ICANN85 Mumbai | CF – SSAC Work Session: DOC Work Party
Tuesday, March 10, 2026 – 16:30 to 17:30 IST

KATHY SCHNITT

Hello, and welcome to the SSAC DNSSEC Operational Considerations Work Party meeting. My name is Kathy, and I am the participation manager for this session. Please be advised that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Regarding participation today, this session is primarily designed for the internal work and discussion of SSAC members. To join the speaking queue, SSAC members must be logged into the Zoom room and use the Raise Hand feature. When called upon, please state your name for the record. For observers, please note that comments or questions in the Zoom chat will not be read aloud. However, the chair of the session may invite in questions from the audience at their discretion. I will now hand the floor back over to Ram Mohan.

RAM MOHAN

Thank you, Kathy, and welcome, SSAC members, to the DNSSEC Operational Considerations Work Party. Chaouki is not feeling well, so he is not going to be in this session, but we will try and make some progress. Michael, good afternoon, is it morning for you?

MICHAEL PUCKETT Good afternoon, Ram. Yes, it is morning for me.

RAM MOHAN Okay, welcome. Thanks for dialing in early. We have an agenda for today, Michael?

MICHAEL PUCKETT Yes, we do. I am going to share my screen. Just a second. For today's agenda, we have an outline of the remaining sections that the work party still needs to write to finish the report. We can discuss that outline, and then the other agenda item is to talk about plans for disseminating the report after publication.

RAM MOHAN Got it. Great. Thank you. I think that is entirely what we need to do. SSAC members should have access to that document. It will be in the calendar invite that Kathy sent out. You can see what is on the screen, but if you want to get to the document yourself, there is another way to do that.

First order of business is what are the sections remaining and what do we want to do about them? Michael, you have some color coding, so do you want to walk us through the color coding?

MICHAEL PUCKETT: Sure. This blue-green color represents sections that have been drafted. As you see, we have 2.2, 2.3, 3.1, and 3.2. We have already drafted these sections and moved on to work on other parts of the document. These are all pretty dense sections, so getting them out of the way early has been useful for the work party to focus on the nitty-gritty.

I have this peach color that represents sections in progress. This is the current section that the work party has been working on: non-technical considerations, also known as the human resource component. We have just been drafting the findings and recommendations as we go, drawing from the body of the text.

RAM MOHAN: Okay, so the only things for us to discuss here are the ones that are not colored. Is that right?

MICHAEL PUCKETT: Yes, that is correct. I do have a separate tab with a detailed outline showing bullet points that we currently have that we can expand on.

RAM MOHAN: So just to understand, the detailed outline is only for the sections that we need to discuss today?

MICHAEL PUCKETT Yes, that is correct.

RAM MOHAN Okay. Before we go to the detailed pieces, any comments from the work party members on the sections that are here? Do you think they are the right sections? Do we need to cover them? Any comments? Okay, none. Let's go to the detailed notes outline, Michael.

MICHAEL PUCKETT All right. As you can see along this bar, we have 2.1, design goals, 2.4, and so on.

RAM MOHAN Let's do our normal thing. Let's set a ten-minute timer and have our members read this piece and then come back with any comments. A link to the document is in the calendar invite. What was that, Maarten?

MAARTEN AERTSEN Comments in the documents.

RAM MOHAN Comments in the documents because we do not want to burden Michael with remembering everything that everybody is saying in this call.

MAARTEN AERTSEN Is this document only for SSAC members?

RAM MOHAN Correct.

MAARTEN AERTSEN Okay. Thank you.

RAM MOHAN All right. We are at time. Michael, shall we go to the top of this document and start looking at what our members are saying?

MICHAEL PUCKETT Yeah. Our first comment is from John Levine.

JOHN LEVINE I can say something about it. I have DNSSEC signed all of my domains. I can tell you that the main advantage I get is that I can do DANE stuff. The other things are not as compelling.

MAARTEN AERTSEN So...

WARREN KUMARI I agree. You can do DANE stuff, and that is awesome. However, other than for mail, sadly, things do not seem to be using the DANE stuff much.

