DAN GLUCK: Hey everyone, welcome to the RZERC call, maybe annual call, I don't know. On the 9th of December 2024 at 20:00 UTC. This call is being recorded and is subject to ICANN's expected standards of behavior and community anti-harassment policy. I guess we can get started off with some introductions. I'm guessing everyone is pretty familiar with each other on this call, but I might be a new face to a lot of people here. So I can get started with an introduction if that works for you, Geoff. I'm going to lean on you as our presumptive chair.

So yeah, I'm Dan Gluck. I'll be supporting the RZERC, I guess starting today. So I've been in ICANN now for two years, mostly supporting the GAC and the expedited policy development process on internationalized domain names, as well as some other things like public comment here. Really getting excited to work with Carlos, who can't make it today, and the rest of our policy team supporting the technical communities, Kathy and Andrew are here now. And yeah, no, I've been, you know, tabs deep in all of our documentation for this and the other technical communities. So yeah, really looking forward to this. And Geoff, do you want to take it from here?

GEOFF HUSTON: I think I know everyone on this call other than you, Dan. And like I said, in the absence of a quorum, we're still kind of fishing around a bit, but I believe I was the only person to put my hand up to sort of guide us through this. As you probably all know, apart from you, Dan, I work at APNIC as the chief scientist there. In other related ICANN work, I'm the IETF nominee to the Root Service System Governance Working Group.

And I'm also a member of the Security and Stability Advisory Committee, which I think is kind of related in some vague way to this work as well. Other than that, I think, like I said, you all know me, don't you? Other than you, Dan. So yeah, I'll hand it onwards.

DAN GLUCK: All right. Well, I guess something that we can talk about in the meantime are disclosure of interest statements. That is something that needs to be updated annually on our website. But as not all of our names are updated, I'm guessing that means that not all of the statement of interests are updated either. So I'm going to work on gaining access to being able to update this page and as well as our email lists.

If you do have any changes to your SOIs that are listed here on the RZERC membership page, you can send them my way and we'll get those updated as soon as possible. But yeah, that is one of the things that we need to do annually for the RZERC. So I might as well get started there.

And yeah, I know. Everything else from our website, I believe, is fine. After this call, of course, we'll update this call information with our recordings and transcripts. And we'll also make sure to update our email lists as well in case there are any errors there. I don't believe there are. I think everything should be updated on the RZERC email list. I don't think anyone's left out. But definitely potential until we actually gain access to the ownership of that list to see what's going on there.

GEOFF HUSTON: Yeah, look, I have forwarded on a notice that was sent on the 6th of August, Dan, coming out of the IAB, Cindy Morgan, noting a one-year term for Willem Toorop to serve on the RZERC. I did not see any acknowledgement anywhere, and I'm actually unsure if he's on the mailing list. So, Dan, if you could check that he's actually is on the mailing list. I don't think he's sent any messages at all to this list.

DAN GLUCK: Understood. And we just got another apology to the list from Carlos. So that means there's two apologies and there are one, two, three, four, five. So that's seven. Yeah, that could be, yeah, one of the people that we're missing. And then also Lars Johan, right?

GEOFF HUSTON: I'm looking at the old list and I'm trying to understand whom Lars replaced.

UNIDENTIFIED SPEAKER: He replaced Daniel. He's the RZERC appointee.

GEOFF HUSTON: So after the email exchange, Lars certainly knows when we are and where we are. Maybe he's asleep or something.

And so that's just Kalina who has not responded. I believe Kalina.

UNIDENTIFIED SPEAKER: Kalina's here. She's on the call.

KALINA OSTALSKA: Hi. For some people who do not know me, I'm Kalina Ostalska. I represent the registry stakeholder group.

GEOFF HUSTON: I actually think now we are about as quorate as we're ever going to be.

DAN GLUCK: Okay. So should we proceed with the election?

GEOFF HUSTON: Yep.

DAN GLUCK: All right. So there's only been one name mentioned on the list and that would be you, Geoff. So based on our operating procedures, we just need to have a simple majority of people that are present to elect you. So I guess we'll go by voice vote, maybe. So feel free to unmute your lines when I make the call. Say, you know, I guess aye or yay or cowabunga, whatever you guys feel, for voting in favor. And then afterwards we'll do all against or abstaining.

