DAN GLUCK: Hey everyone, welcome to the 49th RZERC Teleconference on the 24th of February 2025 at 20 UTC. This call is being recorded and is subject to the I Can't Expect Extended Standards of Behavior and Community Anti-Harassment Policy. With that, Geoff.

GEOFF HUSTON: All right. So, Dan, I assume that you can do the roll call from the meeting attendees in your screen. So we're cool for that. And thank you all for coming. I hope the pushing it back by one hour works for Kalina and works for everyone else. So it seems that everyone else is on. I'm not sure if anyone's missing, but we're good. So in the last meeting in January, we heard from Willem on the study that we had requested back in the dim, dark mists of time on whether or not Rootservers.net or, in fact, the name service for the root one way or another should be signed. And at the end of that presentation, there was some sort of uncertainty about, well, what to do then. And it's kind of uncertain, at least as far as I recall from this conversation, as to who had the ball and what could they do with it, which is an interesting kind of question. It's a very good study. But I think there are some conclusions there. And again, if I'm wading through your slides, Willem, I'm trying to remember the exact slide that actually had your conclusions.

WILLEM TOOROP: I can put it on screen. Yes. So in the study, we put a number on how much the risk would be reduced, which is not a very high number. But furthermore, we note that only 0.1% of resolvers depend on or actually

query for all the root server addresses authoritatively, or they request the authoritative version of the root server addresses. So if you would sign it wrong, it would only affect those 0.1% resolvers. And the other ones are also basically less affected. They also use the unsigned additional addresses and will not be affected by whether or not those addresses are signed wrong, so to say. And by the way, that 0.1%, those are likely Knot resolvers.

GEOFF HUSTON: As in KNOT rather than NOT, right?

WILLEM TOOROP: Yes. Yes. KNOT, yes. KNOT or Knot resolver has the property that it does query for all the root server addresses during priming. Oh, Duane.

DUANE WESSELS: Oh, thanks. Willem, can you remind me, the 0.1% Knot resolvers, are they also validating?

WILLEM TOOROP: I don't know, but I assume they are. In the study, we assume they are validating. At least they are querying for all the addresses. And if they would be bogus, then they have a problem.

DUANE WESSELS: Okay. Thanks.

WILLEM TOOROP: If they are validating.

GEOFF HUSTON: So I would like to put forward, I suppose, the proposition that RZERC write a note to the ICANN board referencing this report and recommending that rootnameservers.net be DNSSEC signed. So, Duane, I take it that's a new hand in response to my proposition.

DUANE WESSELS: Yeah, yeah. Yeah. I think maybe before we get to that point, there was something that I think we could discuss, which is, you know, the study that sort of prompted all this was considering different names for the root servers, right? And that always seemed to me to be a cleaner solution to this, although maybe a little bit harder pill to swallow because it's an important change, right? But in terms of DNSSEC and security, it seems cleaner. And I feel like that is still something that RZERC has not come to a conclusion on. So I guess my other point is I think it would be unfortunate if RZERC recommended signing in the current situation, right? And then RZERC went and said, well, let's change everything. Let's change the names. And then, you know, you've sort of wasted some effort. So I just wanted to raise that and see what people thought about that.

PETER KOCH: Yeah, thanks, Geoff. This is Peter, for the record. I would like to agree with what Duane just said. We might not want to jump the gun here and

wait what the exact details of such a scheme would look like or what would be the recommendation for RZERC in that case. And on a second note, we got this number, 1.2% risk reduction. The counterweight seems to be the 1.1% of resolvers that might have an issue, but everybody hopes they don't. This is – I'm not sure that this paints the whole picture. And I can't tell at the moment what I think is missing. And that would only be the risk assessment. The question is, what is the overall effort for all the parties involved to achieve this and to make sure that this is then operationally feasible? And maybe we should, in that note that we would write to the board at any point in the future, we might want to add some considerations along those lines. Thank you.

