KATHY SCHNITT: Welcome to the SSAC Evolution of the DNS Resolution Work Party Teleconference on Thursday, the 3rd of March 2022. Barry, I'll hand it back over to you.

BARRY LEIBA: Thanks, Kathy. So, Andrew, I guess we'll just go over the things from the previous meeting.

ANDREW MCCONACHIE: Sure. So there were three actions. Barry, you tweaked the charter based on input during this call, which I'm guessing you probably didn't have much input to base that on.

BARRY LEIBA: Yeah. There were some things I knew I wanted to do and I didn't get to doing it. And I should go ahead and do that now while you're going over that.

ANDREW MCCONACHIE: Okay. Then the other one was work party members to watch this video on Apple's approach to DoH and DoT. Then work party members to read three e-mail threads on DoQ. So those are the only action items for the work party.

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.

WARREN KUMARI: Not only did I watch the Tommy Pauly video, I also contacted him to get the example source code because apparently they never posted it. I don't have that exact code, but I've got some similar implementing encrypted DNS on iOS thing which I will finish building some time.

ANDREW MCCONACHIE: Is there any way you could share that, Warren?

WARREN KUMARI: I don't know because I don't remember what he shared it with me as.

ANDREW MCCONACHIE: Okay.

WARREN KUMARI: But I think that at least some of it, he found a public thing. As soon as I find that, I will send a link.

ANDREW MCCONACHIE: Thank you. Anyway, back over to you, Barry and Russ.

BARRY LEIBA: All right. What I'm just doing, I just put a placeholder in the charter. Can you bring up the charter on the screen? Good. And scroll down to where I edited it which is near the end of section one. So I just stuck this placeholder in because I don't have time right now to put in what I had meant to put in. But that was dealing with Warren's concerns that

there's not that much to say about the DoH, DoT, DoQ, whatever things that we didn't already say. But there's other interesting stuff to talk about here. Well, interesting for some value of interesting about using blockchain and things like that. I want to add a paragraph in there talking about those sorts of proposals for alternative DNS repositories and/or alternative DNS systems entirely. Is that the sort of thing you were looking for, Warren?

WARREN KUMARI: I think so.

BARRY LEIBA: Yeah. So I just need to flesh that out in my head to put in what I really want to say there. But the idea is—yes, go ahead.

WARREN KUMARI: It's not actually very specifically looking for something. It's more that I was confused about what the scope actually is.

BARRY LEIBA: Right. What I meant was that was the part of the scope that you thought was going to be there that wasn't is what I gather. And yes, certainly that is part of the scope of what we're going to talk about, at least I think it should be, unless people want to speak up and say, "Oh no. I think that should be way out of scope."

I'm hearing nobody jumping in right away. So after this call, I will put that sort of thing in, something about that. With that sort of thing added in and maybe a tweak in the scope section to make it clear that we will be talking about that, is there anything else that people think should or should not be in scope for this that we want to talk about now?

GEOFF HUSTON: Whoops. Wrong reaction. I did raise my hand there. So let me just get rid of all the rest of this crap.

BARRY LEIBA: Yes, go ahead. I'll just say Tara said she'd mentioned blockchain and stuff in the first meeting also. So yeah, go ahead, Geoff.

GEOFF HUSTON: Part of the issue here is actually understanding how strict this title is, DNS resolution as distinct from the way the DNS protocol does things, right? There is a distinction. And part of that issue is actually an evolving understanding that if you think about it a bit more, query names are merely lookup keys into a distributed database. You can structure the query names to produce a dynamically generated response based on attributes inside that label space. You can encode a whole bunch of fields inside the query name to produce varying and differential responses.

Now, we've always thought of a name as a name is a name, it's a static object. But when you think of a name actually being a piece of, let me

say, microcode as a convenient sort of way of describing what I'm trying to get to, the whole issue of DNS resolution becomes an issue of distributed computation. Why is that useful? Increasingly, we're placing more and more load on the DNS to do things that otherwise take more round-trip times. The client knows what it wants to do. The server is able to satisfy that request for knowledge if it understood more about the client's intentions than merely "I want to go to this service." And extended negotiation takes time. The more you front load the query with ancillary information, the more the response when RTT can be given back, which precisely matches expectation.