So yeah, all in favor of electing Geoff Huston as chair of the RZERC for 2025, please unmute your mics now.

PARTICIPANTS: Yay.

DAN GLUCK: All right. Anyone against or abstaining? And that is silence I hear. So congratulations, Geoff, on being elected chair of the RZERC for 2025.

Do we have an acceptance speech or victory statement or anything like that you'd like to give now?

GEOFF HUSTON: Nothing like that. I think we need to acknowledge Tim April's extraordinary work in guiding us through the charter review and the forming of a new charter. That was a very long and tedious process that I think he handled extremely well. So in his absence, thank you. And Dan, if you'd want to send him a note of thanks, because I'm not even sure we did anything around August when Willem was announced as replacing him. Just dropping a line to say thanks from RZERC. That would be a good thing.

DAN GLUCK: On it.

GEOFF HUSTON: Thank you. There's very little else on the agenda at the moment. However, I think there are a small number of things that probably need some attention over the coming months. I know formally we have no particular engagement with the IANA KSK roll, but I felt an update, at

least to let us know how it's going and the timelines that are being followed and any testing that is being contemplated of that might be helpful.

And Kim, if you've got any comments on that, it would be appreciated. Do you have anything to talk to us about that?

KIM DAVIES: In terms of giving a spontaneous update, I mean, I can riff a little bit and give you a high level overview, but I suspect you're looking at a future meeting to bring in the actual operational team that does the work and they can talk in great detail about what's happened, what's being done and so forth. I'm happy to arrange that.

I think my only minor concern is obviously we've wrestled a little bit throughout the whole life of RZERC about what constitutes in scope versus out of scope. I think for us, we've not considered the subsequent rollover of the KSK in line with the previous rollover, which is essentially what we're doing to require RZERC to provide advice. It's an operational re-implementation of an existing process. So it's not something we've organically considered would be an RZERC item, but with that said, there's certainly no harm keeping everyone apprised of what we're doing and stimulating dialogue around that. So is that a fair assessment? As I said, I can give a contemporaneous update of where we are beyond that.

GEOFF HUSTON: I think it's a very fair assessment, Kim, I don't think we are formally in an advisory role in any capacity, but on the other hand, as one of a number of groups whose primary interest is the carriage of the root zone, it seemed reasonable, I think, to at least if you've got something to appraise us of and to keep us informed, I think that would be a good thing. If it's not adding in too much to your burden, it just seemed to be appropriate.

KIM DAVIES: No, not at all. I mean, so just to update you where we're at, in terms of, well, the posture of the KSK generally. So, in terms of the KSK that we operate today, it has been in service since 2018 when we successfully conducted the first and last rollover in 2018. You know, we polled the community and essentially all the feedback we got was that the rollover was successful and that we should essentially repeat that process, and that was our full intention. I think the one key piece of feedback was a more predictable schedule and, you know, certainly some expressed that it should be a more routine activity, that we should be doing rollovers more often.

So, we did a closeout report, lessons learned, et cetera, and in that report, we'd stated our ambition to do a rollover every three years. So, that was our full intention back in 2018. In 2019, when we finished that last rollover project, unfortunately, the pandemic happened and the pandemic really limited our confidence that we could do all the necessary operational elements associated with a rollover in such trying conditions. We couldn't travel, et cetera, et cetera. So, we took the decision to just keep the lights on throughout, you know, 2020 through

2022 and it was only really 2022 where we really felt we could start resuming operations towards a rollover.

So beginning 2023, we actually generated the next KSK in, I think it was in April 2023. Unfortunately, another turn of events is we learned that the vendor of our HSMs was exiting the business of producing HSMs and we felt it wouldn't, whilst the expected lifespan of the HSMs, vendor support, et cetera, would last some years beyond that, we felt it wouldn't be prudent to use a KSK that isn't even in production yet on equipment that we knew was end of life. So, essentially, we had, shortly after generating it in the first half of 2023, we hit pause and essentially researched alternative vendors and that work took the better part of six months to identify an alternative vendor. We settled on one. That new equipment involves some different procedural elements. A lot of the procedures around exactly how we do key signing, summarizing, et cetera, was tailored to the specific quirks of the equipment that we used. So those need to be adjusted accordingly.

