Making the Grade with InCommon

WebAssign gives the Federation high marks.

WebAssign operates a homework delivery system that has become increasingly popular with professors around the country. By harnessing the power of the Internet, WebAssign provides faculty members with the tools to create assignments from a database of textbook questions, or write and customize their own exercises. Instructors enjoy a streamlined system for making homework assignments, communicating due dates and providing feedback to students.

The Problem

WebAssign typically works with individual professors, not with university IT departments. Professors can sign up for their own WebAssign accounts and begin using the service almost immediately. As a result, the company could have hundreds of accounts on a single campus, with no coordination of information.

In addition, the individual faculty member has responsibility for entering and updating roster information as students drop and add classes.

“The primary problem was how to enter student and roster information, including passwords, and then disseminate that information,” said Brian Marks, chief technology officer at WebAssign. “What was needed was a secure, standard method of sharing such information with an external entity in a trusted way.”

The Solution

WebAssign joined InCommon as a service provider and installed Shibboleth federating software. This allowed WebAssign to stop managing user accounts and focus, instead, on the company’s applications.

“The solution to sharing the information ended up being the integration of Shibboleth and InCommon with WebAssign,” Marks said.

“The role of InCommon was to provide the trust layer so that institutions would feel comfortable sharing student information with us,” Marks said.

That trust layer results from InCommon’s federated approach, in which organizations agree on a set of privacy-preserving user attributes, technologies, processes and policies to exchange selected user information. Users receive single sign on convenience, using the user ID and password from their home institution.

The Result

WebAssign’s InCommon university partners no longer need to upload and update rosters and other information. Students and faculty members also have Single SignOn convenience.

For example, **Penn State’s** physics department help desk saw a 70 percent drop in calls once the university installed federating software. Those calls had little to do with physics help and everything to do with forgotten passwords.

WebAssign has also seen measurable benefits from their InCommon participation, including customer confidence with the online experience.

“A primary benefit of being a member of InCommon is that the trust mechanism is already in place when another institution expresses interest in integrating their class rosters,” Marks said.

> *“The role of InCommon was to provide the trust layer so that institutions would feel comfortable sharing student information with us.”*
>
> *—Brian Marks, WebAssign*

This scalability means that WebAssign and Penn State can interact with many more organizations, using multiple applications, with relative ease.

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 http://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.