CACTI Public Meeting Notes from 11-June-2019

CACTI call of Tuesday, June 11, 2019

Attending

Members

- Chris Phillips, CANARIE (chair)
- Warren Anderson, University of Wisconsin-Milwaukee /LIGO
- Tom Barton, University of Chicago
- Rob Carter, Duke
- Jessica Coltrin, Portland State University, liaison from InCommon TAC
- Nathan Dors, U Washington
- Jill Gemmill, Clemson
- Todd Higgins, Franklin & Marshall College

Guest

- Shilen Patel, Duke

Internet2

- Kevin Morooney
- Ann West
- Steve Zoppi
- Nick Roy
- Emily Eisbruch
- Mike Zawacki
- Dean Woodbeck

Regrets

- Marina Adomeit, GEANT
- Les LaCroix, Carleton College
- Karen Herrington, Virginia Tech
- Tom Jordan, University of Wisc - Madison
- Christos Kanellopoulos, GEANT

Action Items

- [AI] (Emily and Nick) set up consultation for the eduroam Advisory Committee Charter
- [AI] (Emily, Nick, Chris) draft an email for ChrisP to send to kick off the eduroam consultation

Pre-Reads

- Identity space is heating up to levels not seen since early 2000's:

• Identity space is heating up to levels not seen since early 2000's:
• Apple's announcement of Single Sign On with AppleID: https://techcrunch.com/2019/06/03/apple-sign-in-privacy/
• For a robust view:
• Microsoft and decentralized ID (Sovereign?):
• https://www.forbes.com/sites/darrynpollock/2019/05/14/microsoft-looking-to-build-decentralized-identity-network-on-top-of-bitcoin-blockchain/#1866b2f71de5
• https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/
• AWS https://aws.amazon.com/cognito/

Reminders/longer term

- **Slide deck for value proposition for research for the Trusted Access Platform (Jill and Ann)**

DISCUSSION

New InCommon.org website

- New Incommon.org website is live as of Thursday June 13, 2019
- More of an integrated picture on how Trust and Identity offerings fit together.
- Puts together the InCommon website, Trust and Identity website and TIER website
- Uses simpler and more direct language

- Focus on solutions, such as guest systems and affiliates
- using google analytics code to track usage
- Feedback: this is great work

eduroam-US advisory committee charter (Mike Z, Rob C, Nick R)

- Approval vote, (will happen after the consultation)
- Next steps
    1. Consultation takes 4-6 weeks
    2. [AI] (Emily and Nick) set up consultation for the eduroam Advisory Committee Charter, draft an email for ChrisP to send to kick off the consultation
    3. ChrisP will share the consultation at TNC
    1. Community consultation/awareness-building with PAG
    2. Prospective members - building a list and recruitment, will happen after the consultation

Web authentication (Fido/W3C Webauthn) (Rob)

- Environment is heating up
- Apple's announcement of Single Sign On with AppleID: https://techcrunch.com/2019/06/03/apple-sign-in-privacy/
- TAC is interested in this as well, invited Shilen Patel from Duke to present at the May 9 TAC call (see presentation in pre-reads)
- Duke's WebAuthn plans
- FIDO2 project
- Strong public key authentication
- WebAuthN supports MFA
- Can be used as two factors
- Attestation feature allows the org to limit what authenticators to accept
- Strategy is go live with a pilot soon at Duke
- WebAuthN on Shib IDPs
- Planning to get UX team involved to do user testing
- Followed by a limited pilot
- IOS support is limited now, waiting to see that develop
- End users don't like using passwords on their mobile device
    - And don't like going thru the 2nd factor on mobile
- Q: re attestation statements trustworthiness
- A: UB Keys are burned in and securely stored
- Need to decide which types of authenticators to allow
- telephony credits is a large cost https://duo.com/docs/telephony-credits
- May need to forgo some of the DUO options
- To restrict authentication types thru DUO, might add some code in Shib authentication to restrict SMS from DUO, to realize cost savings
- Shilen did demo of registration interface. Looking forward to the UX team's user testing in coming months
- Code from Ubico? Is there application persistent storage behind this?
- For the pilot, storing reg info in local database for now
- IDP/WebauthN, is this a better pattern versus a separate site?
- This is a separate servlet within the IDP. This will be part of self service and will live in a different domain before rollout
- Works similar to cookies, relying party ID can be a subset
- Reg site can be within self service
- Same credential must be used by application process and by reg process?
- No Attributes are carried with WebAuthN story, how does that square with what Federation is doing?
- WebAuthN is an alternative credential, you still need to have an identity at Duke
- Linking a new credential to your identity, similarly to how you might link a DUO credential to your identity
- Will Duke open gates to some of the services around campuses to get off of Shib IDP and do WebAuthN?
- Not explored yet, probably this won't happen soon, the belief is SAML is best solution for on campus. Want to make it easier to navigate. Moving rapidly towards centralized authorization. More likely to want to keep the IDP in the flow for most things. Need that for central authorization.
- Could deprecate central identity provider in favor of WebAuthN. But this does not seem a likely strategy for now.
- Duke is Not deprecating passwords for now, not everyone will be in position to engage with WebAuthN . Some people don't have a smartphone.
- Duke has a single flow to handle all of authentication; this was set up before DUO
- And whether registered for WebAuthN
- Could set up without Duke Kerberos password
- Duo saying they will support WebAuthN, there are tradeoffs of control
- Is there possibility that the academic collaborative service providers might move away from federation and move to WebAuthN or other?
- Warren: depends on the size of the scientific enterprise
- For a VO like LIGO, ready to adopt whatever comes down the pipeline.
    - Attribute release is less of an issue than it used to be due to opportunity to use proxies
- For smaller collaborations
    - adoption of federation has been slow, but is increasing
    - collaboration as a service could be useful.

- What if this WebAuthN work was baked into the IDP? Depends on how much adoption WebAuthN gets. Hoping for adoption by IOS
- WebAuthN could get stronger without us if we don't get involved.
- WebAuthN is solving real use cases for Duke.
- Note of caution:
    - About 20 years ago, each app had to do its own thing, so returning to that would be a step backwards.
    - Some concern about switching to a different model, reverting back to old way of doing things, logging in and creating passwords, doing things by hand again.
- Thanks to Duke for sharing the Proof of Concept

Status Updates

- Close-out of MACE-DIR transition to REFEDS
    1. URN registry transfer - status
    2. Sunset doc finalized! Repository location: http://doi.org/10.26869/TI.109.1

- Topics being tracked
    - https://techcrunch.com/2019/06/03/apple-sign-in-privacy/
    - Build on last meetings outcomes focusing on the 5 areas we highlighted :
        1. infrastructure, services to end users, software dev, infrastructure as a service, and outreach and education
        2. Focus of conversation: to identify high priority items/quick wins in the above areas
    - "Sign In With Apple": WUWT?
    - Continue prioritizing CACTI FIM4R recommendations (Chris/Jill)

    - ID Pro (Chris has next touch point)

Next Call: Tuesday, July 9, 2019

(June 25, 2019 CACTI Call is cancelled)