



Shibboleth®

Web Single Sign-On and Federating Software

Attributes and Security Drive Florida's Choice of Shibboleth for SSO

The Problem

Since 1997, the University of Florida has operated, with great success, a home-grown single sign-on (SSO) system to provide access to web services and all of the main enterprise systems on campus. Security concerns began showing up in 2006, causing IT professionals to think about the next step in single sign-on.

The Solution

"Rather than completely rearchitect, redesign and rewrite the home-grown system, we decided to implement Shibboleth," said Mike Conlon, associate CIO, IT architecture, at the University of Florida.

Conlon and his implementation team spent eight months in public discussions, meeting with small groups and holding larger town-hall discussions to provide the rationale for replacing the legacy system.

"We had to convince people that, despite the fact that this thing was working great for them, there were significant problems and it had to be replaced," Conlon said.

Florida's primary interest in Shibboleth was as a robust SSO solution. "What we get with Shibboleth is a secure, controlled release of attributes," Conlon said. "We did not have that in the old system."

Shibboleth® Single Sign-on and Federating Software is a standards-based, open-source system providing individual access to protected online resources while preserving individual privacy through the use of attributes.

Attributes carry information about an individual – whether the person is a student, or is in a certain major, or even in a specific course. If a resource is limited to biology students, for example, attributes allow the authorization decision to be made without manual intervention and without necessarily releasing personally identifiable information.

By carefully crafting policies for the exchange and release of attributes, identity providers and service providers can provide very fine-grained access control.

Florida staff members spent considerable time defining the ways in which Shibboleth would be used, then creating attribute release policies (ARPs) to cover 90 percent of those cases. "We involved a group of 20

people, representing all of our enterprise system groups, as well as identity and access management thought leaders," Conlon said. "We were expansive in our thinking about attribute release policies, to make sure to cover our use case territory."

The Result

"We have gotten very good reactions from a wide variety of people across campus," Conlon says, "such as distance education, the health center, our research community, and the library."

Florida has a large Active Directory implementation and, much to the delight of departments across campus, included an attribute release policy related to their local groups. "One of the ARPs is to determine a person's local groups," Conlon explained. Such groups include such things as classes and majors. A system administrator can manage groups in Active Directory and, because of SSO, a user will have access upon signing in.

Conlon said Florida plans to provide Shibboleth integration with all future software and enterprise systems. "We plan to use Shib to access PeopleSoft, our course management system, and our legacy student system," he said. "We made sure Shib could handle the capacity of all of our enterprise systems running together."

Florida has also begun taking advantage of the federating aspects of Shibboleth. "We were not interested in being SSO innovators," Conlon points out, "and it turns out our timing was very good for our Shib implementation, in terms of federating." That's because of the growth in the number of vendors joining the In-Common Federation. The university has started working with several InCommon participants.

"All of this has really come about in the last 12 months," Conlon said. "When I go to the InCommon list and see the participants, I'm interested in that right-hand column (where the sponsored partners appear). "These are people that provide services to us and wouldn't it be cool if they just took our credentials. And they do." See more information on the other side of the page.

We plan to use Shibboleth to access PeopleSoft, our course management system and our legacy student system. We made sure Shib could handle the capacity of all of our enterprise systems running together.

— Mike Conlon, Univ. of Florida associate CIO



Shibboleth®

Web Single Sign-On and Federating Software

Shibboleth software provides single sign-on convenience for your users on campus or across the web. The approach to policy-driven authentication and authorization enables you to maintain control over your institution's data and the user's privacy. Your service providers retain control over who accesses their resources and don't have to worry about maintaining up-to-date account information for your user community.

What's the Shibboleth Advantage?

Single Sign-On for Campus and External Services

More and more, universities, companies and government agencies offer services and collaborate online. Users typically access online resources both inside and outside the organization to do their work. For example, students log into a learning management system and link to a campus project wiki space and a licensed homework site hosted by a third-party service provider.

In the past, each of these services required its own ID and password and, for the user, that meant adding another set of credentials to that collection of sticky notes. For the institution, closing the security holes and just keeping up with the access changes for the services on and off campus was quite a challenge.

Shibboleth was developed specifically to address these challenges. An individual uses his or her campus userid and password to access resources offered by the institution and provider organizations. And campus IT shops can use their authentication technology of choice — Shibboleth sits on top and provides the web single sign-on functionality.

Build and Manage Locally, Access Globally

But it's not just about single sign-on. Because Shibboleth leverages the local identity and access management system, the net effect is that the individual's relationships with the institution determine the person's access rights to services, hosted both on and off campus. If you build your identity and access management system for campus applications, chances are you can use it for federated third-party ones too.

Protect Your Data and Users' Privacy

With Shibboleth, the campus manages authentication of their users, but the service provider decides whether the individual can access the resource. The campus sends just the minimal data that the provider needs for authorization and nothing more. For example, if the name of a student isn't the main criterion for access, but current enrollment in a particular Biology course is, then that is what is sent. And all this is done at the time the user accesses the resource, so the data is delivered just-in-time and governed by policy, according to your institution's approach to privacy.

Partner with your Service Providers

From a service provider's point of view, Shibboleth can substantially reduce the risk and time involved in offering services.

In the past, IT departments sent large files of identity data to a service provider to create and update separate accounts. Now, using Shibboleth, the provider receives the information each time the user accesses the resource—they don't need to maintain campus identity data that goes out of date. And the provider still has control over access to its protected services without the concerns of potential spills of your campus data or mis-configured IP-based access methods.

How Do I Get Started?

To learn more about the Shibboleth authentication and federating software, visit the Shibboleth website (shibboleth.internet2.edu). You can become active in the community by joining email lists and attending the workshops and presentations offered around the country.

About the Internet2 Middleware Initiative

Led by the Middleware Architecture Committee for Education (MACE), the Internet2 Middleware Initiative comprises a number of projects that address challenges in the middleware space, such as identity and access management. For more information, visit middleware.internet2.edu.

Acknowledgments

Development of Shibboleth was supported with funding from Internet2 and the National Science Foundation through their NSF Middleware Initiative (Cooperative Agreements OCI-012393, OCI-0330626, and OCI-0721896).