ICANN84 | AGM – RSSAC: SSAC Community Open Mic
Wednesday, October 29, 2025 – 9:00 to 10:00 IST

KATHY SCHNITT

Thank you. Hello, and welcome to the SSAC and RSSAC Open Mic. My name is Kathy and I am the participation manager for this session. Please note this session is being recorded and it's governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. If you have a question, you can raise your hand in Zoom, or if you are in the room, we have a roaming mic. When speaking, please state your name for the record and speak clearly and at a moderate pace. I will now hand the floor back over to SSAC chair, Ram Mohan.

RAM MOHAN

Thank you. And to my right is the RSSAC Chair, Jeff Osborn, and together we host this session for you in the community. We have a few slides to get started. So, let's go to the next slide. Okay. So, this is what we're looking to do. I'll provide a quick introduction to the SSAC, Jeff will provide an introduction to the RSSAC, and then it's hit us with whatever you've got, and we'll do our best to duck and weave. No, we'll do our best to answer the questions, actually.

So, let's go on to the next slide, please. Next slide. So, who are we? The SSAC is chartered by ICANN, and we are key part of the fulfilling ICANN's mission on ensuring the stable and secure operation of the Internet's unique identifier systems. Next slide, please.

And the way we do it is to engage with the technical community, analyze risks and threats to internet security naming and adverse allocation systems, coordinate with the various entities that are involved in this area, mostly in the technical community, again, but that the technical community inside as well as outside of ICANN, inform the ICANN Board and advise the ICANN community with our recommendations.

Next slide, please. Now, the SSAC is focused on five keystone topics, five areas where we have an enduring interest and where we strive to be an authority and be able to provide a clear technically grounded advice. And those five areas are DNS abuse, new gTLDs, DNSSEC, alternative namespace, and the security, stability and resiliency aspects of internet governance.

So, those are the five areas that we consistently work on and provide opinions and advice on. And if you look at the body of work that we've published, and we have 132 reports that we have published, you'll find that almost all of them will conform to one of these five major areas of work and study. Next slide, please.

And this is kind of what I was talking about, quite a bit of work, and I won't go through all of this, but this is a smattering of some of the main areas that we have focused on. And we continue to do work

in several of these areas. Right now, we have two work parties, one that is looking at DNSSEC operational and considerations.

We have a work party that is looking at responsible integration into the DNS ecosystem, which is focused on identifiers in the blockchain and other spaces and how they responsibly integrate into the DNS system. We are chartering two new work parties, one on DNS abuse and artificial intelligence. And another one that we are tentatively calling DNS transparency, but that's focused on the potential value of much faster updates to zone files because of a phenomenon that we're terming transient domains, domains that are registered and deleted within that 24-hour zone file update window.

And in that 24 hours, those names are used for multiple purposes, including malicious purposes. And for a security researcher point of view, they are effectively invisible because of the zone file update frequency. More on that area.

Next slide, please. These are some of the things that we have done recently. SAC127, at the Prague meeting, the last meeting that we had, ICANN83, we spoke about that to the community, we had earlier opined on DNS blocking, we updated our advice, and I would say the foundational pieces there were to say DNS blocking is now more mainstream, and our exhortation to the community and to regulators in particular was, hey, be aware that there is collateral damage.

It is often futile when you try to implement DNS blocking the way it's often implemented, and we also strongly recommend that if you do have to implement DNS blocking, that you adopt some of the protocols that are being developed that allow for transparency in blocking. So, you announce that you're blocking.

We've also provided some updates to the ICANN Board and the ICANN Org on name collision guidelines and some focus on the framework, the name collision analysis framework. And we just recently, SAC131, we provided some comments on the functional model for root server system governance.

And I think the summary of that is we appreciate the work that has been done, but we point out that it is not the end of the beginning, it seems like that is the beginning of the beginning of the work that actually needs to be done. And in our document, we point out several areas where we think real focus has to be provided. Next slide, please.

This is the group. We have 22 members in North America, two from Africa, you see the geographic listing there. We have been diversifying, if you will, across multiple ways of looking at diversification, and it's a fun group. It's a collegial group, and we try to get as much done as possible. Next slide, please.