What we're talking about here in the broader context is as we try and refine and differentiate the DNS, we're no longer looking for better quality names. I'm like, that was always a crap exercise destined for nowhere, my name is better than your name, etc. We're actually going to start differentiating on behaviors. In this area, I can do more in the authoritative server than you can. I can generate tailored responses to match requirements in area of evolution to try and make the DNS more responsive to requirements of users. And if you will front load the query with more information so the answer can do more is actually a critical part of this issue of the evolution of DNS resolution. If you're looking far enough, you've really got to think about what's the query name and what's its role. It goes way beyond where we are right now and talks about evolutionary directions in terms of refinements of behavior. Like I said, it's all a case of how much you take the title literally. How far out do we need and want to look?

BARRY LEIBA: Okay. Jacques?

JACQUES LATOUR: I guess a little bit in parallel to that. The one aspect we didn't cover is the trust in the name resolution over time is eroding. So the evolution brings less trust in the overall scheme to resolve the right domain name, because you don't know if an application is dissociated from the OS. You lose trust in the integrity of the system.

BARRY LEIBA: Okay. I certainly can put words in about trust into the charter. I think that speaks to the stability and resiliency issues, I suppose. Is there some aspect of trust specifically that you were thinking of apart from the stability part?

JACQUES LATOUR: Well, in the good old days, if you had set up a computer, they have two name servers. You know where they went to resolve everything. Now the operating system is resolving one place and application is resolving somewhere else, another application can use something else. And then if you have firewall feature, you don't know what is being protected where, and you basically lose trust in your ability to manage that environment because—

BARRY LEIBA: Right. Is that something that needs to be in the charter or is that something that we would be putting in a document that we create?

JACQUES LATOUR: The charter should say we should look at the trust maybe, implications. I'm not sure. But it's a big thing.

BARRY LEIBA: Okay. I'll try to find a place in the charter to put a few words about that.

RUSS HOUSLEY: I'd like to push back a little bit. Because anytime I hear trust, I want to know trusted to what or to not what? Could you put a bit around that?

JACQUES LATOUR: A user point of view or enterprise operator?

BARRY LEIBA: Yeah. I think Jacques is not talking about trust boundaries and that sort of thing. He's talking about the trust the user has that the system will behave the way it's expected to.

RUSS HOUSLEY: So it's stability related.

BARRY LEIBA: Right. That's what I was getting at. But I'm happy to put the word trust in there somewhere relating to the user's view of the stability of the system.

RUSS HOUSLEY: Yeah, or confidence, right?

BARRY LEIBA: Confidence. That's a good one. I like that. Jacques, does that cover your issue?

JACQUES LATOUR: That's what I was thinking about. It turned out trust in English. So yeah.

BARRY LEIBA: Okay. That works. Andrew, do you have sufficient notes about what Geoff said that we might be able to riff on that after the call?

ANDREW MCCONACHIE: You mean on the changing nature of DNS resolution as it relates to new kinds of competing computation? Yeah. Is that much different than what we already have in the charter from Geoff?

GEOFF HUSTON: I didn't see aspects of the underlying assumption most of the time that in current resolution, the query name is a static lookup key against information held in the authoritative server. And even in the recursive resolvers, that binding is static. If you permit the query name to actually be a trigger for a set of actions on the part of the server that isn't just a simple static lookup, you change the very nature of what the DNS is

meant to be doing. You change what caching is. There's a whole bunch of issues. The motivation behind is pretty clear and simple. You can make the DNS richer and faster, and it's clear that folks want to explore that space. But it's worth discussing exactly what that would mean in terms of how the current infrastructure would cope.

BARRY LEIBA: Right. You started that off by saying that it depends on how strictly you want to look at the title of the work party.

GEOFF HUSTON: Right. If you want to look at the evolution of resolution then the current form of resolutions, basically a static lookup using the query name as key.

BARRY LEIBA: Sure.

GEOFF HUSTON: It's a database. It's as simple as that. But once you start allowing the query to have qualifying expressions which are computed on the fly, which are not attributes appended to the query, you can embed the attributes that you want to talk about inside the query name. At that point, the whole nature of the DNS starts to evolve and change. And the question is why would you want to do that other than just for grins in computer science? Because if you want the DNS to be faster, you give it more information and context in order to get back precisely what you

want within one round trip time. You increase the accuracy of matching the desire to the response.

BARRY LEIBA: Sure. I guess what I'm asking relative to the title is why that is not an evolution of DNS resolution? Resolution doesn't mean using the DNS protocol as we have always. It means going from a name to an IP address through some process, and that process can be entirely new. That process can be exactly the sort of thing you're talking about.

GEOFF HUSTON: Well, I think we're violently agreeing.

BARRY LEIBA: Yeah. So I don't think it twists the name at all. I think that discussion of that sort of thing ought to be in scope.

GEOFF HUSTON: Well, other parts of this document were touched upon encryption of transport. I'm not sure that's an evolution of DNS resolution as distinct from an evolution of the mechanisms to do that. You know it's a subtle distinction, but it's all about, I suppose, the payload versus the carriage.

BARRY LEIBA: Okay.

WARREN KUMARI: To me, I think Geoff—

BARRY LEIBA: Let's see what Rod and Russ will say and, Warren, put your hand up for next. Go ahead, Rod.

ROD RASMUSSEN: Yeah. Thanks. Can you hear me?

BARRY LEIBA: Yeah.

ROD RASMUSSEN: Sorry, I'm driving so I don't have the charter in front of me. So I got two comments. One refers to what you were just talking about with this idea of using the DNS … It's an interesting thing about using that as basically a communications mechanism. Look at [tunneling] as the early use case. I'm just throwing that out there.

On what Jacques had brought up—and since I don't have the charter in front of me, I don't know if it's in there. This whole concept around we're going to break up the DNS resolution from being uniform on a platform to being per application or even sub application in a way. I hope we have that in the charter. I don't remember from reading through it earlier. But this whole idea that there's a lack of consistency between the responses you get on a platform that used to be—ubiquitous to the platform what the DNS response is going to be, we're

moving into a realm where you cannot assume that everything on the platform is getting the same thing back. Thanks.

RUSS HOUSLEY: Yeah, Rod, we talked about that the last two calls and how that can lead to surprising the user when his e-mail and his browser have different responses to the same query. I'd like to respond to one thing Geoff said. Evolution is a temporal thing. And whether we're planning to talk about the evolution from [inaudible] RFC until today or we're going to talk about the evolution from [inaudible] RFC to today, and then forecast into the future what that evolution trajectory might be. And I'm not sure that we captured that.

BARRY LEIBA: Warren, you had something to say about in response to Geoff, or to add to what Geoff said?

WARREN KUMARI: Yeah. I think it was mainly just that Geoff had mentioned what I've been trying to say for the past few days that what the transporter seems much less interesting than what's actually changing in the DNS protocol when you carry it over X or Y is kind of eh. But the implications of how things change is a lot more interesting. SC, VC records and CNAMEs at the root or not, or apex behavior—those sorts of things seem more like evolution to me and carrying the same protocol but over a different transport close.

BARRY LEIBA: Given the discussion we had about DoQ around the last ICANN meeting, whenever that was, the thread that we were supposed to look at. Maybe that when we discuss this in the work party, we'll decide there isn't anything more we need to say about it beyond what we said in the previous document.

Anything else from anybody as we nail down the charter? Okay. If we make some changes to address what Geoff said and with the notes that I'm trying to put in as placeholders for now, does everyone think we have a charter that we can start moving forward with that we could start discussions that lead to a document? I should say, does anyone think we aren't there? Okay. It looks like we can start discussions of what goes into a document. Do we want to start that now? Start batting things around maybe more about what Geoff was suggesting or where? If anybody's been following the proposals about blockchain or any of that kind of stuff. Or do we want to give back some time now and think about it and continue the week after next. Geoff?

