

# Federated Identity Management

---

Prepared by:  
Gene Kovacs  
Assistant Vice Chancellor for  
Information Resource Management and CIO  
Florida Board of Governors

## **Initiative: InCommon Texas University System Federated Identity Management**

### **Purpose**

Provide a common identity management federation foundation to allow institutions to enhance collaborations, implement technology integrations, and improve computer application security.

### **Description**

The University of Texas System is one of the nation's largest systems of higher education, with nine academic institutions and six health institutions that educate more than 216,000 students and employ 87,000 faculty and staff.

Realizing the need for increased collaboration, technology integration, and security among U.T. institutions, in early 2004, the U.T. System Strategic Leadership Council made the decision to begin an Identity Management Initiative, which focused on standardizing identity management policies and practices across the 16 entities/institutions of the U.T. System and on developing a standards-based middleware infrastructure capable of meeting the objectives of the new initiative. The resulting governance framework and technology infrastructure was designed to enable identity information to flow in a trustworthy and reliable manner not only throughout the U.T. System, but also to any external trusted entity.

The U.T. System chose to affiliate with InCommon, an Internet2 group established to help support identity management federation for US research and education, and their sponsored partners. InCommon serves more than 6 million end users through federated identity management.

Contact: [Dr. Clair Goldsmith](#)  
University of Texas System  
[clair.goldsmith@utb.edu](mailto:clair.goldsmith@utb.edu)

### **Outcomes**

The U.T. system has experienced enhanced collaboration among institutions and application security improvements (the elimination of password retention by applications makes them more secure). The federated system creates an environment where different applications can be deployed and seamlessly integrated into institutional access management with little or no extra overhead. Seven U.T. institutions are moving to a hosted Peoplesoft ERP solution and having the system wide federation has lessened the migration impact of this project. U.T. notes that the Peoplesoft project would not have been possible without the existence of the federated model.

One unexpected outcome discovered was enhanced public-private collaborations among Texas' educational community. Once the federation capability was made available, universities began to find new ways to collaborate within and outside of their institutions.

### **Lessons Learned**

The implementation of the InCommon federated system was not the U.T. System's first attempt

# Federated Identity Management

---

at the deployment of a common identity system. U.T. learned from its initial attempt that local institutional buy-in and local control of identity provisioning systems was essential.

One key factor to the successful implementation of the federated system was a 'Training and Distribute Deployment Model'. The U.T. System office brought key technicians to a central location. These technicians were required to bring a laptop from their institutions. Upon leaving the training session, each technician had a fully functional Shibboleth Federated Identity Provides on their laptop and the know-how to administer the system. This model provides each institution with the needed expertise to install and administer the Federation Identify Provider.

Managing the release of which Identity attributes are used in federating should be a local decision while the framework of these attributes should be managed from a central authority. This allows each institution to be nimble in expanding usage of the federation system and lessens the need for large central helpdesk services.

## Status

Eight of Florida's twelve state universities are InCommon members. Several research universities have already met the InCommon federation standards and have deployed federated identity systems. These systems are currently in use with registered applications being shared among research institutions both inside and outside of Florida. None of Florida's public colleges were listed as InCommon members; however, all have some form of local identity management.

## Opportunities

The expertise for deployment and management of a federated identification system currently exists within the State University System. This expertise could be leveraged in developing institutional federated systems. These systems would become a building block for other collaborative innovations. Once established, any collaborative computer system or application project, both hosted and internal, could be readily accessed for both student and faculty usage.

Many higher education vendors have already configured their products (i.e. LMS,ERP) to integrate with the InCommon Federated product, Shibboleth. The ability and effort involved in integrating with applications that are preconfigured to operate within a standard federated framework greatly enhances an institution's capability to use collaborative systems.

## Challenges

Many smaller institutions do not have the capital or human resources to implement or maintain a federated identity system. InCommon membership, maintenance, and system support for a federated system are reoccurring expenses and would require continued funding.

Florida's differing higher education governing models would require more coordination and communication for managing metadata attributes across higher education systems. For consistency, a common metadata model, maintained centrally and adopted by both systems, would be required. Ownership and responsibility for this key component would need to be determined prior to implementation.

Although the federated identity expertise exists within the university system, the added workload for these experts during training and implementation would need to be considered when planning the project. The most time and resource intensive portion of the project would be the institutional InCommon assurance qualifications process. These experts would need to be available to consult with institutions as they seek qualification.

## Comments by the Innovation and Online Committee's Advisory Group: