services through third-party providers, rather than use valuable and scarce staff resources to add or maintain services."

*Joel Cooper,
Carleton College*

Cooper also said that federating can help a college or university strategically outsource services without consuming scarce resources.

"InCommon provides a way for us to expand our services through third-party providers, rather than use valuable and scarce staff resources to add or maintain services. Federating enables outsourcing while making it secure and transparent for our users. We can take advantage of services and applications that already exist, without having to worry about managing a different set of user accounts."

About InCommon

You can read more about InCommon on the back of this page and at www.incommonfederation.org.

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.incommonfederation.org.

10/10/2008