2020-June-16 CTAB Public Minutes

CTAB call of June 16, 2020

Attending

- David Bantz, University of Alaska (chair)
- Mary Catherine Martinez, InnoSoft (vice chair)
- Brett Bieber, University of Nebraska
- Tom Barton, University Chicago and Internet2, ex-officio
- Ercan Elibol, Florida Polytechnic University
- Eric Goodman, UCOP - TAC Representative to CTAB
- John Pfeifer, University of Maryland
- Marc Wallman, North Dakota State University, InCommon Steering Rep, ex-officio
- Chris Whalen, Research Data and Communication Technologies
- Jule Ziegler, Leibniz Supercomputing Centre
- Albert Wu, Internet2
- Emily Eisbruch, Internet2
- Jessica Fink, Internet2

Regrets

- Pål Axelsson, SUNET
- Rachana Ananthakrishnan, Globus, University of Chicago
- Chris Hable, University of Michigan
- Richard Frovarp, North Dakota State
- Jon Miner, University of Wisc - Madison
- Robert Zybeck, Portland Community College
- Ann West, Internet2

New Action Items

- AI CTAB members put your name in spreadsheet next to organizations to which you want to reach out
- AI DavidB and Albert work on assigning outreach duties to CTAB members, contacting orgs with endpoints failing BE2 proposed encryption requirementAI DavidB and Albert Schedule Additional BE V2 Office Hours

DISCUSSION

Intellectual Property reminder

Baseline Expectations V2

- Albert shared a spreadsheet "Contacts for Orgs with endpoints failing BE2 encryption requirement" with list of entities
-
  - data is based on analysis from a few months back
  - Report grade from March 2020. Some have changed
  - As CTAB uses this list for outreach, keep in mind that the entity may not longer be failing the test
  - Both SPs and IDP are on the list
  - A significant number are test/dev entities
  - Some are test development staging entities
  - What are our expectations of test/dev/experimental entities in the metadata?
  - What should be minimum acceptable grade ?
    - Is a score of B acceptable?
    - A score of T is a fail (T = certificate not trusted, typically because the name on the cert does not match the host)
  - For entities that cannot comply, how great a risk is it to federation if we allow some entities with low grade?
  - Suggestion to ask ScottC of the Shib development team and Shanon Roddy of Internet2 for a threat assessment
  - It makes sense to bring in experts to consult with CTAB and to conduct this conversation with the community's involvement
  - **AI CTAB members put your name in spreadsheet next to organizations to which you want to reach out**
  - **AI DavidB and Albert work on assigning outreach duties to CTAB members, contacting orgs with endpoints failing BE2 proposed encryption requirement**

Planning for next phase - community consultation https://spaces.at.internet2.edu/display/BE/baseline-expectations-2

  - Pre COVID we had thought about a 45 day community consensus process,
  - Suggestion to end consensus on Aug. 15
  - Consensus list has about 12 subscribers
  - Hope that outreach to Orgs with endpoints failing BE2 encryption requirement will generate some feedback
  - We should use email to remind people of the consensus
  - A reminder of the consensus period is included in the June 2020 InCommon Newsletter with a link to this blog

  - **DECISION**: schedule **additional three Office Hours** in addition to the office hours that occurred on May 5, 2020
  - Concern that we might not get much participation
  - JohnP will encourage involvement in BEv2 (Big10 IAM group)
  - Focus on SSL and encryption and **include security experts, such as Shannon, in the office hours**
  - **Implementation plan** is needed
    - For BE v1, CTAB had the implementation ready to go for consensus

        - Implementation plan helps the InCommon operations staff to be ready for the upcoming effort

    - **AI DavidB and Albert schedule Additional BE V2 Office Hours**

Updating exec and contact info for InCommon participants

- As part of BE V1, we updated the InCommon participants contact info.
- But some of that contact info is now out of date
- InCommon participation agreement specifies the requirement to have an exec
- Perhaps InCommon staff should periodically reach out to verify contact and exec info
- Would be good to automate the process
- SIRTFI requires having updated security contact
- BEv2 Implementation plan might include details on getting updated exec and contact info

Deployment profile - 10KM view and potential future BE - Albert & others

- Deployment Profile For Kantara, also known as SAML2 INT https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

  Working Group that began in InCommon TAC, moved to Kantara as a cross industry working group
- Developed deployment profiles around interoperation
- Released in Dec 2019
- Includes statements tackling the interoperability vagueness
- Makes sense for InCommon to adopt this as best practice
- With Baseline Expectations caliber requirements
- InCommon TAC is looking at the Deployment Profile
- Questions: If InCommon adopts the Deployment Profile, with what priority and to what extent to require?

- Issue of subject identifier
- Related profile, the **SAML subject identifier profile** https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html
- To replace edupersontargeted ID
- Replacing subject identifiers is agreed on
- The moving over to using new subject IDs for all SPs and IDPs is a big deal and Heavy left
- Could require an approach like that used for BE
- How much should we include in Baseline Expectations?
- Some of the items we should put on the roadmap

Next CTAB Call: Tuesday, June 30, 2020 (office hours call)