CACTI Public Meeting Notes 24-Nov 2020

CACTI Call Nov. 24, 2020

Attending

Members

- Tom Jordan, University of Wisc - Madison (chair)
- Jill Gemmill, Clemson (vice chair)
- Rob Carter, Duke
- Nathan Dors, U Washington
- Matthew Economou, InCommon TAC Representative to CACTI
- Michael Grady, Unicon
- Les LaCroix, Carleton College
- Chris Phillips, CANARIE
- Bill Thompson, Lafayette College

Internet2

- Kevin Morooney
- Ann West
- Steve Zoppi
- Emily Eisbruch
- Mike Zawacki

Regrets

- Marina Adomeit, SUNET
- Margaret Cullen, Painless Security
- Karen Herrington, Virginia Tech
- Christos Kanellopoulos, GEANT
- Nic Roy, Internet2
- Jessica Fink, Internet2

Action item review (from Oct 27, 2020 CACTI call)

- AI TomJ reach out to Albert, Janemarie and KeithW around signalling MFA

Discussion

Debrief from Virtual CAMP and ACAMP, Nov 16-20, 2020

What were the big themes? What stuck with you?

- **MFA signaling issues**
  - Issue of IDPs lying to Service Providers about MFA.
  - See notes from these two ACAMP sessions:
    - Refeds MFA- Signaling MFA, Signalling MFA/loa capabilities (for discovery) via entity category(ies) in metadata
    - What does a campus really need to do to meet NIH requirements/ Assurance MFA/ Identity
  - There has been an assumption that MFA would fail closed but some allow fail open
  - There are Service Providers (SPs) that are not ready to tolerate risk of Single Factor Auth
  - The current processes allow self-assertion for MFA, which leads to unacceptable security exposure for some Service Providers
    - Currently there is lying about the MFA transaction, not just failing open
    - Some campuses have faculty needing access to resources, so they assert MFA even though it does not really exist
    - One example: when Duo is “down” there is a way for an IDP to fake it to provide access to needed resources
    - Should there be a change to the REFEDs MFA Profile around signaling MFA?
    - Perhaps there should be use of the SIRTFI process to communicate that something is down and should be worked out at the business layer
    - Suggestion : If a service requests MFA context, then you can’t fail open
    - Had not been a big issue in the past, but it is now
  - Failing open is distinct from grace period, but it is adjacent
  - **Context**:
    - A few years ago, there was a struggle to get any MFA release
    - IDPs would say: “I can’t guarantee MFA 100% so how can I signal MFA”
    - IDPs with those concerns were told that if it’s good enough for local campus purposes it is good enough to signal
    - It was made a local decision
  - The MFA signaling issue may relate to vocabulary around Baseline Expectations. In some cases higher assurance is needed.
  - Working on a resolution to the MFA signaling issue is part of the normal process of working towards increased trust. The community develops an approach, it gets put into practice, it’s not quite what we think it should be. There is a balance needed between IDPs and SP needs.

- Ann: Suggestion to convene a working group to work with NIH on specifics of what NIH needs for MFA and assurance, and through that create a recommendation from NIH. Then work the measures back into the REFEDs MFA profile.

- **Other important items discussed from CAMP / ACAMP**
  - Service Provider refactoring
  - Open roaming for eduroam
  - Security and notes from CERN, relationship with SIFTFI
  - Containerization story

- **CAMP / ACAMP Logistics**
  - Great organization of virtual CAMP/ ACAMP
  - REMO room worked well, bigger tables may be needed in future
  - Remote ACAMP was well organized
  - Felt out of the office mentally, a good space to collaboration
  - Tools and technology worked well
  - Encouraged by new participation from collaboration success program Collaboration Success Program campuses and other

- **How to deploy the InCommon Trusted Access Platform components is still a topic on which the community needs more guidance**
  - Concrete guidance would be helpful, sharing a Trusted Access Platform configuration that works for 80% and is "preferred"
  - Need more resources on how to deploy ITAP for real
  - Through line from InCommon Trusted Access Platform (ITAP) to a real world deployment
  - See notes from ACAMP session on Deployment Guide for ITAP