GEOFF HUSTON: I've put myself in the queue in responding to Duane, and I must admit I think it's hard to make a decision that in retrospect is going to be absolutely right. I think in some ways we can only figure that out once it's been tried, once it's been deployed, and then sort of pick up lost strands if there are any. I don't think the signing of this zone and the use of that zone for the names of the name servers is difficult to change if RZERC wants to then change those names. I think the principle and practice of allowing validating resolvers to validate those names in terms of the authenticity of their association with an IP address is sufficiently useful, even if it mitigates a small risk, to be worth recommending to do. And if RZERC wishes to change the name structure at some point, then the signing of that name structure can flow with it rather than separately consider signing if at any time the name structure is being changed. So while I appreciate it might be, I

suppose, less of an overall change if we wait for RZERC, I'm inclined to lean to the idea that we can recommend signing now and RZERC would, I'm sure, be queried by the board to say, are you ready, do you think this is a good idea? They would then have their opportunity to respond to that at that time in any case. It's a tough call, I admit, and quite frankly, the amount of validation going on in this space is indeed, as we've sort of seen, quite small. The use of not is not overwhelming in the internet at large, as far as I can tell, but it does seem to me to be an overall risk benefit that weighs in favor of signing, but I will shut up at this point and ask Andrew.

ANDREW MCCONACHIE: Yeah, thanks, Geoff. So after last meeting, I wanted to get a handle on kind of who was waiting on who or if anyone was waiting on who between the board and RZERC and RZERC. So I looked into all the various recommendations in 028 and RZERC 002 and I sent a mail to the list and basically the answer is everything is closed. There's not, as far as the ICANN paper trail or the ICANN action request register is concerned, there's no party within ICANN that's waiting on another party within ICANN to do something. So I just want to make that clear that whatever this group decides to do, it's not going to be bound by something which exists in some ICANN system where there's a pending action item for someone that's been open for years, as there often sometimes is. So essentially, you're free to do whatever you want. And the RZERC isn't going to pick this up unless maybe the RZERC prompts them.

LARS JOHAN LIMAN: Hi, and thanks. I'm sorry for having missed the two previous meetings, but they clashed with travel. So I'm glad to be here, but I feel a bit, what's the term, parachuted in. I raised my hand and then I thought a bit more. So the thing I was thinking about was would signing the root service.net zone with its current name schedule, would that put in a denial of service possibility from a process standpoint as we have to step through net to validate rooservers.net? So would it give the net operator a power to create denial of service? But then it struck me that the net operator is Verisign, Verisign already operates the zone for root and for root service.net. So they have all the tools they need if they want to create havoc already.

GEOFF HUSTON: While I notice that Kim and Duane are in the queue, Willem, could you think about your answer from the report and maybe add yourself to the queue afterwards? Meantime, I will ask Kim.

KIM DAVIES: Yes. So I just had a comment on the procedural notion that RZERC should make a recommendation and then the board would consult with RSSAC subsequent to that. I'm just looking at the charter of this group of RZERC and the implication in the charter is that we should be consolidating all the necessary inputs before we make a recommendation. The committee will not necessarily be the group that considers the details of the issues raised but will be responsible for ensuring that those involved in the recommendations to the board include all relevant and impacted bodies and will have access to the

necessary expertise to provide the best possible recommendations. The committee will coordinate with the committee's respective organizations and communities and as appropriate external experts to ensure that relevant bodies and impacted parties were involved in this discussion and recommendation development. So I don't know if that then, you know, my reading of that is perhaps the burden is on us as a group to make sure that RZERC is aligned and has considered our recommendation in advance of making it. Thanks.

GEOFF HUSTON: Thanks, Kim. I'm just making a note that if we were going to do that, my initial shortlist would be something like RZERC, the Root Zone Manager and of course the IANA. But Duane, you had your hand up.

DUANE WESSELS: Yeah. So thanks. This is Duane. So in response to the point that Liman raised, so not so much that there's an attack or denial of service opportunity here, but the point you raised, I think, was one of the reasons that RZERC took on what became RZERC 028 initially. People said that the root server should have names that can be validated, but they were uncomfortable with the idea that there was this in-between zone dot net, not for reasons of DDoS, but maybe for reasons of just process failure, that it adds some extra complexity into the whole signing process, more DS records to maintain and whatnot. So that was a concern. And I think that was one of the reasons why RZERC started the work to look at alternative naming schemes.

GEOFF HUSTON: Thanks Duane. So Willem, I seem to recall outside the PowerPoint, the actual report that I admit I read a month ago considered this at length. So what did the report have to say on this topic?