This is the leadership team. Our approach is that staff from ICANN are a part of the team. It's not just the community members who run the SSAC. SSAC wouldn't run without those amazing people who are on the second row of this slide. So, there's just a terrific

collection of skills and abilities and personalities here, and that's what makes the SSAC tick. Next slide. Over to you, Jeff.

JEFF OSBORN

Thank you, Ram. Hello. Thank you. I'd like to thank Ram and Tara and the whole SSAC team for inviting us along to come on a joint open mic. Hopefully, you'll find it interesting and informative and hopefully we get some interesting questions. Next slide. RSSAC is boring to the point that we don't do graphics very well, we basically use mono font Sans black and white. So, this is indicative of the organization.

The role of the Root Server Advisory Committee, RSSAC is to advise the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the root server system. And the reason I read that out is that's the scope. That's it. We don't have five major points, we don't have three major areas we run, we advise the community and the Board on the operations of something we all do. Next slide.

RSSAC is the committee that produces the advice, and as I said, primarily, the advice goes to the Board in terms of documents, but its advice to the community, that's our primary function. The root server operators are represented in the RSSAC, but RSSAC doesn't involve itself in the operational matters of the root server operators.

RSSAC is made up of a primary and alternative representative from each of the root server. There are 12 bodies, so therefore one primary and one secondary, each is 24, plus incoming liaisons from other bodies, which makes up a total of 28 members, which isn't nearly as unwieldy as that makes it sound. Next slide.

There is in addition, an RSSAC caucus body, whereas to be part of the RSSAC, you need to be either the primary or secondary operator of a root server operator or the liaison. The caucus is made up of, it says 128, I think it's just over 100 actually, DNS experts from around the world who can apply freely from anywhere with a public statement of interest and let us know they'd be interested. I'm actually also the chair of the Membership Committee.

We are a pretty open organization, but the thing I'd say is this is not a forum for coming and learning how DNS operates, it's a functional group of experts who are expected to perform some fairly serious work. So if you come and want to learn, we can offer you a mailing list membership, but actual members of the RSSAC caucus are expected to be experts in their field and have operated and implemented some fairly major DNS works just to set that bar. With this bigger group of experts, we bring broader experience to the stuff we write. We have better transparency, we hope, and we try to get things done.

Next slide. We too put out publications. I think SSAC dwarfs us in the volume of what they put out. But again, we have a very narrow

remit. We're really concerned primarily about the root server system. Recently, two reports we put out, involve changing IP addresses and a security incident reporting document. These are sort of for the geeks, these are not light reading, but if you're interested, we do fully document what we do. We're very transparent, we're very open, and we publish our work. So, these are some of our recent topics.

Next slide. And the better looking gentleman on the right is vice chair, Hans Petter Holen to my left, and this makes me realize, I'm glad I shaved the beard. But Hans Petter is just joining on, I'm serving in my second term, and it's been a pleasure. I think this is the last slide. Next slide. There we go. Thank you.

RAM MOHAN Thank you, Jeff. And Danielle to my left is gonna help manage the queue. So, now is the time to ask us anything.

DANIELLE RUTHERFORD All right. Feel free to wave your hands wildly or raise your hand in the Zoom, and I will get your questions in the queue. The gentleman on the right of the U, please go ahead.

ANDREW MCCONACHIE Okay, thanks. My name is Andrew McConachie, I work for ICANN, speaking for myself, obviously. I finally got around to reading the DNS blocking paper, and as I was reading it, there was like this one sentence in the middle of it. This is a really nitpicky question, by

the way. There's one sentence in the middle of it that I just couldn't get past and I just kept thinking about it.

So, I'm just gonna read the sentence because I don't expect everyone to have the report ready. But it's from page 11, section 2.1, and the sentence reads, "The use of DNS blocking for security and anti-abuse purposes is pervasive, and most internet users in organizations are protected via DNS blocking."

And I was reading that sentence and I was thinking, okay, because there's no citation, there's no reference there, and there's really no proof for that sentence. And in my gut, I feel like that sentence is true, I think that's probably true, but looking through the paper, I don't see any justification for how you would prove that.

So, it's kind of a question of like, I think that's true, I don't know how one would design an experiment to prove that. And also, shouldn't the paper, not necessarily make a bigger case for that sentence, but make a justification for that actually being true. And maybe that can't be via citation, maybe there is no way to prove that, but I just got really hung up on that sentence.