GEOFF HUSTON: I'd like to build on Russ's comment. I think blockchain is, in some respects, somewhat of a distraction. Blockchain is more about uniqueness and intermediaries more than it is about the nature of DNS resolution per se. But this issue of evolution, where do you start in trying to sort of convey the concepts of a changing space? Now, it makes sense to me and I wouldn't stop it today, Russ. I'd keep on going. But the issue is to try and encapsulate the early assumption that was basically smearing host.text in a distributed form by using a structured namespace rather than a flat space. And that was sort of the key

thought bubble that created the DNS as we know it today, and looking at that evolution and the reliance on caching to compensate for the inefficiencies of a dynamic discovery algorithm that is implicit in the DNS. And then look at the evolution of tailored answers that, in essence, our demands of the DNS have become more sophisticated. We can look at successes and failures such as NAPTRs and S-NAPTRs, the issues around CNAMEs, the whole issue of server load versus client load, where do you place translation? And, if you will, chain following, who gets to see that? And then we kind of land up into what are the demands that are being placed on it today when we look at things like SVC and SVCB records where, in essence, we're placing that back again with an SVCB of saying, "You're trying to get to the mail server associated with Geoff.foo but you really want to think about making a Port 892 connection using Quick to warren.foo because that's where Geoff's mail services. That kind of level of evolution is actually worth putting down as an initial commentary here about why this document, why now, what's changed already, and what are the pressures? Thank you.

RUSS HOUSLEY: Geoff, just for the closure, yes. I agree. I just wanted to make it explicit.

GEOFF HUSTON: Cool.

BARRY LEIBA: Okay, Warren?

WARREN KUMARI: So, two comments. First off, I kind of disagree with Geoff that blockchains not interesting or that it's the same sort of thing that it's kind of uses the same resolution. Or maybe I misunderstood him. I mean, to me, it seems like if it actually gets deployed, a huge paradigm shift, right? When you try and resolve a name, instead of it using the DNS, it uses some completely different lookup system. And there is no way to know from the name itself whether it's going to be looked up in the DNS or whether it's going to be looked up in a blockchain type system or whether it's going to be looked up in any other type of resolution thing. So maybe I just misunderstood what he said. But I think those things are wildly different.

GEOFF HUSTON: Oh, Warren, I think we were talking past each other. If that's what we're talking about with blockchain, you're quite right.

WARREN KUMARI: Okay, cool. And then my other thing is—

GEOFF HUSTON: I'll finish the thought. It was just a replacement for this registry is the unique holder of tokens that go for this part of the DNS space and we replace that with blockchain. It's just a registry change. We're talking of much bigger thing.

WARREN KUMARI: No, no. Meaning, other resolution things like what you use for .onion? Or what you use with .crypto or .cell or .eth? Like the Ethereum naming service. I have wkumari.eth and that actually works now. Is it a DNS name? Well, no. But it works in the same places that one does. And I thought that was a fair bit of the original purpose of this.

But then my other thing was, when Geoff was going through a list of all the things we could cover, that sounds like a huge document. It's basically the history of the DNS and everything related to it and basically covering all of the RFCs that have been written at a relatively high level but everything that's changed. I'm wondering how long we expect this document to be, who we expect to read it, and how long we expect us to take to write it.

GEOFF HUSTON: I'll take the bait, Warren, and say I was thinking about paragraphs, not pages. I was thinking about noting that the DNS is not your mother's DNS. Things have changed already. They have been in the past. And there continue to be pressures to evolve what is DNS resolution. I would almost leave it at that level, noting that some of these evolutionary changes impose load on the server side in a query response model of client to server, and some of them impose more load on the client side. The server says, "This is not the answer you want, you need to look elsewhere. Keep looking, client." And that tension between server load and client load is an interesting tension. But I would say no more than a page and certainly not the encyclopedia or the history of the DNS, because that's unworkably big.

