21 January 2009

Building Identity Trust Federations

Wednesday, January 21 at 4:00pm ET
Bridge Number: 877-944-2300
Passcode: 99205#

In attendance:
Brian Burkhart, OneNet
Paul Caskey, University of Texas System
Sujay Daniel, NJEGge.Net
Renee Frost, Internet2
Clair Goldsmith, University of Texas System (presenter)
Rich Greenfield, University of Alaska (co-chair)
Linda Hilton, Vermont State Colleges
Gavin Hogan, SUNY
Matt Howard, eTech Ohio Commission
Ken Klingenstein, Internet2
George Laskaris, NJEDge.Net (chair)
David Purcell, California State University
David Rohwer, University of Alaska
Mike Rohwer, Ottawa Area Intermediate School DIstrict (MI)
Andy Rosenzweig, Merit Networks
Mark Sheible, North Carolina State University
Craig Stephenson, WiscNet
Garret Sern, EDUCAUSE
David Walker, University of California, Davis (presenter)
Ann West, Internet2
Mary Fran Yafchak, SURA

Notes
This conference call featured presentations from the University of Texas System and University of California, Davis as to their motivations behind building a federated identity management, their progress to date and recommendations to higher education institutions who are exploring this option. Each presenter was asked to structure their remarks around a set of questions.

Clair Goldsmith, University of Texas System
Structure: 9 general and 6 health institutions for 15. There are however, 16 entities, if you include the overarching institutions. All are independent with own HR depts., presidents and provosts. 81, 000 faculty and over 194,000 students.
1. What motivated the UT system to build a federation? What goals did you have?
- Looking to increase collaboration which is looked for by state legislatures. Looked to create sustainable, interoperable infrastructure and improve some security.
- Need fairly close control over how we vetted employees and students, which is not a hallmark of Internet2's InCommon agreement. Instead they have a 10 page member practices document that institutions must be compliant.

2. Who were the identified stakeholders? Who was (were) the sponsor(s)?
- Almost everybody. Strategic leadership council of CIOs and chief business officers

3. How did you build the federation? Brief overview of process.
- Started in 2004 with vision statement of what we wanted and is only a 1/3 of a page long and can be found on UT system website.
- We would have an LDAP directories on each campus, support eduperson, create UTperson if there was anything we needed to specify for the institutions, use id management trust policies.
- Extending the reach grant which allowed us to hold a Shibfest for all participating institutions and train them on how to have machines configured.
- Governance and policy work conducted in parallel with technical work. Submitted all documents to legal review.
- Began production on Sept. 1, 2006 and are up to 40 applications. Currently bringing up ECERT, which has to do with meeting reporting requirements with NSF and NIH. Support Dreamspark and local applications such as legal tracking.
- Initial set of applications were two small ones - Monthly Financial Report (one user at each institution) and wireless access to the UT system administration network for visitors from the campuses.

4. What challenges did you encounter and how did you address them?
- Getting the campuses to participate at a production level which we addressed by providing applications that met needs on the campuses
- Acceptance of the policies required which was done through discussion with legal and with the campuses

5. What recommendations would you make to others just starting this process?
- This is infrastructure, so it's akin to building a subdivision. No one cares until you start doing something with it. Helps to start with applications used by the community.
- Caution: authentication is easier to do than authorization for resources.
- Plan support model carefully. Who do users call? Local help desk? Or federation help desk?
- Demonstrate business value immediately.
- Leverage things other people have done.
- It's all about trust; we found institutions were happy if they were siloed and didn't have to think about other institutions.

6. What were the first applications used?
- Some institutions used it for Blackboard and have been for almost three years.
- System-wide compliance training with Adobe Connect
- Recently had one of our institutions come up with Forensic Assessment Center Network. Caseworkers enter information into a database used by pediatrics physicians to search for patterns of child abuse.

David Walker, UC Davis
Structure: Single entity, with 10 campuses of varying sizes. 5 campuses have associated medical centers.
1. What motivated your system to build a federation? What goals did you have?
- Common authentication project or PKI, for ability to access campus-wide systems (1998). Revolt in 1993 among campuses, feeling it was not helpful.
- Targeting transactions of university business, starting with employee data.
- Once we had a critical mass of campus involvement, applications started increasing.

2. Who were the identified stakeholders? Who was (were) the sponsor(s)?
3. How did you build the federation? Brief overview of process.
- Push to eliminate the original process, looking for a quick replacement.
- Did Shibboleth tech demo to introduce users to self-service system.
- Need to start building the policy.
- Instead of building a separate federation from Uncommon, requested all campuses to join and put out additional requirements for Incommon.
- Used extensive vetting with user groups.
- Set requirements for identity insurance using UC trust identity assertion requirements.
- Still building out the federation. Campus still building out

4. What challenges did you encounter and how did you address them?
- Integration issues

5. What recommendations would you make to others just starting this process?
- Starting out with simple applications may be easier.
- Making sure everyone is buying into business and policy issues is the big task.
- Leverage InCommon as much as you can and don't do anything you don't have to.

6. What were the first applications used?
- Shared Wiki's,
- Growing interest in using this for library access, with San Diego campus taking the lead on this.
- UCLA and UCSD have decided to use Shib for even local applications, so they are capable of being federated by default.

Questions
1. Why does the UT System feel they need a separate campus trust agreement?
- Bringing in some uniformity drove the document. Unclear at the time whether we could get all of their institutions to join InCommon, but could make them join something built within the system.
- Want control within our system and having a federation provides that.

2. Buy-in critical from campuses critical?
- Yes, this was important.

3. How one may go about federating is becoming clearer via case studies, but when to federate or using existing system is becoming murkier. When do you determine when to have a separate federation?
- Clair - Europe has individual federations and is starting to inter-federate. States are starting to do this, but not necessarily all things to all people, but sector-based.
- Jean (U of WI, Madison) - are InCommon fees from central funding? UC Davis required all campuses to provide their own fees.
- Mark S. (NC State) - we're in the middle of running a pilot for K-20 in NC, and whether to use InCommon will run into K-12 funding challenges which runs into idea of having their own federation, which could create more challenges.
- Clair - use protect network, general id provider for consultants not on the UT system network. Just need e-mail account to get into the system.
- Steve Carmony - might be worth our while to have someone from Becta of the UK to present to this group if many of use deal with K-12 community. What support must be done for K-12 community?
- Clair - many federations in Europe run an IDP.
- Steve - know of a consortium of private universities that want to run a joint IDP or help establish their own.
- Garret will follow-up with COSN.

4. More comments on planning your support model carefully?
- David - just trying to make information available to people, including requiring that campuses share help desk contact information and contact information for real people that are doing these applications.

Future Conference Calls
March 18, 4:00-5:30pm (EST)
April 15, 4:00-5:30pm (EST)
May 20, 4:00-5:30pm (EST)