JOHN LEVINE You know better than I do why browser makers stick their fingers in their ears and say they cannot hear you when you talk to them about DANE.

WARREN KUMARI I formed and ran the DANE working group for a long time. I wished it would take off. The market didn't like it.

JOHN LEVINE I was actually pleasantly surprised. It really does work for mail. My canonical example is that I misconfigured my DANE setup, and the next thing I knew, my wife was saying, "Why can't my mother write to me?" Fortunately, I fixed it before there was any major relationship damage.

WARREN KUMARI I think that is a really useful and important point. We keep talking about DNSSEC to prevent cache poisoning or other things. I think we should focus more on DNSSEC for mail because that is where it is actually providing visible and useful wins. We should use that as our poster child for good stuff happening here.

JOHN LEVINE: It's not super widely implemented, but Comcast is a large provider and they implement it. There are some European ones that do too. There is some experimental stuff like Paul Wouters' project that tries to put PGP keys for individual email addresses in DANE-signed records. I think he did it wrong, but it is an interesting thing to look at.

RAM MOHAN: My higher-order question is: Is there value in stating design goals of DNSSEC, or is there value in saying the current utility of DNSSEC?

JOHN LEVINE: I would talk more about the utility. It is a historical accident that the design goal was that cache poisoning is bad and this will fix it. In fact, we fixed cache poisoning a different way.

BARRY LEIBA: Ways.

WARREN KUMARI: I think we can point at mail/TLSA. It is basically mail. Also, ZoneMD is a useful sales pitch. For the mail stuff, I think I left a note. Barry can probably give us the right word. It's not mail delegation; it is securing the destination of an MX record, but I am sure there is a better way of saying it.

JOHN LEVINE: It is validating that you are talking to the mail server you think you are talking to. It prevents man-in-the-middle attacks.

BARRY LEIBA: It is just a replacement for the certificates.

WARREN KUMARI: Right, but how do you word that in a clear and succinct manner that readers of the document can understand? It ensures that the MX record that the thing is pointing to is actually where you really intended.

BARRY LEIBA: You can say it authenticates the server and prevents man-in-the-middle.

RAM MOHAN: Yes. Who is writing that wording? Barry, are you going to write it?

BARRY LEIBA: No.

MICHAEL PUCKETT: I will do it.

RAM MOHAN Okay. Back to 2.1, my concern is that we are setting it up to go back in history and say this was what it was meant to do. I do not know if that belongs in an appendix, but the value in this document ought to be how DNSSEC is actually being used and the utility and value of DNSSEC.

MICHAEL PUCKETT Mark?

MARK The heading above says "Motivating Forces," and this seems very motivating. Maybe reuse that word.

MICHAEL PUCKETT I have a peeve about that use of the word "motivate," but it is widely used that way, so I should get over it.

RAM MOHAN We will get to the wordsmithing part at another time. This is more about the structure and what actually has value when we produce a report.

WARREN KUMARI What do we think of changing 2.1 to say the benefits and utility instead of the design goals?

RAM MOHAN That works. We should add all the bullets and then prioritize the bullets to go to the best use case first.

WARREN KUMARI Cache poisoning was largely the original motivation, but in the real world, that is not actually important anymore. We should list it, but it should be further down. While these are unordered bullets, people still read them as ordered.

RAM MOHAN Michael, you have that as an action?

MICHAEL PUCKETT Yes, I did. Russ has his hand up.

RUSS MUNDY Thanks, Ram. I was looking at this section, and it almost seems like the words were lifted out of the RFCs. The age of the RFCs makes them probably less accurate and meaningful at this point in time. The one that caught my attention was the first one that says DNSSEC enables end-to-end origin authentication for DNS and data integrity. It does not really. It does that for the data from the authoritative servers for a zone to the validating resolvers that are using the data. Non-validating resolvers have to secure the path between the validating resolvers and themselves. In this whole section, do we want to try to make it more understandable for a non-DNS or non-DNSSEC-centered person?

MICHAEL PUCKETT Your point here is that it is not end-to-end.

RUSS MUNDY Right, it is not end-to-end.