But we essentially established a new vendor after trying trial units from different vendors and weighing in and so forth. Suffice it to say, 12 months later in April 2024, i.e. earlier this year, we generated the prospective new KSK again, this time on the new vendor's equipment. As is our practice, three months later, we replicated that key into our second facility. So we then, by June or July, I can't recall exactly when, we now had two fully independent copies in two data centers that were 2000 miles apart. And that's the point at which we feel confident that it is securely stored and available for further propagation.

I can't recall the exact timing, but later, a few months after that or sometime August, September, we actually published the trust anchor, the new trust anchor in our XML file that we used to distribute the root trust anchors. That was the first step. We then, since then, given speaking engagements, notified operational analysts, et cetera, that this XML file has been updated. And we encourage people that rely upon the XML file for the trust anchors to start updating their configurations accordingly.

The next step will be come January 11th next year, so in a little over a month, for that DNS key record to be added to the root zone itself. And this will start RFC 5011 adoption of that new trust anchor. Beyond that, our plan is to have the key not operational until late 2026. So, this gives us two plus years of propagation time to have clients update their configurations accordingly.

I can't speak too much of the monitoring situation right now. I'm not directly involved in those discussions. I know that our team is more operationally focused, but being advised by OCTO team in ICANN on that front, I suspect you'll want to hear more about that aspect. So, I would defer to bringing them to a future meeting to talk about that in a bit more depth. But assuming all things go to plan, the intention is October 11th, 2026 is the actual date of the rollover event.

And then I think the last piece of the update would be to say that everything I've just mentioned does not alter the algorithm for the KSK. We did convene a community design team to look at what an algorithm roll for the root zone would look like. It came up with a set of recommendations. Essentially, we made the assessment it would not be

possible to do it for this time around with any level of confidence to do an algorithm rollover for this particular rollover. But we fully expect it to be a key consideration for the next rollover.

And assuming we can now adhere to a three-year interval between rollovers, that would mean shortly after the successful rollover in 2026 that we're doing right now would be the generation event of the next KSK in early 2027. And with that propagation period of two plus years with an eventual rollover on October 11th, 2029. But to be ready for a 2027 generation event, we need to have all of our equipment, software, et cetera, validated in advance of 2027. Which means the fundamental work of readying ourselves for future algorithm change needs to happen soon. So that project internally got charted quite recently. And we expect our teams to be working throughout 2025 into 2026 on those kinds of questions.

And the exact mechanism of consultation on what the algorithm should be hasn't been designed yet, but we know that there will be consultations. So at some point throughout the life of this project, there'll be some engagement, undoubtedly involving RZERC, to essentially validate the algorithm choice, whether we should change or whether we should stay the same. Again, we're assuming that probably it will prevail that we would like to see a change, but nothing's off the table. The community feedback might be actually better to keep it the way it is, but we'll see what happens.

So that's a quick tour through all the facets, but I'm happy to try and answer any questions that you might have.

GEOFF HUSTON: Thanks, Kim. Any questions, anyone?

PETER KOCH: Yeah, this is Peter for the record. Not really a question, but taking up the suggestion made by Kim that we put the algorithm role on the 2025 work plan as a sticker at the moment, or as a post-it, so that we not only review the work, but maybe have some discussion about criteria, given that the role of RZERC is to make sure that everybody who should be involved is involved. So not so much judge on the technical merits, but also have a discussion of who should be involved, maybe beyond the usual ICANN community. And at least for Geoff, this is probably duplicating a discussion that we're having over in the RSS GWG, the root service system governance working group, in terms of the stakeholders, but that's life.

GEOFF HUSTON: Thanks, Peter. Certainly, I think if we can schedule possibly the next meeting, Kim, but the timing's really up to you is what's convenient, a more extended walkthrough on what's being planned with some highlight on this planning work on the algorithm potential for algorithm change.

I also think it is useful to work on the key lifetime issues associated with DNSSEC, as distinct from the more generic NIST specifications. I've seen an awful lot of presentations around post quantum algorithms and their application to DNSSEC. And while such things certainly get research

funding, I'm still scratching my head to understand why a DNSSEC piece of encrypted data needs to be secret for 20 years. I don't understand what the replay issues are that might dictate hefty algorithm change in the near future. And that consideration of cryptographic security and lifetime is certainly part of this.

