DANIELLE RUTHERFORD: Hello and welcome to the RZERC monthly teleconference held on Tuesday the 19th of January 2021. Duane, would you like me to do the roll call?

DUANE WESSELS: Yes, please.

DANIELLE RUTHERFORD: All right. From ICANN Board, Kaveh Ranjbar?

KAVEH RANJBAR: Present.

DANIELLE RUTHERFORD: From PTI, Kim Davies?

KIM DAVIES: Present.

DANIELLE RUTHERFORD: From the SSAC, Geoff Huston?

GEOFF HUSTON: Yep.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

DANIELLE RUTHERFORD: RSSAC, Daniel Migault?

DANIEL MIGAULT: Yep, I’m here.

DANIELLE RUTHERFORD: ASO, Carlos Martinez?

CARLOS MARTINEZ: Yeah, present.

DANIELLE RUTHERFORD: IETF, Tim April?

TIM APRIL: Present.

DANIELLE RUTHERFORD: RySG, Howard Eland?

HOWARD ELAND: Yes ma’am.

DANIELLE RUTHERFORD: ccNSO, Peter Koch?

PETER KOCH: Yes, present.

DANIELLE RUTHERFORD: And RZM, Duane Wessels?

DUANE WESSELS: Yes, this is Duane. Thanks, Danielle. All right, thanks for the roll call. So, hopefully, everyone can see their screens, see the agenda we have today. I'm hoping this might be a short meeting, but we'll see. After we review the minutes we'll talk about the election and then we'll talk about our two work items. So, anyone have modifications or anything they'd like to add to the agenda at this point? You can let us know in chat or when we go for the AOB call at the end. Right, so let's move on to the minutes from the last meeting.

Back in December, we had a meeting—and Danielle split them up on the screen for us—everyone should have had time to review. Does anyone have comments or concerns about the minutes from December? Doesn't seem like it. So, I think we can approve those and have them published on our website. And I think Danielle, you wanted to go through the election procedure, correct, or did you want me to do that?

DANIELLE RUTHERFORD: I can do that. So, the upcoming chair election—Duane's official second term will end at the close of our March meeting, which is scheduled for

March 16th by the RZERC operational procedures. Nominations will then open on the 16th of February, which is also our February meeting, and go through till the 9th of March, a week before the March meeting. RZERC members can self-nominate or nominate another RZERC member. The only person who cannot run for chair at this time is Duane Wessels, as he is currently term-limited. And then at our March meeting on the 16th of March, if there's only one candidate, the RZERC can confirm the new chair by acclamation. If there are two or more candidates, I will organize an online anonymous vote to take place for seven days and then we'll announce our new chair. Does anybody have any questions about this process? All right, seeing none—Howard?

KAVEH RANJBAR: Danielle, just a quick—sorry.

HOWARD ELAND: Sorry. Just a quick question, if we do have more than one nominee on the 16th, which we'll know—sorry. If the nominations closed on the 9th, and you have more than one, then could we not be doing the voting between the 9th and the 16th, so on the 16th we do indeed have our chair, so we don't have that gap? I know it's a week gap, but I just feel like you could do your second bullet under the March meetings on the 9th through the 16th.

DANIELLE RUTHERFORD: So, I think the selection procedure is laid out. Duane is the chair until the close of the March meeting. The nominations are supposed to close seven days before that meeting, the meeting where the election would take place, and it's not until that meeting that we're supposed to determine whether or not to do an online poll afterwards, if that makes sense.

HOWARD ELAND: I'm just saying, we could have a one week where we have a chair-elect, right? And they could take the reins during the March meeting.

DUANE WESSELS: Yeah, they could. I guess [going strictly] about the procedure, I would still be the chair for the March meeting. I don't remember exactly why this schedule ended up the way it did, but it might be because people wanted that extra week in between in order to hear from the candidates, a little statement of candidacy I guess about why you should vote for them.

HOWARD ELAND: Fair enough. I was just trying to streamline a bit but I'm fine either way.

DUANE WESSELS: Yeah, I think in terms of schedule, we're okay. And Danielle has the link to the procedures up there. So, I think, I'm guessing we should follow those. Kaveh, did you want to say something before?

