ICANN85 Mumbai | CF – Joint Session: ALAC and SSAC
Sunday, March 8, 2026 – 13:15 to 14:30 IST

YESIM SAGLAM

Hello and welcome to the joint session ALAC and SSAC. My name is Yesim Saglam and I'm the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

During this session, questions or comments will only be read aloud if submitted within the Q&A. Interpretation for this session will include English, French, and Spanish. If you would like to speak during this session -- when called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak.

Please state your name for the record, the language you will speak, if speaking a language other than English, and please speak at a reasonable pace. I will now hand the floor over to Claire Craig, ALAC Vice Chair, and Ram Mohan, SSAC Chair.

CLAIRE CRAIG

Thank you, Yesim. This is Claire Craig, for the record. Hello, everyone. Good morning, good afternoon, and good evening, and welcome to this ALAC session with the SSAC. This is always a really good session for us. I'm here holding on for Jonathan, who should be joining at some time. Sorry, I can't be there with you. Hope you

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.

all had a wonderful lunch. If not, that you had some good networking taking place.

So, let's get this show on the road. Let me just go through the agenda, and then I'll give Ram an opportunity to welcome you. So, the agenda for today, we've had part of the welcome, then we are going to discuss the DNSSEC for end users. The next item, so yes, the next item would be the SSAC Work Parties Priorities for 2026 by the SSAC Work Priorities Chair.

Then we have some open brainstorming for the next steps with respect to the safe cyber campaign, and then the closing remarks. So, on that, I will just turn it over to -- before I turn it over to, let me just ask you if you could please manage the queue internally because it's difficult for me. I can only see persons who have their hands up in the Zoom room. So, if you could manage that as well as the persons in the room as well, I'd appreciate it so much. And now I hand it over to you to continue the rest of the session. Thank you.

RAM MOHAN Thank you, Claire. And good morning to you. It must be a really crazy hour for you, so kudos on keeping up all hours of day and night. Your dedication is really remarkable and I appreciate it. So, thank you so much. And for the queue management, if the SSAC staff people who are here, if they could help me do that, I'd

appreciate that. Because while I do have access to my screen, I'm not sure I always am diligent in seeing it.

So, we are always glad to come here and engage with you in the ALAC. There is a lot of shared ideas that we have now started to put into practice. So, I'm looking forward to continuing the discussion, Claire, and with your committee and finding a way to move our common goals together.

So, with that as an introduction, the first thing we wanted to do was to have a couple of our SSAC members, Matthias, you know, of course, and Peter Thomassen, they're both to my right here in the room, to speak a little bit to you about DNSSEC, but not from the standard DNSSEC for techies point of view, but really DNSSEC from the user's perspective.

So, we wanted to do that, have a little bit of a conversation with you on that, maybe even share something live with you, the demo gods willing, and then we'll have a conversation on that. So, with that as a model, let me hand it over to you Matthias.

MATTHIAS HUDOBNIK Please, can you take the next slide? Yeah, hello everyone. My name is Matthias Hudobnik. As you know, I'm an ALAC liaison to the SSAC, and I'm also an SSAC member. Perfect. Is it better now? Okay, great. Yeah, so my goal today is to give you a brief DNSSEC intro about, let's say, principle of operations and where it helps and where it has limits.

So, just to give you a bit of context, yeah, the DNS is the phone book of the Internet, more or less, but it was, let's say, designed in a more friendlier time ago, and today we need to ensure that the answers we get from this phone book are the real ones or at least that we can detect when something is wrong. Next slide, please. Thanks.

So, yeah, I say the postcard analogy. So, think of a standard DNS query like an unsealed postcard, and it's sent in the clear. Anyone, let's say, along the route can read it, or worse, erase the address and write a new one, sending you to a, for example, malicious site instead of your bank, for example.

And DNSSEC, we know Domain Name System Security Extensions, adds a digital seal to that postcard, and it doesn't hide the message. So, there is no encryption, but it allows your resolver to see if the answer was tempered with and forged responses.

The two key benefits or let's say the two things you should get from my presentation are origin authentication, so knowing the answer came from the right source, and the second thing is data integrity, so knowing it wasn't modified along the way. Next slide, please. Perfect.

So again, at its heart, DNSSEC uses public key cryptography. So, the zone owner has a private key to sign their DNS records, and this creates what we call an RRSEC, like a resource record signature, which is essentially a digital stamp. And then we have a verification process, and it also publishes a DNS key, so the public key, and when your resolver receives a DNS answer, it uses this public key to

verify the signature. And if the signature is valid, the data is authentic. If not, it's rejected. And this protection only works when the zone is signed correctly and your resolver is doing DNS validation, which is still not universal today on the Internet, as we know.

Please, next slide. Thanks. So, then we have the chain of trust. So, here is a key question. Who or how do we know the public key itself is legitimate? So, an attacker could publish a fake key, and this is where the chain of trust comes in. So, the DNS has a natural hierarchy. So, each parent's own vouchers for its child. And the parent stores a hash of his child's key called a DS, or let's say a delegation signer record, and the chain itself, this creates an unbroken chain from your domain up to the TLD, like, for example, for .eu or .com, and finally to the root zone. And the root zone key is the, say, trusted anchor. So, the starting point of trust for the entire global DNS.

Please, next slide. So, also providing a kind of negative example. So, the challenge is one clever part of DNSSEC is how it handles things that do not exist. So, in standard DNS, a hacker could forge a not found message and redirect you elsewhere. And the solution is that DNSSEC uses special records called NSEC or NSEC3 records to provide signed proof that the name doesn't exist. It's like a, let's say, notarized document saying there is nothing between entry A and entry C.

