

Link to 2020 ACAMP wiki

Title: OpenRoaming and it's relation to eduroam. Are we eventually a group within their topology? Do we stay a peer? What does this mean for eduroam SPs? -

Advance CAMP Wednesday Nov18,2020

1:20-2:10 pm ET

Room - Stable

CONVENER: Sara Jeanes

MAIN SCRIBE: Mike Zawacki

ADDITIONAL CONTRIBUTORS:

of ATTENDEES: 15

DISCUSSION:

- Sara on context: In the states we're looking at broader deployments through regional partners, K12 deployments at the statewide level. Looking for how we interact with OpenRoaming, opportunities. similar in scope/impact as OIDC a few years ago
- Rafal : Recently we (CANARIE) we had a commercial provider to do an OpenRoaming pilot. We would light up high density urban areas with eduroam - trick for us is how to maintain brand while partnering with a commercial provider. Have others done something similar? If so, what's that conversation been like?
- Sara: Internet2 has had some early conversations with WBA, but very few inquiries from users. Lots of talk about connectivity/broadband coverage, less on OpenRoaming. Focus on physical plant

- Rafal: In our case the option presented was to leverage existing Hotspot2.0 infrastructure to push out eduroam. But eduroam SSID wouldn't be broadcast. Existing users could connect but there would be no brand exposure
- Stefan: If you want to enable Hotspot2.0 you can add your own text to SSID field. But the UI differs from device to device, experience isn't consistent. Sometimes "eduroam" doesn't show up until after connection
- Klaas: Stefan, can you share some of the use cases in the EU?
- Stefan: We have lots of Hotspot2.0 peerings with commercial operators, so use case isn't new to us. Usually these automatically associate with eduroam SSID. Lots of variety of agreement details with commercial providers. OpenRoaming is a different use case. We're still working on that :) OpenRoaming isn't just network discover and logging in - it's a federation. So there are agreements, legal component. More an issue of making their federation work with our federation. We're focusing less on SPs and endpoints. We can't compete with ease of onboarding of many of the commercial SPs. Focus for us has been on the IdP side
- Rafal: Any risks to commercial entities broadcasting the eduroam SSID?
- Mike: Are there reputational risks?
- Klaas: Possibly, yes. We like to raise the bar of the eduroam experience globally. With partnering with an external party we give up some control. But consider that we have an analogous problem with campuses doing bad implementations now. Users confusing eduroam with the campus infrastructure
- Rafal: Is there a risk for users? Could user data be endangered?
- Guy Halse: One thought is that if you mine the use data, even just DNS lookups, you could derive commercial value from that.
- Stefan: We say nothing about that within our community - there's an unspoken ethical standard that frowns on that. But that's a risk for commercial partners. Looking at OpenRoaming, however, the SP service agreement forbids that sort of profiling. So it's arguably better than ours.
- Ann West: To be clear this is just about hotspots, not accounts, yes?
- Rafal: correct - it would be an expansion of only SPs. They also have an integration with US carriers, so Canadian users could connect through that infrastructure as well. Good opportunity but we're looking hard at issues of reputation, ethics, etc. Our partner has stated that they have no commercial interests but are already asking about reaching out to our connected institutions. Looks like they're seeing eduroam as an entry point to our community.
- Klaas: Are there concerns that this would disincentivize campuses to invest in eduroam?
- Rafal: It's a concern from the SP side of things, less so than on the IdP side
- Klaas: Understand, but there's a wariness about commercial providers' tendency to look at users as a commodity.
- Licia Florio: Also a concern in terms of direct user statistics, user experience, etc. Has anyone thought about those impacts?
- Rafal: We're wrestling with that - we've slowed down the engagement because they're moving too fast. We're engaging with our community to gather thought/consent. From

my end there might be an uncommunicated opportunity that they're acting on. Need to look at all the angles and impacts before moving