RAM MOHAN I'm wondering if Gabe is on the call. Maybe too early for him. Warren. Co-chair.

WARREN KUMARI Yeah, I don't think there is any citation, and I believe there was some discussion in the working group on whether or not to include that.

DANIELLE RUTHERFORD Warren, can you speak a little bit closer to the mic?

WARREN KUMARI Sure. Yeah, there's no citation, and I don't think there is a way to prove it or disprove it. There was also some discussion in the working group on whether or not to include that sentence because it's not necessarily clearer if it is provable or, yeah, I'll just stop talking now.

RAM MOHAN Thanks, Andrew. Wes.

WES HARDAKER Andrew, you pointed out a problem that is generic. We actually have a similar problem on the RSSAC side of, we know that there's a lot of resolvers out there that don't cache. Can we prove that? No, not easily. We know that we get requests from IP addresses that are too numerous, we don't know if they're behind a gnat and that's why we don't get them.

We don't know if they're rebooting every five seconds and their cache is gone. We don't know the reason behind it, but we know the net effect. And you're 100% right, in an academic conference,

that sentence wouldn't fly. So, how do you document things that are generally widely accepted, but actually have no proof? It's a generic problem, and it's a fantastic question.

DANIELLE RUTHERFORD I've got a hand from Peter Thomassen, SSAC.

PETER THOMASSEN Hi, Peter Thomassen. So, I actually took my hand down, but anyway. So, the large resolver operators like Quad8 and all of these, they do adhere to court orders when they're legally justified to block things. And now I don't know the exact fraction of internet users that use such resolvers, but I think there is numbers for that. So, probably the claim in the paper isn't so unfounded as it seems like.

WARREN KUMARI Who's next? The claim in the paper is that it's protecting them from security things in the majority of cases, government blocking is not necessarily protecting people from security things. It's protecting them from influencing their view of the internet for other reasons. So, the way the sentence is phrased, yeah.

DANIELLE RUTHERFORD Maarten.

MAARTEN AERSTEN So, thank you for reading it that closely, and now I'm looking forward to you reading our latest report. And I'm not sure if I should be happy about that or scared, but I'm looking forward to the next session in, what is it, Mumbai, where you'll ask a hard question about a new report.

ANDREW MCCONACHIE If I can just respond. Thanks a lot for taking this question. I guess now I'm wondering maybe it's not possible, but is it possible to design an experiment that would actually show whether or not this is true? I don't know if that's possible, but that would be really cool.

WARREN KUMARI You could, without too much difficulty, decide on what you think are bad security issues and try and resolve them through, for example, Atlas, and see how many users are able to resolve them versus not. That would require trying to resolve a reasonable number of bad things and decide where you think a reasonable cutoff line is for that. But you could measure it. Not entirely sure how Atlas people would feel about you resolving all of the bad names on the internet through their resolvers, but.

DANIELLE RUTHERFORD All right, I'm looking around the room once again. Yes, sir. Please go ahead.

WOUT DE NATRIS-VAN DER BORGHT

Yes sir. Thank you. I'm not one of your community, but here as a guest, more or less. My name is Wout de Natris-van der Borght. Yes, I'll speak up closer. Thank you. My name is Wout de Natris-van der Borght, and I am the coordinator of an internet governance forum Dynamic Coalition on Internet Standard Security and Safety, and what we try to do is promote the deployment, mass deployment of internet standards and IT best practices.

As a short introduction, we produced six reports in the past four years on many different sort of angles to the topic, and the last one is on post quantum cryptography. And we published that in Oslo at the IGF. And we've been asked by one of the ccTLDs here, and I'm signing the contract on Friday, so I can't disclose the name at this point because that would not be in need.

But we've been asked to set up two working groups on DNS and RPKI and the deployment of PQC in the future, and to bring together experts from different stakeholder groups, including, of course, ICANN and the RIRs. And my question is, who would potentially be interested to join this working group?

Because what we will do is set the agenda more or less at the first phase and see what are the challenges, what are the timeframes we should be looking at, and what should the next steps be? So, anyone interested, please speak to me because then you will get an invitation to a kickoff meeting somewhere in the coming months.

