18 April 2012

Building Identity Trust Federations Conference Call

April 18, 2012

1) In Attendance

- Suresh Balakrishnan (University System of Maryland)
- David Bantz (University of Alaska)
- Tom Barton (University of Chicago)
- Mark Beadles (OARnet)
- Joseph Giroux (California Community Colleges)
- Michael Hodges (University of Hawaii)
- Dave Jaskie (University of Wisconsin -Milwaukee)
- George Laskaris (NJEDge.Net)
- Mark Rank (University of Wisconsin -Milwaukee)
- Mark Scheible (MCNC)
- Steve Thorpe (MCNC)
- Valerie Vogel (EDUCAUSE)
- Ann West (InCommon)

2) InCommon Silver and Bronze Assurance

- David Bantz, Tom Barton, and Ann West provided a presentation on Identity Assurance Profiles and Trust Federations.
- David briefly reviewed Level of Assurance (LoA).
    - Technologies for LoA specified in Assurance Profiles.
- Issues/Concerns in terms of meeting IAP requirements
    - Control or constraint of entrenched processes; member may use less robust authN for legacy apps
    - Multiple stores for credentials with multiple controls by (some) federation members
    - Onboarding & vetting procedures may be lax per IAP
    - Meeting LoA profile might entail a second more secure credential store or use of 2-factor authN (lack of clear applicability of 2-factor authN to meet LoA Silver profile)
- Ann noted that the InCommon assurance program was written in response to ICAM requirements for trust framework providers. If you want to federate with the federal government, InCommon needed to become an Approved Trust Framework Provider.
- Assurance Program Components:
    - Profiles/Framework
    - Federation Operation Policies and Practices
    - Legal Framework
    - Certification Program
    - InCommon Metadata
    - Practice and Implementation Outreach
    - Program Oversight: Assurance Advisory Committee (this group is chaired by Mary Dunker, Virginia Tech)
- Two primary profiles: Bronze (LoA 1) and Silver (LoA 2)
- Identity Provider Process
    - Support Profiles
    - Go through audit
    - Submit signed legal agreement
    - Audit summary/qualifications
    - Assurance addendum
    - Pay the fee
    - Configure SAML software
- Service Provider Process is fairly simple
    - Determine which qualifier to request
    - Configure SAML software to check metadata and request qualifier
    - Notify InCommon of your intent to request
    - No fee!
- Established graduated fees for IdP operators between 2012-2015 (to reflect increasing value and early adopter contributions).
- The New Bronze
    - October 2011: Federal CIO Memo
    - 30+ Federal Apps at LoA1 in InCommon now
        - List of NIH apps (doesn't include all apps): https://spaces.at.internet2.edu/display/InCNIH/InC-NIH
    - ICAM encouraging broad Bronze deployment
    - New Bronze available for review (reduces requirements to simplify deployment; removes profile audit requirement)
    - Review site
- Resources
    - Institutional peers on assurance@incommon.org (new resources announced here)
    - Community Resources (e.g., AD Silver Cookbook and Multi-factor Authentication Guidance)
    - Webinars (IAM Online and monthly calls)
    - Meetings (e.g., InCommon Confab, April 26-27, in DC)
    - Auditor Toolkits (coming soon!)
- Tom spoke about the CIC (Committee on Institutional Cooperation) InCommon Silver Project.
    - CIC CIOs set a goal in 2009 of all members achieving InCommon Silver in Fall 2011. IdM staff and internal auditors were involved.
    - Steps included performing a gap analysis, providing feedback to InCommon, and developing documentation.
    - CIC Silver project is now transitioning to Phase 2.
- InCommon Silver adoption pipeline
    - CIC Silver Project: 12 CIC schools, plus Virginia Tech and University of Washington

- University of Florida
- UW-Milwaukee
- Many expect to be Silver certified in 2012
- US Government formulation of LoA (references provided by David):
  - OMB Memorandum M-04-04: E-Authentication Guidance for Federal Agencies, December 16, 2003
  - NIST Special Publication 800-63: Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology

3) Next Call

- The May 16 call is canceled. The next call will take place on Wednesday, June 20, 4-5 pm EDT.