InCommon Forum, April 27, Spring Member Meeting

InCommon Forum, Internet2 Spring Member Meeting, April 27, 2010

InCommon Update

John Krienke provided an programmatic update from InCommon.

- The federation ended 2009 with 199 participants, compared to 124 at the end of 2008. There are 220 participants as of today.
- About 120 Internet2 university members are not InCommon participants - this seems like a natural place to encourage participation.
- The new affiliate program has its first two members: Unicon (provider of Shibboleth training and support) and AegisUSA (provider of IdM consulting and an appliance for joining InCommon).
- InCommon is offering a new certificate service that is both pragmatic (unlimited server certs for one fee) and innovative (unlimited personal certs are included). There will be a test rollout in May with a few participants, then full rollout in summer 2010. Internet2 members receive a 25 percent discount. Must be an InCommon participant to use.

InCommon @ the National Science Foundation

Ardoth Hassler from the NSF provided an update on the status of federating various applications.

- Research.gov, an application that provides streamlined research grants management services across several federal agencies. It is expected to be compatible with the InCommon Bronze assurance profile.
- NSF is also planning to federate its FastLane application. It is expected to be compatible with the InCommon Bronze assurance profile. The NSF has tested pilots with Penn State and the University of Washington and has started testing with the University of California Davis. Testing is pending with Colorado State and Georgetown.
- External wiki - a pilot is coming soon for this application, to be used for collaboration both internal and external to the agency.

InCommon Operations Update

- Enabled multiple IdPs per organization
- Increased number of SPs available from a cap of 20 to 50.
- Enable self-signed certs in the federation metadata
- Introduced two new email lists in conjunction with a new metadata change management process. One list provides one-way notifications to campus InC admins, the other is to notify participants with metadata diffs.
- In phase one of platform and database upgrades in anticipation of Silver and direct XML submissions.
- Upgraded site administrator interface to include automatic defaults populating the web form.

In the works:

- DIFF - daily production-production diff email and archive (May)
- Metadata signing key update (May)
- WAYF/Discovery Service upgrade (May) and community discussion group (summer)
- New alerts for urgent matters
- Direct XML submissions (summer)

Attributes - User Consent

Luke Tracy from the University of Michigan reported on the use of uApprove for user consent to release attributes. Originally, a user would be presented with uApprove the first time he or she went to an SP, then subsequent visits would not include the prompt. There was a policy question, however, over what would happen if the data being released would change. Subsequently, users are presented with uApprove each time they visit an SP. UMich has implemented this with just a handful of SPs. The long-term goal is to not have users presented with uApprove every time they visit an SP.

Keith Hazelton reported that the University of Wisconsin-Madison will be implementing uApprove.

Attributes - Default Sets

Mike Grady (University of Illinois) reported that the CIC is looking at developing a pre-approved set of attributes able to be released. In many cases, the IdM people do not have the authority to make decisions about what to release and it can become cumbersome to gain approval for each SP. They are looking at pre-approved bundle of attributes to eliminate the ad hoc nature of this process. A group of CIC registrars and IdM folks will be meeting on this, and the set of attributes has not been developed, but would likely include EPPN, TargetedID, Affiliation (standard and scoped), entitlement, assurance, email, and several forms of name. It would still be expected that a service would ask for only what they need, not the whole bundle.

There is also discussion about extending the metadata to describe the service that is being provided; just having the entityID is not enough.

Bronze and Silver Identity Assurance Profiles

InCommon has submitted its Bronze and Silver identity assurance profiles to the U.S. General Services Administration's (GSA) ICAM (Identity Credentialing and Access Management) program to gain approval as a Trust Framework Provider. The requirements include such items as not releasing as few attributes as necessary (minimalism) and protecting personally identifiable information during the registration process. The submission has been through preliminary review and resubmitted after comment.

One next step will be a strategy to facilitate adoption of Silver among participants, including determining the drivers for Silver, engaging auditors, working out a process to fielding and answering questions - basically having a roadmap for this.

Tom Barton reported on the CIC work on Silver. The CIC has developed a three-phase approach to implementation: 1) impact/implementation with ordinary operations, 2) developing the credentialing process, and 3) understanding how the technology works.

The CIC has also committed to documenting these three phases to provide information for those future adopters.

The University of Washington has its own project going and has joined some of the conference calls. The CIC has also engaged some auditors.

Achieving silver does not mean that every authentication that occurs need meet the Silver specifications. The IdP can decide under which circumstances Silver is necessary. It may involve only a couple of hundred researchers, for example.

The University of California is also working on Silver, as is the University of Texas system. As a community, we need to start another cohort along the CIC three-phase process soon to keep the momentum going.

Federating at the NIH

Debbie Bucci from the National Institutes of Health reported that the NIH has been federating for about two years. A key driver has been the CTSA application, and people are also setting up communities on the wiki. There is a pilot underway for the eRA application - which would require Silver - involving Penn State, UC Davis and Johns Hopkins.

----
eduRoam

eduRoam is a federated wireless network access system that has widespread deployment in Europe, but is just making inroads in the U.S. This is another project that the CIC is involved with. Currently the effort is centered at the University of Tennessee (with an NSF grant), but there is interest in defining what role InCommon might play.