15 July 2009

Building Identity Trust Federations Conference Call

July 15, 1009

In attendance:
Rich Greenfield, University of Alaska
Charles Hedrick, Rutgers University
Chris Holsman, University of Wisconsin
Galvin Hogan, SUNY System Administration (presenter)
Matt Howard, eTech Ohio Commission
George Laskaris, NJEDge.Net (chair)
Bob Morgan, University of Washington and Internet2
Paul Schopis, Oarnet
Mark Sheible, North Carolina State University
Tim Poe, MCNC
Garret Sern, EDUCAUSE (scribe)
David Walker, University of California-Davis
Ann West, Internet2
Dean Woodbeck, Internet2

On this month's call, we heard about the developing efforts to build a system wide federation across the State Univeristy of New York. Gavin Hogan from SUNY System Administation in Albany described the system's strategies and approaches as well as lessons learned in deploying a system-wide federation.

Strategies from SUNY (Slides)

- SUNY currently has an Oracle shop and is moving forward to interoperate with the shibboleth federation
- SUNY comprised of 64 campuses plus the research foundation and other entities are involved.
- Technical capabilities are distributed - very disparate, but the higher you go, the more capable they are.
- Historically - centralized management. Looking to develop a decentralized management structure and web portal. (see slides)
- 60 of our 64 campuses have enabled LDAP.
- Built in Java
- Beginning to show lack of featured applications and need to retool and/or replace.
- Looking to move away from current model to interact with third parties.
- We don't have an existing system for third parties to access. Looking to federate identities with other campus offices.
- Moving to SUNY Federation has been a long process. Adopted the eduperson attributes with Sunyperson attributes.
- We have been evaluating multiple technologies. Expect to integrate with services we plan for later.
- Motivations - existing system meets most of our needs, but looking to integrate with other services and put more ownership with the campuses.
- Implementation Team - System & Information Technology Exchange
- Alliance for Strategic Technologies - combined view for the whole universities. Each group brings different skill sets.
- Key sponsors are not well defined- SUNY System Administration & SUNY Information Technology Exchange Center (ITEC).
- Shared attributes - not in a position to use them. Only custom attributes are the Student ID and Person/Employee ID
- Started a Shibboleth proof of concept stated with 1.x moving to 2.0 implementation. Highly likely to be used by many campuses.
- Oracle is current POC; key advantages - access control and entitlement services.
- It is critical that it work with shibboleth and we have been ensured by Oracle this will be the case.
- Shibboleth 2 is supported by the project, but Shibboleth 1 is not.
- Have had different approaches to technology design and approach from Oracle Consulting.
- Finally completed the project definition.
- Next Steps - need to focus on Oracle product training. Basically, this is training the trainers kind of approach, akin to I2. Already have some trainers and detractors within the university system.
- In the process of drafting policy documents. Looked at UNC policy documents; while not appropriate, they were a good starting point.

Questions and Comments

Q. How do you plan on addressing the issue of auditing the way campuses are distributing the credentials?
A. Concept of having ID and access controlled on the campuses is something we're already doing, so no need to draft new policies to address this. However, we need a way to blackball ID's/users no longer associated with the campus or acting inappropriately. With limited employees, Gavin's group can't make this decision, rather campuses are better able.

Q. Any campus audit requirements?
A. Don't have a mechanism to audit at this time. Comes up in other critical ways at this time via other policies.

Q. How is Incommon establishing level of partnership?
A. The partner decides for themselves by applying for a particular level. Incommon won't be conducting audits, instead, relying on an independent auditor. Know the campuses are audited internally and by the state.

Q. Relationship with Oracle - what levels of assurance to you have they will maintain developments of Shibboleth?
A. They are committed to being standardized in this realm, but can't provide details due to NDA. They allow you to interplay with Java transaction; ADIs are one example of evidence they will meet this commitment. They want to get into higher ed market and realize fed id management requires interplay. When they identify what is important to them, they dedicate the resources. OIF is meant to integrate with many access control engines.

Q. Anyone else with Oracle experience in this realm?
A. U of Wisconsin has had the same experience with Oracle Consulting and inching along with OIF. They are going to have to overcome some of the lack of the communication leading up to the project. Their experience with sales process has been more difficult than the actual consulting.

Q. Do you think you'll be taking this federation in the same direction as the Texas or California model?
A. Looking at closed federation for SUNY Universities, not exclusive to InCommon membership. Not seeing a telling reason to follow this approach, although senior management disagrees right now.

Q. Does SUNY have a document that illustrates how to create and run your own federation as best approach?
A. I don't think so, although it would make sense. There is room to make uninformed choices based on perceptions. Add this to the list of marketing materials for InCommon. There is a key study from the University of California system that talks about what they did.

University of California can see moving away from UC trust and using InCommon Silver Identity Assurance Profile. A principle of UC Trust was not to replace anything InCommon can do for us.