www.incommon.org
incommon-admin@incommonfederation.org

InCommon Provides Platform for National Student Clearinghouse

Stanford, Clearinghouse federate Student Self-Service application

Since 1993, the National Student Clearinghouse (www.studentclearinghouse.org) has been a non-profit education partner to the nation's colleges and universities, providing them with critical educational reporting, verification and research services.

Stanford University (www.stanford.edu), founded in 1891 and located between San Francisco and San Jose, is recognized as one of the world's leading research and teaching institutions.

The Problem

Since 2000, the Clearinghouse has provided colleges and universities with its free Web-based Student Self-Service application. The application provides many useful options for students, including printing enrollment verification certificates, ordering transcripts (if their school offers this option), viewing enrollment history and verifications provided by the Clearinghouse on behalf of the school, and other features.

Given the sensitive nature of this information, maintaining and improving security is of vital importance to the student, the Clearinghouse, and the college or university. The Clearinghouse originally developed a custom authentication mechanism, which requires work by the institution to integrate with existing authentication methods and portals.

Stanford was providing access to Student Self-Service through the Clearinghouse's custom authentication mechanism, something officials agreed was time-consuming, and began searching for a better authentication model. "We wanted to replace that with a standard mechanism already in use at Stanford and at peer institutions," said Bruce Vincent, chief IT architect and strategist at Stanford.

The Solution

Stanford favored using a federated approach, allowing the institution to leverage its membership in InCommon and use Shibboleth Single Sign-on and Federating software. This would allow Stanford to retain the role of the authentication authority, which provides security control and accountability.

The Clearinghouse was interested in a standards-based solution that improved security and did not involve creating a separate identity system. The Clearinghouse and Stanford saw that they could leverage their InCommon memberships to solve this problem.

As part of its overall focus on security, the Clearinghouse regularly seeks strategic partnerships with entities, like the inCommon Federation, which allows delivery of services to participating institutions using the latest standards in information security.

"The growing popularity of single sign-on, and the emergence of InCommon as a new standard for authentication, represents a winning combination for institutions seeking alternate ways to access Clearinghouse services," said Doug Falk, chief technology officer for the Clearinghouse.

"The InCommon platform enabled us to deploy a single sign-on option for Student Self-Service on a proven framework, which could easily be adopted later by other federation members that also participate in the Clearinghouse," noted Falk.

Stanford also worked with other universities, through the InCommon Student Collaboration Group, to define the common attributes that would be used with the Clearinghouse for the Student Self-Service pilot. These attributes are used to securely and privately pass information between the identity system and the service provider application. With these attributes now defined, other universities can more easily federate with the Clearinghouse.

The Result

The Clearinghouse and Stanford successfully completed their pilot early in the summer of 2009, and students began accessing Student Self-Service with their Stanford credentials.

"We were able to leverage our existing Shibboleth instance, and our membership in InCommon, to replace the custom authentication mechanism," according to Tom Black, Stanford's registrar. "The stakeholders are happy that another custom authentication system has been replaced with one of our standard services, and the change was transparent to students."

You can read more about InCommon on the back of this page. Visit www.incommon.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.

2010-04-CS-INC-NSC