Making the Grade with InCommon

WebAssign gives the Federation high marks.

Penn State and Symplicity

symplicity Symplicity provides software applications to manage many facets of college recruiting, from career fairs to on-campus interviewing. The company works with 600 institutions providing an end-to-end career service management suite.

PennState Pennsylvania State University has thousands of students using career services at any given time. With 24 locations across the Commonwealth of Pennsylvania, the sheer size and complexity of offering quality, unified services can be daunting.

The Problem

Rather than develop its own system for on-line job posting and on-campus interviewing, Penn State conducted an extensive review of various vendors. The university chose Symplicity and used the company's software for a year.

During that year, every student received a user name and password – separate from their existing Penn State ID and password – to access the career services system.

"Our office was constantly getting phone calls from students who couldn't log in to Symplicity," said Larry Kolbe, a programmer/analyst with Penn State's career services office. "We wanted to eliminate the assignment of yet another user name and password to students."

The Solution

Penn State was already an InCommon participant, using the federated identity management for other campus applications. "We were asked to investigate and implement a way to integrate access to Symplicity's system with Penn State's log-in," Kolbe said. "Because Symplicity did not, at that time, work with Shibboleth®, we worked closely with their developers to make this happen."

"Penn State approached us about a federated single sign-on system, so we Shib-enabled our applications because of them," said Symplicity's Brent Franks. "Since then, we have started working with the University of Maryland-Baltimore County toward using InCommon and have just opened talks with NYU."

Franks said this is part of a process he has seen with other institutions. "A typical scenario is that a school will deploy Symplicity software and, after it has been up and running, begin discussion of a federated single sign-on system."

The Result

For Penn State, the result has been a streamlined authentication and authorization system. "For the year that we used Symplicity prior to implementing this solution, we were constantly fielding phone calls from students," Kolbe said. "The office no longer receives these types of calls, which has resulted in significant savings in staff time."

> *"The result (of using InCommon's federated identity management) has streamlined the authentication/authorization system for Penn State students while protecting their privacy."*
>
> *—Larry Kolbe, Penn State Career Services*

As a service provider, Franks said it all comes down to customer satisfaction.

"Ultimately it comes down to helping us drive sales or make our customers happier," he said. "InCommon and Shibboleth provide a good SSO solution and makes it much easier for students to use our software."

About InCommon

You can read more about InCommon on the back of this page. InCommon is operated by Internet2 and managed by an independent steering committee representing the higher education and research community. For more information visit 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.