Please, next slide. So, now a bit to the end user experience. And here it's very important, it's a kind of invisible protection. So for end users, this is almost entirely invisible. So, you do not need to install, for example, the DNSSEC app. Your recursive resolver usually provided by your ISP or, let's say, a public service like Cloudflare or Google, does the checks for you. And what happens on failure, so if validation fails, the resolver won't show you the fake side.

So, instead, it returns a serve fail. And while it might look like a broken link, it's actually your kind of, let's say, silent bodyguard preventing a hijacking attempt. Or sometimes just a sign that someone misconfigured DNSSEC for that domain, which can be also the case. This brings me to my last slide, to the conclusion.

So, in summary, or in short, as I said, DNSSEC provides, firstly, origin authentication, which is very important, and the second thing is data integrity. So, it helps make the Internet's foundations more trustworthy, and it's also very important where it is deployed and maintained correctly. So, also for you to know, it does not encrypt your traffic, it does not block all phishing or malware by itself, and if it's set up badly, it can even take a perfectly legitimate site offline. So it's a powerful tool, but not magic.

And now I would like to hand over to Peter. He will take this a bit further and also discuss whether DNS can be like and kind of car airbag. Thank you.

PETER THOMASSEN Hey, yeah, the car airbag thing relates to that you just have a car airbag. You don't need to turn it on usually or install an app. So, my name is Peter Thomassen from the SSAC. I'll give you some more practical DNSSEC considerations. Next slide. Exactly. Thank you.

So first, DNSSEC is not a standalone security solution, and once you have it, you're all secure. It is embedded into a broader suite of security measures. And DNSSEC takes care of securing the information about domains, in particular translating domains to IP addresses or to the responsible mail server or whatever else you want to store in the DNS.

There are other things that need security in the Internet, particularly the routing system. So, which part of the Internet can advertise that it is in charge of a certain IP address range, for example. These advertisements cause traffic to actually get directed to that particular park of devices, so to speak, and that routing system needs to be secure as well so that people cannot just claim they own the IP addresses of certain other people and then get their traffic.

That security measure is called RPKI, so that's a supplementary technology to DNSSEC. And so, both of those, as Matthias said, do only add a seal, they don't protect the content from being inspected.

So, you also need confidentiality on the connection contents. That's called encryption. And so, that's done using the TLS method. And for example, in HTTPS, that is used. So, ideally, whenever you connect to some service, like web or mail or chat, the three things that will happen is that the IP address is looked up, and ideally that would be secure, so there would be domain integrity.

YESIN SAGLAM Peter, I'm sorry, can you slow down for the interpreters?

PETER THOMASSEN Okay. Thank you.

YESIM SAGMLAM Sure.

PETER THOMASSEN So, the first step would be to look up the IP address secured with DNSSEC so that you have integrity on the domain information. The second step would be that you prepare your request with the email you want to send, for example, and encrypt that for transport using TLS. That's content secrecy or confidentiality. And the third step would be that you actually send the request somewhere, and the routing of that packet is secured with RPKI, which gives you routing integrity. So, these things sort of go together. Next slide.

So, here are some examples of attacks that DNSSEC actually protects against. So it does protect against nameserver takeover

or nameserver hijacking. So, in 2019, there was a quite notable attack, some people call it the Sea Turtle attack. Not sure why.

And so there, through phishing attacks, registrars, for example, were attacked, and the name servers for certain important domains were changed. That affected certain government agencies and military and intelligence agencies, but also telecoms and ISPs. And so, then the DNS traffic would be redirected to the attacker's name servers, and the goal of the attackers was to then, for example, be able to redirect mail traffic to their own servers and inspect user credentials like mailbox passwords, for example.

And so, there was a CISA alert, for example, on this attack from the Department of Homeland Security in the US, and it says that the attack would redirect user traffic to attacker-controlled infrastructure and also obtain valid encryption certificates enabling men-in-the-middle attacks. And that's because the process of obtaining a certificate also involves the DNS, so when you hijack a domain on the DNS level, you can also get a fake certificate that will be accepted by browsers or email software. Next slide. Thank you.

So, the packet clearinghouse, which runs infrastructure for a lot of ccTLDs, one slide back, please, was also affected by this attack. And two slides back, please. Thank you. One slide forward, please. Thank you. Okay.

And so, they were also attacked, and the attack was largely not successful because they used DNSSEC. So, there is an interesting

talk about this on YouTube by Bill Woodcock from PCH that's linked here in the Packet Clearinghouse bullet. So, if you download the slides later and click on this, you can hear all the details. The point was that the fake name servers were installed at the registrar and the DNS traffic actually got there, but because PCH employees used DNSSEC validation, the responses from the fake name servers were not accepted, and then their mailboxes were not accessible, and the password hijack did not happen.

So, this is not directly a DNS spoofing attack, because the name servers were actually changed in the delegation, but DNSSEC still would have prevented it because the DS records were not changed, and they were locked, so they couldn't be changed.

The second type of attack that would be mitigated by DNSSEC would be Routing attacks where an attacker claims that it's in charge of the IP address range of some. For example, in 2018, attackers claimed that they own the IP address space of the Amazon Route 53 DNS service. That DNS service is used by myetherwallet.com, which is a crypto coin wallet. And the result of this was that DNS requests for that domain ended up at the attacker servers, and they could present a fake website and then steal crypto coins worth about $150,000 before the problem was resolved.

Now, DNSSEC would not have -- I mean, this was not prevented, and DNSSEC was not in use. But if DNSSEC would have been in use, then, of course, the IP packets for DNS requests would also have

ended up at the attacker's name servers. But just like in the first case, the fake name servers would not have been able to serve responses that would be accepted by the validating resolvers.

So, the point of this slide is to tell you that DNSSEC not only protects against direct manipulation of DNS packets that are in transmission or something or in a Wi-Fi or whatever, it protects against attacks that exploit the DNS but are executed through some other attack vector, and DNSSEC still can help with that. Next slide, please.

