InCommon TAC Meeting 2018-03-29

TAC Meeting Minutes - March 29, 2018

Attending: Mark Scheible, Heather Flanagan, Eric Goodman, Keith Wessel, Judith Bush, Eric Kool-Brown, Matt Brookover, Janemarie Duh, Mike Grady, Albert Wu

With: David Walker, Dean Woodbeck, Kevin Morooney, Nick Roy, Shannon Roddy, David Shafer, Ian Young

Ops Update

- New release of the Federation Manager (v3.2.4) fixes a bug that could prevent site admins from deleting service providers.
- The next release will include certificate functionalities for IdPs
- Shannon reported on ongoing vulnerability strategies and how to communicate when/if vendors don't fix the problem. Exploring options of partnering with REN-ISAC or operating some sort of restricted collaboration space for this purpose
- Internet2 is close to posting positions for Federation Service Manager and a Trust/Identity Support Engineer
- Self-service entity attribute support is moving up on the FM roadmap (mainly to support R&S)

Trust and Identity Updates

- Internet2 has a board meeting next week. The April meeting typically sets up the budget for approval at the fall meeting.
- Recent meeting of the Trust/Identity PAG and the TIER Campus Success Program CIOs both demonstrated interest among the CIO community to hear plans about the future of software development post-TIER program.
- The TAC agenda included the latest version of the Trust/Identity Project Portfolio

International Activities (Heather)

- Asia-Pacific Advanced Network (APAN) meeting is happening in Singapore. IAM task force (led by Terry Smith from the AAF). Nicole Harris was there. Federations talked about their challenges (particularly the newer federations). eduGAIN is a big driver, but many service providers don't know about eduGAIN, even if they are in it. Heather is working on a white paper to share with the scholarly publishers to try to help with this situation (explaining to them how to find out if they are in the eduGAIN metadata using MET.
- There is a blog post on the REFEDS website about what is happening at APAN
- RA21 - starting user testing with discovery services; release of position paper "How Identity Providers and Federation Operators Can Improve the Federated Identity Experience for their Users" expected soon - will be released first to DPWG, RA21 Advisory Committee

Working Group Updates

- Attributes for Collaboration in Federation - working on their recommendations as the result of survey and interviews. Will invite Brad Christ (chair) to a future TAC meeting, once recommendations are finalized.
- OpenID COnnect meeting - Roland Hedberg joined the call - working on use cases
- Streamlining SP Onboarding - Work is continuing
- Deployment Profile WG - reached a milestone - ready to release SAML2-int draft for community review. This will go to the community review process. There are some folks going to IIW and will start to socialize this work there.

TAC Charter

- Mark, Janemarie, Nick have been editing this to remove some out-of-date references and to reflect how TAC operates today. Particularly how the increase in Internet2 T&I staff has changed the role/relationship of TAC and InCommon Ops.
- TAC members should take a last review - also look to see if anything is missing. The intent is to provide this to Steering for their meeting on Monday, April 2 (although they are unlikely to act on this until their May meeting).

Okta and Other Identity as a Service (IDaaS) providers

- Nick discussed issues with Okta, specifically and Identity as a Service providers in general. Mainly, these vendors do not handle metadata consumption or multilateral federation well (if at all). One of the issues is the entityIDs that are generated and whether the customer (e.g. the campus) can control the name space. If not, these entityIDs do not meet InCommon requirements (must be in a domain owned by the organization). This has led to the perception that "you can't run Okta in InCommon," which is not true. Okta now, in fact, allows their customers to create their own entityID. The problem still remains that they can't consume metadata, which also means no support for R&S and other entity attributes
- A recent post on the educause IDM list discussed someone setting up a proxy to deal with this situation.
- There is concern that campuses that purchase an IDaaS vendor solution are limiting or preventing their use of multilateral federation in the future. Should these types of implementations (that don't really support federation) even be allowed into the federation?
- Nick - had an interesting discussion internally this morning about some help desk tickets coming in that shows people don't understand multilateral federation.
- The implementation profile work is very helpful, as will be the SP onboarding work. However, this will continue to be an issue that we, as a federation operator, will need to think about.

Next TAC Meeting - April 12th

Chris Phillips (Canarie) will talk to us about ADFS as a federation IdP and, in his role as chair of CACTI, will discuss areas of potential partnership with TAC

Global Summit

Clarification that there is no formal TAC meeting at the Global Summit. Those that are there may get together informally or for dinner.

Next Meeting - Thursday, April 12 - 1 pm ET