eAC Meeting 2023-2-17

Friday February 17, 11am-12:30pm ET

Attendees

Brett Bieber - Nebraska

Saira Hasnain - UF

Josh Howlett - Independent

Rob Gorrell - UNCG

Jeremy Livingston- Stevens

Nadim El-Khoury - Springfield College

Mike Dickson - UMass Amherst

Kendra Ard - California State University

Dion Baird - Oregon State University

Amel Caldwell – University of Washington

With

Kevin Morooney

Sara Jeanes

Mike Zawacki

Ann West

Romy Bolton

Regrets

Jeff Egly

Tom Rixom

John Buysse

Agenda:

- **Intellectual Property Reminder** - All Internet2 activities are governed by the Internet2 Intellectual Property Framework
- **Public Content Notice** - eAC minutes are public documents. Please let the eAC and note taker know if you plan to discuss something of a sensitive nature.
- Agenda bash
  - Bashed!
- Introduction of Chair, Vice-Chair
  - Brett Bieber: Chair
  - Mike Dickson: Vice-Chair
  - Many thanks to Jeff Egly for his leadership of the committee in 2022!
- Approval of last meeting's minutes
  - https://spaces.at.internet2.edu/display/eduroam/eAC+Meeting+2023-1-20
    - Saira motions
    - Rob approves
    - Jeremy seconds
- Update on GEANT SP issue (Sara)
  - Sara: Have been working with our colleagues in GEANT on this. Core challenge around the way the US community signs in, IAM attributes which are used. GEANT's SAML SP stated that it accepts R&S set of attributes, but there's a mismatch between how GEANT and US community approach those attributes. Working toward a fix, could involve changes both on GEANT and US and other impacted NROs. US eduroam community is large, tends to adopt newer standards more quickly, can cause these sorts of issues from time to time. There's consensus on the cause, working toward common solution
    - Rob: Is there a US best practice recommendations that could help provide guidance to SAML IdP integration to address this issue.
    - Kevin: Here's a presentation from the South African colleague Sara just mentioned. Powerful stuff.
    - https://indico.geant.org/event/1/contributions/82/attachments/17/23/Halse%2CG%20-%20shouting%20across%20the%20chasm.pptx

- Brett: So one of the approaches could involve an intermediary proxy? Sounds like the South African NRO is also engaged to address this, which is great.
- Sara: Yes - we've been having discussions with CANARIE staff on this as well. There are great examples internationally around this work. There's a GEANT led group that talks through CAT development work
- MikeZ: We could post link to mailing list archive and/or meeting notes for this committee to get acquainted with the work
- Brett: Sounds good. Sara and MikeZ can also provide updates to this committee.
  - MikeZ: I'll take an action item to post a link to the public meeting minutes of that group
  - Link to wiki page w/notes from previous meetings: https://wiki.geant.org/display/gn43wp5/Development+VC%2C+20230214