I talked about the three complementary technologies earlier. RPKI, which protects routing, is 62% deployed. That's from the NIST RPKI monitor from yesterday. Actually, that number is going up steeply. Over the last few years, it was introduced not so long ago. And the reason why that deployment works well is because it can be deployed by ISPs and the regional Internet registries alone. It doesn't need collaboration from end users or domain owners, and so there is no need to educate the public about this, for example.

For HTTPS, which protects content, the deployment now is about 95%, and the reason for that is that after the Snowden scandal, Let's Encrypt came around and invented automation, and that automation is now included in all web server software pretty much, and makes it a no-brainer to turn it on. DNSSEC is only 7% deployed globally. I mean, 7% of the number of registered domains have DNSSEC enabled.

Amongst the top 1,000, according to an ICANN ranking list shown in the footnote here, it's a little better, it's 18%. But anyway, the number is much lower than for the two other technologies. And the reason for that is that you need two steps to turn on DNSSEC. One is to sign the zone, or one reason for that is you need two steps. You have to sign the zone, create the signatures, and the second step is you have to put your key information into the parent domain where the chain of trust is connected, as Matthias was explaining. And that second step is often incomplete.

Next slide, please. So, when the registrar operates the DNS service for the domain as well, they can just do it, but if you have a registrar that's different from your DNS provider, then the registrant often needs to get involved, and that's a step that many are not aware of, and that's quite error-prone. I'll show you how complicated that is, and it's needlessly complicated. Maybe it should be automated, just like the other technologies. So, next slide, please.

So, I'll just show a few example forms of how different they look. You don't need to read all this. But this is one form of some registrar to introduce a DS record for a domain. It's just one long field you have to paste along string. You have to get that from your DNS provider. That's one way of doing it.

Next slide. This is another form for the same thing, which seems weird. And, yeah, so you have to select various things and paste other components of the DS record. It's hard to know what to do unless you have very precise instructions.

Next slide. And this is again another form for the same thing, and, well, I think I made my point.

Next slide, please. DNSSEC has an accessibility problem, so it's not that the technology in itself is brittle, it's just hard to configure. And, yeah, so in the interest of end users, it would be good if we could make progress and together push for more accessible and more automatic DNSSEC. That doesn't mean that everybody must use DNSSEC. It means that if you want to use it, it should be just a switch and then you have it.

Next slide, please. So, actually, there are solutions for that. If you remove the manual intervention completely, there is less chance for error, it's more accessible. And the way that works is that the DNS operator of the domain can tell the registry through some special records, hey, I would like to turn on DNSSEC, and I can prove that this is an authentic request. I'll show you on a very high level, in an example, how that works.

Actually, we did a webinar with the EURALO group a few weeks back, and there we showed a live demo, which actually takes about an hour because you have to wait for zone files to update in the TLD. So, I will instead show screenshots of that. But at the time, we did a live demo.

So, next slide, please. Let's say you register the domain euralo-webinar.cz, which we did at the time. Then the provider of euralo-webinar.cz can talk to .cz and say, look, here's my proven request to enable DNSSEC with the following details. And that happens

behind the scenes. You don't have to paste that manually as a user. And so, once that request is signaled from the child to the parent, then, next slide, the .cz registry will look at that and we'll verify the validity of that request, and then they will put in the DS record.

So, next slide, please. So, this is a status thing from the DNSSEC analyzer website where you can put in any domain and they will show you the DNSSEC status of it. This was before we registered euralo-webinar.cz. And as you can see at the bottom, it says zone.cz returns annexed domain for euralo-webinar.cz. It means the domain isn't registered. That was before registration.

Next slide. Once we registered the domain, there is additional information at the bottom about the signatures that are there, but the DS record is missing. It's the red cross that is circled here. So, initially the domain is registered, no DNSSEC is in use yet.

But the next slide, without any user interaction, when the automation is turned on, like the car airbag, if you wait for some time, then this red cross will turn green, and the interaction will have happened in the background between the DNS operator and the parent domain, and then you have DNSSEC. So, it seems like this would be a good way of enabling the functionality for those registrants who want that without manually dealing with this problem.

Next slide, and I believe final slide. Yeah, so the status of this is that it is in use at some ccTLDs. I mentioned .cz, there is also Switzerland, Sweden, Uzbekistan, some SLDs in South Africa, Costa

Rica, I think, Liechtenstein. And so, there are a few RFC standards for that. I'm not going into details. What's important to know is that for gTLDs, they're currently not eligible for this technology because the devil is usually in the details, and there are some minor implementation differences you can have. For example, when the registration has an update lock, it's not clear whether that means that DNS automation is allowed or not.

And so, these inconsistencies between how you could do the implementation need to be addressed so that things work the same way once it's allowed for gTLDs, so that if you have 10 domains across gTLDs, that you can expect it to work the same. There is a document in the IETF that is recommendations for how to do this.

It's expected to become an RFC later this year. And then once that's done, it would be great if DNSSEC automation would be allowable across all TLDs who want to implement this. And this way we can maximize interoperability, make DNSSEC more accessible, less error-prone, minimize surprise, everything works the same. And essentially, that's the recommendation of an SSAC report from two years ago, SAC126. which has surfaced some of these issues.

So, I hope this was a nice and helpful rundown of how easy it could be and where the current culprits are. And so, I guess this is the time to take any questions.

CLAIRE CRAIG Hi, Peter. This is Claire.

PETER THOMASSEN Hi, Claire.

CLAIRE CRAIG I have my hand up in the chat, but taking the opportunity to ask a question before others jumping the queue. So, you spoke about the difficulty of implementing DNSSEC, and I'm just wondering, in small markets particularly, can DNSSEC be implemented at an internet exchange point and would that be useful?