KAVEH RANJBAR: No, thank you. Yes, I had a question, but I looked at the operational procedures and found it. I just wanted to know where it is spelled out about [anonymousness] of the vote and all, but I saw it clearly in the procedures. So, very clear. Thank you.

DUANE WESSELS: Okay. If anyone cares, we did use that procedure last time there were two candidates, and we did have an online anonymous vote and I think it all worked out very well. Yeah.

When I think about the election, the only thing that comes to my mind is I remember there were some unresolved questions about the way that the chair’s term aligns up with members’ terms because some members have one-year appointments or two-years appointments, that may not necessarily be in sync with the chair election, but in my opinion, that’s something that we can deal with when that becomes a problem. All right. So then, I guess, we should move on to the work items. Is that all right with everyone?

First up, let’s talk about signing the Root Zone Name Server Data. As you’ve seen on the list, Peter and I have been having a sort of very slow conversation about this. I think we might be in a pretty good place with respect to some of Peter’s concerns. I’m not aware of any other really outstanding concerns about this document. People have had a chance to share it with their constituencies, there’s no lingering issues or comments in the Google doc at this point. Peter, maybe you want to take a moment to share any concerns you still have or your thoughts that you put on the list?

PETER KOCH: Yeah, thanks, Duane. My hope was that the message I sent would say it all, but I understand that it was too close to the meeting so that not everybody might have seen it. So, basically what I said is in response to a question regarding concerns about why the root is special or why the document might be read in a way that would suggest the root is special is exactly this signing of the delegation and then we had that back and forth—well not too much back and forth, but that two-way exchange, whether it's really about the delegation or the names.

And I think I tried to put some of the history in the document understanding that most everybody on the call actually was part of the history, interestingly enough. Anyway, so I do think that the changes that were applied at one point are good enough and since we are only suggesting to now really conduct this research, I don't think there's any harm.

The other question I had, what makes the difference if we now again say in addition to RSSAC that the Board please really now follow the advice in RSSAC 28? But I think I've been convinced that again this brings it up on the table and people who could become—could be involved, [I] believe that it would help. I have nothing to add or nothing to object to moving this forward.

I must say though that I failed to circulate this in the other document with the community, other than some of the others. We don't really have a completely closed list, so anything that I would post to the usual ccNSO list would likely be in the public and I didn't feel comfortable to do that.

DUANE WESSELS: Right. I see your hand up, Geoff, but I just wanted to respond to that last point, Peter. And I think we talked about this last meeting. I don't think you should be concerned about this not being public. I think it's fine to post it on open lists or relatively open lists. The URL for this document is referenced in our mailing list archives, which are public, and this and the other documents I think have been circulated to other groups already. So, I think that should be fine if you still want to do that, for example.

PETER KOCH: Thanks a lot. Yes.

DUANE WESSELS: Geoff, go ahead.

GEOFF HUSTON: Look, I think Peter Koch raised an interesting question about why are we recommending this when RSSAC 28 already recommended this? And I think there is a useful answer here that we're forestalling what could have been an inevitable question, that quite frankly anyone who took just RSSAC 28 might well say, "Well, what does RZERC think about this?" because it's a change in, if you will, the fundamental contents of the root because you're mucking around with the answers on the priming query. And so, in some ways saying it again is actually a good thing because it forestalls this extended delay that's been going on in any case.

I think it's a useful piece of work to study; my suspicion is that the algorithms we use for signing the root might well come into this because I think any naive reader who looks at 3800-bytes in response to a priming query is going to have a hissy fit. It just doesn't work that cleanly at that size. So, I like the recommendations. I think it's precisely a useful recommendation and a useful reminder to actually kick this study off and quite frankly I think there's enough capacity in the organization, ICANN Org, to actually undertake this study in a meaningful way. So, I'm happy with this as it stands. If you honestly want me to go back to SSAC and say, "Yes, please," I can do so, but I didn't see much point considering the recommendations are what I would call, relatively vanilla, but useful. Thanks.

DUANE WESSELS: Okay. Thank you, Geoff. Peter, your hand is back up, go ahead.