RAM MOHAN If it is configured that way.

WARREN KUMARI We say "enables," which implies that somewhere it currently is not.

MICHAEL PUCKETT That is fluffy.

RUSS MUNDY I would like to point out examples I used at ICANN meetings. I had a cell phone running DNSSEC, and I could validate stuff from signed zones from anywhere. That was really end-to-end. Honestly, I have not seen anything else that is really focused on executing on an end-to-end basis.

WARREN KUMARI We said we are going to reorder these, but I do not think we helped figure out what the right way is. If we were to order these, I think it would go D, C, A, B.

RAM MOHAN With A being changed. Russ, will you change A based on what you just said?

RUSS MUNDY I put the words in the wrong document, but I think I've already written them.

RAM MOHAN I wonder whether the non-goals and limitations section is even of use now that we have renamed this section "Benefits and Utility."

WARREN KUMARI It is worth noting that DNSSEC does not provide confidentiality. That is important because people get that wrong all the time. Maybe we remove "non-goals and limitations" and just list the good things it does. By design, it doesn't do confidentiality.

RUSS MUNDY We should also include that it does not provide any security for the zone content provisioning. There is nothing in the registrar space at all to make sure that the correct data for the DNS zone gets put into the zone that gets signed with DNSSEC.

MICHAEL PUCKETT It is only the responses; it is not any of the zone data itself.

MAARTEN AERTSEN I know of at least one operator that likes DNSSEC because it allows them to trust their Anycast nodes in certain areas of the world less. If you are going to make that point, you need to be precise about it, otherwise it is not correct anymore. This relates to the registry side of it and not to the provisioning of zone data, because that might relate to what an operator is doing as part of an Anycast deployment.

PETER THOMASSEN That last point relates to ZoneMD because one way of validating that your secondary has the correct data is by computing ZoneMD and checking the signature on it. That point could be made in the first bullet where the ZoneMD aspect is raised.

MAARTEN AERTSEN I thought you could already do this prior to ZoneMD.

PETER THOMASSEN Yes, you can, but then you have to validate every individual signature. With ZoneMD, it is just one. I also wanted to note that we have reordered the bullets already. We now have things that enable and things that mitigate. We could group it by what it enables and what it mitigates.

RAM MOHAN Got it. Let's get Michael to work on that. Barry?

BARRY LEIBA Is it worth putting something about giving you a confirmed absence of something?

WARREN KUMARI NSEC is cool, but I have never found a use for it other than aggressive NSEC. It really is not useful to me to know that foo.barry does not exist other than for aggressive NSEC.

JOHN LEVINE In principle, it is useful for DNSBLs, but I do not think anybody actually uses it for that.

MICHAEL PUCKETT I have a few hands up in the Zoom room: Peter, Warren, Russ, and Eric.

WARREN KUMARI Where we say DNSSEC does not provide confidentiality, it is worth noting that it neither provides confidentiality of the DNS data nor the actual connection that you finally make using that data. That is a comparison with other things like TLS. We need to word that clearly.

RAM MOHAN Warren, you should try to get some words in that we can react to.

BARRY LEIBA I would put those as two separate bullets: one about the confidentiality of the response and the other about the confidentiality of the transmission.

RUSS MUNDY We have a challenge in the document from a global perspective. We do not have any illustrations to show the readers what we are talking about when we say certain things, such as authoritative servers, validating resolvers, or non-validating resolvers. I wanted to ask if folks thought it was worth the effort to have some kind of illustration that would help clarify some of the terminology.

RAM MOHAN Russ, I think some of it depends on who our audience is. If we are aiming this at people who intend to deploy DNSSEC, I do not know that you need the diagrams. If you are aiming it at the suits, then diagrams would be necessary.

RUSS MUNDY I am not sure which audience is our primary target. Perhaps a way to defer this is to see what we end up with in the final text. I know we've published documents that had relatively easy-to-understand pictures, like the evolution of DNS document.

WARREN KUMARI

I think the audience is both people who are going to implement and suits. Even if it was just for implementers, we provide a lot of justification and introductory stuff. Having some diagrams so people can see where this fits into their architecture would be really useful. I think diagrams would be great, though I am not volunteering to make them.