PETER THOMASSEN So, the internet exchange points deal with delivering data packets from a sender to a recipient and they connect different networks, for example, let's say the Vodafone network with the Google network or something. And so, that's in the routing area. We have the RPKI security technology and shows that things work the right way. Domains are not concerned at the Internet Exchange Point level, so DNSSEC has no role there.

CLAIRE CRAIG Okay, thank you. Are there any other questions in the room?

RAM MOHAN Claire, I see Mr. Nath has a question, and I see Maarten has a question. So, Mr. Nath.

MR. NATH Hello?

RAM MOHAN Please, go ahead.

MR. NATH So one is, you've mentioned some ccTLDs have already used automation and you've given some status. So, what are the challenges for the other ccTLDs to use it, and when was this implemented? What was the time it took for you to get these ccTLDs on board?

PETER THOMASSEN I wasn't involved in getting them on board, I think they just made the decisions themselves. Most of these implementations have been around for a few years. I don't know exactly when they started, maybe, I don't know, 2020 or something. Since then, some of the operational aspects, like the locks thing that I mentioned, have been clarified and some implementations have adjusted the way they work.

For example, Switzerland. What were the challenges? That's a good question. I think at the DNSSEC workshop, which I believe is on Wednesday, Olli Schacher from .ch will give a report about exactly that. So, before I second-guess what his thoughts are, I suggest that we all listen to his contribution.

RAM MOHAN Thank you. Amrita.

MR. NATH Thank you.

AMRITA CHOUDHURY Thank you, Ram. The question is, we've seen a lot of DNSSEC training being done, at least in Asia by the RIRs, even ICANN, et cetera. Is it something to do with mindset in terms of implementation by ISPs and others? Because for an end user perspective, I have no role, but it is the ISPs or the others who are providing services who has to do. So, is it something which has to be a top management down approach? Because many times new implementation is looked at as a cost addition to the infrastructure.

PETER THOMASSEN Yeah, that is certainly true. So, there's the signing and the validation, right? So, in both cases, there is a certain cost associated with it and oftentimes, people or entities are not willing to pay the costs until something happens. So, if we look at the nameserver hijack incident from 2019 that I mentioned, there's a few articles about this. Some of them say that particularly organizations in the Middle East were targeted, for example, Saudi Arabia.

And if you look at DNSSEC deployment statistics for Saudi Arabia, it was, I don't know, 20% before that, and then the year after, it went to 99%. So, there are some incentives when something has happened. Despite the cost to implement things, the question is whether you want to wait for something to happen or not.

RAM MOHAN Thank you. Herve?

SETONDJI HOUNZANDJI Okay, I'm going to speak French, if you allow me. I'm waiting for Peter. He's not ready yet. Hervé, I am the Secretary of AFRALO. I have a personal question. I am an engineer, a computer engineer, and I have already implemented DNSSEC in certain domains, and I always wonder why haven't we done it a long time ago.

Today, when you want to configure a web server, so besides the certificates, you can use a Latin script. And you just have to launch a script, and the system will tell you how to do your configuration. So, I always wonder why haven't we done it for DNSSEC? And my question pertains to what you're doing. You know you have ccTLDs in Africa, so how will you proceed to make sure that this is also used in Africa? I come from Benin.

Our ccTLD is .bg, and when I want to do a DNSSEC in a sub-level, I have to create keys, I need to send the information to .bg. So, with your script, I think they will have an automatic update. Is there a

process in place to have more impact on ccTLDs in Africa? I'm not sure how you will be able to help them.

PETER THOMASSEN

Thank you for the question. I'm not aware of any particular process that is in place for that. However, the degree of difficulty depends a lot on the software that you use. So, there is quite modern software like NodDNS, for example, and certain registry software, FRED, I believe from CZNIC, which is open source and can be used by others as well.

And that software supports the automation technologies, and for registries that use such software, it is not very difficult. I mean, still you have to do the configuration, but you don't have to implement it yourself. So I don't know what is the software that are used by .bg. We could talk about that maybe after the session. And certainly, me and the rest of SSAC would be willing to advise. But there's no particular process. Is that a helpful response?

RAM MOHAN

Thank you, Peter. Thank you. Pari, did you want to speak? Okay. Maarten?

MAARTEN AERTSEN

Yes, so this is just a small addition to the answer that Peter gave to Claire at the beginning of the Q&A. I don't believe there's anything in particular holding back the deployment of the technologies that Peter talked about in smaller markets. So I think his answer

focused on whether or not an exchange point is to do with DNS. But if we ignore that part and focus on the other part of the questions, which was about small markets, I think some of the ccTLDs that Peter showed as having deployed this already are small markets. So, yeah, just a small addition.

PETER THOMASSEN: So, to let me add to this very briefly, DNSSEC has been around for a while and the automation is sort of new. Without the automation, it's in fact quite difficult and lots of failures have happened, misconfigurations, outages. And the image of DNSSEC has suffered as being unstable and too complex. So, to some degree, there's certainly also an image and narrative problem, and some of these things have changed, however, because automation now is technically available.

There's a very interesting article by Barbara, who's sitting here, on this particular problem in CircleID, I'll paste it into the chat. And if you're interested into what are non-technical factors that might drive or prevent DNSSEC adoption, I encourage you to read that article. Thank you.

RAM MOHAN: Billy, and then…

JONATHAN ZUCK: Sebastien has had his hand up for a while.

RAM MOHAN

Okay. Thank you for helping the queue. So, Sebastien, then we'll go to Billy, then we'll go to Matthias, and then you have one there, and then we'll draw the line with that question. Thanks.

SEBASTIEN BACHOLLET

Thank you very much. Herve, you helped me by speaking French? I have domain names, how can I ensure whether I do have DNSSEC or not? What can I do to have the name from the point of view of a DNS user? Thank you.