PETER KOCH: Yeah, thanks. I believe the hands don't disappear automatically; I'll take it down. Yeah, as with so many other occasions, Geoff opened my eyes—and it's actually a remark that you, Duane, made on the list as well—supporting the recommendation and asking the organization to conduct the study claims the territory for RZERC, or say the responsibility for RZERC I should say, to evaluate the result and then derive maybe a recommendation towards the Board from that very result. So, that's the policy side of why we would do this, and I don't think we need to add that to the document, but it might be helpful to gauge the common understanding that when we recommend this, RZERC also commits to and believes it should review the result and derive a recommendation from that. Thanks.

DUANE WESSELS: Okay, great. So, in my opinion, this document is ready for us to vote on, maybe not today, but I think that we have taken it as far as we can, and we have lots of feedback on it. I guess Steve is not on the call today, is he?

DANIELLE RUTHERFORD: No, he had a conflicting leadership call.

DUANE WESSELS: Yep. So, Steve is usually very good about this. Danielle, do you know exactly what we should do next—I think Steve would suggest a 48-hour stable period and then a vote. Maybe an e-mail vote would be good?

DANIELLE RUTHERFORD: I can consult with him after the call, but I think that's the correct procedure to do.

DUANE WESSELS: Okay.

DANIEL MIGAULT: I asked for RSSAC to provide feedback, I've received none, so I guess there is implicit support on that document. And I've seen also—but Tim ...

TIM APRIL: Yeah, I was going to say IETF had three people that were supportive of it, no other comments came in.

DUANE WESSELS: Okay. Yeah, that's what I saw as well.

So, Danielle and I and Steve will work together to do the last steps in formalizing this for a vote and put that on the list, I think. All right, unless there's anything else people want to talk about this, we can move on to the other work item.

All right. So, this is the document on adding zone data protections to the root zone and I'm optimistic that we are in a similar state with this document. I can update you a little bit on the status of ZONEMD as an RFC, that the draft or the RFC is now in the AUTH-48 state. It has been assigned an RFC number, although, I think only the authors and chairs and what not know that at this point, but it's getting closer to completion. Myself and the authors have sent back some feedback to the RFC editor; I don't know exactly how long it's going to take to get published, but it feels like not very long to me.

Again, I think there's no outstanding issues. It's been a while since we've had comments/changes to this document that has been circulated with constituent groups and so on. But I'll open it up to the floor to discussion about this document and if anyone thinks it's not ready for the final step of voting and approval. Geoff?

GEOFF HUSTON: Yeah, thanks. Look, there's a bit of a [race] condition between RFC and this document. And quite frankly, I don't think it's worth doing this in parallel considering that if it is an RFC, we should say so by the time the recommendation goes to, well I assume, the Board technical committee, point one. So, if a delay in waiting for an RFC to be an RFC is on the order of weeks not months, I would suggest we wait and reference the RFC.

Suggestion two is typographical. In the previous documents looked at, the recommendations were abundantly clear: bold text, section called "recommendations" etc. In this one, it's just running text on page six, without any necessary calling out. I mean it's a numbered list but not in some ways called out in the same format that the other document called it out. And if we're going to be consistent here, we should actually use the same typographical convention of headings called "recommendation N," colon and then bold text. Thank you.

DUANE WESSELS: Okay, yeah. That's good feedback. Again, that's something that Steve and his team usually handle very well for us. So, I will work with him on the formatting and that kind of thing.

GEOFF HUSTON: Yeah, I've come to expect consistency. So, I was looking for the recommendations using the same search technique and oh, didn't find them that way.

DUANE WESSELS: Right. Okay, and to your other point about the timing, what I can do is, I'm not sure I'll get an answer, but I guess I can ask the RFC editor if they think that we are indeed weeks away versus longer.

GEOFF HUSTON: Thanks.

DANIEL MIGAULT: Do we know what is missing?

DUANE WESSELS: There's nothing really missing I would say, Daniel. They made an editing pass and had a bunch of suggestions for the document which we have largely agreed to and excepted. There was one change—so, the RFC, the document has an appendix with some example zones and example digests and we are considering updating one of those examples to cover a case that wasn't previously covered. So, no updates to the text of the RFC or the protocol itself, just one addition to one of the examples would be the only thing that's really outstanding at this point. Does that make sense?

DANIEL MIGAULT: Yeah. I had in mind a missing reference or something like that. Sometimes it takes very long, but it is not the situation we are in.

