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

iTunes U: Apple is InCommon-ly Good for Universities

Pilot program tests iTunes U protected access through InCommon.

Several universities and Apple have completed a successful pilot, using Shibboleth® Single Sign-on and Federating Software and the InCommon Federation, to provide federated access to iTunes U. A federated iTunes U provides universities with an ideal platform for offering online course content to students around the globe.

The goal of the pilot was to develop a standards-based, vendor-neutral approach to authenticate and authorize users of iTunes U. And leveraging a university's identity management system means only students enrolled in a specific course can access the materials.

Professors and students love iTunes U. Students can revisit a lecture and view other multi-media content made available by the professor. Professors record lectures and add related audio and video content to provide examples, background information or context for a course. Students can then listen or view the podcasts from a computer, iPod or iPhone.

Students sign on with their university ID, access iTunes U and go to school!

The Problem

iTunes U has proven to be a very good tool for students and faculty. Universities, however, needed a scalable solution for authentication and authorization, ensuring that only those registered for a course can gain access to materials distributed via iTunes U.

Apple provides a proprietary transfer script that allows students to authenticate with their university credentials; a script that released only the information needed to provide access. However, with more than 100 universities now members of InCommon – each potentially working with a number of service providers – the issue became one of scalability. How many vendor-specific implementations can one IT shop support?

Federating through InCommon and Shibboleth also provides an elegant solution for universities using iTunes U to provide online courses for their own students and for students from other universities.

As an example, in 2007, Penn State produced more than 3,500 podcasts for 300 courses, and that number grows every year. "We are seeing growth even without much of a marketing effort," says Renee Shuey of Penn State's information technology services. "That's why we knew we needed the scale that InCommon brings to the university community."

"The demand is growing," said Bill Corrigan of the University of Washington. "At this point, there are a lot of students expressing desire to get more course materials online."

This growth means that any solution has to scale.

The Solution

Apple and the universities agreed to operate a pilot program, using InCommon and Shibboleth, to federate iTunes U. The pilot developed a way to use the standard authentication and authorization process involved with Shibboleth and federated identity, rather than Apple's transfer script, for those universities that are members of InCommon.

> *"With iTunes U now supporting federated identity, we can now take next steps towards making this service the place for secure rich media digitally delivered for teaching and learning."*
>
> *Cole Camplese, Director of Educational Technology Services, Penn State University*

Through the use of the InCommon Federation, universities can use Shibboleth to authenticate their students, releasing only the necessary information to provide access to the course materials, and Apple will authorize access to the appropriate iTunes U content.

The Result

For those universities conducting the pilot, it is full steam ahead with federated iTunes U. The pilot reached its goal of successfully using InCommon and Shibboleth for the authentication and authorization of users for iTunes materials.

With this successful pilot complete, universities can now use their InCommon participation, and Shibboleth, to integrate with iTunes U.

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.

10/9/2008