PETER THOMASSEN

Maarten wants to answer.

MAARTEN AERTSEN

So, if I understand correctly, the question asks how you could check if things are set up correctly. And I think there is very -- you want to add, Matthias? So, there's various relatively user-friendly tools available online to check that your domain is set up correctly. One of them comes from my country, and it's called internet.nl.

And you can run a little check, so you can input your name, and it tells you if DNSSEC is configured on a domain. But you can also check if your ISP has validation set up, so you can test your connection, so to say. So, I'm not sure if that answers the full question, but there's tooling available, and in one such tool, there are many internet.nl domain?

PETER THOMASSEN: So, Sebastien, maybe just very practical. So, I mean, if you buy a domain, you have an admin panel, and there you can also see, for example, if Let's Encrypt, which is a free service, is enabled. So, you just log in with your user credentials and look if you can enable it or not. A lot of registrars are offering this service. So, it's just like tick the box, and that's it.

RAM MOHAN: Thanks, Matthias. Billy.

VASYL "BILLY" BRATCHENKO: Matthias mentioned that as a user, when you are receiving errors, this may mean that it's an interception attempt or something is misconfigured. Is there a technical way to make it clear whether it is an attempt or it is a misconfiguration?

PETER THOMASSEN: That is very hard to detect in general. As Matthias said, DNSSEC is your silent bodyguard. If your bodyguard makes a mistake because you gave wrong instructions, then, access is blocked. But this is exactly what automation is supposed to prevent because it's supposed to prevent misconfigurations. It's similar like with HTTPS certificates. Before automation came with Let's Encrypt, it was common to see expired certificates. It still happens, but it's much more rare.

RAM MOHAN Yes.

MATTHIAS HUDOBNIK Yeah, so actually I just wanted to emphasize once more. So, we had this webinar, EURALO DNSSEC webinar and if you're very interested, you can look at a webinar. So, it's recorded and we have all the speakers. There were people from .ch, from .pt, and then from CORE, from Cloudflare, and EURALO was hosting it. And also, Barbara has her presentation there. So, please have a look if you're interested. It's like one and a half hours, and you can learn a lot. So, it's quite hands-on just that you know it. I will try to post the video link into the chat. Thanks.

RAM MOHAN There was a question from there. Please.

AVIRAL KAINTURA Thank you. I'm Aviral for the record. So, thanks, Peter and Mathias, for explaining DNSSEC. So from an end-user perspective, so when a DNSSEC validation fails, it is seen in the slide as well that we get a generic serve fail error. But it can have a multitude of issues, underlying issues, right?

And then, so there is just this particular error that we get, server fail. So, yeah, it can mean a lot of multiple underlying issues. Either it can be like a security problem or it can be a misconfiguration. So,

as an end user perspective, is there a scope of more transparency on what could actually go wrong in this case? Thank you.

PETER THOMASSEN I'm sorry. I was distracted. Can you ask the question again?

AVIRAL KAINTURA Yeah. So like, when a DNSSEC validation fails, right, so we get this error, server fail, right? So, it's a generic error. So, it can mean a multitude of things, right? It can be maybe a misconfiguration or something like related security. So, I was asking as an end-user perspective, is there a scope of having more transparency to the end user what could actually go wrong?

PETER THOMASSEN Yes and no. So you're right, the server fail error code is generic for any sort of error. Now, there are various extensions to the DNS. For example, DNS extended error codes are similar. I'm not exactly sure what the abbreviation is. Anyway, so it allows the resolver to include a piece of information in the response that says what went wrong.

For example, I couldn't reach the name server or the key was expired. Not the key, the signature was expired or something like that. Now, even if you have that, that information doesn't surface to the browser level because the browser usually asks the operating system for a website IP address, and then it gets only the

IP address or no response, but there is no data structure that allows forwarding that error information to the browser level.

However, there's work in the IETF to change that. And so, in the future, browsers might display more advanced information about why things are not reachable, which might include things like DNS filtering also. And that work is underway. I believe that the major browser vendors are on board, but I would think that it would easily take, I don't know, a year or two for that to become operational.

A more interesting question, however, is I think not how the end user can determine what the problem is, because if it is a misconfiguration, then actually the operator needs to learn about it. So, there's a different way to deal with that where resolvers can tell an operator that they observed an error, and that is more important for fixing misconfigurations, but it's not visible to the user because it goes in the other direction.

RAM MOHAN: Thank you. I am actually going to close the queue with whoever is in the queue right now because it seems like it's a really interesting topic with a lot of questions that have come through. So, online I see Mourad. We can hear you now.

MOURAD MELLITI: Mourad Meliti speaking. Yes, hello. I just wanted to come back on the security issue, and is it enough to have DNSSEC on a root zone or not? There are several stakeholders involved in the security of a

domain. It's not only the end user or the registry. It's also the service providers or the registrars who offer DNSSEC to the end users.

And there's a slight difference there in that chain. For the domain to be secured and signed, well, it's a necessary condition, but it's not enough for the domain to be well protected, right? So, I am in charge of .tn, which has been secured since 2014, but there are registrars who do not offer DNSSEC to the domain names who use .tn.

So, to automate the DNSSEC activation for ccTLDs or gTLDs, is not all the time the end solution to have DNSSEC automatically activated. It means that registrars also need to offer this to the end users. I just wanted to come back on this because it's very important to really involve all the stakeholders in this.

PETER THOMASSEN Yes, that's true, it's a multi-party problem. Yes, it's right. However, in the end, when you turn on DNSSEC on the domain and parent level where the DS record is configured, you need to get the DNSSEC parameters from the child DNS operator to the parent operator. The registrar is an intermediary party, but it only happens to be like that. It is not a party that needs to do anything besides forwarding the information.