BARRY LEIBA: Okay.

GEOFF HUSTON: My question back to Warren. Does that sound more tractable, Warren?

WARREN KUMARI: Kind of. Somewhat dubious whether we can cover many of the things in a paragraph or two and I'm sort of looking at things like the Routing Security Work Party, which we started off being, "This is going to be like a couple of paragraphs," and then we have spent much time writing stuff. And instead of trying to figure out who the audience is and who in ICANN is going to pick up this document and read it and what they're going to take away from this. Stuff keeps changing, I should keep paying attention or do they just have more background info? What are they going to take away from this document?

GEOFF HUSTON: The silence is kind of telling because I actually thought this was a throwback to the Admin Committee and to you, Barry, why are we here and what was the envisaged idea when we talked about this is actually still a relevant question. If it's just to educate the masses, yay, but fair enough. But that's all it is. If there's a deeper or different point to be made, I'm unaware or unsure what that point is as well. So I share Warren's sort of uncertainty at this point. What are we trying to do is his question.

BARRY LEIBA: My vision of it was that it would be educative. I doubt that we will have, for instance, recommendations to the Board on this. We may have recommendations to application implementers, we may have recommendations to people who are going off and developing extensions to or new types of DNS standards or that sort of thing. But that was my image. Russ, do you have other thoughts on that?

RUSS HOUSLEY: No. I think that the last paragraph of the charter talks about that.

BARRY LEIBA: Yes. Jacques, would you like to say what you said in the chat?

JACQUES LATOUR: Yeah. Well, the discussion, we're all saying the same thing but some of the discussion are how people use DNS, like for many users, and then there's implementation, so I'm thinking the recursive, authoritative. So there's discussion around that. But there's evolution around the DNS all over the map. It's too broad. I don't think we can address everything. We need to pick a poison and stick to it, and then I'm not sure. Like on my part, I think the people losing confidence in the DNS is an important aspect to address—or not the DNS but the name resolution—and trying to explain that clearly would be a good scope. But talking about CNAME, DNAME evolution around that, DoH, DoT, it's super broad for the evolution.

BARRY LEIBA: I've opined that it would not be a bad thing if we wound up doing multiple documents, perhaps two, perhaps three, I don't know. Or maybe we'll do one. I think we'll figure that out as we start getting content. We may start pairing off things that we find are not so interesting as Warren pointed out.

JACQUES LATOUR: Where you say people losing confidence, you know who? My IT manager at CIRA. The guy that's responsible for the security, stability for CIRA, all of our employees have lost confidence in the DNS. Obviously, we do DNS filtering as a layer, and then we have application, and we have browsers that can resolve names all over the map. And he certified [Galore] on security stuff. He doesn't get how it works today. So my top security guy doesn't get it.

BARRY LEIBA: Warren, when we talk about your auntie, no, of course, your non-technical relatives don't know the DNS from bagels, but what they might see is things not behaving consistently, things happening differently when they're using one app than when they're using another. And that may cause them to lose confidence in the system as a whole, in the Internet as a whole. And that's what I think we're talking about as well. It's not necessarily that they understand that they're losing confidence in the DNS. But that's what's causing the conflict, the loss of confidence. Rod?

ROD RASMUSSEN: I lost audio there for a few minutes, I don't know what may have gotten discussed in between when you were talking about the scoping and the design and the ambience and intended outcomes here. I heard Admin Committee mentioned. So I just wanted to chime in.

This was a conglomeration of several different things, factors of putting this work party together. It's still up to the work party to define its own charter. One of the main intents was to look at where things are going and what the implications of that are, particularly the vis-à-vis people of the DNS ecosystem, ICANN-related spheres, but potentially overall as well. But that was at least the thinking in putting this together initially was that we want to take a look at where we think things are probably going to be heading and what that means, some of the implications, and potentially provide some recommendations, but really take a look at where we think things are going to provide some inputs for people who have to run infrastructure, plan, etc. Thanks.

