

# 17 March 2010

---

## Building Identity Trust Federations Conference Call

March 17, 2010

The topic was a case study of the University of Wisconsin system and their process to build a federation, featuring Keith Hazelton, Senior Information Technology Architect at the University of Wisconsin Madison and Brad Schwoerer.

Brad Schwoerer, University of Wisconsin-Madison (Presenter)  
Joseph Giroux, California Community Colleges  
Keith Hazelton, University of Wisconsin-Milwaukee (Presenter)  
Todd Piket, University of Minnesota State Colleges & Universities  
Mark Scheible, North Carolina State University  
Garret Sern, EDUCAUSE  
Craig Stevenson, WiscNet  
David Walker, UC Davis  
Ann West, Internet2/InCommon  
Dean Woodbeck, Internet2/InCommon

### U of Wisconsin System Process for Rolling Out a Federation, Keith Hazelton

- \* UW-Madison joined InCommon three years ago; primary issue was one sentence in the participation agreement that stated limitations on dispute resolution, waiving sovereign immunity in the state of Wisconsin.
- \* On campus they are using Shibboleth for Moodle and university central support
- \* Library is another place we have been working with and are near the final stages of rolling out shibboleth.
- \* InCommon membership used for access to Wikis; bio-statistic personnel using to access NIH services; Google Docs.
- \* CIC is also part, rolling out a collaboration suite.
- \* MONK (see Keith's previous e-mail) collection of digitized library materials, creating Shib access to MONK has been set up. Issue has been the need to provide e-mail addresses.
- \* Rolling out U-Approve for access to MONK, to provide one-time consent at time of use.
- \* Soon after we signed the InCommon agreement, we received approval from HR and registrar to release user ID without a targeted ID process.

### Questions

1. On U-Approve, did you determine one-time access is sufficient, or do they have to approve every time?

A. Still TBD. Talking with registrar.

### WI Statewide System Federation, Brad Schwoerer

- \* Purposely named federation because we envision other state schools joining. Have not discussed in detail including K-12 at this juncture.
- \* UW system has had an authentication for 6.5 years, a reduced sign-on system that had back end directory to each campus system (i.e. one log in page). However, policy was way too restrictive.
- \* Looked to change from this approach to a federation. Didn't go anywhere because we were moving towards picking a product.
- \* Two years ago purchased Oracle ID Management products.
- \* Used OAM with Oracle virtual directory so you could merge university LDAPs into meta-directory.
- \* Designing out the federation, we chose Shibboleth IDPs and Oracle products for service providers.
- \* Exposed all of the data in our person hub and aggregated that with central HR information to represent the first federation.
- \* We have a system IDP that is a system authority, from 16 of the universities.
- \* 16 institutions as part of the federation to date. Posting 14 of the IDPs on two virtual machines.
- \* At this point we use name, e-mail, personal ID.
- \* Still in the mindset that this should be used for central applications.
- \* Need to educate campus CIOs on the need for federated identity management.
- \* Since the first major use of the infrastructure is for the forthcoming HR system, people didn't have to rethink this notion. Each campus was using its own set of credentials, unchanged from earlier System authentication solution. (Ann West compared this to "implementation by stealth".)
- \* What will force the question of setting up some governance is an application that will require a different set of attributes.
- \* When smaller, centralized campuses start showing the "wins" of this system, other schools will want to take this over themselves.

\* It's not that much work setting up 14 IDPs, given the access to the data.

\* Working on creating one identifier, known as a "start ID".

\* Imagine for the UW systems, we'll be providing a suite of ID management systems that will be helpful for the campus. Not palatable for us to solve other campus management issues, before solving our own. Questions

1. Do you have a diagram of your architecture to share? Interested in attribute service concept as well.

A. Yes, although very rudimentary diagram. New functionality is to take an identifier and incorporate into an identity manager profile

#### **Follow-Up Discussion on CAMP, Ann West**

1. Would you be willing to stay for another half day to attend a meeting of state federations?

A. Most call participants say yes, pending travel budgets. While not optimal, we Ann may try to an adobe connect phone conference as an option.