18 May 2011

Building Identity Trust Federations Conference Call

May 18, 2011

1) In Attendance

- Suresh Balakrishnan (University System of Maryland)
- David Bantz (University of Alaska)
- Mark Beadles (OARnet)
- Paul Caskey (University of Texas System)
- Paul Erickson (University of Nebraska-Lincoln)
- Larry Gilreath (Microsoft)
- Michael Hodges (University of Hawaii)
- Keith Hazelton (University of Wisconsin-Madison)
- Dave Jaskie (University of Wisconsin -Milwaukee)
- George Laskaris (NJEDge.Net)
- Eric Olson (University of Florida)
- Rodney Petersen (EDUCAUSE)
- Tom Piket (Minnesota State Colleges & Universities)
- Mark Rank (University of Wisconsin -Milwaukee)
- Keith Runkle
- Mark Scheible (MCNC)
- Steve Scholz
- Craig Stephenson (University of Wisconsin-Madison)
- Jack Suess (UMBC)
- Steve Thorpe (MCNC)
- Valerie Vogel (EDUCAUSE)
- Ann West (Internet2/InCommon)
- Jason White (Iowa State University)
- Mike Wiseman (University of Toronto)
- Dean Woodbeck (InCommon/Internet2)

2) Integrating Active Directory Federation Services (ADFS) with Federation Trust Services (Paul Caskey, University of Texas System)

- *Today's slides: USFeds-Call_5-18-2011.pptx*
- Speakers: Paul Caskey is CTO at the University of Texas System and Larry Gilreath is a Technology Specialist at Microsoft.
- ADFS can be an identity provider and service provider at the same time. SharePoint sees ADFS as an IDP. But Shibboleth sees ADFS as an SP.
- ADFS does have a robust scripting environment.
- Note: Security Token Service (STS) = IDP
- UT System is currently using ADFS strictly as a service provider. They haven't tried using it as an IDP (they currently use Shib, which they're happy with and it integrates well with Active Directory). They've been in the testing phase for 6-9 months.
- First application for this will be SharePoint 2010, followed by Office365.
- In the future, ADFS support will be built in, so they'll consider this for any future applications that come with ADFS SSO support.
- Background – SharePoint 2007
    - They operate a large SharePoint 2007 installation – widely used by every member of the UT System Federation. It's also used externally by a variety of entities (most of whom use ProtectNetwork to log in). They even sell SP sites to other campuses within the UT System.
    - Paul noted that CIC shared their code when they started this project.
    - Based on a custom form-based authentication with Shibboleth integration.
    - Authorization is a multi-step process for users (validation by site owner). Still easier than the first install with separate user name and password. (The first install was not used as much as this one because people forgot their user names/passwords.) No "automatic" authorization (no attribute-based groups).
    - Despite some issues, overall it's a great collaborative tool and the users are very happy.
- SharePoint 2010 – ADFS
    - Everything will be "claims-based" through ADFS (hopefully). No more dual sites for same content.
    - Better onboarding for IdP
        - Anonymous page to describe process and required/desired attributes
        - "All authenticated users" page to verify asserted attributes
    - Automatic authZ (group membership) based on attributes/claims
        - eduPersonAffiliation, eduPersonEntitlement
    - The only custom code is an HttpModule which hooks the 'OnSignedIn' event in the ADFS module
        - Pushes asserted personal info attributes into the SP User Profile
    - They also customized the ADFS "Home Realm Discovery" to mimic the Shibboleth Discovery Service (for user familiarity)
- Current Issues/Concerns (SharePoint 2010 – ADFS)
    - People picker mode
        - Claims mode resolves anything, even typos
        - Site collection mode resolves only existing users
        - Might need a custom claims provider
    - Configuring claims-based groups
        - People Picker must be in Claims mode (but it remembers what you set)
    - Possibility for "internal things" maybe still relying on NTLM
        - Exchange integration
- Useful URLS
    - Shibboleth wiki page: https://wiki.shibboleth.net/confluence/display/SHIB2/MicrosoftInterop
    - Microsoft document on InCommon and ADFS interoperability: http://technet.microsoft.com/en-us/library/gg317734(WS.10).aspx
- UT System Federation Policy Background

    - UT Federation has been in production operations since 9/2006 (17 entities). All members are contractually bound. Some external participants are inter-federated from InCommon
    - Policy documents – Federation Operational Practices (FOP) and Member Operational Practices (MOP) – are available at: https://idm.utsystem.edu/utfed
    - UT System established a quasi-LOA2
        - Never validated by an external authority, but suitable for our needs
        - Currently re-writing for Silver/FICAM2
    - Current effort with system-wide research cyberinfrastructure likely to drive need for LOA3
    - Working to institutionalize (across the UT System) formal IdM auditing (so far, federation LOA assessments have been self-asserted)
- Are you asserting who is LOA2 in an attribute? Yes, eduPersonAssurance.

Next Call: June 15