2021-Aug-10 CTAB Public Minutes

CTAB Call Tuesday, August 10, 2021

Attending

- David Bantz, University of Alaska (chair)
- Brett Bieber, University of Nebraska (vice chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- Ercan Elibol, Florida Polytechnic University
- Richard Frovarp, North Dakota State
- 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
- Tom Barton, Internet2, ex-officio
- Johnny Lasker, Internet2
- Kevin Morooney, Internet2
- Ann West, Internet2
- Albert Wu, Internet2
- Netta Caligari, Internet2

Regrets

- Pål Axelsson, SUNET
- John Pfeifer, University of Maryland
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Robert Zybeck, Portland Community College
- Eric Goodman, UCOP - InCommon TAC Representative to CTAB
- Emily Eisbruch, Internet2

Discussion

- Intellectual Property reminder

Recap of InCommon Steering update

- DavidB provided an update to InCommon Steering last week.
- Slides were emailed to CTAB.
- Highlights:
    - We are ahead of where we were in the cycle with Baseline Expectations V1.
    - We are approaching 80% compliance for BEv2
    - On track to have almost complete compliance by the end of 2021.
    - Will need to handle a small number of non complying entities at the start of 2022.
    - At some point in the future, probably in Baseline Expectations v3, CTAB will need to deal with entity categories and with Assurance
- KevinM: David B provided an excellent update to InCommon Steering, thanks.

BEv2 Office Hour August 3, 2021 - debrief

- BEV2 Office Hour went well
- Many questions about encouraging ADFS or Azure to join the InCommon federation
- ADFS:
    - issue of **policy issues** of how organizations stand up IDPs
    - Most using ADFS or Azure are running enterprise SSL solution
    - ADFS working with Shibboleth
    - Meshna: is the question around ADFS a technical question?
    - Albert: there are several scenarios
    - Issues w metadata because of how ADFS or Azure makes use of metadata
    - Compatibility with what federation requires
    - Consumption of InCommon metadata becomes an issue
    - How to "grab" the aggregates
    - How entity ID is named
    - Can't choose entity ID in Azure
    - Questions around MFA
    - How to configure Azure to support REFEDS MFA profile

- Did not come up on this Office Hour call ..
- Question: should we talk with Microsoft about this?
- As InCommon Federation, could we be a good partner for a conversation w Microsoft
- TomB: many have tried over the years
- There have been some successes in the past
- The people at Microsoft who "got it" left Microsoft
- Our Higher Ed community does not have enough influence currently
- It was noted that having common customers can sometimes help
- TomB: we would like to get Microsoft to enhance their products, but short of that, technology is available for bolting onto ADFS:
  - Cirrus Identity https://www.cirrusidentity.com/ Federation Adaptor (it's in Microsoft's calendar) https://www.cirrusidentity.com/products/bridge
  - ADFS toolkit https://github.com/fedtools/adfstoolkit
  - Unicon Federation Gateway

Summary

- There does not seem to be a lot of concern in the community around BEv2
- We expect that people will come to the final BEv2 Office hour, just before the deadline.
- Next BEv2 office hour is Tuesday, August 31, 2021
- We will have placeholder for office hour monthly, until end of December 2021

2021 NSF Cybersecurity Summit (Brett/Rachana)

- https://www.trustedci.org/2021-cybersecurity-summit
- Rechana encouraged Brett to submit a proposal for 2021 NSF Cybersecurity Summit
- The proposal has been accepted
- Closely related to Trusted CI https://www.trustedci.org/
- Proposal references our work with NIH
- This is an opportunity to expand the partnerships beyond the NIH, perhaps to organizations on NSF side
- Brett is interested in your ideas on what to include as part of a call to action

Walk through of "I can't meet SSLLab A requirement" scenarios (Albert)

- Please chime in if you are aware of other scenarios or if you have other approaches to these scenarios
- There are various scenarios from organizations that can't meet the grade of A at this time
- There are potential legitimate reasons for this situation
- How should we respond to these organizations?
- How do we manage exceptions?
- Scenarios:
  - Scenario 1: Legacy Browser Support
  - Scenario 2: Legacy Application/OS support (Backchannel)
  - Scenario 3: External monitoring tool compatibility
  - Scenario 4: Entity not testable
  - Scenario 5: Load Balancer is handling SSL processing

For each scenario, what is the risk in granting an exception?

- Comment: in each scenario, except Scenario 4, the organization is increasing exposure to a range of risks because of one application. It makes sense to **partition**, to minimize the damage. We should likely ask for a plan around partitioning.
- Discussed scenario 1, Legacy Browser Support, on this call. Discuss the other scenarios later.
  - Ideally, we want an IDP to use BE requirements as an added incentive to rally SP operator to update its application to support modern encryption.
  - Further details are recorded in the Scenarios document
- All are encouraged to provide their ideas on the Scenarios document

Resume BE2 Notifications (with minor wording updates)

- December 17 will be communicated as the deadline to meet Baseline Expectations v2.

- Schedule of additional BE2 Office Hours (Albert)
  - Next, August 31st, 2021

Not discussed on this call: Recruiting new members this Fall at CAMP

Next CTAB Call: Tuesday, Aug. 24, 2021