WILLEM TOOROP: Well, the report on the second recommendation, this is the conclusion for the report on the second recommendation. It says that the value of signed root name server data is if resolvers use those authoritative addresses. And one of the consequences, so if all resolvers would do what Knot resolver is doing and check all those addresses or queries for all of them, then traffic to the root will increase with a 30%, which is substantial. With RZERC 28, we only studied all the different naming schemes again, and studied open source resolver behavior. So Bind, Unbound, Knot resolver, and PowerDNS recursor, and several older versions of this software, because the assumption is they cannot be changed, right? If the Google resolver does something crazy, or the Cloudflare resolver, then we can reach out and say, you know, your resolver should be adapted to work with this alternative naming scheme.

So a few naming schemes, well, fell out of the consideration, because those open source resolvers can't cope with them. One of them is the 5.4 scheme. I can perhaps also put all the schemes on the screen. But what I want to mention is that the one with the least issues was 5.5, a name delegated to each operator. But this would, I assume, would be most cumbersome, because then each root server operator would have to host their own TLD, so to say, to host their own IP addresses for their

own server. So that's a big change. Though the open source resolvers have the least issues with this naming scheme.

Then there were two naming schemes, 5.3 and 5.6, that had all names authoritatively within the root zone, which is easiest operational, I think. Then you just, it will be signed alongside the root zone, and all is good. And the issues that we had with those naming schemes were mostly introduced by how the open source authoritative software handles it, right? Because BIND, for example, if the additional addresses to an authoritative priming query do not fit in the additional section will not include any address in the additional section which is problematic for PowerDNS recursor. But those open source authoritative servers can be adopted so that they don't have this behavior which will be problematic for old and new open source resolvers anymore. So it's a subtle story, I think, with pluses and minuses.

GEOFF HUSTON: Thank you. I must admit that I was looking at the proposal based on the recommendation to sign the names as they exist today. I think the RSSAC study on potential name changes is correctly being done by RSSAC. I wouldn't necessarily say it's none of RZERC's business, but nevertheless, that study is being done. I don't think we need to enter into that area uninvited and unbidden. I think we can leave that alone and consider this on its merits of should root nameservers.net be signed and note that were names to change, the signing issue would need to be carried along with it and not necessarily assume that any new name system would be unsigned. The default would be that once this is signed, it would be signed thereafter in any new name system. And that

is, I suppose, my working assumption. If others disagree, perhaps now is the time to say so. Willem?

WILLEM TOOROP: Yes, I want to add that the conclusion that the 1.2% benefits and the 0.1% resolvers who would be at risk are independent of the naming scheme used.

GEOFF HUSTON: Right. So, in the light of Kim's comments, which I take to heart, and I think it's appropriate, that rather than saying to the ICANN board, you consult, we take it upon ourselves to conduct a consultation, my shortlist of folk to say, here's this report, here's its recommendations, we are considering making a formal recommendation to sign it, that that request for comment would go to RZERC, the root zone manager, the RZM, and the IANA. Are there any other folk who would be considered, as we should ask them as well, for their views? Lars Johan?

LARS JOHAN LIMAN: There is a group that we might want to talk to. It popped into my mind, and I'm not quite, I haven't really made up my own mind, but I'll put it on the table, and that's the ICANN OCTO people. They're not formally involved, but they have a good bunch of good people, and frankly, they would probably be annoyed if we didn't ask them. Thanks.

GEOFF HUSTON: A minor procedural question, and others more familiar with the internals of ICANN might help me answer. Can we ask them? Like, whose resource is OCTO?

WILLEM TOOROP: Yes, so I want to note that these studies were commissioned works coming from the ICANN OCTO. So they are well aware of these reports, and have studied them themselves as well, or read them, and commented on them.

GEOFF HUSTON: Okay, Kim.

KIM DAVIES: I wouldn't take it to the bank, but my gut reaction is that you don't need to consult with OCTO as its own entity. I mean, part of PTI's relationship with ICANN is we would consult with ICANN as our contractor to find out, and I mean, just knowing how things work. I mean, IANA internally is closely involved with OCTO, so we're very familiar with what everyone's doing. So I don't have any concern OCTO won't be consulted, whether it's formally or informally. I don't think it's necessary to formally request something of OCTO on this kind of review.

GEOFF HUSTON: Okay, I appreciate that input, thank you. Lars Johan?

