Security, Scalability Make the Case for Federating

NYU, PeopleAdmin use InCommon for human resource management.

PeopleAdmin provides human resources software to higher education and the public sector. The software provides an electronic workflow for an online application and tracking process, as well as a method for electronically managing position descriptions and performance evaluations.

NYU Founded in 1831, New York University is the largest private university in the United States, with more than 40,000 students attending 14 schools and colleges at five major centers in Manhattan and in more than 25 countries around the world.

The Problem

Searching for a way to improve workflow and automate some processes, the NYU human resources office contracted with PeopleAdmin to outsource its online application process, as well as its process for managing and tracking position descriptions and performance evaluations. Initially, 200 people would have access to PeopleAdmin, but that number could grow to more than 2,000.

NYU's central IT office became involved early in the process to determine the most efficient and scalable way to manage access to the new HR system, which would be hosted outside of the university. While PeopleAdmin supports an LDAP interface, the university has growing concerns about providing outside access to its directory services.

For its part, PeopleAdmin saw that the use of LDAP could present roadblocks. "More and more, we are finding that IT professionals are not keen on exposing their LDAP to external applications, for security reasons," said Matt Thomas, director of business development and integrations at PeopleAdmin. Maintaining a database of user IDs and passwords presented its own logistical problems for the company. "If you have thousands of people across the entire institution, user maintenance can become quite a problem," Thomas pointed out.

The Solution

NYU introduced PeopleAdmin to the benefits of federating, including the ability to leverage NYU's identity management system.

"Early on, we raised the issue of federated access and the use of Shibboleth® [Single Sign-on and Federating Software]," said Gary Chapman, senior information technology architect at NYU. "We proposed sponsoring PeopleAdmin to join InCommon if they would implement the Shibboleth service provider and federate their application. They agreed rather quickly on doing this."

"NYU made a very strong case for the use of Shibboleth and InCommon," Thomas said. "Shib has created this great platform and the federation allows all universities to talk together. That matches our business model and our interest. It is a natural fit."

The Result

"NYU is our first customer using Shibboleth and we expected it would take longer the first time," said Heather Tufts, lead integration project manager at PeopleAdmin. "Since we are a hosted system, we have three URLs that Shib has to sort out – a production URL, a test/sandbox URL and a training URL which correspond to NYU's live site, testing site, and training site, respectively."

> *"In the end, the nice thing about working with InCommon and Shibboleth, over other protocols, is the common, agreed-upon standardization. This will be much easier to replicate with other institutions."*
>
> *Matt Thomas, PeopleAdmin*

"This process was all new to us and the community involvement is very, very helpful," Thomas said. "We would throw out questions to the Shibboleth users list and, many times, would get a response within minutes. We worked through the issues, thanks to the help of NYU and the community."

"In the end, the nice thing about working with InCommon and Shibboleth, over other protocols, is the common, agreed-upon standardization," Thomas said. "This will be much easier to replicate with other institutions."

PeopleAdmin has now experienced significant interest in its federated application. "We plan to highlight our ability to federate at our upcoming client conference and we've entered into discussions with institutions that we know are InCommon members," Thomas said.

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.incommon.org.

200904-CS-INC-PeoAdm