InCommon TAC Meeting 2020-06-04

Minutes - June 4, 2020

Attending: Heather Flanagan, Mary McKee, Janemarie Duh, Mark Rank, Mizuki Karasawa, Keith Wessel, Matthew Brookover, Judith Bush, Eric Kool-Brown, Eric Goodman

With: Les LaCroix, David Bantz, Dean Woodbeck, Nick Roy, Jessica Fink, IJ Kim, Dave Shafer, Albert Wu, Steve Zoppi, David Walker, Shannon Roddy

Intellectual Property Reminder - All Internet2 activities are governed by the Internet2 Intellectual Property Framework.

Public Content Notice - TAC minutes are public documents. Please let the TAC and note taker know if you plan to discuss something of a sensitive nature.

T/I and Ops Updates

- Minor patches made to the new version of the Federation Manager to fix some bugs
- Need to update middleware libraries for our integration with Cloud HSM for metadata signing. Ian Young is helping with that.

International Report

Next week would have been both TNC20 and Identiverse 2020. TNC20 was cancelled, along with the associated side meetings (e.g., REFEDS). Identiverse, however, was moved to an 8-week series of sessions that anyone can watch:

https://identiverse.com/detailed-agenda/

Identiverse tends to put on a solid conference, so I strongly encourage you to go check out the agenda and make time to sit in on a session or two, or three, or ten. These will also be recorded and posted on YouTube at a later date.

There are a few other virtual meetings going on that are likely of interest:

 1- UK federation "Town Hall" sessions across a whole week of 8th-13th June (at lunch times 1-2pm), using Zoom. Contact Mark Williams (Mark.Williams@jisc.ac.uk) if you're interested in attending. Topics will include:

- Baseline in the UK federation
- CoC, R&S, Sirtfi & other attributes
- Shibboleth health check lessons
- Publisher round table: Ask anything
- SSO & aspects of content piracy
- Delegated authority
- Readiness for Shibboleth v.4
- VerifID: Commercial Student Verification
- About T&I Consultancy

2 - GÉANT Data Protection Code of Conduct update, 8th June 2020 at 11:00 CEST: "The team working on the next generation of the GÉANT Code of Conduct would like to give an overview of where progress is with version 2 of the Code following on from feedback from the Dutch DPA." This is a bit early for US participants, and several people have asked if the session will be recorded. Rumor has it that it will, but regardless notes are likely to be available after the session.

Seamless Access Update

The beta phase for SeamlessAccess is officially being extended through at least this calendar year. There are several things still going on that basically see us "kicking the tires" to see what's working and what isn't. There was a webinar on how some of the expected browser changes will impact identity flows, including the SeamlessAccess IdP discovery and persistence process, which might be of interest:

https://www.niso.org/events/2020/05/browser-changes-and-identity-federation-impact-identity-flows

Heather did a presentation on Seamless Access Entity Categories and Attribute Bundles WG.

- Working with various constituencies (libraries, service providers, others) to develop categories to make it easy for an IdP to configure for non-R&S entities. Also to offer common language/terms expectations to feed into contracts.
- Proposing three categories
  - Does not affect bilateral agreements
  - User consent is out of scope
  - Category must not be used in combination with other categories (example, can's be authN-only and R&S
  - Wants successful authentication and just enough information to make authorization requirements (organization and entitlement)
  - Organization identifier, entitlement data, pseudonymous pairwise user identifier
  - Authentication Only - no attributes at all. Just need to know that the authentication is successful.
  - Anonymous Authorization
  - Pseudonymous Authorization
- Working group is almost finished, then will pass this to REFEDS where the Schema Board will conduct a public comment period (likely 6 weeks long), which will be open to a broader group than the REFEDS usual suspects.

There was discussion about the role of the federation and of the IdPs in this process.

Prioritizing Deployment Profile WG recommendations

Deployment Profile WG Survey Responses

Deployment Profile WG report

Keith referred to the new OASIS identifier attributes.

- These were rated in the survey as needed but hard to implement
- We should plan on a communication effort for adoption

What are the next steps?

- Transition is the most challenging thing. For example, this will be a challenge for use in R&S. When will an IdP know when the change has taken place?
- From InCommon operations - we're at a point where this is viable. The IdPaaS work paves the way for this on the IdP side.
- Seamless Access draft lists the expected attributes. An appendix discusses how to deal with legacy stuff.
- Keith recommends a phased plan for adding these to the FM and providing guidance on use. Marketing to IdP operators on configuration when asked for these. Another concern is the defaults in Shibboleth. Update the documentation on identifiers.
- Start with the federation making a declaration of which identifiers are supported (e.g. you should be asserting subject identifiers). Then provide some information about how you map these new identifiers to your existing identifiers.
- Likely track adoption rate to determine when to push these to Baseline Expectations
- Over time, we push the new identifiers and don't talk about the old ones. At some point we can then drop the legacy identifiers

Next step to sketch out a plan (AI - Keith)

Next Meeting - Thursday, June 18, 2020