InCommon®

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

InCommon Flies High With Student Verification Provider

University of Washington, StudentsOnly provide student discount services.

StudentsOnly provides automated student enrollment verification for companies that offer discounts to college students. The companion company, StudentUniverse, provides student discounts on travel.

Founded in 1861, the University of Washington is one of the oldest state-supported institutions of higher education on the West Coast and is one of the preeminent research universities in the world.

The Problem

Airlines, large retailers, computer manufacturers, restaurants and other merchants see student discounts as a way of building their businesses. For colleges and universities, such programs provide added value for students. But when you conduct business online, determining whether or not someone is a current student can be a befuddling and time-consuming process.

Enter StudentsOnly, which provides this service using a number of verification methods, from using university directory systems, to making phone calls to registrar offices, to having students submit proofs of enrollment manually. Many of these methods do not scale and some, like accessing university directories, raise security concerns at colleges and universities.

“We wanted to offer the discount travel program as a service for our students,” said Todd Mildon, registrar at the University of Washington. “But we did not want a third party accessing our directory and we did not want to generate many phone calls or visits to our office seeking student verification.”

“We have always known that working with universities is key for us,” said Bjorn Larsen, executive vice president at StudentsOnly. “But the methods for verification are very scattered. Some would allow us to hit their LDAP, but even that method means adapting from university to university. Some universities do not provide directory access and do not want calls from us, so the student has to email or fax us their documentation.”

The Solution

If StudentsOnly could rely on a single sign-on system, accepting students’ university credentials as verification, the process would soar. “Using federated single sign-on with Shibboleth is our preferred verification method,” Larsen said. “We just need an attribute confirming enrollment and the student’s first and last name to match our files.”

Using InCommon and Shibboleth Single Sign-On and Federating Software, the student signs in with college or university credentials. The home institution authenticates the student and passes the appropriate attributes to StudentsOnly, which does the authorization. No extra baggage. No delays at the gate. The student makes the online purchase and starts packing.

> *“InCommon is our preferred method for enrollment verification. The process scales and the work to build the infrastructure takes place just once.”*
>
> *—Bjorn Larsen*
> *StudentsOnly*

“We already had Shibboleth in place at the University of Washington,” Mildon said. “Once we had the contract and agreement in place with StudentsOnly, adding them as another service provider took just a few minutes. The students could start using the service the next day without any training or documentation.”

The Result

Students using a federated StudentsOnly find a streamlined process that is convenient and transparent to them. StudentsOnly does not have to negotiate a verification method with each new federated identity provider. Colleges and universities no longer have the security concern of providing access to databases and StudentsOnly does not store any information about the user. They simply compare it to the information already provided by the student.

“InCommon is our preferred method for enrollment verification,” Larsen said. “The process scales and the work to build the infrastructure takes place just once. Everything is database-driven here and it is very easy to add additional identity providers. As we move into other services, the federation will become even more valuable.”

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

InCommon®

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.

200907-CS-INC-StuOnly