And so, Peter, your suggestion about the appropriate folk and folk with knowledge around this area being involved in this discussion is certainly a key one when we look at how to consult with the community on the appropriate algorithm. While I understand that browsers, et cetera, have a real post quantum problem today, I personally find it hard to believe that DNSSEC does. But I'm open minded and willing to be educated if folk have views on that or if there are folk who could help inform the root folk about what is appropriate to think about in a new algorithm. Are there any suggestions on folk who might be knowledgeable in that area, NIST related or similar?

KIM DAVIES: So we have an active stream of work in OCTO to sort of monitor these developments. I think my first instance would be to ask them for suggestions. I mean, Geoff and others on the call, you've been at the same working groups and presentations at IETF, et cetera, recently. There was a number of presentations that ride on post quantum cryptography as well. I would not claim myself to be an expert at all, but I think there's a lot of discussion happening who the right parties are to bring this group up to speed. I don't know, but I'm happy to refer this to OCTO for recommendations.

GEOFF HUSTON: I think it sounds like a good idea, Kim, and perhaps in the absence of anything particular for our next meeting, we could devote the meeting to this area of the KSK role and the algorithm role in more generic terms. And it would be good if someone from OCTO could help us with that, because as you know, I appreciate that there have been folk in OCTO who've been working on this for some time. Any other comments on this topic? No.

There's a couple of other items. One is listed here in the agenda, and there's one, I think, that I haven't, but they are ill-formed thoughts, and I really don't know at some point if we wish to go there or not. The first is RFC 8806, the local root. I was wondering if there's anything that this particular group needs to be informed about, or if there's data that would be useful to understand its operation and effectiveness in the broader scheme of the root environment. Is that a topic of interest to this committee or to members thereof?

PETER KOCH: I do think it would be useful to look at this, and we've had part of the discussion when we discussed the ZoneMD record, because of this potential but not really expressed recommendation to support local roots more broadly, where at some point, this infrastructure, if it was deployed in the field, would rely on the, quote-unquote, availability or distribution mechanism of the root zone in total, as opposed to root servers that answer root zone queries. And while the response has always been, yeah, that works somehow because the zone is available

here and there, there is probably a question of scaling, and I'm pretty sure that has been addressed in one or the other study, but pulling these strings together and then probably come up with a recommendation here, might be useful work.

GEOFF HUSTON: I tend to agree. I was actually setting up a local recursive resolver at home today, or it was yesterday, looking through the log files and finding the poor old resolver stuttering to try and find an appropriate zone publisher to yank the complete zone down. I know that Wes has been intimately involved in this, in his work with B-Root, and I'm certainly kind of thinking that maybe we could finger Wes to give us his impressions of how that's going and what work needs to be done. I think it's worth pursuing. Any other members with comments? No?

Any other exploratory areas, because I don't believe there's anyone with particular topics of specific proposals for the root zone. The only one that I think is kind of a watching brief, and I think it's even too early to bring up in any formal sense, is actually the ongoing work inside the IETF circles around the DELEG proposal. In theory, in very advanced theory, at some point, sooner or other, this may have some relevance to the root zone. But exactly how, why and when, I think is very much an open topic. And I think the way the IETF is going, hammering away at a requirements draft, it is still some time away. But nevertheless, I think it's worth keeping an eye on DELEG, if nothing else. And I'm more than happy to do an update after the next IETF meeting, and others might too, because I'm sure we're all in that room, as to its progress. But like I said, I don't see any.

KIM DAVIES: I would agree with your assessment. I think the only thing I wanted to add was that, you know, I think I see myself, but I think that's more broadly this group, you know, could see itself as providing important input to the ongoing work to make sure any particularly unique considerations for the root itself are considerations of that work. And because, you know, there's nothing that I know of where ours has to act as a body to, you know, involve itself at any time soon. But, you know, we have a number of experts here that are very familiar with root zone requirements and needs, et cetera. So just keeping a watching eye on the evolution of that work to make sure nothing is introduced that might cause difficulties for root zone operations, I think would be one thing to be mindful of.

