

CSUconnect, 23 Campuses Adopt InCommon

Federation provides inexpensive and scalable technology model

The California State University (CSU) is the largest university system in the US, with 23 campuses, 437,000 students and 44,000 faculty and staff. The CSU awards more than half of the state's bachelor's degrees and one-third of the master's degrees, educating approximately 60 percent of California's teachers.

The Problem



The California State University system is a

large, complex organization with a mix of centralized, decentralized, and externally managed technology services in production across its 23 campuses. The ITS leadership of the CSU, responsible for system-wide direction, identified a need to improve access to this diverse application portfolio. This portfolio includes protected system-wide applications and local campus applications that have users from different campuses. Examples include PeopleSoft ERP modules, campus visitor access to the Chancellor's Office wireless network, system-wide reporting applications, and system-wide faculty collaboration applications.

The Chancellor's Office faced the considerable task of identifying a solution to coordinate the authentication to these applications with a potential constituency of several million users managed in 23 separate campus enterprise directories. The goal was to leverage this existing campus infrastructure to provide simplified access to many applications regardless of the service provider and the service's hosted location.

"We needed to find a way to take advantage of existing campus resources, keep the cost reasonable, and avoid forklift upgrades (requiring a large investment or upgrades of hundreds or thousands of individual machines)," according to Michael Trullinger, associate director of identity management at the CSU Chancellor's Office.

The Solution

The CSU selected a solution that would allow each campus to continue operating its own identity management system and maintain control of its own privacy and security obligations. Each CSU campus has joined both the InCommon Federation and the system-run CSUconnect Federation.

In a federation, identity providers and service providers agree to a set of common policies, practices and identity data standards. When combined with a product like Shibboleth Federated Single Sign-On Software, users can access protected resources with their campus credentials.

The CSUconnect Federation provides for single sign-on access to CSU system-wide resources, while giving campuses the ability to access a wide range of contracted resources from the list of InCommon sponsored participants.

"We believe that a federated approach will provide a lightweight, inexpensive, and scalable technology model compared to other options available."

Michael Trullinger,
California State University

The Result

"We had an early success with federated access to library resources by faculty and graduate researchers affiliated of the CSU's Moss Landing Marine Lab," said Mark Crase, senior director for strategic initiatives and planning at the CSU system's information technology services office. "Now we have some system-wide applications driving adoption and we're seeing much more interest from the campuses."

Crase said that, this summer, the CSU will federate its new common financial system and related data warehouse, as well as the Microsoft SharePoint collaboration environment.

"This improves access to some of our existing applications, opens up new opportunities for faculty and students to collaborate across traditional campus boundaries, prepares the CSU campuses to offer shared application services, enables cross-campus access to educational materials, and eases integration with external partners," said Trullinger. "It is becoming increasingly clear to folks why this is necessary. This is about doing business in a different, more effective and efficient way."

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 the number of off-campus resource accounts grows, 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- or four-year higher education institution can join InCommon. 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.