If you find a way to get the information to the registry some other way, that is also workable. And this is actually how the currently

successful ccTLD implementations work. They do not go through the registrar. .cz, for example, will talk directly to Cloudflare, if Cloudflare is the domain DNS operator, and they will directly fetch the DNSSEC parameters and turn it on in the registry.

The registrar is only an observer to this process. So, that's possible. It's also possible for the registrar to do the automation. So, it's a policy question. It seems like it would be easier if the registry takes the work off the shoulders of the registrars. At least that's what all the ones that currently exist have decided to do.

If you're more interested in more detailed considerations around this question, that is part of the operational recommendations document that is linked in the center bullet on this slide that you can click when you download the slides. And, yeah, so the registrar can be involved but doesn't necessarily need to.

RAM MOHAN Thank you, Peter. Robert.

ROBERT GUERRA Sure. So, I just wanted maybe to go back to a level and just like the last conversations have all been issues about issues and problems that come up. But let's not lose track because this helps with data integrity and authenticity of the DNS, just like enabling HTTPS through Let's Encrypt helped, and something that users and also all the ALAC groups here that do user education, it's very important

to reach out to tell the folks that you're engaged with that this is a choice now that registrars have.

Registrars may have an option for DNSSEC, and those are ones that will allow for better authenticity. It's a mechanism that's there. It's going to be invisible to the user, but that's a user choice that's particularly important. And in an era where, unfortunately, there are more attacks on the infrastructure and other issues, picking the right registrar that has features that help protect you is definitely, and the users that you deal with, are something particularly well, and that they get the implementation right.

And so, I think let's not lose track. We're getting into the small issues, but some of the registrars are finally deploying it. They are putting in automation. The error codes are going to be getting better in the future, and this is something that I would just definitely just look up. If you have a domain name registered, look it up, whether it has DNSSEC or not and how easy you can do it or not.

And as you recommend that to others, because I was just having a conversation at lunch around an issue that in terms of registrar choices, people think it's just maybe I'll get back into a cheap registrar or not, but it's the features that they offer. And so, that's something to look into. So, let's not lose track of the error codes and the messages. In fact, this is a good thing to deploy, and it's only going to get easier over time.

RAM MOHAN Thank you, Robert. That was almost the end of a substantive session. We have you as the very last commenter.

FREDERIC TAES Frederic speaking from EURALO. Thank you very much, Ram. Really interesting content. So, at EURALO, we have organized a roundtable on DNSSEC. We were really successful. I have to say that the feedback survey we had from participants was really positive and most were convinced, between 80% and 100%, to move on and to implement DNSSEC afterwards, which is really a great result.

And especially to say that it was really complex, abstract, what is DNSSEC, what's the added value, how to do it, and that was really concrete after this one table. So, that is one feedback. Another one to answer to previous questions about the end users. An ALS of EURALO has also developed a browser extension to improve the trustworthiness on domain names, and I am putting that also in the chat.

So, it's trust.org. You can all go there. It's a free browser extension also implemented on the website itself. Who can display it to you and to end users? Do we have DNSSEC implemented for this domain name? Yes or no? Because even that information is not, without this add-on, easily available. And also, giving other

information about domain names. That was to close it. Thank you very much.

RAM MOHAN Thank you so much. That's wonderful feedback. And thanks for sharing with us that this session went well, it's a credit to the folks who are able to do that work and convert all the technical jargon into things that people can actually understand.

FREDERIC TAES Yeah. And I would add that there were also participants from business companies. So, not people really from the ICANN world, I would say ICANN community having attended, really experts about Internet security, and they have learned themselves. a lot from those meetings. Thank you.

RAM MOHAN Thank you so much. Sure.

JONATHAN ZUCK I don't think it's an issue, but if that was a recorded session, we can take the snippet out of it that is a good explanation and begin to have a library that's aimed at a different audience. It doesn't have to be the whole Zoom recording. It can just be a presentation if it's clear. Let's get in the habit of doing it, especially if you guys don't mind us doing that, so -- okay. Yeah, let's take a snippet.

FREDERIC TAES Yeah, for sure. Thank you for your remark, Jonathan, and it is also covered. So, we are improving on LinkedIn and all the social media, also the communication, and this is the kind of thing that we are now promoting to all broader communities. Thank you.

JONATHAN ZUCK You have the social media goddess next to you.

FREDERIC TAES Indeed, yeah.

NATALIA FILINA Just a minor addition, thanks a lot for your help with organizing this DNSSEC roundtable. And Joly MacFie from ISOC helped a lot. It was very well-structured information with short summaries, with recording. So, I may put the link to the chat now for sharing the information. Thanks a lot again.

RAM MOHAN Thank you so much. So, one of the takeaways, I think, for you in the ALAC and from the SSAC point of view that we would like your help on is you're hearing from us saying automation helps. Automation makes things not only just easier, but that tooling means that the errors are reduced, the complexity of this whole topic is kind of put under the cover of an automation.

So, there is work that is happening inside of ICANN as well. The SSAC put a report out on automation a little while ago, but we're also encouraging gTLDs to start having automation as a standard mechanism. So, when that comes up, and there's a policy discussion there, we would appreciate your support, lending your voice to what we bring to the table, which is the technical piece of it.

Okay. So, we have only a little bit of time left. So, what I'd like to do is to skip straight through to the safer cyber topic. And this, Jonathan, is kind of a reprise, but also a, hey, where do we go forward idea. For those of you who are new to this topic, SSAC and ALAC for the last couple of years have engaged in a really productive conversation that converted from an idea into reality.

We were able to help provide content that the ALAC then took and made this fantastic educational material with explanatory text, slides, things like that, that took away the technical pieces of what do you do when you get phished and made it into something that is directly applicable for an end user. So, we're very encouraged with that.

And we wanted to share with you some things that we're doing with other parts of the community. And we want to share that with you, and then open up for an open brainstorm on what more we could do together.

