InCommon TAC Meeting 2018-05-24

TAC Meeting Minutes - May 24, 2018

Attending: Mark Scheible, Matt Brookover, Janemarie Duh, Judith Bush, Mike Grady, Eric Goodman, Tom Demeranville, Kim Milford

Regrets: Keith Wessel, Eric Kool-Brown

With: Nick Roy, IJ Kim, Dave Shafer, David Walker, Shannon Roddy

T&I Updates (Mark/Nick)

Updated TAC Charter - Mark sent the updated charter to Sean Reynolds, chair of InCommon Steering, and asked to have it on Steering's next agenda for approval (Steering next meets Monday, June 4).

Status of MACE-Dir / next steps with REFEDS - MACE-Dir work will move to REFEDS, since this is a global activity. At the Global Summit meeting, MACE-Dir members thanked Keith Hazelton for leading this for so many years.

Ops Update

Baseline Expectations - Release of the Federation Manager Tuesday, May 29, will strongly recommend metadata changes conform with Baseline. CTAB and the project team are working on communications leading up to the PA change (June 15) and beyond.

eduGAIN Steering Meeting - Voting members approved an eduGAIN SAML policy change requiring federations to do specific things with their metadata. Entities need a technical and support contact. There will come a time when eduGAIN will drop a federation if they submit metadata without those. When that happens, if there are InCommon organizations that do not have those contacts, we will stop exporting those entities to eduGAIN.

eduGAIN also recommends submitting metadata with a 4096-bit key. This is planned as part of our MDQ rollout. Also, eduGAIN has a "should" to adding mdrpi:RegistrationInfo to every InCommon entity descriptors. We do not do this.

Federation Manager - Released some bug fixes this week and will have more next week when we do the Baseline Expectations update.

MDQ Implementation - As part of automating metadata signing, we need a Hardware Security Module. We are having trouble with getting the Shibboleth MDA to work with the Amazon HSM via PKCS#11, so we are working to develop a signing bean for the MDA that will work with the HSM via Java API supplied by Amazon.

Working Groups

Streamlining SP Onboarding - reviewing feedback from community consultation. Suggesting a late June wrap-up.

Attributes for Federation - Consultation ends June 4, then the working group will meet to discuss the community input.

OIDC Deployment - Met recently. Coordinating discussions to take place at TNC. Discussing architectural deployment profiles.

Deployment Profile - Just met. Comment period has ended and the WG has discussed those at the last two meetings. Looking at the end of June as being finished with that. Also talking about a community call to discuss the comments.

"Federation 2.0" / REFEDS group

Janemarie, Heather, and Judith have been holding discussions via email. Judith has agreed to serve as one of the co-chairs. The group needs to look strategically at where interfederation needs to go. The hope is to recruit a co-chair and spin this group up in June.

The long-tail of support and IdPs

This has simmered for many years. Service Providers in science projects, for instance, continue to have problems with IdPs providing attributes and accurate attributes. InCommon is seeing more problems with participants entering metadata using IdP software that doesn't work in the federation. Are there ways we can encourage people to participate and pay attention to email and email lists. Here are some excerpts from a TAC email thread.

- The onboarding problem
    - IdPs
    - SPs
- The 'staying connected and up-to-date' problem
- The loss of institutional knowledge problem
- The impact of the MD aggregate size - SPs no longer consuming

Possible solutions?

- Baseline will help
- Developing a test federation may help
- Should have have tiers of participants - 1) those that maintain their software and interoperate well, and 2) those that don't
- Figuring out how to address participant onboarding and communication gaps
    - Example - the attributes WG found many in their survey who weren't aware of R&S
- Part of the problem is that people stand up the IdP and figure they are finished, when really they are just beginning

- How can the policy issues get to the right people on campus? Library people? VPs for research? IT security people? [Not the federation's job to do that, but maybe provide some resources]
- Those who attend IAM Onlines aren't our target audience. They tend to be doing the right thing and know what they are doing.
- TAC is focused on federation. CACTI is focused on trust and identity more broadly. One thing might be to have a joint task force to look at Federation 2.0 and some of the challenges we've been discussing today.
- IdP proxies for people who want to live in the cloud
    - Example: Cirrus Azure IdP->InCommon proxy, should we invite Dedra Chamberlin or Mark Rank to an upcoming TAC call to discuss? Other services we should be looking at?
        - Who
        - How
        - Requirements
        - Cost
    - Hosted IdP (IdPaaS)
    - Testing environment

Next Meeting - Thursday, June 7 - 1 pm ET