2023-April-18 CTAB Public Minutes

CTAB Call Tuesday April 18, 2023

Attending

David Bantz, University of Alaska (chair)
Warren Anderson, LIGO
Tom Barton, Internet2, ex-officio
Ercan Elibol, Florida Polytechnic University
Richard Frovarp, North Dakota State
Eric Goodman, UCOP - InCommon TAC Representative to CTAB
Mike Grady, Unicon
Kyle Lewis, Research Data and Communication Technologies
Jon Miner, University of Wisc - Madison (co-chair)
Andy Morgan, Oregon State University
Andrew Scott, Internet2
Rick Wagner, UCSD
Ann West, Internet2
Albert Wu, Internet2
Emily Eisbruch, Independent, scribe

Regrets

Pål Axelsson, SUNET
Matt Eisenberg, NIAID
Scott Green, Eastern Washington U
Meshna Koren, Elsevier
Johnny Lasker, Internet2
Kevin Morooney, Internet2

Internet2 Intellectual Property Reminder: https://internet2.edu/community/about-us/policies/internet2-intellectual-property-policy/

DISCUSSION

Working Group updates

- NIST 800-63-4 review (Tom B)
  - Done and submitted.
  - Report for InCommon is being prepared with a few suggestions of things InCommon might do
  - Q: Will implementation of FALn levels be required? Not sure, perhaps after a finding from a federal law
  - Fallout from IG report finding login.gov doesn't actually provide IAL2.
  - NIH looking at alternatives to login.gov
  - People looking at alternatives to IAL realize login.gov will not necessarily be the answer in all cases
  - Id.me is one option
- SIRTFI Exercise Working Group
  - Meeting biweekly
  - Targeting last full week of November prior to Thanksgiving for exercise
  - Will publicize the SIRTFI exercise at TechEx
- InCommon TAC
  - Postponed metadata signing change discussion (Nicole was unavailable)
  - Detailed discussion about deployment profile value statement.
  - Reviewed status of TechEx session proposal
  - Ran out of time for Hackathon discussion
  - InCommon TAC workplan has 3 or 4 items, including deployment profile propagation adoption work. At TAC meeting, discussed to what extent the deployment profile will provide value
- CACTI (Richard)
  - No meeting in past 2 weeks
- REFEDS MFA Profile 2.0
  - There are parallels in OIDC (maxage rather than ForceAuthn)

- Both are intended to indicate “when” authentication was performed, but both are single values.
- If 2 independent factors are authenticated at different times, there is ambiguity in what the “authentication time” should be (e.g., the most or least recent factor authenticated), so it is ambiguous. And implementations vary in how they are able to set this value.
- Two different existing notions (authninstant vs. independent MFA factors) not playing well together
- Looking at how to signal MFA, different characteristics and reconcile with SAML
- How to interpret AuthnInstant and ForceAuthn, with independent MFA factors
- Workgroup is focused on defining technical approaches for signaling how and when authentication was done, not really focused on “how important is it to be able to signal these distinctions”. Community input has indicated interest, but assessing the importance is beyond the scope of the workgroup.
- ForceAuthn, or max age for (OAuth/OIDC) authentication, has been around for a while
- At this point, we need more input to decide on the profile
- Need to come up with implementable path forward; need to understand community preferences
- Want to make things clearer and maintain compatibility
- Shibboleth will also need changes
- CILogon does not pass authentication context requests to IDPs because of lack of support. At campus level, must select so a user can select MFA. But coming in there is an issue
- Ability to signal metadata publishing is an issue in the profile

- REFEDS Assurance Framework - what’s changing from 1.0 to 2.0 and expected timing? (Kyle)
  - RAF2 clarifies and updates discussion around its various assurance components.
  - The IAP (identity proofing) criteria have been in-sourced, ie, implementers no longer need to pick and interpret for themselves one of several external standards for identity proofing.
  - The IAP criteria, in the current draft, might actually be a little higher for IAP high by requiring supporting identity evidence to include either physical or electronic security features.
  - The RAF 2 IAP criteria also support unsupervised remote identity proofing, which was unaddressed by those external standards.
  - It also addresses the binding of authenticators that were previously issued (and not necessarily by the same CSP doing the identity proofing).
  - More news in later part of May

TechEx 2023 proposal (David Bantz)

- TechEx is Sept 18-22, 2023
- (joint CTAB & TAC) draft abstract (David, Jon, Albert, Keith Wessel):
  The InCommon Community Trust & Assurance Board (CTAB) and the InCommon Technical Advisory Committee (TAC) have been working this year on several important initiatives to increase trusted interoperability among InCommon participants. First part of this session will describe the progress in these areas to date and how it will benefit scalable federation, including:
  - better user identifiers
  - new entity categories
  - completion of Baseline Expectations v2
  - operationalizing baseline expectations

  Second portion of this session will invite broad input on potential next directions to increase levels of assurance, interoperability, security, and streamline integration of relying parties.
  Come to be part of current and future enhancements of the InCommon federation.
- We can add speakers for this session

Operationalizing BE - updates (Warren Anderson)

Working through item by item in Baseline expectations, using spreadsheet Warren created

- Items for IDPs mostly done; next will look at those for SPs
- Good framework for how to detect and alert participants of any issues around baseline expectations adherence and to reaffirm adherence
- Checking URLs, contacts
- Plan is that once per year, ask participants to attest to compliance
- T*his plan will increase informative engagement throughout the year*
- Hope to bring recommendations to CTAB before long

Next Up on CTAB Work Plan

- https://spaces.at.internet2.edu/display/ctab/ctab-2023-work-plan
- Work Plan bash: any new items since we finalized the 2023 Plan in Feb?
- Next Up on the plan:
  - Framing the next chapter of federation maturity
  - Assurance next steps (in light of pending RAF 2.0)
- Albert will update the CTAB work plan to indicate when items are complete
- Agreed that ongoing updates should go first to the google doc instead of to the work plan wiki page

- Framing next chapter of Federation authority
  - CTAB has been concerned with Baseline Expectations, but there are other areas where work would be useful to increase trust. Some of those would not fall under baseline expectations. So looking at a maturity model that participants can use to judge their level of maturity and determine work for themselves. Another component would be signaling so an SP that needs some level of maturity can find that out.
  - Initial step is a high level framing of things we care about
  - Then we could task working groups to tackle

    - Changing context: We are moving from federation of architects running things to administrators running things
    - We need to provide more how to information
    - For InCommon admins to use SAAS tools, we need to provide detailed, explicit info
    - There are general tools that can be used as plug-ins with lower level of security
    - Define several dimensions and categories
    - Security, user experience, etc.
    - Define maturity levels
    - Question about batching
    - Albert: Hope for explicit statements of capabilities
    - Important to be **interoperable**, not just technically,
    - but also: do we share the same notion of trust
    - SIRTFI is about operationable standards
    - Large collection of ideas here, could be too large and abstract
    - Suggestion to identify a small number of problem cases / use cases and constrain ourselves to address one or more at a time
    - Could CTAB be the discovery group to find use cases and capture them?
    - We are not starting from scratch; We have interoperability standards and specs throughout the federation
    - We can look at how they are doing and what needs updating
    - CTAB will put on the agenda for May 2, to talk about use cases in which we would like to see greater maturity, have that be the starting point for this work item
    - An example of a maturity model: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

- Also on CTAB work plan:
    - Next steps on Assurance -- we will wait on the RAF group to come back with a fuller report
    - REFEDs entity categories, TAC is taking the lead on this, hope for CTAB volunteers to work on this along with TAC

Next CTAB Call: Tuesday, May 2, 2023