BARRY LEIBA: Warren, you took your hand down. You don't want to say? Okay, Ram?

RAM MOHAN: Thanks. Look, I think one of the audiences, even though you were even saying earlier that this is probably not aimed at ICANN Board. I don't think it's aimed to the ICANN Board, but I do believe that there is a subcommittee there, the Risk Committee of the Board, where if we write something that is educational, it would be very useful for them

because most of the folks in that committee are either are technical or used to be technical, but at least can understand the difference between something technical and non-technical. As a Board committee, that committee is actually charged with thinking about evolution and risks to the identifier system and the namespace. And in that light, I think a document that is educational in nature has value for that group.

BARRY LEIBA: Great. That's useful input, Ram. Thanks. All right. So my inclination will be to wrap up this meeting now, give you back a few minutes of time. We'll look at when the next meeting is going to be and by then we will have the placeholders in the charter fleshed out and be ready to start discussing content.

RUSS HOUSLEY: The next one is St. Patrick's Day, right?

BARRY LEIBA: Patrick's? Oh, yeah.

RUSS HOUSLEY: Green beer all around.

BARRY LEIBA: Yeah. Let's see what Andrew says and then we'll get when the next meeting is. Andrew?

ANDREW MCCONACHIE: Yeah. That was going to be my question, when the next meeting was going to be. Typically, we don't have meetings after ICANN meetings. But we also stopped meeting at ICANN meetings once they became virtual.

BARRY LEIBA: Right. The issue that I see is next week is ICANN so we're not having one then. The week after is right before the IETF meeting starts, and I personally will be in the middle of travel at the scheduled time for that. And the next week is the IETF meeting, which is time-shifted so that we could have this call but it will be late in the evening after a full day of IETF crap. So my inclination would be to have our next meeting on March 31. I know that's a big gap. But given that we haven't gotten anything started yet, that gives us plenty of time to think about what we want to put into the first draft of a document.

RUSS HOUSLEY: So, Barry, if you could get the placeholder text done in the charter, I think it would be worth even having a half hour call on the 17th just to go over that. Because obviously your thoughts will be in it even though you'll be on a plane.

BARRY LEIBA: Okay. That works for me. Does anyone think that's not a good idea? Rod?

ROD RASMUSSEN: I'm not saying that's not a good idea. I think that's fine. I just want to remind from a process perspective, once the work party's done with the charter, we do pass that back to the full SSAC for review. So if there's a way we can take advantage of the time, cover the gap time we have to get the full SSAC review of the response and feedback on the charter, that would be a really useful thing to do. So that would really hit the ground running in April with substantive work.

BARRY LEIBA: Okay. Well, then good. Then that supports Russ's suggestion. So I will definitely get the charter text fleshed out and you guys can all have a call on the 17th. Russ, you will be able to chair that. You're not going to be in the air or anything?

RUSS HOUSLEY: Yeah, I'm going to attend IETF virtually.

BARRY LEIBA: Okay.

WARREN KUMARI: Actually, isn't next week and the following week IEEE 803.11 week? I'm not sure if Russ participates in that as well.

RUSS HOUSLEY: No, I'm not doing it this time.

WARREN KUMARI: Okay, cool.

BARRY LEIBA: All right. So our next meeting is the 17th and our next meeting after that is the 31st. So does anybody have final thoughts, or are we done?

ANDREW MCCONACHIE: So just to confirm, the only action item is for Barry and I think myself to finish up the charter?

BARRY LEIBA: Yes.

ANDREW MCCONACHIE: I see Rod's hand is up.

BARRY LEIBA: I think that's an old hand.

ANDREW MCCONACHIE: Okay. Then I'm done.

BARRY LEIBA: Okay. Then we're wrapped for today and the rest of you will see each other on 17th.

RUSS HOUSLEY: Safe travel, Barry.

BARRY LEIBA: Thank you. Bye all.

KATHY SCHNITT: Bye, Barry.

RUSS HOUSLEY: Thanks.

[END OF TRANSCRIPTION]