ICANN69 | Virtual Annual General – RZERC Public Meeting
Tuesday, October 20, 2020 – 16:30 to 17:30 CEST

DANIELLE RUTHERFORD: Hello and welcome to the RZERC public meeting. My name is Danielle Rutherford and I am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. We'll read questions and comments aloud during the time set by the chair of this session. If you would like to ask a question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute your microphone at this time to speak.

For all participants in this session, you may make comments in the chat. To do so, please use the drop-down menu in the chat pod and select "Respond to all panelists and attendees". This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session hosts, cohosts, and other panelists.

With that, I will hand the floor over to Duane Wessels.

DUANE WESSELS: Thank you very much, Danielle, and welcome everybody to the public meeting of the Root Zone Evolution Review Committee. We have these once a year, more or less, and this is our chance to update you on things that have been going on in RZERC.

It's good to see a lot of people here. I think we have more people here online than we would typically have with an in-person meeting, so it's great that we're able to reach more of you.

Why don't you go ahead to the next slide and I'll get into the presentation here?

This may be a kind of short meeting. I don't know. It depends on how many questions we have. I want to give just a brief introduction to RZERC, go through the committee members. Then we have two work items to talk about and then the rest of the time can be for Q&A. Next slide.

So, if you're not familiar with RZERC, this is a very brief overview of what the committee is about. You can read the purpose here. The purpose of the committee is expected to review proposed architectural changes to the content of the root zone, including hardware and software systems and mechanisms for distribution of the root zone.

The committee makes recommendations to the Board for the Board's consideration. The scope of responsibilities are that we consider issues that are raised to us by any of our members on the committee

which also includes PTI, and the Customer Standing Committee which does not actually have representation in RZERC.

And just as a background, RZERC has been in place for four years, since the transition away from … Since the IANA transition took place with NTIA. And although it was agreed that there didn't need to be anybody that oversaw and improved routine changes to the root zone, there did need to be a body that considered and talked about more significant architectural changes to the root zone and that's what RZERC is for. So, next slide.

So, this shows the current membership. We have nine committee members. From the ICANN Board, we have Kaveh Ranjbar. From IANA, we have Kim Davies. From Security and Stability Advisory Committee, we have Geoff Huston. From Root Server System Advisory Committee, Daniel Migault. From the Address Supporting Organization, Carlos Martinez. From the IETF, Tim April. From the Registries Stakeholder Group, GNSO, Howard Eland. And from the Country Code Supporting Organization, Peter Koch. And from the Root Zone Maintainer which is Verisign, we have myself, Duane Wessels, and I am also the chair. Next slide.

So, this is one of the two work items that we want to update you on today. The first is protecting the root zone content. So, historically in the DNS, the primary way of transferring zone data has been with zone transfer protocol or AXFR. And there is a way to use AXFR that provides channel security but there is no part of the protocol, or no feature in

the DNS, that provides data security for the entirety of the zone as a whole.

We feel that as locally served zone data becomes more commonplace, there's a need for a reliable technique to verify zone content as a whole.

There's a proposal currently going through the IETF. Hopefully, [inaudible] process. There's an Internet draft titled "Message Digests for DNS Zones" which is one way of doing this. That draft is just finishing up its ISD review and hopefully the next step is to go into the RFC editor queue on that.

This proposal is not specific to the root zone. This is applicable to a wide number of zones. It is sort of limited at this time to zones that don't get updated very often but it is not specific to the root zone, although this is one of the ways that the [root zone is being used].

The way that it works is it adds a new record type to the zone and that record conveys a cryptographic digest of the entire zone data. That new record type is called ZONEMD record or ZONEMD resource record. And when that record is signed with DNSSEC, then you have very strong security guarantees about that digest and then we can verify the zone received matches the zone that was originally published by the zone [inaudible].

So, within RZERC, we are monitoring the progress of this Internet Draft and RFC and finalizing our recommendations that we'll make to the Board to deploy this record type to the root zone.

All right, let's go to the next work item.

So, the second one is the signing root server name—nameserver data, and this is something that has come up also within RSSAC so we're kind of taking this up again a little bit. As you probably know, the rootservers.net zone was created a long time ago—1995—as a way to name root nameservers. The purpose of that zone is to be the place where the authoritative data for root server names and addresses is [signed.]

Although the root zone itself has been signed since 2010, that authoritative zone is not signed and the delegation data [for the] root zone is not signed [and it gives away how DNSSEC works.]

So, having signed name server data may be of benefit to recursive name servers that they can validate responses that they get related to those names are correct and haven't been spoofed.

RZERC is currently working on some recommendations on this to be made to the ICANN Board. Those recommendations are not focusing specifically on signing the rootservers.net zone but instead, going back to the recommendations from RSSAC's work, which is RSSAC 028, in the RSSAC's work, there was a number of—well, the focus of the RSSAC work was to consider changes to the names of the root servers. So giving them names not in the root server.net zone but using some other schemes.

The RSSAC 028 document recommended no changes at the time, but further study. So essentially, within RZERC we are also recommending

that further study happen. That's the nature of the recommendation [inaudible].

I think that's it. Next slide is just the Q&A slide, I believe. So, happy to take all of your questions at this time. We've got some RZERC committee members on as well who may be willing or able to answer some questions. So if you have any, please, [inaudible].

Not seeing any questions. Kathy, do you have any questions?

KATHY SCHNITT: No, we don't have anything in the chat and I don't see any hands raised.

DUANE WESSELS: I can also mention that RZERC has been meeting monthly and we actually have one of our monthly regular meetings today. Those meetings are generally closed, however, if you want to follow along [the work of] RZERC, we have a mailing list whose archives are open. That's one way to follow what's going on, and our minutes and the transcripts are published on the RZERC website within a week or two after the meeting [is done.] So that's another way to follow along.

Yes, and Danielle put the link to the group there in the chat [inaudible].

KATHY SCHNITT: We have a raised hand from Ulrich Wisser. Ulrich, you should be able to unmute your mic and ask your question out loud.

ULRICH WISSER: Hello. This is Ulrich Wisser from the Swedish Internet Foundation. I would like to ask what the original intention to not making the root zone authoritative for the IP addresses of the root servers.

DUANE WESSELS: if I understand your question correctly, you're asking why were the IP addresses not—I guess more correctly, why were the names of the root servers not just within the root zone itself such that then your addresses could become authoritative.

ULRICH WISSER: Yes.

DUANE WESSELS: That, I don't know. That was really such a long time ago, I don't even know if any of my committee members were around. Does anyone feel like they can speak authoritatively on that? I really don't know. That was 30+ years ago, and I guess we could try to find out.

As you may know, RSSAC has a history document which speaks to some of this, but I don't believe that it addresses this particular question. Sorry I couldn't give you a better answer.

KATHY SCHNITT: Peter has his hand raised, Duane.

DUANE WESSELS: Hi Peter, go ahead.

PETER KOCH: Thanks. Maybe in addition to the reference to the written history of the root server system, way back then, the names weren't purpose built. So the very initial set of root servers—or maybe I shouldn't say the very initial one, but the very initial one I can remember which goes back to like the early '90s, that were like the regular names of those nameservers. And at some point in time—and the exact time can be read up in that document—the naming scheme was changed to allow for better compression of the names to allow for a reduction in the packet size, so to make certain queries stay within the then 512-byte boundary. And I'm speculating now, but at that same point, having the addresses or having that very domain that would have been chosen in the root zone would probably have had an adverse effect on that intention, getting compression in there. We don't really know.

DUANE WESSELS: That's a good point. Thanks. I'm not seeing any hands up or questions, so I'll do one last call, and if there's no more questions, then I think we adjourn the meeting. Okay, well, thank you, everyone, for attending, and thank you, committee members, for being here as well. See you later today. Goodbye everyone.

KATHY SCHNITT: Thank you so much. Please stop the recording.

[END OF TRANSCRIPTION]