- eduroam Support Organization update (MikeZ)
  - Blog post and copy of eduroam Support Organization 2022 Annual Report
    - MikeZ: eSOs and eduroam team collaborated on report of program activities, goals of the program participants, lessons learned, etc.
    - Brett: Encourage you all to look at the report, keep current on the work being done around this program and in the K12 space
    - Kevin: Speaking of growth and jic you didn't see it: https://connect.geant.org/2023/02/14/eduroam-reaches-new-heights-a-new-record-of-6-4-billion-authentications-in-2022
- Representation on CACTI calls
  - Brett: The eAC is an advisory body reporting up to CACTI. On quarterly call for committee chairs the topic was brought up to have eAC representation on CACTI. Rob's name was put forward and he's willing to begin joining those calls. Good opportunity for cross pollination. Any concerns from committee?
    - None! Rob accepts.
  - Brett: We'll add a standing agenda item for report outs
    - Rob: Worth noting that we have some experience with interfacing with CACTI - Best Practices Guide and other work outputs were run past them.
- Review of work priorities
  - 2-5 minute overview of each item, including work done to date
    - Brett: Chairs and I2 staff met to discuss agenda, came up with the following list of work priorities. Want to provide overview, invite discussion around prioritization.
  - Windows TLS issue (MSCHAPv2 depreciation) / Transitional Technologies (MikeD)
    - Background material:
      - https://lists.geant.org/sympa/arc/cat-users/2022-10/msg00040.html
      - MikeD: Windows 11.22H2 was an update that included changes to 802.1x protocols. It disabled MSCHAPv2 by default, which caused auth failures for clients using that authentication method. Also enabled TLS1.3 over TLS1.2. EAP-TTLS still works (tunneled credential transfer seen as less of a risk). Caused support issues, users failing to authenticate. Additional wrinkle was that some versions of FreeRADIUS don't fully support TLS1.3. Will accept TLS 1.1 or 1.2 if asserted by client, but might refuse 1.3. Fixes could
        - Sara: I think there's an opportunity to generalize the conversation. Around conversations of TLS1.2 vs TLS1.3 there are similarities to move from WPA2 to WPA3.
        - MikeD: True. Depreciation of earlier TLS versions has been signaled but not announced, no timeline. Greenfield deployments easier, but could use best practices guidance.
        - Brett: This could be an item that warrants a working group that focuses on assessing impacts, best practices for configurations, how to communicate this out to the community. Thoughts from the committee?
        - MikeD: That makes sense. Having a matrix of solutions would be good - from least resource intensive/less complete to most resource intensive/most complete. Provide a range of options
        - Brett: Wonder if we could gather some names of folks here to spin up a group.
          - MikeD
          - Nadim
          - Amel :)
          - Rob - Also think that this dovetails into update of Best Practices Guide.
        - MikeD: Another work output of this group could be a blog post.
        - Brett: Others interested add your name to this list above. Also want to think through timing
        - AI MikeZ: Send out scheduling poll for initial call, set up scribing docs
        - Saira: I think there's some urgency here - impacting institutions now
        - MikeD: I agree. We're seeing reports from our schools, hearing about it from others. Could even warrant a PSA type announcement.
  - Update of Best Practices Guide (Rob)
    - Background material:
      - eduroam Best Practices Guide
    - Rob: One of the first tasks this committee took on. A couple of years old now. Some topics are still current but many could use an update. Intent of the guide isn't to provide a "cook book" but more intended to provide guideposts for new and current eduroam admins. We're seeing need for updates in conversations happening in the community around things like Wifi6e, other topics. Other things to consider
      - Updated EAP recommendations, more detail on different methods, changes to reflect the current landscape (e.g. MSCHAPv2)
      - Updates on CAT
    - Brett: Do you see a working group needing to meet more regularly?
      - Rob: I do. Also want to figure out how to coordinate work with the group mentioned above, think through how to coordinate on messaging.
    - Brett: Sounds like it would also be good to put out a call for participation from others outside this committee. Also want to provide opportunity for public comment period
      - Rob: Agree. Also a good thing to bring to CACTI.
    - Brett: Volunteers for this group?
      - Rob
      - Josh
      - Amel
      - Nadim
    - AI MikeZ: Send out scheduling poll for initial call, set up scribing docs
    - Brett: This feels like a much longer term project than the deprecation/changes group.
    - Rob: THink we'll need to also look ahead to the work of deprecation/changes group and incorporate that input into the BPG