RAM MOHAN Thank you so much. I'll speak on behalf of the SSAC and then pass to Jeff. From the SSAC's point of view, this sounds on the surface like something that is within our remit and might be interesting. If you could please send a note to me with our SSAC staff copied into it, we'll put a process together to find the right people who are qualified and who have the time available to be able to contribute to this effort. Jeff.

WOUT DE NATRIS-VAN DER BORGHT Thank you very much, and let's change cards so we can say easily, of course.

RAM MOHAN Sounds good.

WOUT DE NATRIS-VAN DER BORGHT Thanks.

JEFF OSBORN Excuse me. Yeah, as I said before, our remit is really narrow, but we cover a lot of territory. I literally have a staffer who's getting his PhD in post quantum crypto. So, let's talk because we may have people who'd be interested to do it, but I don't know, it's so much in RSSAC as the individuals within RSSAC.

DANIELLE RUTHERFORD All right. And I believe we have a hand and a new question from Ram Mohan.

RAM MOHAN Thank you. I just wanted to, for those who may have not, probably as many of you, paid attention to one of the documents we wrote, SAC 131, in SAC 131, we had specific comments on the governance in the root service system process. And we have here one of our members who helped co-write that report and who has also been integrally part of it. So, I'm wondering if I could call on you, Suzanne, to just speak to the main points we are trying to make in that report which I alluded to in my intro comments.

SUZANNE WOOLF Thanks, Ram. I feel a little bit silly being the one to speak on this since most of our RSSAC colleagues were also involved in that process. But sure, I can address that. The effort to come up with a more institutionalized governance body or set of processes for the root server system has been going on for quite a long time, partly because there are some complexities that it's hard to engage with and partly because it has not been urgent.

The system has worked and worked extremely well for a very long time. So, there is often something more urgent that sort of occludes the need to do that. However, people have committed on it, and the GWG has come up with a document that lays out a

roadmap for continuing to formalize root server system governance.

Because the effort has been going on for a long time, there were actually a number of public comments to the effect that there was still some major questions that the DWG has left open. But the document that was produced and put out for public comment does represent significant progress. And we are happy to encourage and participate in further progress towards a robust and resilient and trustworthy system of root server governance.

RAM MOHAN Thanks, Suzanne. Warren, did you have anything you wanted to add in this area? Because I know that you've been interested in this area as well.

SUZANNE WOOLF Yeah, if any of the RSSAC folks in the room that were also part of the GWG, I'd certainly encourage you speak up.

JEFF OSBORN Hello. Abstinent of any other input, I can provide what I said to the Board when we met with them on this yesterday. We look forward to the continued support of the Board and Staff of ICANN and we're continuing.

Having sat through a lot of those meetings over the last very long period of time, I think the fact that we haven't gotten as far doesn't

have as much to do with the lack of urgency as a-- oh, good god, I can't believe I started that sentence. I'm gonna withdraw that sentence. But I don't think you can blame it on a lack of urgency. It's something else harder to define.

RAM MOHAN Other comments? Quiet crowd today. Must have a lot of good email to catch up on. Ken.

KEN RENARD Thanks. This is Ken Renard, RSSAC root server operator. Just a quick comment on the PQC question from before. Just to put things in context with respect to RSSAC and root server system, a lot of us are engineers, we're very interested in this stuff and have a real thirst for working in this area. But officially from the RSSAC and the root server system perspective, we aren't involved with the crypto, we just get the root zone already signed and serve it.

So really, the only really place where it affects us is how those new signatures are going to affect packet sizes and how the operations on our systems handle that. So, we as RSSAC, the individual RSOs are definitely following that, very interested, but the immediate concern for RSSAC is pretty small with respect to just packet sizes and not the fun cool, nerdy cryptography. Thanks.

RAM MOHAN Any questions or comments from remote participants for this meeting? Hans Petter.

HANS PETTER HOLEN Hans Petter Holen, and I'll put this on with my CEO of RIPE NCC hat. And one thing that's popped up now internally is in the crossroad of numbers and names, which is [0026:33 - inaudible] .arpa. And what I'm looking for is not folklore, but hard sources of what is the criticality of [00:26:44 - inaudible] .arpa for the stability of the internet. Does anyone have a good answer to that?

WES HARDAKER Anti-spam, that's probably the number one usage of it.

HANS PETTER HOLEN So, you're saying only mail, no other protocols?

