Oct-18-2018 Open CACTI meeting at TechEx in Orlando

Oct. 18, 2018 Open CACTI meeting

At Technology Exchange in Orlando

12:10pm to 1:30pm ET

Oceana Grand Ballroom 11

https://meetings.internet2.edu/2018-technology-exchange/detail/10005257/

Attending

- Chris Philipps - CANARIE
- Robb Carr - Duke
- Jill Gemmel -
- Scott Koranda - tOSU
- Michael Gettes - University of Florida
- Marteen Kramers -
- Todd Higgins -
- Mark Schieble - MCNC
- Les -
- David - GEANT
- Hannah.... CERN
- Nathan Dorrs -
- David - University of Alaska
- Jon Miner - UW Madison
- Klaas Weirenga - GEANT
- Matt Brookover - Colorado School of Mines
- Gabrie
- Roland
- Niels Van Dijk -
- Jim Basney - UIUC
- Eric...
- Cristos...
- Kevin Morooney - Internet2
- Ann West - Internet2
- Steve Zoppi - Internet2
- Nick Roy - Internet2
- Shannon Roddy - Internet2
- Dave Shaffer - Internet2
- Erin Murtha - Internet2
- Mike Zawacki - Internet2
- James Babb - Internet2

Agenda

Intellectual Property reminder

- **https://www.internet2.edu/policies/intellectual-property-framework/**

1. **Administrivia**
    a. Intellectual Property reminder https://www.internet2.edu/policies/intellectual-property-framework/
    b. Overview of CACTI for newcomers
    c. Looking for feedback, guidance from the community
2. **Updates**
    a. eduPerson and MACE-DIR
        i. Sign the yearbook poster in the ACAMP room.
        ii. Will have a sign-off ceremony.
        iii. Intend to preserve mailing list archives, other artifacts from MACE-DIR
    b. Developments around OIDC within R&E
        i. Coverage throughout TechEx, ACAMP sessions
        ii. OpenID Foundation WG created: https://openid.net/wg/rande-wg/
            1. Designed to keep track of activities within the community.
            2. Strategic way to get R&E viewpoint into the technology
            3. Seeking feedback from community, fill in gaps in work
3. **Main Business**
    a. initial draft FIM4R gap assessmentundertaken by CACTI (chartered by Kevin)
        i. Consultation document available on Internet2 wiki (link here). Please lend your thoughts there.
        ii. Overview: Moving from FIM4R recommendations to assessment.

- iii. Iterative process to complete the gap analysis. Had ~10 gaps; send prioritized list to I2 with gaps to later turn into digestible recommendations. Kept working through this process and ultimately discovered the key was collaboration.
    1. TIER components meet service need but not implementation
    2. Universities support science as part of their mission, which is a team project spanning institutions. All scientists need this.
    3. Smaller institutions don't have the resources to build a complex infrastructure but they still need to be able to participate, collaborate
- iv. Worked with subgroup in CACTI to develop this document along with Nick Roy and David Walker.
- v. Recommendations
    1. Support collaboration-as-a-service.
        - a. Provide IdP-as-a-service
            - i. Niels: Not surprised by this requirement for smaller orgs, but larger one wouldn't need it. Is there competition with commercial/3rd party providers?
            - ii. A: Competing IdP service may not support R&S, wouldn't be able to offer the level of assurance as solutions that come from academic environment
            - iii. Nick: Need to be clear between IdP as a Service and IdP of last resort. Niels seems to be speaking to the latter
            - iv. Q Klaas: Is the idea that you are concerned with attributes for all services, or just the ones the campus uses
                1. Eric Goodman: Both in the recommendation, but IdPaaS is SAML based, talks to a school's identity server.
            - v. Q Christos: The hope that we could get away from manage individual accounts, move to federated accounts.
                1. Chris P: Speaks to the need for clarity, similar to IdPaaS vs. IdP of last resort discussion above. Need to define the service, make the scope & function clear.
                2. Jill: Addresses long tail schools
            - vi. Q Niels: I encourage I2 to spin up a collaboration platform. You aren't the only ones doing this work - suggest looking at/participating in work ongoing in the EU (e.g. AEGIS Group)
                1. Jill: Yes - I2 should take a more proactive role in fostering international collaborations is a recommendation in the report.
            - vii. Michael: Be mindful of classifying this as a solution gear toward the "long tail" could create confusion, concern at R1 level.
                1. Jill: We were hoping that by raising Baseline Expectations (BE) to include FIM4R requirements in the future. Review and revise in future BE.
            - viii. Scott: Hesitate to be too agressive re: R&S. If we want R&S to reflect updated practices we may want to put that first. Or decide on how to future proof R&S first. Should decide which to go with.
                1. Scott: Example would be move between SAML versions
            - ix. Jim: Concerned about sentiments expressed in document that CILogin isn't sustainable. I encourage discussion on that topic.
                1. Jill: Agree. We were trying to be provocative,
                2. ...: Part of the problem is the "Post-Jim Basney" approach. If it's in the critical path then we need a roadmap for how it will be sustained by more people than just Jim.
                3. Gabriel:Not clear in the wording why an IdP as a service is needed.
                    - a. Jill: Ok, we can look at this - part of earlier discussion and will readdress it.
                4. Niels: If we're doing a gap analysis then need to consider the above carefully. It's a gap.
            - x. Jill: Anyone see anything missing? Or misstated? Please review the doc and reach out if you see anything.
                1. Scott: I think there are some assumptions about the SP side, their functionality & behavior. Could be worth calling out more explicitly. For example BE needs to be defined for SPs.
            - xi. Gabriel: Oblique references made to OIDC, but isn't called out explicitly. Seems like it should be dealt with more directly.
                1. Chris: What's your suggestion there?
                2. Gabriel: I get that it's a gap analysis, so I get hat some things don't need to be called out.
                    - a. Scott: Guessing the assumption is that problem right now is solved with proxies. We could just say that. We don't feel like there's a need to move all SAML architecture to OIDC. Maybe we just say that.
                    - b. Eric: Isn't this addressed by the requirement for periodic review?
                        - i. Jill: yes, I think so. Also, as Chris has mentioned that CACTI is looking at OIDC and what does it mean for the current and future architecture. Looking at schemas, etc. We don't have a path forward to recommend yet. We suggest documenting current best practices for things not handled well by SAML.
                    - c. Scott: Question is what's the gap around OIDC. If the need is being met by proxies then we can just say that. If that's not true then we're missing something.
                    - d. David: We deliberately avoided protocol discussions. Trying to separate needs from methods. So the obliqueness was intended
                        - i. Scott: Developers will read into it, draw their own conclusions, could cause confusion.
                    - e. Gabriel: Seeing some things missing. SIRTFI, etc. Feels like it needs another pass
                        - i. Jill: this is the very first draft; we have more work to get the rest of the way there. The folks drafting the paper need to have a conversation whether mentioning OIDC with proxy is best practice or address this differently.
                        - ii. Gabriel: What we (IdP operators) need to do is summarize the state of things on our end
                        - iii. Chris: we felt that we got that. If you still feel that there's a gap, then we need to address that.
                        - iv. Gabriel: Sometimes language in the draft is generic, doesn't go into detail.