DUANE WESSELS: Yeah, there was nothing like that. All the changes that they wrote to us about were really editorial changes. Yeah. Tim?

TIM APRIL: I was just going to say similar to the previous document, I had one comment back on this in support of having the work done. And then I was also contacted by one person from the IAB, asking if we would like them to poke the RFC editor to see that status. But seeing as it switched to AUTH-48 in the interim, I'm not entirely sure it's required right now.

DUANE WESSELS: Okay. That's good feedback. Thank you. Peter?

PETER KOCH: Yeah, thanks. Just because I don't know whether the chat is archived or goes into the minutes, I wanted to go on record supporting the move that we now wait for the publication. And then of course our document would be edited to include the RFC number and also language around the draft, which is I think at some point, would be corrected so it is more stable.

DUANE WESSELS: Okay.

PETER KOCH: And I see that the chat is not archived, so it's on record now; I'm fine with that. Thanks.

DUANE WESSELS: Okay. Thanks for bringing that up. Howard?

HOWARD ELAND: Yep. So, I also agree with doing the wait with one caveat, and that is of course if some unforeseen bump in the road should occur, that we readdress it in either e-mail right away or at the next subsequent meeting, so we can take a look at how that changes the length of time for this to come out right. So, other than that reservation, I think I'm good to go.

DUANE WESSELS: All right. That sounds great. Like I said, I will reach out to the RFC editor and I will ask them if it's okay to use the RFC number that they've assigned to this, into our document even though it hasn't been published yet and then we can get ahead on that as well. All right, if there's no further discussion about that, I think we're to the AOB section?

DANIEL MIGAULT: So, I have a personal question. We had an active discussion regarding a proposal to lower the requirements to register cryptographic algorithms. Currently, they require a standards track and the idea was to lower that to specification required or RFC required and so on. But I was wondering if there are any opinions because some of those algorithms are going to be mentioned into the root zone. So, I was just curious to understand if we do have a position, an opinion I would say, more than a position. So, it's an open question.

DUANE WESSELS: Yeah, thanks, Daniel. I'm happy to spend a little bit of time talking about this. I'm not sure that it will end up as something that RZERC takes on as a work item, but I think we can discuss it. My interpretation of the, I don't want to say issue, but what you're talking about, it was to bring consistency to how the different registries for DNS work. If I understand correctly, some algorithm registries require only a specification, and some require a standards track RFC. And the idea was to bring them in sync by lowering the bar for I think it's the DS algorithm type, right? So, to me, that's a good thing but again I'm not sure that it's really something that RZERC needs to take on as a work item. Peter, you want to go ahead?

PETER KOCH: Yeah, thanks. So, I think, and I believe that we agree that there's a difference in the IETF lowering the bar for algorithm registrations and a decision to deploy this particular algorithm in the root or for the root zone. And the other aspect, of course, is what the IANA is able and willing to receive from TLD operators, and there, different issues kick in. One is, of course, that of operational stability, but then at least for the CCs, there's certain independence on the other hand. So, there might be something to discuss at some point. I do see that trend or tendency in some of registries in the IETF, or that is the protocol numbers to lower bars and hand out identifiers more freely. And one can have different opinions around that; I don't think that's something for RZERC but making the decision and some guiding that or just making a statement that there might be a difference could be useful at some point in time.

DUANE WESSELS: Geoff?

GEOFF HUSTON: Look, I'd like to remind everyone of RFC 8624. The implication is because this is a standards track document with normative language of "must" and "must not", that while registration of an algorithm for use by DNSSEC might have a lower standards bar for an IANA registration, the use of an algorithm in DNSSEC for signing and validation is now explicitly enumerated as "must not", "may", "not recommended" and "recommended". So, there's actually a higher bar of a standards track document that actually talks about what algorithms "may", "must", or "recommended" be used in DNSSEC.

If I think [we were] going to say anything about the signing algorithms used by third parties that are covered in DS records in the root, then that might be appropriate, but I tend to take a more liberal approach that, quite frankly, this is third party data. And it's the signing algorithm used by the root that's actually dependent on RFC 8624 amongst other standards documents.

So, I'm not sure we should be concerned personally about the algorithms used in delegated zones, but I think if there is a change to be contemplated for the root, and I believe that is an agenda item in the coming years, irrespective, then we need to be mindful of this RFC, amongst others. Thanks.

