Foundations for a Federation
UCTrust builds its system-wide federation on top of InCommon.

UCTrust is a federation providing access to resources for member-campuses of the University of California system. Six of the 10 UC campuses belong to UCTrust, taking advantage of business service applications. All UC locations are expected to join UCTrust by the end of 2008.

The Problem
With ten campuses, plus five medical centers and three national research laboratories, the University of California has more than 375,000 computer users that could take advantage of self-service applications, saving the university time and money.

However, those users will also need access to resources on their own campuses as well as outside resources like library databases or services offered specifically to students. Each campus may have a license to access different resources, or they may form consortia to share such resources.

The main problem, then, is to develop a way for a user to access the appropriate applications and resources – whether those come from the central UC system office, the individual campus or from a third party. And this needs to include single sign-on convenience.

The Solution
The University of California system has created UCTrust, a federation serving just UC campuses and related entities. UCTrust is built on InCommon – essentially one federation built on top of another. This allows the UC campuses to take advantage of InCommon's existing trust arrangements and operational infrastructure. Six UC campuses, along with the UC Office of the President, now belong to UCTrust and InCommon, providing single sign-on convenience for users, access to intra-university resources, and to the external resources of a federation of more than 60 identity providers and service providers..

"InCommon provides the tasks related to federation and UCTrust offers a level of assurance appropriate to UC's federated services," said David Walker, Director of Advanced Technology. "So far, we have focused on applications we offer centrally. Since most applications are hosted at our campuses, however, we anticipate our greatest future growth with intercampus collaborations that are not necessarily system-wide."

The UCTrust framework offers a level of assurance equivalent to National Institute of Standards and Technology (NIST) Level 2 through a rigorous set of policies governing participants' identity management.

"We know that when the federal government starts offering services, people will want to use them," Walker explained. "This high level of assurance means we are ready to go."

The Result
Six of the 10 UC campuses take advantage of federated access to a growing number of services:

- At Your Service Online (AYSO), a self-service application that allows employees to update personal information, access W-2 information and view benefit and tax information.
- UC Grid, the platform for UC's federated cyberinfrastructure.
- The Effort Reporting System, used in conjunction with research grants and contracts.
- A training management system is coming soon to operate mandatory employee training programs.
- Also coming soon, a travel portal that will allow university employees to gather travel information and to book their own arrangements.

Walker appreciates the flexibility provided by InCommon. "A campus can do what's good for that campus," he said, but still have the option to take advantage of outside resources made available through UCTrust. Because campuses are members of both UCTrust and InCommon, they can take advantage of services from both federations."

The UC system relies on InCommon to operate the underlying federation infrastructure for them. InCommon manages the registration and maintenance of the necessary information about each participating organization. This applies to all manner of collaborations, whether from university to university within the same system or from university to its many service partners — arrangements that may have completely different privacy and access constraints.

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.

10/2/2007