ERIC

The NSEC design does enable offline signing, and that enables scalability, which is one of the things that came up when we were discussing deeper down in the document. I am mentioning it in case there is appetite to flag that it is an aspect of the design that makes the protocol a standout. It is beneficial for operations and was a design goal.

In regards to the figures, I think it is a great idea. If there was an architectural skeleton diagram that broke things into relevant parties for validation, provisioning, and signing, it could be a nice way to pull things together as we talk about benefits to different members of the transaction ecosystem.

RAM MOHAN

On your first point about NSEC, can you please write that down in the 2.1 bullets?

ERIC

I am happy to. I can forward-reference it because we talk more about it further down. On the diagram point, it can be useful to have a broad diagram that breaks out DNSSEC deployed on name server infrastructure versus the relying party side, showing a transaction path. If an architectural diagram showing some elements of the transaction or control path is at the beginning of the document, we can point to which parts help where. It could be useful for both technical and management functions.

RAM MOHAN

We have agreement that diagrams are useful. What about the bullet that says channel transaction security is not a part of DNSSEC? Is that important to say? It feels like it does not fit into the benefits and utility section.

WARREN KUMARI

I do not think we need to say that because if people are not doing the DNSSEC stuff, then they are not going to get the benefits anyway.

RAM MOHAN

Let's strike that out. When I read the "who may find DNSSEC beneficial" section, I did not think it belonged here because the section is talking about the benefit of deploying the protocol, while this is talking about "who." Some of it seemed self-evident.

WARREN KUMARI: Now that we have renamed this as the benefits, we can remove these bullets. We are saying parents should do this so that their children can. We should remove these bits or note that if you want your children to be able to do it, you should do it to facilitate their ability. We can just strike that.

RUSS MUNDY: For this placement in the document, I agree it does not fit very well. It seems it would be worth saying in some summarizing part of the document as a wrap-up after we have gone through the other parts.

RAM MOHAN: I resonate with that. Michael, that finishes up 2.1. Why don't we pivot to the second agenda item? Welcome, Chaouki.

MICHAEL PUCKETT: The second item on the agenda is discussing plans for disseminating the report after publication. The current estimated publication date is prior to ICANN 86 this coming June. Chaouki, if you want to share any of your ideas as chair, please feel free.

RAM MOHAN: Chaouki, do you think it is realistic that we will be able to get this published by ICANN 86? I see a couple of heads nodding no.

MICHAEL PUCKETT I do not think that it is realistic. If we push that deadline to ICANN 87, I think that is doable.

RAM MOHAN If you set an arbitrary timeline, we can find a way to make the document happen, but we will end up having to cut or make decisions about which sections should be there. As a work party, we should look at the overall outline and see if there is anything essential. That will help drive an estimation of how much time is needed. That is homework for the work party: to look at the detailed outline and determine if each section belongs in this operational considerations document.

WARREN KUMARI One of the big things would be if we change how we work. If we have people write a whole bunch of sections, then we could be done by ICANN 86 or 87. If we continue in the current method of let's do online word editing during the call, even 87 might not happen. We clearly have the ability to write a bunch of stuff.

RAM MOHAN We ought to look at who volunteers to contribute content for individual sections. For section 2.4, non-technical considerations, is there someone who volunteers to write some content? We need folks to sign up to contribute content. I can make this a homework item for all of you to look at the document and say in the comments

| | |
|---|---|
| | what you will write. My fear is that if we do not go through it here, we will go through it at our next work party meeting. |
| WARREN KUMARI | Some of us are reluctant to put our hands up now because we have the IETF right after this, so we are not likely to be available for the next two calls. |
| RAM MOHAN | I think we should cancel the next two calls because many of our members are going to be traveling or at the meeting. But people should still look at the document and say which sections they would be willing to contribute material to. I think ICANN 86 is out of scope. |
| MICHAEL PUCKETT | I would say so. That would require a lot of effort on everyone's part, and I do not know that that is realistic. |
| RAM MOHAN | Let's rule ICANN 86 out of scope already. Warren? |
| WARREN KUMARI | I am volunteering myself and Peter to do sections 3.3, 4.2, and 4.3. |
| RAM MOHAN | Eric, what are you going to sign up for? |

ERIC I am happy to help. I have written extensively about key rollover, so people can crib stuff from the peer-reviewed literature in that regard.

