

---

YVETTE GUIGNEAUX: Hi, Geoff. This is Yvette, the host in the room. Can you hear me? Is your microphone working?

GEOFF HUSTON: [inaudible] My microphone is working, yes. Thank you.

YVETTE GUIGNEAUX: Oh, perfect. Loud and clear. Excellent. I just wanted to make sure. Thank you.

GEOFF HUSTON: Thanks. So the real question is, in my mind, if Don, Boban, and Denise are all saying they're not going to make it, does that just leave myself and Eric from the review team and Brian and Steve and Yvette and Jennifer as stalwart staff members?

YVETTE GUIGNEAUX: Hi, Geoff. Currently, that is the case. I know sometimes Mr. Matogoro due to some of his connection challenges does join late. The others I would have no idea about. But currently, as you spoke it, that is how the status stands, yes. So it's you and Eric and then Brian, Steve, Jennifer, and myself. And Karen's joining right now.

GEOFF HUSTON: Okay.

---

*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.*

---

ERIC OSTERWEIL:                   And this is Eric.

GEOFF HUSTON:                   Hi, Eric. I was, I suppose, just mulling over the fact that as far as I can see the wheels are largely falling off the momentum behind this effort. And if it's just you and I, Eric, I'm not sure why we're doing weekly phone calls to do this. I'm pretty sure there's a better way of doing this, and this way really doesn't seem to be me to be optimal.

ERIC OSTERWEIL:                   Yeah, that's a fair point. I think if no one shows up – it's only two minutes past, and I know we definitely prefer people to be punctual, but maybe give them a couple more minutes to see if stragglers show up. Is that fair?

GEOFF HUSTON:                   That's fair. But while we're here and while Steve certainly is around, that's a useful place to start a meta conversation here. Steve, a lot of this document is about the way the root zone of the DNS is managed. Some of it is policy, as we all know, but some of it is just straight day-to-day operations.

Who would be the appropriate folk within ICANN who could take some of the open questions in this document and from a management of the root zone perspective provide some perspective on what they actually do?

---

STEVE CONTE:

Hi, Geoff. That's a great question. I think the best person to be the point person [inaudible] can be depending on the depth of DNSSEC with maybe [inaudible] as a supporter for that. But for the day-to-day IANA root zone management stuff, Kim is probably your go-to guy to and then he could probably take it from there.

It might also come off – I'm hesitating because I just don't know. Maybe Terry Manderson and his group be of DNS engineering, but I think they're mostly L-root which is as you know a clearly different entity than root zone management itself. So I think Kim is probably your guy.

GEOFF HUSTON:

Right. None of these questions particularly relate to L-root in and of itself. It's more when someone says change the name servers in the root zone, how do you know it's the real person? Or how do you tell the difference between a genuine request and someone trying to deceive you? How is this process of doing DS records for DNSSEC? Again, how do you know it's the real thing?

Those are kind of mechanical questions. Due diligence is saying we should be at least asking the questions and ensuring at least to our satisfaction we think that the appropriate safeguards are in place to make sure the thing operates with integrity.

So if it's Kim, a whole bunch of this stuff can be directly done by basically a conversation with Kim, can't it?

---

STEVE CONTE: Yeah, probably. In retrospect of what I just said to you, in hindsight, if any other questions come up about the KSK roll in specific, then we would also involve OCTO. I know that Ed Lewis was working on the roll as well as some other members: Matt Larson from OCTO team.

So I think you're right. I think starting a conversation with Kim is probably going to knock off a lot of the root zone management stuff with maybe some setting up of conversations with [inaudible] or Matt and/or Ed for or if KSK comes into play too.

ERIC OSTERWEIL: I think that's actually a really good point. I think it's an exemplar. I can't scroll through the document and I don't have it in [inaudible]. Did we talk about the KSK roll in the document? Thank you. I don't think we did.

GEOFF HUSTON: Eric, no we did not talk about the KSK roll. I suppose maybe it's my own bias here, but being closely involved with it over the last couple of years, frankly as far as I can see, due diligence has been exercised to quite an astonishing degree and a difficult problem has been dealt with as well as it can be dealt with. That doesn't mean it's going to roll out seamlessly. Some folks who do manual key management are going to get left through the cracks, etc. That level of risk has been, I think, adequately quantified and the work has been well done.

Is that part of an overall security and stability review given that it's just one incident, one case, one kind of operational thing? That was why I didn't put it in.

---

ERIC OSTERWEIL: A couple ideas around that if I could really quick. I was going to just jump in real quick on that.

GEOFF HUSTON: Yeah, go ahead, Eric.

ERIC OSTERWEIL: Without touching that third rail and just acknowledging that the third rail exists and that it powers [big things], I will say that there are those that anticipate and some that even look forward to the prospect of ongoing KSK rolls whereby this wouldn't be a single event but it would herald a sequence of events that would become operational doctrine.

So there's that aspect. There's also the aspect of how successful did the process turn out to be after the KSK roll is completed. There was the long leadup process and, like you said, there was a lot of vetting. There was a lot of analysis. Certainly after it's done, there's the opportunity to look back and ask, how did it go? Was that useful? Did it work? Because it's possible that those sorts of operational processes and considerations get used in the future for other things.

So, yeah, I agree with you, Geoff, in the sense that I don't think memorializing this particular KSK rollover in an SSR2 Review Team report with recommendations necessarily makes sense. I just wonder, especially if it winds up becoming a recurring process, if we don't want to say how it affects SSR.

---

GEOFF HUSTON: And, Steve, you had a comment.

STEVE CONTE: Yeah, just two really quick points around that. I agree with actually both of you. Just two points about that are this roll is going to end in October and probably end way before recommendations come out. Any recommendations that are made about this roll will be months after the key has already been rolled.

However, with that said, the last SSR Review Team was five years ago when we started signing the root (five-years-ish). So if we're looking at ongoing and when the next SSR is, Eric brought up a good point. Maybe if it's a recurring thing, maybe a review of roll process with recommendations of what worked or what didn't for the next time it rolls or if it rolls again.

GEOFF HUSTON: The one thing that highlights for me is a draft, it might even be an RFC at this point, and I've forgotten who was involved with it. I think Ed Lewis and Mike St. Johns. There was this idea at one point – oh, Matt Larson – that a resolver that asks [inaudible] which is the top of the chain of recursives occasionally through EDNS0 leaks its [inaudible] state toward the root server in its queries. "I have key ID this."

It highlights the fact that if you want better control over the process and better visibility, you need different resolver behaviors. But if you need different resolver behaviors, you need the IETF and standards and

---

specifications and agreement. Because at this point, the DNS as it stands isn't necessarily giving you the information that you need no matter how often you roll the key.

My takeaway in some of this is, within the constraints of the system that it works within, we're doing as well as we can. Then comes this meta conversation of, how do we ensure that the boundaries are pushed a little bit to make the entire process go better when the problem is actually in the way things behave at the moment according to standard specification?

This kind of introspection gets you so far. Improving your own processes gets you so far. But at some point, you need to look beyond that to figure out what to do about it if you want to improve it.

There's nothing particularly specific there. It's more this observation that we can't test until it happens and won't be able to test until it happens unless the DNS changes. It's frustrating to some extent, certainly, but that's why I said I can't fault anyone who is doing what they're doing at the moment. It seems to be a task that has an appropriate degree of attention, has a lot of eyes on it, and is being managed as well as the DNS will let us manage it.

So it's hard to say where to go from there. If the answer is, let's make it better, the answer is you need to change the way the DNS works to make it better. That's why I have two minds about putting the KSK in or not in.

