2021-Sept-21 CTAB Public Minutes

CTAB Call Tuesday, Sept 21, 2021

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska (vice chair)
- Pål Axelsson, SUNET
- Ercan Elibol, Florida Polytechnic University
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Jon Miner, University of Wisc - Madison
- Andy Morgan, Oregon State University
- John Pfeifer, University of Maryland
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Robert Zybeck, Portland Community College
- Tom Barton, Internet2, ex-officio
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Ann West, Internet2
- Albert Wu, Internet2
- Netta Caligari, Internet2
- Emily Eisbruch, Internet2

Regrets

- Rachana Ananthakrishnan, Globus, University of Chicago
- Richard Frovarp, North Dakota State
- Meshna Koren, Elsevier

DISCUSSION

- Intellectual Property reminder

Working Group updates

- **R&S 2.0 WG updates** - draft of **Personalized Entity Category** profile to complement Anonymous and Pseudonymous
  - community consultation now open for comment -- Consultation
  - Draft
  - Overview: Candidates for the Personalized Entity Category are Service Providers that have a proven need to receive a small set of personally identifiable information about their users in order to effectively provide their service to the user or to enable the user to signal their identity to other users within the service.
  - There will be an ACAMP session on this topic
  - Q - Is this a different model for the same reason as we talk about using consent?
  - A - Yes, it is related. Some orgs cannot use consent
  - In the US there is a concern around the extent to which institutions will rely on the federation operator to make authorization decision
  - This is related to getting registrars to agree that complying with the Research and Scholarship Entity Category is a good enough reason to release data
  - CTAB needs to promote use of entity categories
  - We should be sure our community understands what the entity categories are and can apply them appropriately
  - DavidB:
    - this version of the profile tries to ease the transitions.
    - You can keep using eduperson, send some values of eduperson assurance to indicate how much it's a unique identifier
    - Concern people won't be motivated to do the right thing
    - Will still be hard to rely on IDPs to adopt a new entity category
    - We should have moved to subject-ID,
  - EDUCAUSE IAM has a conversation going that suggests CIRRUS Identity as a solution
    - http://listserv.educause.edu/scripts/wa.exe?A1=ind2109&L=IAM&X=O210B17B0CC95DBFA36#1
  - There is time for CTAB to provide collective comments on the consultation if we want

- **InCommon TAC updates**
  - Discussion on subjectID adoption models and ways of improving uptake of deployment profile
  - Steering endorsed InCommon adoption the deployment profile
  - Rolling it out all at once could be too challenging

- Has divided the profile into 4 portions
  - Already adopted
  - Should quickly adopt
  - Will take time to implement
  - Not practical
- Preparing new section of wiki with this deployment profile info, hopefully prior to CAMP

- REFEDS Assurance Working Group
  - Group working on version 2.0 REFEDs assurance framework
  - To clarify community assurance levels
  - Draft Recommendations are here
  - Focused last meeting on relative roles of local enterprise and on low, medium and high assurance profiles
  - Not sure when consultation will start, likely before end of year
  - On Oct. 4 there will be an update at CAMP from Jule and Brett

- REFEDS MFA sub group
  - Focus is on creating more concrete documentation for questions like am I allowed to do xyz (e.g., fail open, use bypass, etc), and practical recommendations for implementation,
  - Eric and DavidB: struck by the recommendation to NOT use REFEDs MFA internally in your institution
  - FAQ
  - Albert: regarding the local use issue, there may be changes in future edition of the REFEDs MFA profile
  - Two wiki spaces: Assurance space and profile space…. Need to consolidate. Looks like the profile wiki space should be authoritative

Review/refresh Community Dispute Resolution Process (Brett)

- Dispute Resolution Process diagram is helpful
- http://doi.org/10.26869/TI.118.1
- Background: In 2018, when CTAB was launched (from what had been the Assurance Advisory Committee) we developed first iteration of Baseline Expectations. Community Dispute Resolution was a process for community to police its own
- Phases of dispute resolution:
  - 1. community resolve among themselves
  - 2. reach out to InCommon, if its an incident, there is an incident response plan
  - 3.. If the concern has merit, InCommon will track and assist in the resolution process
  - 4. If that does not work, it moves on to CTAB for review
- CTAB referred to the dispute resolution process towards the end of Baseline Expectations 1 process, in outreach and figuring out what to do about non-complying organizations.
- We may want to have a refresher with the community on dispute resolution at some point

- CAMP planning - what does CTAB want to accomplish at CAMP/ACAMP?
  - Hope for feedback from community
  - Can present BEv2
  - Can talk about BEv3 - Assurance and MFA
  - Quit saying R&S?
  - Soliciting new CTAB members will be important
    - There will be a callout for recruitment on the main Canvas page for CAMP/ACAMP
  - At CAMP, CTAB is doing a presentation along with other advisory groups
    There will be a social hour / camp fires / open Zoom rooms

BEv2 Office Hours

- Note: there is a BEV2 office hour on Tuesday, Sept 28 at 1pm ET
- Perhaps solicit input for our CAMP and ACAMP presentations

Develop process to adjudicate Endpoint Encryption disputes (David)

- Settle larger issues around endpoint encryption
- Based on recent CTAB calls, CTAB wants to move ahead with:
- Assumptions
  - SSLLab grade of “A” (as measured by InCommon) is the bar for success
  - If an entity does not have A, follow up action is needed…
- Question: is endpoint encryption a requirement on RFPs?
- Does not support TLS versions lower than..
- Answer : it is part of the procurement process
- Follow Up Actions
  - Varies depending why not A
    - Requires response / request from non-comforming participant
    - And Plan to remediate
    - CTAB grants extension to warranted good faith remediation efforts
      - How long of an extension? Can we avoid individually tracking entity extensions and instead use a standard timeline for all entities in the federation and this particular baseline expectation.
    - How do we deal with entities we cannot test from InCommon side?
  - Need to define cadence, pattern, and tracking of reminder/follow ups

- Assign roles and responsibilities

- Eventually SSL Labs will change criteria, in which case all organizations will drop in score.
- Need a process for extension, then move on to dispute resolution
- The more explicit the procedure, the easier it will be
- Default: we create an extension process, if they fall into one of the conditions we automatically provide extension period, after that we do testing, at some point non complying entities go into dispute resolution process
- Didn't we settle on 90 days as a default? With the idea we would revisit that.
- Dispute resolution process does not have any time limits
- 90 days is about CTAB initiating a process
- Proposing we keep things in the 2nd stage, extension tracking process
- If you go past 90 days extension then you bump into stage 3
- Good idea to focus on stage 2
- Info provided by InCommon to its members about the SSL labs changing evaluation criteria
- Everyone has 90 days to catch up
- Self service
- Tweak process to have end of quarter cycles
    - Submit extension, you have whatever is remaining in term plus 90 days
- For entities we cannot test, such as in the case of test SPs or test IDPs that are not open to the Internet, we may have different way of handling

AI - Albert will create a Brett-friendly™ diagram for the process.

Next CTAB Call: Tuesday, Oct 5, 2021