

2021-Sept-7 CTAB Public Minutes

CTAB Call Tuesday, Sept 7, 2021

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska (vice chair)
- Pål Axelsson, SUNET
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Meshna Koren, Elsevier
- 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
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Albert Wu, Internet2

Regrets

- Rachana Ananthakrishnan, Globus, University of Chicago
- Jon Miner, University of Wisc - Madison
- Robert Zybeck, Portland Community College
- Tom Barton, Internet2, ex-officio
- Ann West, Internet2
- Emily Eisbruch, Internet2

Discussion

Intellectual Property reminder

Working Group / Related Committee updates

- [InCommon TAC](#)
 - InCommon TAC has been discussing subject identifiers
 - also focusing on CAMP / ACAMP planning
- [REFEDS Assurance WG](#)
 - At last meeting, addressed identifier uniqueness and eduPersonPrincipalName
 - Next meeting, looking at section on identity proofing
 - [Draft Recommendations](#)
- [REFEDS MFA Sub Group](#)
 - Working on FAQ for MFA profile
 - Categorizing questions and adding high level navigation so people can find answers
 - May present recommendations on the future MFA profile
 - Not touching the current MFA profile
 - Next week: Two hour call to wrap up the FAQ work
- [Entity Categories Working Group](#)
 - AndyM and DavidB participating
 - The R&S Working group has been working on a new entity category called Personalized Entity Category.
 - This is in connection with [Anonymous Authorization and Pseudonymous Authorization](#)
 - Meeting notes: <https://wiki.refeds.org/display/GROUPS/Entity+Category+Development%3A+Meeting+Notes>

BE2 Progress - [Dashboard](#)

- Resumption of biweekly email notices around BEv2 led to a slight uptick in compliance
- Albert will start to create the dispute resolution docket
- Still 1000 Service Providers with a score of B
 - Could be one organization with a large number of SPs

- Reminder that results shown on the dashboard graph do not include endpoint encryption score
- There is an asterisk on Federation Manager for those who do not meet the Qualys SSL Labs score of A
- There is a trend to greater compliance with each Qualys SSL Labs scan we conduct.

Endpoint Encryption Scenarios review

- How should we communicate to the community around endpoint encryption?
- Issues around how to track
- Will we require some level (A or B) ?
- We will have to decide as we get closer to December/January
- At the last CTAB call, there was discussed of Scenario 1: **Legacy Browser Support**
- It may be reasonable to grant an exception if the organization is doing mitigation.
- Challenge of CTAB's long-range tracking responsibility once we provide an exception to an organization around endpoint encryption
- Suggestion: if an entity requests an exception, it should need to be renewed on a periodic basis
- Scenario 3: **External monitoring tool compatibility**, comes from one commercial vendor who made that claim. It is likely a one off, so we likely should not place too much emphasis on it.
- If we spin up too heavy a tracking mechanism, it can be too much work for InCommon operations
- Albert: we need to think of the purpose of Baseline Expectations
 - Is it our responsibility and obligation to police/enforce?
 - Or rely on the dispute resolution process?
- Perhaps we only remove entities with a failing Qualys SSL Labs grade? But not work to remove those with a B grade?
- The requirement for grade A in SSL Labs score is not required in the Baseline Expectations primary document
 - it is in the implementation guidelines document
- KevinM: The Federation Operator is not the accountability enforcement persona for Baseline Expectations
- Accountability enforcement is peer to peer responsibility through the [community dispute resolution process](#)
- We are working on
 - 1. making the federation better and more trustworthy
 - 2. making using federation easier
 - *These two are sometimes at odds, and CTAB has to manage this*
- There is no silver bullet answer to the question of how to "enforce" the secure endpoints requirement
- One scenario is for CTAB to refrain from trying to enforce the secure endpoints requirement and allow SPs that are concerned to use dispute resolution
- DavidB: CTAB should not allow 200 or even 100 non conforming IDPs. CTAB should take steps to increase compliance.
- Use case: a member of CTAB is not getting an SSL Labs A grade for the IDP at his campus.
- Does not "own" all the infrastructure involved.
- There is a need to update scripts, this may not be an organizational priority right now.

Discuss via email

- CTAB at CAMP - what would CTAB like to talk about? How would CTAB like to leverage ACAMP?
- Aug 31, 2021 Office Hour Recap
 - Office Hour Notes:
 - <https://spaces.at.internet2.edu/x/7IQTD>
- (time permitting, but will need more than 10 min) Happenings in entity categories - primer and next steps
 - SA Entity Categories (anonymous and pseudonymous)
 - R&S 2.0 (or "Personal" entity category to complement anon and pseudo-anon)
- Upcoming election: member rotation / recruiting / etc.
- Upcoming: review Dispute Resolution process (for next CTAB call)

Next CTAB Call: Tuesday, Sept. 21, 2021