---

[ERIC OSTERWEIL]:

I think that there's a fundamental problem. I think that is that the KSK rollover is not something that the protocol has any semantics to discuss. It's a hierarchical namespace space that has been overloaded to do hierarchical key learning. Unfortunately, that gives no semantics for what to do if the root key needs to change, only things below it necessarily by design. It simply is missing the semantics it needs.

So the idea of we've done the best that we can do, I think that's a fair comment because the protocol gives us no ability to even discuss how to do it a different way. But I think that's suboptimal. If I want to change either of the keys in my zone, it's well understood how I do that. I can, of course, do it the wrong way. And, of course, bad things can happen. But [inaudible] the protocol is a well martialed set of operations that I have to follow.

With the root, there is just no way to do it except to close your eyes and jump. One thing that could happen is that we might say, yeah, there's too much at stake to leave it that way. Someone needs to do something else. I don't think it's [inaudible] come up with a proposal like, I think a protocol like this would be great.

But at the same time, we certainly could recognize that something needs to be done to invest in some sort of programmatic, process-driven something to do this. Certainly, having watched a KSK roll over some number of months in the future, we might actually have some observations that help us figure out what to do. But that's the most I think I can imagine saying. But I think those are probably fair comments from my perspective.



---

GEOFF HUSTON:

It seems to me that at some point if you want the DNS to do things differently, the IETF is a massive stakeholder in terms of any kind of subsequent action. That becomes an entirely different conversation, which is outside the purview of direct control of any of us here in this room, in this review team. Because what it's really saying is we've been handed this technology and its constraints. Here are the standards. Here are the RFCs. Work within them.

What we're finding, particularly in the KSK roll exercises as you have observed, some of the issues lie outside of the norms of the operation of the DNS protocol as we understand its specification. It's not that our understanding is lacking anything. It's not. It's those specifications are kind of mute on how you change the apex, and we're struggling in terms of ensuring that such changes happen with absolutely minimum disruption. That's, I think, the nub of it.

[ERIC OSTERWEIL]:

Yeah, and if I understand at least part of what you're saying, I think there may not be a way to form a relevant recommendation from this examination. I just don't know. So, yeah, I could totally believe that might be the case. I just don't want us to not look at it because we decide ahead of time that we're not going to be able to construct a recommendation that fits within ICANN's purview. I just know that at the end of it if we do consider it and say, "Yeah, what we really need to do is get the IETF to blah, blah, blah," then that recommendation

---

doesn't come out of our team to ICANN because it's outside of its purview.

I was just proposing. I think it does probably have some SSR relevance. If that is the case, then I think we should at least consider it. But that may not result in a recommendation, would be my two cents.

GEOFF HUSTON:

Right. Okay, thank you for that.

I'm still struggling a little bit with where to go from here. I have taken on the role as rapporteur, which in my mind was a role of documenting the discussion of the group. And it turns out that from the review team side the substance of the discussion is myself and Eric, and it's struggling a little bit to go through the processes we've set up to support this exercise. I'm thinking we could do this better if we acknowledge that reality and change things a little bit.

I would certainly appreciate the opportunity to get some of Kim Davies' time for, I don't know, a one- or two-hour slot and go through parts of the questions in this document and find out what answers Kim can offer or what pointers to documents, what procedures. What's the story from Kim's perspective to respond to that?

My own view is I think that would be the most useful way to progress things. Because certainly it's possible to just write more and more questions. The real issue is to understand to what extent those questions have already been answered, to what extent ICANN staff are

---

already right on top of this and really it's a case of just pointing to where there are documents or where there are established practices.

If folks agree with that – or Eric, Steve, and others on this call – if you agree with that, then can we ask Karen I suppose or Yvette, whoever can help us here, to see if we can get an appropriate time to have a conversation with Kim?

ERIC OSTERWEIL: Karen has her hand up.

GEOFF HUSTON: Karen?