WES HARDAKER No, that's the one I know of, and it's, I think, the number one.

HANS PETTER HOLEN Well, that's the one I knew about.

WES HARDAKER Yeah. And probably people use it for reverse lookups to figure out-- trace route's another good example, as well-- as I know it's used

for like SSH logins and stuff because if reverse DNS is not working on the host, it greatly slows down your ability to log in.

And actually, that's a real problem because if you have a badly operating local DNS and you're trying to get in to fix it, you suddenly find yourself incredibly delayed getting in because it's trying to look up your reverse name.

HANS PETTER HOLEN But what I'm looking for is kind of like, is there somewhere this is described, somebody that has looked into this and there is a paper to refer to or something like that.

WARREN KUMARI I'm trying to remember exactly how, but isn't enum.arpa reverse lookups also used with SSH connections? Was it? I was looking for the reference while you were saying that. Trying to find the words.

WES HARDAKER So, that would actually be an interesting study because I believe DITL data contained some servers from enum.arpa, and so there may be a reasonable amount of what's being looked up to try and figure out what's happening there, that it would be a good scientific study for somebody that wants to take it up.

HANS PETTER HOLEN Thank for the--

WES HARDAKER Wes Hardaker from USC-ISI and Google.

RAM MOHAN Danny, you want to speak on this?

DANNY MCPHERSON No, I was just pointing out that ENUM e164.arpa is used pretty extensively as well, but there are lots of other things there. I'm not sure I want to enumerate those here.

HANS PETTER HOLEN May I respond to that? So, when you say use pretty extensively, do you have any source for that?

DANNY MCPHERSON I haven't done a study of this, I know there are lots of queries out there. I'm sure that somebody could enumerate that. I know of a few things that use it, but I haven't seen anyone study what everything that uses it is, so.

HANS PETTER HOLEN The reason for asking that question is that RIPE NCC is the operator of that domain and that service, and on first glances, we did not see very much traffic there.

WARREN KUMARI So, I think your initial question was enum.arpa, but there's a bunch of other stuff that ARPA is used for as well, like the resolver discovery stuff and those things, which I think are actually relatively widely used and are important and sort of critical to a bunch of services functioning. So, are you specifically worrying about the enum.arpa or ARPA as a whole?

HANS PETTER HOLEN Yeah, since RIPE NCC's operating service is in enum.arpa, I need to understand the criticality of that. No, that actually goes for ENUM, but all the other services I may or may not have an operational responsibility for it. So, it's also interesting, but not for this purpose.

DANNY MCPHERSON Seems like RIPE NCC should do that analysis if they have the data.

RAM MOHAN Any questions from the back of the room? From the sides? Okay, please. None back there. One back there.

UNKNOWN SPEAKER I was just raising the microphone. How's everyone doing?

RAM MOHAN I thought-- oh, there you go, please.

ROBERT CAROLINA

Hi. Rob Carolina with RSSAC, I'm also with ISC, which for reasons that will become clear in a moment, I should say maintains open-source software that implements DNS by nine. The SSAC recently came out with a very thoughtful well-constructed document talking about the use of open-source software in the root server system.

And in a session yesterday, I was asked a question about open source software in the root server system, and I tried to give a very brief answer, which said that we view it as a positive aspect of the root server system as a whole, but as a non-technician and a non-member of SSAC, I'm wondering if anybody on SSAC would like to comment more generally on your findings in that paper about the use of open source software within the root server system.

RAM MOHAN

I think we happen to have a couple of people who might be interested. Maarten.

MAARTEN AERSTEN

Sure. Thank you for the question. So, yeah, we wrote a report and we delivered a couple of presentations throughout the week. So, I'm not sure if all the positive things and all the negative things we have to say about FOSS in the report are specific to the root server system as such. But we say that it's a different risk profile to proprietary software.

So, on the one hand, we say that there are some unique risks that come with the way free and open-source software works such as where software is maintained by volunteers. They can have a burnout, they can lose motivation and they'll just stop.

Where it's organizations, they might be threatened in their funding because of new regulations. But on the positive side, if you look specifically at DNS and specifically at the software that we know root service operators to be using, what is in general applicable to FOSS does not necessarily apply to the DNS.