DUANE WESSELS: Thank you, Geoff. Daniel, any follow-up to that or did you get what you needed from that discussion?

DANIEL MIGAULT: Oh yeah, I was just interested. Maybe I have another question, but that's probably for the Root Zone Maintainer. Do we check the consistency of the DS records before publishing to root zone?

DUANE WESSELS: Yeah. So, it's probably a question for both PTI and the Root Zone Maintainer. I can tell you that we do, the Root Zone Maintainer, does check those for correctness as a matter of our operations, and I believe that—well, I'll let Kim answer for himself.

KIM DAVIES: Yeah, thanks, Duane. I think Peter sort of summarized my perspective relatively well, but there is a practical element that Duane speaks to, that we need to implement these algorithms in our systems so that we can do testing in the course of processing change requests. So, it's not so much as it's completely isolated to the child zones which algorithm is selected. If they're to be reflected in the root zone and if we're to do validation checks as a precondition to listing a delegation in the root zone, then we need to have software that's capable of processing that correctly. Historically, the way that's played out is every couple of years or so, Verisign and ICANN have meetings and we talk about the current state of the different algorithms and the maturity of the different software implementations that implement those algorithms. And then we make decisions about which algorithms we might want to add or indeed remove as a consequence of that. I think these are things we might want to explore in RZERC, I'm not sure it's directly related to the topic Daniel brought to us, but certainly something we could discuss and perhaps provide a fuller briefing to the committee.

It does lead to a separate question I had in my mind, not something we've explored in any depth, but to just point out which algorithms that should not be implemented. We have some of those that are eligible for the root zone today and we've not gone through a process of deprecating or removing older algorithms, and I'm not sure, at some point we might want to explore whether that is an appropriate thing to do. It's not something we've really contemplated the impact of today.

I think it raises a number of interesting questions that I don't have a clear answer to, but it is against the model where the IANA root zone management function is basically reactive, rather than proactive, to what our customers want to put in the root zone, and this would change that dynamic a little bit. That we would be basically setting a deprecation cycle for some of these things. Anyway, it’s a long way of saying I think there’s some interesting things to explore here and leave it up to the committee if you want to discuss it at perhaps a future meeting in more detail.

DUANE WESSELS: Okay. Thank you. Geoff, follow-up?

GEOFF HUSTON: You raise an interesting question, and I don’t actually understand relative charters going on here, as to who’s got what role. But if the content and the root zone and what is in the root zone intersects with this committee, which I believe is the case, then it would be my reading that the algorithm choices used to sign the root zone absolutely would be part and parcel of the responsibilities inside this committee, in conjunction with others. So, it’s not exclusive, but I would hope this committee at least has the ability to look, study, and comment.

I draw the line at that. So, the algorithms used to generate the DS records that are signed by the root zone, I believe that the best one could do is point to the current RFCs and say, “It would be a good idea if you read and understood these normative standards because if you use something else, no validator has any role invalidating it.” It’s user beware, rather than an enforced rule. I know that the issues around the validity of even nameserver delegations is a problem in the root. And the ability to take an authorized valid request for delegation change and countermand it by saying, “Doesn’t work for us,” is fraught with all kinds of issues. And I suspect the algorithms used to generate the DS record for signature has the same set of rather thorny issues and I would like to think that we don't go there. The issue of what we use to actually sign the root itself, I would have thought, would be within the area of valid comment by this group. Thank you.

DUANE WESSELS: Thanks, Geoff. So, this conversation reminds me of something that RZERC did right when it was getting started. There wasn't any real work for the committee, but we did some theoretical exercises, or not exercises but I presented the committee with a list of topics that asked people to rate whether or not they thought they were in scope or out of scope for RZERC, and that topic about algorithm choice was there. And as I remember, in looking at my—the results here are sort of mixed. I guess I bring it up just because maybe that's something that we want to revisit. A lot of committee members have changed and RZERC has evolved over the last few years and it may be worth going through that exercise again to see what sort of things people think are in scope and not in scope for RZERC. Something for the new chair perhaps? All right, any last comments before we end the meeting? Anything else?

All right. Thank you, everyone, for your time today and continue on the list. And see you next month.

[END OF TRANSCRIPTION]