    - MikeD: Agree with that. Also may want to include info on how to handle refreshes of infrastructure - more complex than greenfield implementations. Should reflect that in the guide
- Distributed eduroam testing (Rob)
    - TechEx session - Andrew Gallo, George Washington University/CAAREN
        - Presentation from University of Michigan team: https://it.umich.edu/community/michigan-it-symposium/2020/presentations/introducing-pssid-wi-fi-monitoring-system
    - Background material:
        - Writeup on proposal:
        - https://docs.google.com/document/d/1ubu8VzeVJqPCg9f5UcYKfggNUI4lnClO/edit
    - Rob: Especially interesting for eSOs but has value for the entire community. Having a perfSONAR implementation that monitors environment eduroam via rPI test node could provide valuable support info
    - Brett: Agree this might be a more appropriate work item for the eduroam Support Organizations. Could be a working group that they participate in/lead.
    - Rob: Agree with that approach.
    - Brett: Also could involve Sara, looking at ways to monitor infrastructure or takes recommendations from a working group
    - Josh: I think it's insufficient to look at monitoring a single site, consider how to monitor the service, end to end, as a whole. I was involved in a similar project in the past, found that the value of the solution was dependant on the integrity of the test/monitor infrastructure. Poor quality of components can drive false negatives, missed positives. TCO of entire solution could add up quickly. Suggest stepping back, understanding the problem in more detail. The document linked above focuses on a single institution. Also consider that if the network the SSID sits on isn't reliable the service isn't as useful. Probably worth testing the network to some extent as well. Need to have an understanding of the requirements. Suggest working on that first. Then look at solutions
    - AnnW: I agree - very useful to decouple those two things
    - Brett: Second that sentiment. Sounds like a good plan. To Josh's point we recently saw an issue where someone was testing, caused huge spike of failures, looked like a problem but actually wasn't. Wondering about next steps - need a group to come up with requirements document?
    - Saira: I hear both sides. Being able to monitor, increase service resilience makes it more valuable. But to Brett and Josh's point, this work has to be done mindfully, sanely. So is what's being proposed a national level monitoring? Are we talking about standardizing on tools? What's the scope of this monitoring
    - AnnW: If we're trying to solve the problem of users roaming and not connecting, giving organizations tools to monitor that's one thing. Other approach is a Baseline Expectations like effort of standardizing like Saira was asking about. That's actually more of a communications project than technical
    - Brett: Fully support Baseline Expectations for eduroam. Not sure what the community appetite is for different levels of compliance, but maybe we want to use this as a way to gauge community willingness? Consider how we handle out of compliance participants. Monitoring could be a way to get the community to start thinking along these lines.
    - AnnW: Also consider effort for each step. Need to think through cost/benefit, scoping of work.
    - Brett: So where are we with next steps. Josh?
    - Josh: If the eSOs can articulate their requirements that's a good first step
    - Brett: Include a breakdown of different pieces, consider
    - Rob: To Ann's point of cost/benefit the eSOs would stand to benefit the most.
    - Josh: Generally there's a tendency to monitor for the sake of it. Can end up with reams of stats that are never looked at. Want to get a concrete statement from eSOs on what they believe the benefit will be, incorporate that into the Cost/benefit discussion
    - Brett: Volunteers?
        - Brett
        - Jeff
        - MikeZ
- OpenRoaming position paper (Sara)
    - Background material:
        - Summary on OpenRoaming by GEANT staff: https://eduroam.org/eduroam-openroaming-end-user-information/
        - Notes from TechEX ACAMP session on OpenRoaming: https://docs.google.com/document/d/18rJ6A69p0UzI8FCdIKpsHcwYGKCBtpcOUGCvqHJkhjw/edit
        - Sara: This comes up periodically. Basics of OpenRoaming - set of technologies and process arrangements that came out of Wireless Broadband Alliance. Similar to eduroam, wraps those in agreement structures, much more focused on commercial solutions as well. Intended to offer secure, seamless authentication, but includes options for commercial identity providers (Google, Apple, etc). Component of data sharing between corporate partners. Question that comes up for this community is mostly around differentiating OpenRoaming and eduroam. Notes from ACAMP session calls out the need for a document from the eduroam community that articulates the value and benefit of eduroam. Doesn't need to be an explicit rebuttal of OpenRoaming, more focused on differentiation, spelling out explicit value prop of eduroam
        - MikeD: What would be the use case on college campus? I see the use in conference centers, etc? Would it be deployed alongside eduroam on college campuses? I hear about OpenRoaming and it sounds like a good guest system for colleges. If I were a new student why would I choose one over the other?
        - Saira: Is there a similarity to ANYROAM guest accounts?
        - Rob: Conceptually but substantial differences in terms of scale and scope
        - Saira: In Gainesville, FL we've rolled out eduroam to public areas where our students frequent. City wants to provide ability for others to connect. I could see the value of OpenRoaming in this case. Could be useful in agreements with city/local governments. Issue with ANYROAM guest accounts is the lack of user vetting. OpenRoaming could address that.
        - Amel: We see need for something like OpenRoaming in visitors to colleges, especially for events on campus.
        - MikeD: What's the status of ANYROAM?
        - Amel: You have to reach out to them, make config changes on your network to enable it.
        - Rob: Feels like there's a lack of sustainability to the model.
        - Brett: It sounds like we could use some additional input from SMEs. We could then think about position paper draft. Is there another expert who could talk to the committee?
        - Josh: I think the danger of that is that the conversation will focus on the technology and less on the benefits of each. I haven't found an articulation of the comparison between eduroam and OpenRoaming from a benefit perspective. Getting someone who understands both would be good. Klaas Wierenga? Stefan Winter?
        - MikeZ: Stefan provided an overview for the committee a year or two ago
        - Sara: Agree with Josh's sentiment. Klass and Stefan come to mind.

- AI MikeZ: Reach out to Klass, Stefan about presenting to this commitee

  - IdPaas, hosted RADIUS (adjacent to Guest Services report from 2021 - https://spaces.at.internet2.edu/x/cICQD)
    - …
  - Vendor supplied IdP for radius - hosted radius for K12/others - also called a ‘Cloud Bridge’ in some of our conversations (Sara)
    - Demo during eduroam in K12 session, TechEx 2022
  - (Not to forget next steps on the User/Device Onboarding Requirements report - https://spaces.at.internet2.edu/x/ph19Dg)
- Next meeting time
  - Friday, March 17, 11am-12:30pm ET
- Committee members attending Community Exchange? May 8-11, Atlanta
  - Mike can request a working meeting if enough folks will be attending
    - Saira
- AOB?
  - Other items floating around
    - WPA2 to WPA3 transition
    - NPS PEAP vulnerability - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689
  - 6.4 billion authentications! - https://connect.geant.org/2023/02/14/eduroam-reaches-new-heights-a-new-record-of-6-4-billion-authentications-in-2022

Work item	**Your vote (1 per member)**	**Volunteers**
Transitioning Technology Working Group		MikeD Nadim Amel :) Rob
Update of Best Practices Guide Working Group		Rob Josh Amel Nadim
eduroam Service Level Requirements - cost benefit rationalization		(eSOs) Brett Jeff
OpenRoaming position paper		
IdPaas, hosted RADIUS		
Vendor supplied IdP for radius - hosted radius for K12/others		