And in the DNS, we see that there are these long-lived organizations that have been at this for more than 20 years and have gathered a certain amount of operator trust. In the report, we've surveyed operator sentiment about FOSS and its strength, and one of the one of the findings that came out of that survey was that multiple operators cited the transparency in a supply chain as a positive because they were free to do patching at their speed.

So, the example was if you have a name server and there's a vulnerability in a component, in proprietary software, you would have to wait for your vendor. And here they could just patch the component, build the name server, and deploy the software.

Now, finally a positive that we came up with is the independence angle, like the ability to-- I'm sorry, I'm blanking for this one just a little bit. So there's key strengths, and on the notion of security, we're saying open source doesn't determine the security, it's maintenance processes that do. So, when people ask is false

secure, the answer is not no, the answer is not yes, the answer is neither, and it has nothing to do with the license.

So, that's some quick reflections on what we wrote. We have a couple of presentations, short ones, for example, for the GAC, which are, I think particularly suited for a policymaker audience, an hour long one which was yesterday, and we published a report and I'm happy to talk to you at length about it and to others offline.

But I appreciate the question and we appreciate the responses from the root server operators both publicly ahead of this research having been transparent about their use of software for years and also where they had not been by telling us confidentially that they, for example, are using FOSS and choose to not disclose which particular software. So, thank you for that help. We couldn't have written this report without your support. And I'll stop talking at this point.

RAM MOHAN Thank you, Maarten. We presented on open-source software at the GAC yesterday in a striking conversation on the sidelines after our presentation representatives from two governments spoke to me, and they had some interesting questions about some of the findings in our report.

And specifically, they were asserting or maybe questioning is a better way, that open source is far more insecure because anyone could introduce a vulnerability into the source code and

governments would have no recourse in that case as compared to a more proprietary model.

So, I spent some time explaining kind of how it actually works rather than the perception of how it works. But it was interesting to see that that perception is still-- I had thought that after so many years of open source commonly used and being super secure and vulnerabilities being disclosed and really good protocols associated with it.

But it's interesting to see that we still have to continue doing that education on a consistent basis, especially because there are, and this was a big eye-opening thing for me at this meeting, was recognizing that inside of the ICANN community in particular, something like 80% of the representatives in the GAC are brand new.

They were not the same people who were around a year or two years ago. So, all the messages that we have gone and presented, the SSAC RSSAC technical community that we've gone and presented that we believe are accepted ground truths, we have to kind of reassert them, reintroduce them.

And so, that's really a homework for us and kind of a reminder for us that the things that appear boring for us and commonplace and self-evident for us are for many of this target audience are brand new. Maarten.

MAARTEN AERSTEN: Yeah, I can only mirror what you said, and it's not just governments. So, last week I was interviewed by a rather prominent Dutch research institute and they were looking at the security of Dutch critical infrastructure, and they asked very similar questions to the one you have just-- well, it's good that these questions are asked, but the thinking behind them shows that we have a lot of work to do.

And when we published the report, the first feedback I got was from some people in the open-source community, and they were like, ah, man, this is not news, everyone knows this. And bridging that gap between operators, technologists, developers, and people who actually make laws is so important because otherwise, we'll get laws that are just not compatible with what's out there, so yeah.

RAM MOHAN: Please.

WOUT DE NATRIS-VAN DER BORGHT: Yes, thank you.

RAM MOHAN: And Ross, I'll come to you in a moment, I just am keeping on this topic. Back to you.

WOUT DE NATRIS-VAN DER BORGHT: Wout de Natris-van der Borght. I can only speak from personal experience how important it is to keep pushing the same message because it's not only the government people you're talking to here, because they're usually an international policy of some sort. It's about the people behind them that have to be informed correctly as well, and people, there's just a churn in all.

Well, there's an industry, even in your community, somebody will be new at some point, so it has to become DNA of your community to actually always be in the awareness and outreach mode as soon as necessary. And I can only speak from personal experience how important it is that people understand what you're trying to achieve, and only then you have a chance at getting into the mind of people.

RAM MOHAN: Thank you. And I imagine that ICANN's OCTO encounters the same phenomenon in the work that they do. Okay. Let's switch to you, Russ.

