2021-May-18 CTAB Public Minutes

CTAB call Tuesday, May 18, 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
- Jon Miner, University of Wisc - Madison
- Andy Morgan, Oregon State University
- Dave Robinson, Grinnell College in Iowa, InCommon Steering Rep, ex-officio
- Robert Zybeck, Portland Community College
- Chris Whalen, Research Data and Communication Technologies
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Ann West, Internet2
- Albert Wu, Internet2

Regrets

- Rachana Ananthakrishnan, Globus, University of Chicago
- Tom Barton, University Chicago and Internet2, ex-officio
- John Pfeifer, University of Maryland
- Jule Ziegler, Leibniz Supercomputing Centre
- Emily Eisbruch, Internet2

DISCUSSION

- Intellectual Property reminder
- Agenda Bash

Working group updates

Assured Access Working Group (Brett)

- https://spaces.at.internet2.edu/x/XImeCg
- Wrapped up draft of the guidance document titled REFEDS Assurance Framework Implementation Guidance for the InCommon Federation
    - Next step: community consultation for the draft guidance document

- AI Brett - prepare notice of the community consultation to the InCommon community with instructions on how to provide feedback and work with Albert and David on timing (done)

- Update as of May 24, 2021 - the Community Consultation is open here: https://spaces.at.internet2.edu/x/M49YCw

- Suggestion of 30 days for this community consultation. The Assured Access Working Group can monitor how the feedback is coming along and determine if more promotion of the consultation is needed.
- Once feedback on the guidance is received, the working group will review that feedback and make final adjustments
- This is a guidance document to accommodate assurance requirements from NIH and potentially other organizations. This guidance document does not alter any practices of InCommon. Formal approval may not be needed.
- This guidance is not policy, but has implication of becoming convention for how to establish assurance in federation
- The guidance will likely evolve
- Community consultation provides opportunity to receive feedback and to help get the word out to the community
- Albert: On the last NIH Technical Coordination call, the group realized something about implementation of the REFEDs assurance framework that had been missed.
  An InCommon IdP meets the RAF Conformance criteria defined in section 3 of RAF because it must adhere to InCommon Baseline Expectations.
  Document should instruct the IdP (InCommon IdP) to always assert the https://refeds.org/assurance value via eduPersonAssurance to indicate its RAF conformance in accordance with RAF Section 3.
  This input will be fed into the draft document via the community consultation process.

Potential New CTAB Working Group to look at issues around increasing trust in federation (MFA, R&S and Assurance) (Andy)

- Next steps for this potential new working group (led by Rachana and Andy) are not clear at this point
- Wait until Rachana is available

- **AI Andy and Rachana will touch base around the Potential New CTAB Working Group to look at issues around increasing trust in federation**

REFEDS MFA SubGroup (Albert)

- https://wiki.refeds.org/display/GROUPS/MFA+Subgroup
- Group met for the first time on Monday, May 17
- Will meet weekly for next several weeks to produce early set of recommendations
- This is a multi part effort, to work out broader issues on how to signal
- This is an open group, open to new members

REFEDS Assurance Working Group (Pal)

- https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group
- Starting up work, meeting on Thursdays

Baseline Expectations v2 Status and Next Steps (Albert)

- Baseline Expectations V2 adoption rates are climbing steadily
- Every time we sent out an notice, there is a climb
- We are at about 36% of orgs adhering to Baseline Expectations v2
    - Does not include SSL Score
    - Includes Error URL, SIRTFI status , and whether the endpoint is encrypted at all.
- Now sending notices only to InCommon Site Admins
- It is likely time to broaden the bi-weekly notice to include the InCommon Execs, in addition to the Site Admins
- Most common Feedback to the notices
    - “What do I do about SIRTFI?” and
    - “Which entity is missing what?”
- Moving forward, we plan to point alert/notice recipients to the Federation Manager to simplify the emails.
    - The answer to the question of “which entity is missing what?” is in the Federation Manager

- **Important Topic: How do we frame endpoint encryption rating relative to Baseline Expecations v2 adherence status?**
- If we include SSL score, the BEv2 compliance number drops into the teens (from 36%)
- Most endpoints are encrypted, but SSL scoring has a lot of endpoints with score of B
- Albert: currently more orgs are getting a score of A instead of a score of B.
- About 20% of endpoints could not be reached through SSL scoring, for various reasons
- SSL scoring is complex, it’s a moving target
- What should constitute adherence?
- How will we enforce the secure endpoint requirement?
- Logistics of handling at scale is an issue
- It is problematic to drop metadata of those not achieving SSL score of A
- There are many such entities and the scores can change at any time
- At recent BEv2 Office Hours, there were compelling reasons expressed why orgs will not get SSL score of A
- Could handle through waivers, but handling and reviewing the waivers will take a lot of resources
- In hindsight, perhaps CTAB should have pinned standard to something that will not change (instead of SSL score)
- Some community members are saying “I can’t get an SSL labs score of A because I must support older software”
- Some organizations have competing priorities for staff before the issues of TLS can be addressed.
- We are enforcing something (Secure endpoints) that orgs should be doing, but they may not be.
- Initially it’s an informational effort.
- To what extent do we (CTAB) chase that down?
- If there are 20 to 30% out of compliance, what should CTAB do?
- As InCommon operations tests for SSL score, inform the InCommon Site Admins.
- Inform CTAB if percent of orgs out of compliance reach a certain threshhold
- Give orgs time to work it through
- Shannon (InCommon Operations) can how perform SSL scans in about one week
- Suggestions
    - Change the consequence for not meeting the secure endpoint requirement to being published in a less public listing, but still where other participants can see it (instead of having metadata removed after remediation period).
    - CTAB promote the approach that orgs strive to achieve SSL score of A and try to stay at A, but not focus on enforcement
    - We function as a mirror to the organizations

Reflection on May 12, 2021 IAM Online on Increasing Identity Assurance and Improving NIH Readiness

- Went well
- Slides: https://www.incommon.org/wp-content/uploads/2021/05/doc-IAM-Online-May-2021.pdf

Did not get to this item on the agenda

- (10 min) Implications of the Deployment Profile recommendations
    - What is Deployment Profile?
    - What does “adopt” mean?
    - What are the implications if InCommon adopts it?

Next CTAB Call: Tuesday, June 1, 2021