

Microsoft Provides Students with a Sweet Suite

DreamSpark design and development tools available through InCommon.

DreamSpark™

What's not to like about free software?

Particularly when it includes professional developer tools from industry giant Microsoft? Microsoft has made its DreamSpark™ suite of software available to any college or university student in the world. Students can receive professional development and design tools at no cost. DreamSpark includes Visual Studio, Expression Studio, Windows Server and xna Game Studio.

For Microsoft, the program places key tools in the hands of young developers likely to create the next generation of applications. For students, particularly those in engineering, computer science, and other technology-driven curricula, essential software provided at no cost – well, it is better than free pizza for a month.

The key question in the process: how to verify student status in a low-cost and scalable way. The key answer turned out to be InCommon.

The Problem

Microsoft saw value in distributing developer software, free of charge, to college students. But with thousands and thousands of students eligible for free downloads, how would the company verify enrollment in a college or university? According to Microsoft's Scott Blackwell, "This program poses the problem of identifying students in a low-overhead fashion. Some existing [Microsoft] programs work through various academic channels, but don't have the scope or consistency needed for this program."

The Solution

For a solution, Microsoft turned to InCommon and, subsequently, other federations around the globe. Through InCommon and the use of privacy-preserving attributes, colleges and universities could verify enrollment without releasing personally identifying information about individuals. By using InCommon and attributes, Microsoft could leverage university identity management systems to determine whether a potential downloader is a student.

"We saw the emergence of global federations in higher education as a great opportunity to leverage campus

services for student-affiliation verification," Blackwell said. "We're committed to supporting federation in our own products, so it's a direction we want to promote. We worked first with our U.S. colleagues in InCommon, then with many others worldwide."

Rather than dealing with thousands of universities in the U.S. and abroad, Microsoft joined InCommon and 14 other federations, working through the policy and contract issues. The company worked with InCommon to determine which information would need to be exchanged, all the while looking to ensure a smooth and successful user experience.

"We saw the emergence of global federations in higher education as a great opportunity to leverage campus services for student-affiliation verification."

*Scott Blackwell,
Microsoft DreamSpark
Global Program
Manager*

The Result

Microsoft was pleased with the trust services and scalability provided by InCommon. According to Blackwell, "The success of this scheme depends on the scaling and assurance we get from working with national-level federations rather than individual campuses. We had a tremendous reaction when we launched the service. It has received a lot of attention within Microsoft and in higher education."

Microsoft has learned a lot through the process of joining and using InCommon, says Blackwell. "As seamless as the technology is, there are still lots of human relationships involved in providing a great service. Some of the technical elements are still evolving and we're working with the federations and campuses on improving practices for the next generation of the service."

About InCommon

You can read more about InCommon on the back of this page and at www.incommonfederation.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.

10/12/2008