Just as a side anecdote that may or may not be of interest to this group, IANA recently implemented RDAP for the root zone to publish our root zone related data. We knew that we wanted to do this back when the RDAP bootstrap RFC was written. There is specific guidance in that RFC that pertains to how root zone data is published in RDAP. But in real-world experience, we found that almost all clients have undesirable behavior if we were to insert an RDAP record for the root zone in the RDAP bootstrap registry. So that's just an illustrative example of we want to make sure that there's nothing emerging in any new specifications with a DELEG or something else where they might have some kind of unexpected adverse event that is unique to the root zone. So that's in the back of my mind, but as the rest of us follow it, I think that's just something to also be mindful of.

GEOFF HUSTON: Thanks, Kim. You just actually touched upon in my head the interplay between the root zone and the zone update schedule and our local root 8806 and to what extent there is a predictable form of root zone update that whole zone clients can use, or is it just simply reliant on the zone expiries, which seem a bit coarse? But again, that's something we can discuss when we look at 8806 in a future meeting.

KIM DAVIES: Just to follow on thought from the previous topic, and Duane, please chime in if you have anything to add. But one thing that is of interest to this group that relates to expiries and such, there is some feedback we've received recently about the hints file specifically, that there's no sort of update schedule for the hints file. Generating the new hints file in the current publication workflow doesn't necessarily indicate any change to the underlying data. So Dwayne and I in particular have been under some preliminary discussions about possibly updating that to be more in line with the root zone itself. As I think you're all aware, the root zone is updated at least twice a day, even if there is no change to the underlying data. And this provides a mechanism just to be confident you have the most recent version, possibly doing something similar with the hints file itself, possibly adding some additional commentary about when the underlying data most recently changed, possibly adding some commentary about expected refresh times of the hints file itself. So I don't have much more to say on that right now, but I just wanted to flag that since you raised the topic. I think it's relevant.

GEOFF HUSTON: I think it's very relevant when you start going to 8806, when the whole zone is just being transported. How often do you poll?

PETER KOCH: This is a different topic, but I want to point out that in May this year, we received this result of the study on RSSAC002 recommendation two, which is about the signing of, I believe, the root-servers.net zone these days. And my understanding is that there was an expectation that others do something with it. And maybe next time when Willem can join, he can explain the thoughts behind that, but that should probably end up on our list as well.

GEOFF HUSTON: Thank you. I have made a note and hopefully Dan, you have done so as well. Before we break, I do have one relatively informal item. This timing and this date are the result of a doodle poll for this meeting. I think we need to resume a regular cadence and they were monthly meetings. Speaking of someone who inhabits the time zone UTC plus 10 or plus 11, this time zone and anything up to three hours earlier in my day is viable for me. Are we happy with this generic area or should we just ask Dan to go, what's the best time in your calendars for a monthly cadence meeting.

KIM DAVIES: Speaking purely for myself, I would say this should be fine for me around midday on Mondays for me, but we obviously have several

people missing. So I think this has to be a collective discussion with those not on the call today as to why they're not here. Could be timing is the exact problem they have.

DUANE WESSELS: Yeah, this time is pretty good for me as well. It's technically my lunch hour, but that's not a big deal. I do recall when we were doing the charter review work, we spent some time talking about meetings and meeting attendance, because I think particular Carlos Martinez, who's not here today, has always had a hard time joining the calls. I don't know what time it is where he's at exactly, but I just think we should be aware of that.

PETER KOCH: Yeah, so we all know this is survivor bias in a way, given that we're here, but this timing, both the Monday and the time of the day is fine with me, doesn't collide with day work and does also not collide with other ICANN meetings that happen to be on Tuesdays very, very likely.

GEOFF HUSTON: Thank you. So Dan, can I get you to set out a doodle poll for a regular cadence? Just to give us some flexibility and see if we can improve attendance. So I just simply want, you know, day of the week and time zone, one that works also with the support staff to give us some flexibility. But I must admit I have a pronounced bias to early in the morning. You don't want to hear from me any time after midnight until 4:00 AM. I promise you it's not worth listening to. That said, we've

reached the end of my agenda. I don't want to take up time unnecessarily. Any other comments? Thanks a lot, everyone. Dan, doodle poll and result of that doodle poll, we will try and meet again in around one month from now. Happy holiday season or whatever you want to call it. And hopefully we'll talk to each other again in and around this time in January.

Thanks a lot.