RUSS MUNDY: Yeah, thank you, Ram. Russ Mundy, SSAC. I wanted to just respond to Rob's question and thank him for the question. As you probably are aware, SSAC tries to have data behind their statements and comments, and in spite of Andrew's excellent question earlier today about blocking, I have to say that when the work party was

working on this space of where is it actually used, is the open-source use versus proprietary or closed source.

The easiest place that we had to work or area of the DNS that we had to work on was actually the root server system for a couple of reasons. First, that there's a much more constrained number, a much smaller number of activities involved than there are in other portions of the DNS.

And the other reason is we've maintained a close working relationship over time. But to the bigger question, I think you were raising Rob, is what can be taken away in terms of using comments for use of open source in the roots as it affects or as it was pointed specifically at the roots?

And I think that Maarten's summary of what the report contains, I think all of those things may be in varying degrees, but I think they all apply to the root server system. And so, it was, if you will, trying to abstract out of this mass of data that we tried to assemble in the worl party, a useful set of things that could be written down and provided to the community. But I think it applies equally to the roots as well as all the other parts of the DNS. Thanks.

RAM MOHAN Thank you, Russ. Any responses to what Russ said? Okay, no responses that… Onto you, Rick.

RICK WILHELM

Thanks, Ram. Rick Wilhelm, PIR, SSAC. I wanted to come to a comment, Ram, that you had made, you had talked about members of the GAC and the turnover in the GAC, and that's sort of for those of us around ICANN sort of a consistent-- the membership in the GAC is consistently inconsistent. And so, that's not a new thing.

But I think as any technical folks are talking with, whether they be GAC members or government folks in whatever capital you happen to be working in, you need to remember that you're not pushing a point across level ground, you're pushing it into hedge winds that are being created by closed source companies because they have a vested interest in pushing and selling closed source software.

And it's not necessarily DNS closed source software that we're talking about, those hedge winds are created by much larger corporations selling other packages in other parts of the software ecosystem.

But then what they're trying to do is create standards and requirements for all sorts of things, an environment in which it makes it difficult for open source to thrive. And so, you're not selling into a level playing field, you're selling into a playing field that's being created by lobbyists and government affairs that are pushing the points made by large close source companies.

And so, just be aware that when you're talking to people, that's what they're hearing. They're from the other side, and that's what the other side looks like. Thank you.

RAM MOHAN Thank you, Rick. Valuable points for us to all remember and consider. What else do you want to speak about here? There's a good gathering of people. What's on your minds? Wes.

WES HARDAKER I have an answer for Hans Petter. So, I took a million anonymized queries from the last DITL collection at B Root from one site, just randomly, looked at how many ARPA requests there were in those a million, there was 4,602, that was for the ARPA TLD. Inside of that 4,133 were inside of in-addr.arpa, 129 were for ARPA TLD itself with nothing else, 93 were inside of ip6.arpa. There were no queries.

Again, this is a sample of only a million, it's consequential in part. There was none for ENUM at all actually. Interestingly enough, there were 12 for www.zz--icann-monitoring.arpa. Yeah, realtime research. It's always the goal.

SUZANNE WOOLF What was that? Just in time research?

RAM MOHAN Kenny, please.

KENNY HUANG

Kenny Huang, speaking [00:47:07 - inaudible] APNIC Council Chair. And APNIC is actually deeply involved in the coordination and support for the deployment for root Anycast in the Asia Pacific region. And there are two things actually we require, probably require to hear from anyone, from you.

And the first issue is, a lot of economy, actually, they're requesting for root Anycast deployment in the economy, but that kind of negotiation with different label of root Anycast basically is quite… there is not consistent standard because sometimes they require financial support, sometimes they require facility support, sometimes they require highway or provisioning support.

So, we need to negotiate with that kind of support with the local supplier and root server operator as well. So, the first issue, if you can identify any consistent financial model or any consistent deployment model, probably that would be very helpful for us from budgeting point of view.

The second issue will be, same, a lot of economy request for root Anycast deployment in their particular economy, and usually we're just receiving that kind of application, we facilitate and also try to identify the demand and also explore the local environment.

But still very difficult for us because we don't have a very clear picture regarding to what kind of service level are in different region or in different economy. If you can provide some sort of

more clear picture for us so we can better understand what will be the better location best fit for the [00:48:41 - inaudible] Anycast deployment. Thank you very much.

RAM MOHAN Hans Petter.