- Guy: Often what we see is commercial providers trying to take over campus infrastructures, lock in users.
- Sara: Tends to drive to the lowest common denominator type solutions. Could try to provide excellent coverage to stadiums, ignore dorms, etc. Possible leverage point in driving broader benefit for our institutions. But even looking beyond a single campus, they like to address the high profile users, "chase logos" but ignore large sections of our student/faculty communities. Need to be careful of that, look at a longer term sustaining value for our communities.
- Chris: Value proposition for commercial providers is somewhat an unknown. Also consider that the GeGC compliance statement is largely silent on questions of user data sovereignty and good/bad community behavior around that. Also consider Hotspot2.0 concerns with CUI (chargeable user identity) and how that data transits the infrastructure of our commercial partners. This is a landscape we're (NROs) are all starting to confront
- Stefan: Thing about OpenRoaming is that their standards are well developed enough that we (NROs) need to do a bit of catch up. WRT Rafal's user case, consider that NROs have differing rules/levels of compliance for user data sovereignty and similar concerns. That will complicate a unified approach, esp. Given that the GeGC compliance statement provides broad leeway for NROs, which translates to less of the specificity that's needed when engaging with commercial entities
- Chris: Is there anyone working with GEANT and their OpenRoaming initiatives?
- Stefan: We've been told by WBA that there are universities globally that would like to try out OpenRoaming. We're doing our best to approach that via a community based method, running our own OpenRoaming proxy. Slow takeup there, though. SO that's the technical level. But when it comes to the agreement level it's trickier, less finished.
- Klaas: Also have to realize that only a short time ago that this initiative that OpenRoaming was handed over from a commercial provider (Cisco) to a governance body (WBA). We've been talking about the concerns that exist around the technology, but equally important is the opportunity it represents. If this takes off we have an opportunity to massively expand the footprint of eduroam. For the first time there's a way to scale Hotspot2.0 deployments, for example.
- Rafal: Agree - the number of access points we're looking at in Canada is over 100,000.
- Chris: Also, the geographic diversity has been a challenge (e.g. lookups for realms outside Canada - even in proximate US locations - have to go to the GEANT top level servers and then go back to Canada). Notion of proxying via OpenRoaming is exciting
- Stefan: OpenRoaming expects to suss out the relationship between user and home institution via DNS, NAPTR records. Much faster, dynamic (requires IdPs to do some complex config/infrastructure updates that will be hard for less capable connectors). We're doing our best to push adoption of RADSEC, cert solutions to close that gap as well.

- Ann: Consider how we do change management as a community if portions of our infrastructure fall under the ownership of external entities like WBA, commercial providers, etc.
- Chris: Thinking about smarter integrations with commercial providers (like AWS) as an onramp for external entities, from schools to Starbucks. OpenRoaming doesn't change that. Question is should that be corrected?
- Stefan: With OpenRoaming and DNS NAPTR records, the IdP has more choice on how it's connected. Potential risk - could imagine an IdP getting a commercial offering for managed OpenRoaming IdPaaS.
- Ann: We're seeing the ongoing interest from companies and other federations to handle the SPs/access points. Question is - is it easy for them to step in later and offer their own IdP service, lure schools into outsourcing their operations. We're faced with a "which hill do we die on"? Right now we're looking at fighting for the IdP side. There's a perception in the US eduroam community that an eduroam user has a higher trust level than a commercial user. An institution can always outsource eduroam operations. That might be less of a concern.
- Chris: Need to look at whether such a 3rd party is mainly a network provider. Commercial network providers tend to be very competitive, expansion driven, less community oriented. If the community is served and that arc looks sustainable we'd be less worried.
- Rafal: Being very mindful of engaging with this commercial entity because of that.
- Chris: Agree - don't want to stumble in our service delivery, reflect on international eduroam community.

Action Items/Carry Forward

Sara:

- Looking at ways to define our business development engagement strategy with commercial providers/OBA/OpenRoaming.
 - Technical readiness to bridge two consortia together
- Evolution of the value proposition of eduroam and our core competency is.
 - Baseline expectations exercise? Other opportunities?
 - Review compliance statement?

Chris:

Defining, assessing technical readiness for OpenRoaming and other commercial entities

Rafal: Reached out to Hideaki on his approach. They're doing a sandboxed/scoped deployment with commercial providers first. Use it as a way to assess commercial partners. Concern is that commercial entities look at the sort of profiling discussed above, and grooming future consumers, using eduroam to build their brand

- Similar to Microsoft's approach to the edu space - do Office365 for free for schools, get users acclimated to their service
-

Ann: Reminds me of inAcademia, how commercial providers might leverage user data, usage habits to market to those users.

Klaas: For me, it's a matter of keeping our eye on the ball - adding value to the higher ed community. Need to balance that with concerns around being undersold, or giving up our user base and/or their data to parties not acting in community interest. We've set up an ecosystem which can welcome commercial providers with the expectation that they contribute back to the community