              - v. Chris: so some of those things are fortifying activities
              - vi. Niels: I wondering if it would be prudent to put some timeline in here.
              - vii. Hannah: I like the paper as is, appreciate that you're going the recommendations route rather than needs & solutions route.
                - 1. Jill: we were asked for recommendations to Kevin, and it needs to be at an executive level for messaging and research prioritization as recommended by the community. We could have a more global discussion.
                - 2. Chris: Section later in paper addresses this, too. I think the points above reinforce the need for international collaboration.
              - viii. Warren: FIM4R is aware that we're only addressing one particular stratum (via InCommon). Question is how the work gets done across all stratum.
              - ix. Also think this is very useful and good; FIM4R community will appreciate the feedback as well. Better than the version one paper. 🙂
        - xii. Chris: Encourage everyone to continue to comment. Comments are open for the next 30 days.
            - a. Shannon: Did search through for security, but there's a gap. Seems there's room for proactive security assessments
            - b. Jill: we recommend making SIRTFI part of BE. It was established as European communication channels; needs detail who should make contact.
            - c. Shannon: Had a couple of occasions to share security information, but difficult to find the right people effectively.
            - d. Jill: encourage Shannon to review and give feedback
          - 2. Chris: first document we've done like this and we're leveraging new territory. So, Shannon, we rely on working groups below us. We have some gaps, and we want to work with you to help augment our knowledge in this space. CACTI wants to keep T and I workspace current. We need to be in front of the community in a proactive way. Other gaps?
        - xiii. ? - It's hard for InCommon to reach out to campuses. How do we know that our staff's time is well spent by participating in these discussions/developemnt
          - 1. Chris: We speak to need to fill talent gap.
          - 2. ? - I'm speaking more to a management gap
          - 3. Gap between researchers and IT staff on campuses. We need campus leadership to get these people talking and making it a priority to collaborate with identity folks.
          - 4. Jon - We want to participate, but sometimes get pushback from our leadership unless someone else internally (researchers, etc) are actively pushing for something.
          - 5. Davis - FIM4R can't necessarily resolve that. However, would like to bet that all researchers have a similar problem. Research these days is collaborative and solving some of these problems.
          - 6. Vast number of researchers don't know that they need to ask for federated identity.
          - 7. There's a communications gap between us and the researchers. They don't have much/any expertise on the topic of IAM.
          - 8. Ann: need much more broadly represented set of researchers in the government. Harness their contacts and ideas.
            - a. Some of the best outreach for InCommon is putting RS, BE into CCR solicitation.
            - b. Key to integrate research into advisory groups.
      - b. Aggregate existing resources
      - c. Domesticate new appliances
      - d. Create an I2 "virtual office" or "non-profit marketplace"
      - e. CILogin seemed like a good fit, but needs more stable sustainability base.
      - f. Rigorous promotion of current pilots that are using COmanage to replace parent/affiliate guest account approaches
      - g. Non-web applications (e.g. ssh) not well supported; focus on promoting best practices.
    - 2. Increase focus on sustainability practices
      - a. Routine assessments of Trust and Identity
  - i. Q and A
- b. Call for Topics
  - i. What is a priority for YOU we should be talking about?