

InCommon TAC Meeting 2018-06-21

Minutes

Attending: Mike Grady, Judith Bush, Mark Scheible, Heather Flanagan, Janemarie Duh, Eric Kool-Brown, Matt Brookover

With: Steve Zoppi, Ian Young, David Walker, Shannon Roddy, Dave Shafer, IJ Kim

Regrets: Ann West, Nick Roy, Dean Woodbeck

Trust and Identity Updates

TNC - Many were at TNC last week (Steve). Discussions around RA-21 and other things of common international interest. Identity providing services continues to come up. A recurring theme - there is a need for additional (and younger) people to develop interest in this area. This topic will be slated for brainstorming/discussion at a future TAC meeting.

Ops/Security Updates - Federation Manager API is in development, initially for internal use. Working on a proof of concept for the architecture for MDQ. Baseline Expectations monthly metadata health checks continues and the numbers continue to improve.

Working Groups

Streamlining SP Onboarding - No call this week. Continuing to work on feedback to the WG report. Still on target for wrapping up this month.

Attributes for Collaboration and Federation - Brad Christ will present the working group's final report and recommendation at the July 19th TAC meeting, and will then present to Steering in August.

OIDC Deployment - Roland announced the [OIDC federation spec draft](#) is open for comment. He is also encouraging people to join the OpenID foundation (\$25 per year for individuals; \$100 per year for non-profits)

Deployment profile - Reviewing comments on the draft report and editing the draft

International Update (from Heather via email)

REFEDS meetings - The REFEDS meeting at TNC was extremely well attended with over 75 people. We had 22 presentations over the course of the day, and the slides are all online: <https://refeds.org/meetings/38th-meeting>. The meeting was not recorded, so those slides and the names associated with them are the place to start to catch up on topics of interest. The next REFEDS meeting is MONDAY, October 15, in Orlando. Registration (free) happens as part of the TechEx registration process: <https://service5.internet2.edu/reg/events/techex-18/registrations>

REFEDS and the proposed Federation 2.0 WG: On the one hand, lots of interest. On the other, all the non-US people I've approached are too busy to be willing to take up co-chairing the proposed WG. I'll be discussing this with the REFEDS Steering Committee next week.

RA21 update - The RA21 co-chairs and the technical architects for both academic pilots met in a formal bake off on June 7 in London. I'm working on the official write up out of that meeting, but the short, short version is that RA21 will be moving ahead with just the P3W pilot program. Note that from a purely technical perspective, the security and privacy evaluation of the two pilots indicated there was really very little difference between the two. What data is moving around is of very low value and low risk, so the fact that one pilot (the WAYF Cloud) stores that data in a central database was not considered a showstopper. However, technology is one thing; human perception is something else entirely. Anything that stores data (even just a device ID) in a central place is considered problematic. There is no additional functionality offered by WAYF Cloud that makes that concern worth tackling.

The next steps for RA21 are to write up the evaluation and recommendation, to continue with the next level of UX work, and to start formal governance discussions. Several interested parties who want to be part of governing a central discovery and WAYF persistence service are hoping to meet immediately before TechEx. I'll be able to share more information about the outcomes of that at our TechEx TAX meeting during the week.

APAN and TF-IAM: The Identity and Access Management Task Force will be meeting in Auckland August 6-7. I will be there along with Nicole Harris, Brook Schofield, and of course many of our Asia-Pacific federation colleagues to talk about the latest activities in regional federations, how those federations can start their own outreach programs, technical info sharing, and so on.

TAC Membership for 2019

A couple of things to consider: 1) the need for new/younger participants, and 2) the range of institutions represented. First step is to review the representation on TAC, then look at the type of representation we might need (in terms of work items, for example). [This wiki page](#) will serve as the coordinating point.

TAC Priorities for the next six months

There was discussion about potential new working groups to develop to work between now and the end of the year:

IdP as a Service (for InCommon) - Would this be a hub and spoke configuration with one IdP? In Denmark, for instance, the federation handles all of the contracts with service providers. Each IdP then can, for instance, decide which services they want to use.

Another option is a multi-tenant IdP. In this model, the service providers see the different tenants. WS02 is a provider and has source code for a multi-tenant IdP.

Steve - this hits on the question of the model we envision. Steve outlined some of the issues he sees:

- A vendor sets up your IdP, but then things like attribute release policies get threaded through the vendor.
- The multi-tenant implementation gravitates to one-size-fits-all. This also leads to support issues when something goes wrong. The vendor likely uses clones for each instance, so is overwhelmed by support calls from all of its clients.
- Multi-tenant might be the solution, but without the one-size-fits-all nature of vendor implementations.
- We are making architectural choices now, but we need to get a feel for the managed service that might work for smaller institutions. This probably won't work for larger institutions that have high transaction rates.

Mike Grady - what Unicon is seeing are institutions setting up Okta or something similar, then they need the Shibboleth layer.

The big question, then, is how we will structure such a thing and seek and respond to requests. Unicon is seeing the need and looking at how we will respond, but is looking at a scaled-down hosted solution where you are only dealing with the federation layer.

Steve suggests making no assumptions about today's mode of operation, but focus on what we need to do to support our community and then align our services accordingly. Rather than looking at what we do today, we need to look at what services we provide and how we will look in the future.

Federation 2.0 Working Group - This would be a REFEDS working group and is in the process of recruiting a European co-leader (late breaking update from Heather - two US co-chairs would be acceptable). This work might help inform the IdP as a Service topic.

Communication Working Group

- How do we reach those campuses that haven't heard of InCommon? This comes from the Attributes for Collaboration and Federation working group. This is part of their "Building a Bigger Tent" recommendation. "Communication" was a common theme throughout the Global Summit. The message is not being delivered (either to the right communities or with clarity)
- Heather - One of the things that has worked for RA21 is an outreach committee. They keep an eye on calls for proposals at appropriate conferences. They also periodically review the slides and other messages to ensure they are clear and appropriate

Education

- Use the early CAMPs as a model, where the focus is on bringing people up to speed on what campuses are doing, or on specific topics. Even though topics may have been presented before, the new people have not seen those.
- In tracks like the executive track at Global Summit, it would be useful to spread the message that this is *their* problem, too. That they need to educate and nurture their younger staff members.
- Better training opportunities for "newbies"/younguns
 - IAM
 - Shibboleth
 - OIDC
 - Docker/TIER Software

Documentation

- Provide a reference or central place to find documentation
- Improved wiki/website for InCommon and related topics
- ADFS support and recommendations
- OIDC use - While the "deployment" WG is still in place, are there opportunities to promote OIDC use or adoption alongside of Shibboleth?
- TIER software - documentation that introduces and explains the software and use for someone who is new. Why should I use this? We need to make the documentation findable and useful.

MDQ support - Is there anything the TAC can/should do to help with MDQ?

TechEx Schedule and TAC Meeting

The TAC meeting and other face-to-face meetings will be listed on the program later, but TAC will meet at TechEx.

Next Meeting - July 19, 2018 - 1 pm ET