

CACTI Public Meeting Notes 8-Dec-2020

CACTI Call Dec. 8, 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
- Karen Herrington, Virginia Tech
- Les LaCroix, Carleton College
- Chris Phillips, CANARIE
- Bill Thompson, Lafayette College

Internet2

- Kevin Moroney
- Ann West
- Steve Zoppi
- Nic Roy
- Emily Eisbruch
- Mike Zawacki

Regrets

- Christos Kanellopoulos, GEANT
- Margaret Cullen, Painless Security
- Marina Adomeit, SUNET

Intellectual Property reminder

Discussion

Announcements

- CANARIE is looking at the MFA topic, in parallel with the discussions happening in the USA spurred by the NIH call to action.

CACTI leadership for 2021 (Nic)

- New CACTI members have been approved by Kevin
- Nic will talk to vote leader for CACTI chair
- December 22nd CACTI meeting
 - new members invited, bulk of the call will be introductions, latter part of call may be solicitation of topics for 2021 continued (emphasis on new members)
 - Some CACTI members will be unavailable for the Dec 22, 2020 CACTI meeting

Pre-Seeding CACTI Topics for 2021

The following topics have been recently discussed - it may be useful to rank-prioritize them for 2021

- For context, see [notes from Nov. 24, 2020 CACTI call](#)
- IAM futures
- MFA and Assurance
 - Working group with NIH is being planned, Ann has done outreach to NIH on this
 - Other connections (REFEDS, InCommon TAC, CTAB, etc)
- Identity proofing
 - Connect in with GÉANT incubator work on distributed proofing?
- eduroam / open roaming
- Other items for 2021
 - Update to TIER Reference Architecture - [The TIER Reference Architecture \(RA\)](#), include MFA signalling and other topics
 - Better reference implementation to showcase best current practice for implementers
 - Documentation showing full picture of deployment
 - Showcase best in class, from the Service Provider and IDP perspective
 - Maintaining and curating reference implementation takes care
 - See [login.gov](#) as an example (particularly, the Sinatra/Ruby sample applications on [developers.login.gov](#)), and [Ruby on Rails](#), and LINUX documentation
 - AWS / Shibboleth documentation repo from KeithW could provide solution to MFA implementation
 - <https://github.com/aws-samples/aws-refarch-shibboleth>

- <https://github.com/kwessel/aws-refarch-shibboleth/tree/feature/secrets-manager-key-strategy-with-caching>
 - How to draw clear enough lines for groups to pull in same direction, CACTI, Software Integration WG, and Packaging WG
 - Lessons learned from developing the [Grouper Deployment Guide](#) (BillT)
 - We had large history of Grouper deployments in the community
 - There were community practices in place
 - Took about a year to create the first version of Grouper Deployment Guide, including community discussions
 - Community engagement is key
 - The model in the [Grouper Deployment Guide](#) is not specific to Grouper, but functionality of Grouper is required to implement
 - Les: Carleton is using models in Grouper Deployment Guide, without yet deploying Grouper
- SteveZ noted that the Internet2 Trust and Identity software projects are independent. There will be an effort in 2021 to come up with high level overview of goals/activities
 - Keith Hazelton leads a [software integration working group](#) (meets twice per week) talking about interoperability of the TAP components. Dealing with much complexity from the four components. BillT sometimes attends that group.
 - IAM is an integration exercise and there is a palette of tools
 - The search for an "easy button" may be a search in vain
 - Participants need to understand how things work, well enough to be accountable when running them.
 - "I can explain it to you, but I can't understand it for you."
 - Internet2 Trust and Identity can invest in technology or in training/education, but with limited resources cannot invest fully in both at the same time
 - TIER started with prioritization of technology
 - Later a shift was made to invest in training, thus the Collaboration Success Program
 - There can be some conflict of opinion on how to package components
 - Creation of containers with many choices
 - or
 - decorate containers with many knobs
 - or
 - deploy and maintain some number (like 3) patterns
 - There are tradeoffs
 - Component Architects prefer to maintain patterns that describe about 80% of cases,
 - Supplement with proper training
 - [Grouper Deployment Guide](#) provides patterns
 - It may be helpful to have a smaller number of architectural patterns with better connectivity between practitioners
- Question whether the community has difficulty deploying the individual components
 - Or overall architecture problem of "how do I implement IAM with the ITAP tools?"
- Commercial Service providers complexity causes challenge
- Asking major commercial service providers to change their patterns for identity control is generally an uphill battle
- Tom: Suggestion for CACTI in 2021 : exercise leadership across the working groups on this issue of reference implementations
- SteveZ: CACTI members are welcome to join the working group calls where implementation patterns are discussed
- SteveZ: Sandbench concept is being developed.
 - AI: Solicit topics from new members. Tee up on Dec. 22, 2020 CACTI call, continue into first meetings of 2021.

, Lot

1. (From June 9, 2020 call) TomJ - Add as an agenda item for a future CACTI call: Operationalizing containers
2. Representation/shared leadership across TAP groups such as component architects and software integration. (from Dec. 8 call)

Next CACTI Meeting: Tuesday, December 22nd, 2020