KAREN MULBERRY: Yes. Thank you very much, Geoff and Eric. We would be happy to reach out to Kim and see what his availability is and arrange a call. I know you have these slots hard coded, so we'll use that as a guide to see if he can join one of them. And then we can let the group know as well as share this document with him so that he can take a look at it for the questions you've posed and some of the information you've gathered and come prepared to address those.

GEOFF HUSTON: Well you know, frankly, I think that would be a good idea. I personally also think there's no real point of having a next call until we can find a time that's agreeable to Kim because I think that's almost the next step

---

here. I don't really think there's much point in taking everyone's time with more [calls] unless we get some progress. I think at this point, the progress would be best with having Kim provide us with some input. So if you could share this document with him and see if there is a time that's available for him to help us here, that would be appreciated.

KAREN MULBERRY: I will reach out to him as soon as the call ends and see what his schedule is like, and then we'll get back to the subgroup.

ERIC OSTERWEIL: Geoff, I'm going to go ahead and take an action to close the loop with Denise and maybe take a broader view of what you mentioned at the beginning about the wheels coming off the bus or the lack of oxygen that the sub teams seem to be experiencing so that we can see if we can propose some mechanism to get more participation and action out of the team. I think [there's almost] this struggle to be useful and the sub team calls seem like they are increasingly sporadically attended. So I'll see if we can try and stir the pot a little bit.

GEOFF HUSTON: Right. Yeah, I just do think that if I'm supposedly the rapporteur, I find myself being the [man to document, shepherd], the editor, the contributor, the meeting chair, and that's kind of silly. This is not working if it's really just a conversation literally between me, you, and the staff.

---

If that's all it is, I think there are better ways to do this. And as I'm trying to point out, a lot of the questions I have, I think Kim could answer directly. Some of the residuals, I think the OCTO group and Steve and [inaudible] could answer once we phrase exactly what they are. And I would rather do it in a more pragmatic way rather than at this point this almost painful dragging the [chain along] when the level of involvement is really quite sporadic.

ERIC OSTERWEIL:

I totally agree. When I say I'll take it up, I mean literally. I'll take it up and I'll see if I can spend some of my energy to try and get the team to work with some other model that maybe works better. I have a couple ideas. I'll speak with Denise about it and see if we can re-engage the team on the next team call or something like that. I really appreciate you pointing it out.

GEOFF HUSTON:

Okay, thank you.

Is there anything else we have to discuss today or should discuss?

ERIC OSTERWEIL:

Honestly, I think if you and I were to come to parity on anything or everything, it would still need to be run by the rest of the team. I think identifying Kim as giving us a briefing maybe is a really good accomplishment for this, and I don't feel like we need to beat the whole hour to death if basically this is an example of asphyxiation of sub

---

teams. Then we need to go back to the drawing board. Unless you want to chat more, I'm perfectly happy to recoup the time.

GEOFF HUSTON:

No, I'm quite happy to give us all the time back. I think, Karen, if we could schedule our next call in conjunction with Kim, really if we do a call next week, it's because Kim is available. If it stays for a few weeks, it's because Kim can't make it until an appropriate time. So rather than nailing in a call next week, could I leave it up to you to liaise with Kim Davies, passing the document, and work out tentatively offer next week but if that doesn't work, the week after, whatever, a timeslot where we can have a chat with him about this document and see where we can add some flesh to it from his perspective. Is that okay?

KAREN MULBERRY:

Yes, Geoff, I'd be happy to do that.

GEOFF HUSTON:

Okay, well, with that, I think we're done for this week. Thank you all for coming. I'm glad to give you back 37 minutes of your life to do whatever you were doing.

ERIC OSTERWEIL:

Gracias, Geoff.

GEOFF HUSTON:

We'll see you. Thanks a lot. Okay. [inaudible], everyone.

KAREN MULBERRY: Thank you.

GEOFF HUSTON: Thank you.

[END OF TRANSCRIPTION]