LARS JOHAN LIMAN: Thanks. Yeah, thanks, Kim. That's reassuring, and if so, then I will remove my proposal from the table again. But I wouldn't worry about the resources, because it wouldn't be a request that it would be required to respond to. So if they feel under-resourced, they would just say, no, we won't.

GEOFF HUSTON: Thanks. Any other comments? So right now, an alternate proposal on the table is that we foreshadow taking the recommendations from that study and propose signing rootservers.net and send that proposal for comments to RSSAC, the Root Zone Manager, Maintainer, Manager, I forgot, RZM, and the IANA, and then wait for their feedback before proceeding thereafter and fold those comments in with any recommendations we might make to the ICANN board. Is that agreeable to everyone? Peter?

PETER KOCH: Thanks, Geoff. I'm a bit confused procedurally why we would be in the driving seat here. If that is what people have in mind, and I'm the only one in the rough, then that's fine. But I'm wondering whether we should actively recommend doing that rather than—somebody else referred to the charter before where we just need to make sure that everybody has been involved so far and we haven't found any obstacles to make that remark. But then again, if we aren't in the driving seat, the question reoccurs, who should be in the driving seat? And as we heard, nobody at ICANN is waiting for anybody else, but that also seems to mean that ICANN itself, the org, doesn't feel in the driving seat either. Thank you.

LARS JOHAN LIMAN: Two things. The first one is that I don't mind being in the driving seat for this one because if we hand it over to the board, there's a fair chance that it will take twice forever before anything else happens, judging from past experience. But my second comment is that it struck me, most other committees have procedures that involve public comments. Do we need to worry about that or bother about that with this thing? I'm not at all sure that we do, but I just wanted to raise the question.

GEOFF HUSTON: Thanks. I put myself in the queue here and in response to Peter, I am mindful of Kim's comment that in terms of the charter, we indeed have an obligation to consult and that consultation, I think, is perfectly appropriate. And in terms of being in the driving seat to consult, I think that's part and parcel of our charter. In response, Lars-Johan, to your, should it be a public comment period as well, I would offer the view that it's not at the stage where it is, I think, a firm commitment, this is a last chance for public comment. I actually think that if the board chooses to open that for public comment, then that is at the board's discretion. I think we can, I suppose, hide behind or take the view that as a technical committee, as a technical study and as a technical recommendation, as subject matter experts in this field, we are making the following recommendation, having consulted with various bodies, assuming the result of that consultation is we're okay to move forward and do this. It may well be that there are other issues that have not been folded in or emphasized in the existing study that se should review, but that is the purpose of this consultation in the first place. So I would defer the issue

of to what extent that becomes a public consultation to the stage, the latter stage of if it gets to it, it goes and part of the ICANN board issue of consult their processes. And we do not need to do that ourselves. I don't think that is part of our charter in any case to take that as a public consultation. So thank you for that comment. Andrew.

ANDREW MCCONACHIE: Yeah, I'm basically just going to agree with you, Geoff. I think if the RZERC did eventually decide to send this recommendation to the board, the board would not be able to move forward and issue a resolution without a public comment proceeding. So I think, you know, if this actually happens to the root zone, some kind of signing, some kind of name change, whatever, there would be a public comment proceeding regardless.

GEOFF HUSTON: Right. Thank you. So do it once more to make sure we're all on the same page. So the outcome of this meeting is for Andrew and Dan and with my assistance, we'll circulate a copy before it goes off, to create a request for consultation. We propose the following. Please comment on signing root nameservers.net to RSSAC, the RZM and IANA and request their input with maybe a slight comment about don't take forever, please. Do this in not quite real time, but do this reasonably in terms of time rather than take years. And then reconvene on this topic once we get back those comments and input and consider if we're ready to then take that to the ICANN board as a firm proposal based on the study, the result of those consultations and our view as a committee. That's what I

propose. Are we okay with that? Thumbs up from Lars Johan. Thumbs up from Willem. We're good. Okay, let's do that. Thank you. The next topic on the agenda is any other business.

Well, I'm going to give you back 26 minutes of your life. For some of you in Europe, that's more sleep. Yay. For those of us in Malaysia, what do you do at 4:30 in the morning? I don't know either. I'll let you know next time. Andrew and I and Dan will work on those notes. We will circulate them to RZERC before they get sent off to those three groups to give you a chance to comment on that as you see fit. So with that, we're adjourned. Thank you very much.

[END OF TRANSCRIPTION]