Making Music Through InCommon

Universities and non-profits make sweet music together.

DRAM is a database of recordings and liner notes from a number of record labels. The organization grew out of New World Records and offers on-demand streaming access to music that is difficult to acquire commercially.

The Problem

New York University hosts the DRAM site and would like to make this resource widely available to music scholars and music lovers. DRAM has agreements with many institutions and NYU now supports multiple forms of authentication and authorization. Gary Chapman, senior IT architect at NYU, would like to streamline this process.

At the same time, the **University of Washington** (UW) requested access to DRAM, but wanted to use a federated approach to identity management to ease the access issues for IT and the end user. The UW library system had a DRAM subscription to provide access to any student, staff or faculty member, as well as to anyone visiting the library. UW did not want to create another complete authorization process for DRAM users.

"We saw an opportunity to leverage our InCommon membership and simplify the deployment" of DRAM, said Nathan Dors, a technology manager at UW.

The Solution

"We were working on bringing up Shibboleth and on becoming an InCommon member," Chapman says. "At the same time, the University of Washington had the desire to use DRAM and a scalable access management solution."

By joining InCommon, the universities and DRAM eliminated the need to create a new authentication and authorization system, or to set up an IP address-checking procedure. They relied, instead, on InCommon's federated approach, in which organizations agree on a set of privacy-preserving attributes, technologies, processes and policies to exchange selected user information.

Users receive Single SignOn convenience, using the user ID and password from their home institution.

> *"We saw an opportunity to leverage our InCommon membership and simplify the deployment of DRAM."*
>
> *—Nathan Dors*
> *University of Washington*

The Result

"Once NYU and DRAM were registered in InCommon, all we had to do is configure the appropriate attribute release policy and — voila! — logins for on- and off-campus users were enabled for DRAM," Dors said.

"Things are functioning smoothly," Chapman said. "In addition, we've been able to share elements of DRAM itself with other institutions, notably the Virtual Library of Virginia (VIVA) via the **University of Virginia**, for purposes of streaming media."

> *Through InCommon, "we start from a position of mutual confidence and trust for the viability of our technical implementation."*
>
> *—Gary Chapman*
> *New York University*

The scalability provided by InCommon means that both NYU and UW can interact with many more organizations, using multiple applications, with relative ease.

"I think that having the Shibboleth/InCommon implementation in place facilitates further projects," Chapman continued. "We have another digital library project in the pipeline and an externally hosted ePortfolio project slated for fall release. In the latter case, our vendor is an InCommon member, and so in working with them we start from a position of mutual confidence and trust in managing end user access for resources."

About InCommon

You can read more about InCommon on the back of this page. InCommon is operated by Internet2 and managed by an independent steering committee representing the higher education and research community. For more information, visit http://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.