JONATHAN ZUCK You're seeing other people? I didn't know about that.

RAM MOHAN I thought we have an open thing going on here?

JONATHAN ZUCK You would just assume that.

RAM MOHAN Let's go to the next slide. So, since the start of this year, we've begun a collaboration with the ISPCP, and we've announced in coordination with the ISPCP a year-long set of webinars as well as sessions at the ICANN meetings on various topics. Each one of these topics are topics where the SSAC has not only interest, but where the SSAC has provided content and material.

And what we're doing with the ISPs is they're providing the venue, the distribution network, so to speak. We're providing the technical experts to come and speak. So, Billy was actually present at the February one. Do you want to speak briefly about how that went and who was there, how many people showed up? And then I'll speak just briefly to the rest of it.

VASYL "BILLY" BRATCHENKO I think we had 107 people. It was a great discussion about automation of DNS abuse prevention and mitigation. Some good

questions on AI, which is top of mind of our working group in SSAC. And actually, we liked the activities and the level of participation.

RAM MOHAN

Thanks, Billy. And I won't read all the topics up there on the screen, but you see that these ones have a lot more relevance to an ISP hosting provider type of an organization. But I put it up here as both information but also maybe a kickstarter for what else we could do together, Jonathan.

JONATHAN ZUCK

Yeah, thanks. And Amrita may have more to say about this, but we formed a subgroup within At-Large called ACES. And that's the group that's producing that fishing courseware. But we're just looking also at other means of information dispersal through our networks. As you've heard in the past, there's the RALOs, the ALSs.

The ALSs, in turn, have their own members, and how do we get information out through that method? And so, we've come up with a number of ideas, and we're trying to pilot them and test them. One might be a Twitter campaign or an X campaign or whatever, or it could be a phone call-down list. It could be a webinar or a seminar, and the seminar was what the phishing is.

And so, one of the things we had looked at was a Twitter campaign related to universal acceptance. We were thinking of finding a global brand that had not implemented universal acceptance yet and seeing how many tweets we could sort of get acted at that

global brand. And I guess ICANN was working hard to kind of coax those brands, and so they were nervous about that idea.

But it occurs to me, if there's a survey or something we ought to do, if there's something automated, I don't know what the right answer is, but is there a way to identify people that might be the recipients of such a campaign in the DNSSEC space? Part of what Sebastien was trying to get at with his question, I think, is how we draw this DNSSEC automation question closer to the end user.

I mean, they're never going to be doing the deployment themselves. But the end user, if they've learned that their ISP doesn't have it, is there a way we can help them, and maybe it's just to tell them that, but if we engage our network to communicate with some of the larger ones or something like that as an experiment to see if we could raise awareness and get people to consider doing a deployment now that automation is a more realistic way to do it.

Maybe people tried before and it was too complex. All those things are possible. So, if you think about a way to identify who needs to hear that message, then we could potentially mobilize our network to deliver it. Does that make sense?

RAM MOHAN

It does. I'll speak for myself personally, I think for many years now inside of the ICANN community, we've taken DNSSEC, for example. Initially, we treated DNSSEC as a technical issue, and we spent a lot

of time explaining the technology and demystifying the technology. The more we demystified the technology, the more mystical it became.

And then you had implementations of DNSSEC, and then some configuration error would happen, there would be a problem, and then you would have some report that said this TLD had a problem because of DNSSEC. So, now in the SSAC, what we're doing is two things. One, like what Peter and Matthias are doing is to actually take the technology and explain it in a more user-friendly, user-accessible manner. That's one part.

But the other part is we've got a work party that expects to finish its work later this year on the operational considerations for DNSSEC. And in that document, one of the unspoken things in there is we're going to say, or I think it's going to say, DNSSEC is operationally complex, and some organizations may decide that it's not for them.

And Warren has pointed out sometimes that if you look at the top 100 most visited properties on the internet, many of them haven't deployed DNSSEC, and that's not because they don't have the capability or the wherewithal to deploy DNSSEC. It's for some other reason.

So, we have a document that's coming out that is going to speak to, if you want to deploy DNSSEC, what are some things you ought to do to be prepared for it, not just to deploy it, but to keep it deployed, to keep it continued to be in a secure and in an

operationally sound manner. Because that's one thing that we're doing.

JONATHAN ZUCK That's a tough message to boil down.

RAM MOHAN That's the thing, right? So, I'd say that with DNSSEC, we may have to think about if the end user doesn't have access to the tooling and the end user doesn't even understand the value and the benefit of DNSSEC, should we instead focus the energies on the intermediary and have them explain what the value is to their consumers rather than us trying to get to the consumers directly? Thinking out loud.

JONATHAN ZUCK Well, and in fairness, when we're talking about end users, there's a little bit more sophisticated. If you're part of an ALS, that's probably an ISOC chapter, it could be a security-related firm or something like that. It's not the same thing as a true my Aunt Donna in Norwell, Massachusetts end user, right?

So, we're trying to operate to the benefit of those end users. But through our network, we have people that I think are not going to be terribly challenged by the notion that it's a good idea. Many of them don't have the sophistication necessary to do a deployment of it, but certainly could get to a point of messaging around it.

And so, if they knew who to message to, then that might be something that we could help with. That's the real issue is who is the audience for our members to get to help those people's users. So, that's just something to think about, I think.

RAM MOHAN Makes sense.

RUSS MUNDY Ram?

RAM MOHAN Russ. There's a queue over here. There's a queue here. So, in the queue there is Russ, and then in the room there is Herve, and then Amrita, and Sebastien.

RUSS MUNDY Yeah, I'd like to respond to Jonathan's question about who to talk to. In many cases, your folks, if you will, on the ground level have a better knowledge about who to talk to than what the SSAC would as far as specifics. In terms of the general of who to talk to, one of the things that we've heard over the years from a number of providers, and registrars in particular, is there is no demand for DNSSEC. No one is asking for that.