- **IAM Futures**
  - There was interesting discussion of Solid (Social Linked Data) and the role of personal identity,
  - What is the best way to entertain discussion on new and different technologies?
  - **IAM futures discussion** would be helpful
  - With role of Collaboration Success Program in CAMP / ACAMP there was more focus on today's technologies
  - Mike: verifiable credential discussions were of interest, Unicon is looking into this
  - Interest in the IMS standards, tracking educational achievements
  - Self sovereign identity, relates back to discussion of Internet2/ InCommon running a registry?
  - Comment: regarding current and future looking discussions, topics such as WebAuthn
  - there was not a whole lot of discussion on public cloud infrastructure and its impact on identity
  - Appreciated the contribution from KeithW -- AWS Reference Architecture - Shibboleth-IdP
  - https://github.com/aws-samples/aws-refarch-shibboleth
  - https://github.com/kwessel/aws-refarch-shibboleth/tree/feature/secrets-manager-key-strategy-with-caching
  - Gulf is vast between what sites can do and the cloud story
    - This example from KeithW shows a cloud first approach
    - Will help in a Shib v4 upgrade
      - Shibboleth 4.1 is expected in late Dec 2020 or early January 2021

Identity Proofing and Assurance

- Identity Proofing and assurance is related to the MFA failover discussion above
- It would be helpful to **create mapping from regulations in NIST 800-63-3 to what REFEDS assurance** expects.
- could be part of the the REFEDs assurance profile or an addendum
- See scribing doc from ACAMP2020 Thursday on "What does a campus really need to do to meet NIH requirements/ Assurance MFA/ Identity"

- Tom: U-Wisc has adopted 800-63, however there are issues around credential binding and forms of evidence.
  - Almost at Identity Assurance Level (IAL) 2, but not quite, need two forms of strong verification and this is hard to achieve
  - In the USA, the work an HR dept does for an I9 relates to Level of Assurance 2.
  - I9 verification is not always connected with credential binding due to timing issues, (need credential prior to I9)

- Matthew would be happy to attend the REFEDs MFA meetings and work towards the mapping between REFEDs MFA and 800-63-3

Working with NIH on Assurance

- Ann: Hope to establish a group working with Jeff Erickson at NIH, to look at how to leverage a use case and communicate back to the community what NIH needs. Would be helpful to have a representative of CACTI on that community group working with NIH.
- NIH is the anchor tenant around MFA
- ChrisP: There is a potential anchor tenant in Canada

- **Next Steps**
  - Matthew will attend the REFEDs MFA working group and keep CACTI up to date, especially around signaling and mapping
  - Ann will work on establishing a group working with U Chicago and U Wisconsin and others around how their procedures aligns with IAL.
    Ann will check with Chris Whalen and Jeff Erickson on spinning up this working group

- Other item to chew on: Is there a quiet revolution on **how IDPs are being managed with metadata, given new interfaces coming online for testing**. Will this become the new normal? CACTI can better understand this story and look at outcomes and how we can amplify making things easier. Different technique being endorsed. See: https://spaces.at.internet2.edu/display/SMMU/Shibboleth+IdP+Metadata+Management+GUI

CACTI membership (Tom)

- CACTI balloting results 7 members accepted
- Next Steps
    - CACTI chair submits the slate of new members to Kevin Morooney for approval
    - Once approved by Kevin, the CACTI Chair sends email notification to new members (cc: Jessica), asks them to formally accept the nomination
    - Once formally accepted, Jessica will onboard them an invite to the last CACTI meeting in December
    - Jessica will email those not accepted with a nice email letting them know and thanking them for nominating
    - All continuing members are on the ballot unless you opt out. Email Jessica (jfink@internet2.edu) by end of day 11/30 to opt out
    - On 12/1, the ballot for chair will go out & the person with the most votes is chair
    - On 12/8, the ballot for vice chair will go out & the person with the most votes is vice chair
    - Next steps
    - Voting process for chair/vice-chair for 2021

Parking Lot

1. (From June 9, 2020 call) TomJ - Add as an agenda item for a future CACTI call: Operationalizing containers

Next Meeting: Tuesday, December 8th, 2020