RAM MOHAN Same with you, Chaouki. You should look at which sections you can contribute content to.

WARREN KUMARI I am also volunteering Peter and myself for 4.6. When I say Peter and myself, I mostly mean Peter. You do not want me writing 4.5; I will point at Ionics and you will be sad.

RAM MOHAN I think you have data for performance, right?

WARREN KUMARI We have reasonable data for performance and a lot of data on downtime. I do not necessarily know that you want my views on the costs associated with downtime because I will point at the big DNSSEC outages and people will be sad.

RAM MOHAN If the document is about operational considerations, we are going to be a reality check document.

WARREN KUMARI I personally think that having people know that there are notable outages, but that we still think it is a good idea, provides more credibility than cheerleading. If you deploy TLS, there is a cost, and at some point, you will forget to roll a certificate and you will shoot yourself in the foot. You should do it anyway because it is important. John Levine, pick a number. Maarten, you didn't think looking at your screen would mean you weren't going to get picked on, did you?

MAARTEN AERTSEN I have some colleagues who are building a brand-new signer and I can talk to them about providing a review on some of this content. I am not volunteering to write this content.

WARREN KUMARI Presumably, there is stuff we could talk about regarding how much of this is done using open-source software.

MAARTEN AERTSEN If you want to have a paragraph on that, I would gladly type one up. It adds to things like operational considerations. It does not need to cost a million dollars to sign your zone. There is great software like Unbound and NSD that will do it for you.

PETER THOMASSEN I think we should be focusing on those members that have actually signed up as contributors: Steve Crocker, James Galvin, Geoff Huston, Warren Kumari, John Levine, Russ Mundy, myself, and Rick Wilhelm.

RAM MOHAN Michael, John volunteered for 4.7.

JOHN LEVINE I get 4.7, so I can say that DNSSEC assures that the lies you see are the lies they published.

RAM MOHAN What is the aim of 4.6?

WARREN KUMARI DNSSEC used to go boom every time you blinked, but we have been making it better and more stable. If you heard about outages from five years ago, do not worry; it has gotten better. Cloudflare will sign for you, or Peter's tools will make rollover easier.

MAARTEN AERTSEN I will add one sentence that you should use supported software because we will soon have OpenDNSSEC unsupported. It lives in a bunch of TLDs and it will be a problem.

RAM MOHAN I am just trying to see if that point ought to be made elsewhere, like in benefits and utility.

WARREN KUMARI We should stick it in there, and once we've got the text down, we can copy and paste it somewhere. If we say to put it somewhere above, we will just get sidetracked and forget it.

RAM MOHAN Fair enough. ICANN 86 is ruled out of scope. We are going to meet at the workshop in September. My thinking is that we ought to target having it ready for final review at the workshop so it will be ready for distribution at ICANN 87. Does that make sense, Michael?

MICHAEL PUCKETT Yes, that is a good goal to work towards. Russ has volunteered for section 4.1. That will put us on a good track to have this report ready for final review by the workshop.

RAM MOHAN Warren said he would do 4.5.

WARREN KUMARI I said I will do some of it. I am very much interrupt-driven, so please poke me hard and often if you want something to happen.

| | |
|---|---|
| RAM MOHAN | Staff should keep Chaouki and myself in the loop, and we will take the responsibility to poke each of you. |
| WARREN KUMARI | The chairs are more like, "Get your text in now." |
| RAM MOHAN | Kathy is even nicer than that. All right, we are at time. We are adjourned. |
| KATHY SCHNITT | Please stop the recording. |
| WARREN KUMARI | Just in case it wasn't clear, Kathy is awesome and I love her. It was clearly just snark. |
| MICHAEL PUCKETT | Kathy is amazing. |

**[END OF TRANSCRIPTION]**