So, any interactions that you might have or your folks might have with either their ISPs or their registrars or their registries asking for DNSSEC support, for DNSSEC service, is an important thing for folks

to do, because I think many of the people in the ALAC and RALOs and so forth are aware of the importance of DNSSEC and want to have it and make use of it.

But they're the ones that can best carry the message to their providers. And I can say I've changed registrars because some of the registrars I've been using did not support DNSSEC like I wanted it to be supported. So, going to another registrar is another strong lever that a user has. Not in every case, but in a lot of cases, they do. Thanks.

RAM MOHAN Thanks, Russ.

SETONDJI HOUNZANDJI Okay, thank you. I would like to give hope. We talked about artificial intelligence, its inconveniences pertaining to DNS abuse, but I would say that there are a lot of benefits to artificial intelligence, and it enables a better implementation of DNSSEC. And everybody that was afraid or didn't know how to create a key, I know that there are answers, and I am hopeful. I know that many more domains will implement DNSSEC. Thank you.

RAM MOHAN Thank you. And, yeah, as Setondji said, right, hope is a loan made from happiness. So, maybe we'll get there.

JONATHAN ZUCK I can help with the research potentially too, an AI agent.

RAM MOHAN Amrita.

AMRITA CHOUDHURY Thank you, Ram. Two things. One is a question. Do we want to promote DNSSEC because there are, as you mentioned, many companies come. By choice not implementing, understanding it, that's one part. Two, to Jonathan, and obviously we would need the SSAC's help in it. In case we want, and if I look at even ISPs, there are different kind of ISPs.

There are ISPs who are run with just two person or one person doing everything in developing countries. So, there are categories, there are education level in terms of managing, even knowing what is happening globally is very different. Capacity building for many of them is very important.

So, in case, Jonathan, we are thinking of a campaign that, look, you can do this kind of thing, are you DNSSEC ready, or whatever we think of that, why you need to do, and we are linking them to some page which SSAC or ICANN has with resource information which they can look at, because having the right kind of information is also many times difficult, complex, and everyone likes nearly half-baked food.

So, if that also could be done and that kind of an information campaign can be done, which from At-Large we can at least do that

through our RALOs, we could think of that part. And if there is a bigger company we want to think of, Jonathan, your pet project, if we could identify one and say that, look, are you DNSSEC ready because of security issues, as Peter was mentioning, one fine day something happens, everyone runs around after it for damage control, that could also be, and these are wild thoughts which come to my mind.

RAM MOHAN Sebastien.

SEBASTIEN BACHOLLET Thank you very much, Ram. A lot of those topics you put here may be of interest also for us as an end user, and maybe we need to think how we can deal with IPCP and with At-Large. But particularly the two topics for ICANN86 seems to me personally very important because the post-quantum is now, is not tomorrow and you know that better.

And privacy versus security is something we need to deal with as a user. Therefore, those two topics must be embedded in a wider program with us if it's possible, and if our Chair agree with that. Thank you.

RAM MOHAN Thank you, and we're happy to work alongside you. We put this up as, again, as I said, as a conversation starter. Maarten, you will have the last word.

MAARTEN AERTSEN Yeah, so I wonder if ALAC wants to have Peter back once he's done and the others are done standardizing DNSSEC automation, because he mentioned in his slides that there's still some ongoing work. But maybe when that's finished, that's the nice time to start talking campaigns and stuff.

SEBASTIEN BACHOLLET All right. Sorry, please, talk about At-Large. Our 15 members of ALAC will need that, but we, millions of users, we need that much more than just them. Thank you.

RAM MOHAN Okay, I think -- sorry, you had a question, please.

KARAN Hello everyone, I'm Karan for the record. My question is, Ram, domain abuse is a much bigger issue, and DNSSEC would have its own limitations. So, then this initiative is one, but then do we at ICANN believe that DNSSEC is not the whole answer to DNS abuse, the limitations that it has, and what are the steps, I mean CyberSafe campaign is one, but then what are other things that we're doing to cater that?

RAM MOHAN

So, I think that DNS abuse, particularly inside of the ICANN context, DNSSEC is at best a little tiny piece of that. There are much greater issues that arise. And right now if you look at the GNSO and there's a PDP on DNS abuse looking at associated names. So, there's a lot of work that has to go there.

So, DNSSEC is not a silver bullet for the DNS abuse problem. And inside of SSAC, we just have started up a work party on looking at the impact of AI on DNS abuse. And so, we're just beginning that work in that area as well. So, I think this is one of those watch this space because there's a lot more work to be done.

JONATHAN ZUCK

Yeah. There's a lot going on concurrently. There's the new PDP that's on associated domain lookups. There's another PDP coming that's about API usage and bulk registrations. There are trusted notifier programs that are coming into play.

There's recent additions to the contracts that require more immediate mitigation, and OCTO, as part of ICANN, has started building more and more tools for at least understanding where the DNS abuse is coming from and narrowing it down. So, it's definitely something where there's going to be multi-tracks to address a problem that will never be totally solved. But there's a lot going on, not just the DNSSEC.

RAM MOHAN Okay, I think with that, Jonathan and Claire, thank you for your time and for having us with you. We always appreciate being here, and the depth and quality of the discussion today is indicative of both the relationship that we're building but also the quality and the interest in what we're doing together. So, I appreciate it.

JONATHAN ZUCK And we always appreciate having you here, so thanks for coming. As I've said before, you do a lot of incredible work, and we don't want it to be like PhDs that end up in the library and nobody checks out. So, we want to make sure they find their way to the right set of eyes. Thank you.

RAM MOHAN Thank you.

[END OF TRANSCRIPTION]