

VIVA Virginia!

Library consortium offers access to PBS video resources through InCommon.



The Virtual Library of Virginia (VIVA) is a publicly supported consortium of libraries at more than 70 public and private non-profit higher education institutions in Virginia.

Members include research universities, liberal arts colleges, and two-year colleges. VIVA is guided by three fundamental principles: equitable access to information, cooperation across institutions, and cost-effective use of public resources.

In 2006 VIVA licensed the rights in perpetuity for close to 400,000 students and faculty at Virginia colleges and universities to use more than 500 hours of video content from the Public Broadcasting Service (PBS). The license includes popular series like Frontline, the American Experience, and Scientific American Frontiers; as well as specials and mini-series on such topics as Thomas Jefferson, the Tuskegee Airmen, and World War II.

The Problem

The agreement with PBS allows VIVA to make these videos available by streaming (they cannot be downloaded or distributed on tape or DVD).

How, then, to distribute the videos and make the streaming process work at more than 70 institutions with various levels of IT capabilities and support?

“The initial plan was to get everyone up and running with local hosting,” said Ralph Alberico, dean of libraries and educational technology at James Madison University and a member of the VIVA steering committee. “But there didn’t appear to be an easy solution to meet the licensing requirement to authenticate and authorize each user with a user ID and password.”

Other potential roadblocks included different amounts of bandwidth available at each school, varying levels of IT support, and the potential strain on the resources of the smaller campuses hosting the content. Not to mention, as Alberico said, “the tremendous amount of duplication of effort and waste of money by doing it that way.”

The Solution

“This is a poster child for federation,” Alberico said. “Jim Jokl volunteered the resources at the University

of Virginia for hosting, and we were on our way.”

“This seemed like an ideal case for Shibboleth and the InCommon Federation,” said Jokl, director of communications and systems for the University of Virginia’s IT department. “We could just run it here [at the University of Virginia] and end-users could watch the videos from anywhere.”

Under this arrangement, the videos are located in, and streamed from, just one location. Each of the VIVA institutions will authenticate their own users, leveraging their existing identity management systems.

“InCommon membership and the ability to make this type of content easily available helps us meet our goals as a consortium.”

— Ralph Alberico, James Madison University

“From a resource provider perspective, it wasn’t that big of a deal,” Jokl said.

The Result

VIVA federated access to the videos, with the University of Virginia providing the hosting and streaming resources. Now, any VIVA member can join InCommon and gain access for its users through Shibboleth or other federating software.

“Our goal is to get the vast majority of VIVA sites to use this,” Jokl said. “Over time, I expect that VIVA members will take advantage of their InCommon participation in other ways.”

“We are approaching critical mass,” said Alberico. “We have eight schools who are now members of InCommon. In addition, James Madison University has developed a legal template, made available to the other state universities, to help them join InCommon.”

“Our goal as a consortium is to level the playing field,” Alberico said. “Our institutions are different sizes with different academic programs and different sized budgets. InCommon membership and the ability to make this type of content easily available helps us meet our goals as a consortium.”

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.

4/8/2008