InCommon . . . Now That's the Ticket

Lafayette provides students with SSO ticketing convenience.

universitytickets UniversityTickets provides simple, cost-effective ways for colleges and universities to sell tickets and collect payments online. The company provides comprehensive ticket services, as well as options to improve box office operations, ticket and merchandise sales, and event marketing.

LAFAYETTE Lafayette College, in Easton, Pennsylvania, enrolls more than 2,300 students in 45 academic fields. The undergraduate-only, academically competitive college was founded in 1826 and has an endowment of about $780 million.

The Problem

Lafayette sought to provide student-only tickets to campus events through an agreement with UniversityTickets. The Dean of Students office worked with the company, but ran up against the challenge of providing user IDs and passwords for all 2,300-plus students.

"I received a call from the dean's office wanting to know if we could provide access to our LDAP server to authenticate students for this service," said Bob Bailey, senior applications developer at Lafayette. "As you provide more access to your server, you increase the risk. If someone compromises another system, and you are linked to that system, you are compromised, too. We don't want our user IDs and passwords going through a third-party website."

The Solution

Lafayette had already found just the ticket for resolving the user ID and password issue with some of its other resource providers, including library applications and the Moodle course management system. The solution was to federate those applications through InCommon.

With InCommon, individuals can use their university-issued credentials for access to a number of services. Since identity providers do not send actual user IDs and passwords, user privacy is protected. Service providers can leverage an existing identity management system, rather than create a separate user database, simplifying the process for a user and minimizing concerns about security breaches and data spills.

Responding to that phone call from the Dean of Students, Bailey introduced his counterparts at UniversityTickets to the InCommon Federation, and Shibboleth Single Sign-On and federating software. "They had heard of Shibboleth, but had not tried it," Bailey said. "They also had an inquiry from another university to do the same thing."

"UniversityTickets has worked with many higher education clients to implement single sign-on integration with their ticketing systems," said UniversityTickets Vice President Gordon Capreol. "However, in the past, every SSO integration was a custom approach requiring new development and testing. In addition, previous SSO integrations were mixed in terms of the level of security they provided. We were impressed with InCommon's approach to providing a standardized mechanism for higher education clients to share authentication data in a very secure manner."

The Result

UniversityTickets joined InCommon and installed the Shibboleth service provider software. Now, through the federation, Lafayette verifies student identities. The student, with no unique user credentials to remember, gains immediate and convenient access to student-only benefits for campus athletic, performing arts and other events.

> *"We were impressed with InCommon's approach to providing a standardized mechanism for higher education clients to share authentication data in a very secure manner."*
>
> *—Gordon Capreol, UniversityTickets*

"We are getting more and more protective of IDs and passwords," Bailey explained. "By using Shibboleth and InCommon, you don't let any user IDs or passwords outside of your own servers. Once you have this set up, adding additional services is relatively simple."

"InCommon allows us to accomplish the business needs in the box office while, at the same time, satisfying the security and privacy concerns of our clients," said Capreol. "Just as important, InCommon provides a consistent, easy to replicate, and easy to maintain system for campus authentication."

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.incommon.org.

200909-CS-INC-UTix