HANS PETTER HOLEN Yeah. Thank you, Kenny. So, Hans Petter Holen, RIPE NCC, operator of K root. So, with my RSSAC hat on, I don't think there is a consistent model across the root server operators. But some of us, like RIPE NCC have published all criteria or model for how you can do it with us, and I know that other root server operators have done the same.

So, I'll have a look to see if this is easily available in one place or whether that could be compiled as an overview. I see Jeff is jumping in now. But from the RIPE NCC side, from K root side, more than happy to work with you on model for Asia. When it comes to deployment and where to put it, I know some of my researchers have done some work in that recently, but I don't know if that will answer your questions.

RAM MOHAN Liman.

LARS-JOHAN LIMAN

Thank you. Lars Liman from Netnod, also operator of root server and member of RSSAC. This stems, this that you perceive as a problem stems from a very important property of the root server system, meaning it's diversity. We all operate in different ways, and that goes very deep into the system.

So, we have different types of hardware, different types of software, different types of financial model, different types of organization, as many things as we can, and we want to be different because the diversity is a very important strength of the system. As soon as we create something that is common between the root server operators, that becomes a single point of failure.

So, having different ways to operate and engage and interact with our site hosts is good. I understand that creates a problem, but I would argue to involve us in the process. Netnod has a very longstanding and good relationship with LACNIC, where we interact with their staff because they have the local knowledge and they receive requests for deploying root servers.

And we find different funding models for different sites, we find different ways to deploy in different sites, and since we are involved at a very early stage, it works very well. It's also the case that there can be different motivations for deploying a server in a certain region. And the funding model can be different, and sometimes, the root server operator can see a need to deploy in a region and want to push it from the root server operator side.

Sometimes, the local economy or the local community has a wish to have one deployed, and that's a bit of going back and forth. And I honestly don't want to unify that too much, but I would like to be involved so that we can work together and find the best places to deploy, absolutely. Thank you.

JEFF OSBORN

It was a great question. Liman, of course, always puts things better than I can. It is a feature rather than a bug that there isn't a uniform way to do this, because one of the strengths of the root server system is there is no single point of organizational failure. I have that tattooed on my shoulder, but it's still fresh, so I don't want to show it.

Ray Bellis, who runs our root server-- oh, I'm Jeff Osborn, and my day job, I'm president of ISC. So, we are a root server operator, and Ray Bellis, who runs that, posted the link in the chat on here where you can learn how to do it. We've worked with an awful lot of people in the APNIC region to provide free services, set it up and everything else.

And in fact, if you want to talk a little later, I was just looking at how to get somebody to Jakarta, it's about time to do a refresher on how this works. We got interrupted by COVID and we're still catching up, but if there's an opportunity for some of one of us, I know I'm gonna have several people there, maybe that would be a good time to introduce something.

WES HARDAKER

One other thing that you might consider, there's the technology in ICANN known as Hyperlocal that allows your resolvers to pre-cache the entire root zone so that you actually don't need to talk to the root servers. At ISI, I actually started a project called localroot.isi.edu that helps you do the configuration for that.

Based on a trend, we recently tried to look at how much that in usage has been increasing in the past five years. There's a significant increasing rate of adoption of that sort of technology. And in fact, Warren Kumari to my right, and a couple others of us are actually writing a new document for the IETF to make it the recommended practice that resolvers should generally be doing this. It helps your resolver in a number of ways.

And so, you might consider looking at those types of related technologies too. A lot of recent DNS resolver software actually allows you to pull the root zone over HTTPS to not just using DNS itself to try and get the bootstrapping in place just as another consideration. But of course, that's for the resolver side, not for...

KENNY HUANG

Thank you. I think we will pass the information also to the application, who will submit the application from any particular economy. I think the technology advancement is very useful, especially right now you don't need to explain, you don't need to apply for any particular label of root, you just need to apply for

Anycast, but right now, if there's more advanced technology, we're willing to introduce to our member. Thank you.

RAM MOHAN Okay. Any other comments, questions? Thank you, Kenny, for that question. Anybody else? We have about four minutes left for this session to wrap, so you get like three minutes to pose something. Otherwise, we're gonna be done. Going once. All right. That wraps this session up. Thank you everyone.

KATHY SCHNITT Please stop the recording.

[END OF TRANSCRIPTION]