InCommon TAC Meeting 2019-05-23

Minutes

Attending: Janemarie Duh, Mary McKee, Judith Bush, Heather Flanagan, Eric Goodman, Jessica Coltrin, Judith Bush, Matt Brookover, Michael Grady

With: Nick Roy, Dave Shafer, IJ Kim, James Babb, Ian Young, David Bantz

Action Items

- (AI) Nick: prepare a summary of proposed actions for adoption of OASIS SAML Subject Identifiers in InCommon Federation
- (AI) Mary: post to technical-discuss@incommon.org about the stable identifiers challenges
- (AI) Janemarie: give update on badging subgroup on next TAC call

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 Ops Update

- SAML 1.1 entity descriptors
  - May not be useful
  - Ops reach out to the IdPs and SPs (AI: Nick and Babb)
  - Keep TAC updated on these
  - Suggested that these should be considered by CTAB as a possible thing to handle in Baseline 2.0 - David Bantz will take to CTAB for consideration
- Update on FM planning/Internet2 Collab Platform integration/etc.

International Update

- 173 submissions resulting in 203 comments for RA21 comment period. Will be reviewing with RA21 leadership in San Diego next week.
- Eric Goodman and Nick Roy left comments

Working Group/Collab Updates

- OIDC Deployment - meeting this week cancelled due to illness
- REFEDS 2.0 - reviewing comments from surveys, interview feedback, using as input to conversations in Tallinn
- IdPaaS - three calls, good participation, getting together a survey to get a sense for what the market looks like. Getting heads around 'what will allow this to get the momentum it needs with people making purchasing decisions?' Trying to figure out how to get something meaningful from CIO-level respondents. What is compelling to leadership?
- CACTI - possible open meeting at TechEx, eduroam advisory council; overlap of IdPaaS for both RADIUS and SAML, IDPro body of knowledge discussion (Heather is IDPro principal editor).
- CTAB - Baseline 2.0 work

Support for new SAML subject identifiers

- Very early stages of figuring out what to do about this. Deployment profile WG knew that needed to have consistent identifiers. eduPersonTargetedID and SAML2 persistent nameid is subject to significant security risk – some apps handle identifiers as case-insensitive while these are meant to be case-sensitive. Looked at work in OIDC. Want to do something similar to OIDC so that vendors do not have to be able to use eduPerson SAML attributes. Nice because works better between SAML and OIDC. Also attributes defined at OASIS level so these are no longer education specific.
- Signaling mechanism -> SPs can request the type they want and as long as IdP can respond, it will work. Syntax defined to how to express the needs.
- Probably should add support for these new attributes to InCommon Federation Manager. But chicken & egg - IdPs aren't ready yet so not good if SPs are going to start asking.
- Probably need an education campaign and to get these attributes baked into the out-of-the-box TAP containers.
- Thoughts?
  - Published by OASIS: http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html
  - No choice about subject format going forward - has to be transient.
  - Identifier then becomes an attribute.
  - Just need to be thoughtful about the steps involved going forward: webinar, TIER packaging changes, etc. around the time we add it in to the Federation Manager.
  - Highly unlikely that existing apps are going to want to switch. Target audience for this is really new applications, new collaborations.
  - Lots to untangle. Are these attributes from the deployment profile?
  - Fundamentally, this is the thing the deployment profile recommended, but ran it separately through OASIS.
  - Non-education profile out there (healthcare through Kantara) is adopting the subject saml id.
  - Going to take a while to get this change to percolate throughout the community for widespread adoption. Federation Manager change is going to be the easiest part.
  - Probably will need to be added to R&S too.
  - Do we eventually do a Baseline 3.0 like in 2021 to require IdPs to support this? Challenge of wanting to make sure that IdPs are out there to respond to what the SPs are requesting.
  - REFEDS schema editorial board has a workplan for this - taking Scott Cantor's suggestions and incorporating them in it.

- Another challenge: on the IAM system side of things there are a lot of systems out there where a stable identifier does not exist. May be something that IdPaaS supports these identifiers but that means it needs a stable source of person identifiers.
    - Duke does have this but it is not federation-friendly.
    - May want to post about this to technical-discuss@incommon.org
    - Duke has a complicated use case for this: how do we create immutable identifiers for everyone and everyone that we track? Need a standard identifier to handle that there are both internal and external identifiers currently. Want to get ahead of that question.
    - Surprising how many big institutions that do not have an internal identifier that could be used to build out the identifiers for this.
- Going forward: short written summary on what was talked about above. AI: Nick write up draft recommendations for InCommon implementation, share with TAC.

TAC workplan for second half of 2019

- Streamlining SP Onboarding and Attributes for Collaboration Working Group responses - most items in-progress or complete
- Training program - in progress
- Test federation - will review in the future
    - Also a working group recommendation. Likely a WG to gather requirements. May need input from the badging conversation. Will follow up after next badging subgroup call.
- Baseline expectations - CTAB in progress
    - Also badging conversation - one meeting so far. TAC subgroup. Will meet tomorrow. AI: Janemarie give update on next TAC call. David Bantz participating as well.
- Follow up to Deployment Profile work - September/October-ish
    - Revised SAML2int is at Kantara
    - Need the R&E Profile WG in the fall timeframe
- Onboarding for new TAC members
    - Could be helpful to have a one-pager available before the first call. Getting into the wiki before the first call and poking around was helpful.
    - Some of this is in the call for nominations email
    - Some of this is in the charter
    - There are several new members on the call - would something around this be valuable?
    - Onboarding for new TAC members this year will be affected by the lateness of TechEx. Will discuss on the next call.
    - Might be worthwhile checking with those who turned down nominations about why. Was it just the time commitment, or other concerns that we could address with nomination materials, onboarding materials, etc? Will take up in next week's discussion.
- Maturity model outline - fits into badging. That's basically what it is. Gets rolled into badging.
- Nick OK with removing the completed items from the backlog. Suggests following up with the working groups (Streamlining SP Onboarding, Attributes for Collaboration) to let them know "We heard you. Here's what we're doing."
- Two items left in parking lot
    - REFEDS SP Operator WG spinning up. This may be the place for that.
    - Eric G submitted a TechEx session on SP proxy as well. May make sense to follow up on this after the session if it gets accepted. Or ACAMP session if not accepted.
    - IdPaaS WG touches on at least one potential solution to this.
    - Eric G got questions about ADFS and Azure as an SP recently from his user community.
    - SAML SP frontend.
    - ADFS as IdP.

Next Meeting - June 6, 2019 - 1 pm ET