ICANN69 | Virtual Annual General – DNSSEC and Security Workshop (1 of 3)
Wednesday, October 21, 2020 – 12:30 to 14:00 CEST

KATHY SCHNITT: Hello, and welcome to the DNSSEC and Security Workshop Part 1. My name is Kathy Schnitt and I am here along with my colleague, Kimberly Carlson, and we are the remote participation managers for this session.

Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. We will read questions and comments aloud during the time set by the Chair or moderator of this session.

If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute your microphone and speak this time. Please be sure to state your name.

For all participants in this session, you make comments in the chat. To do so, please use the dropdown menu in the chat pod and select "Respond to all Panelists and Attendees." This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also

be seen by the session hosts, co-hosts, and other panelists. With that, I'm happy to hand the floor over to Dan York.

DAN YORK: Good morning. Thank you. Good. Well, I should say good morning, good afternoon, and good evening, wherever you may be. If we were in Hamburg today, we would be saying that, we could say guten morgen. All of that and we could begin this session, but we are virtual brought to you here by this powerful entity known as the Internet here. This global network connects us all together and we're here today to talk about DNSSEC and security. So, next slide please.

My name is Dan York. I work for the Internet Society. I am part of the Open Standards Everywhere project and other projects within that group. The Program Committee that has brought you this day's worth of agenda—and it is three sessions. This is the first of the three. There will then be a half an hour break and there will be another session and a break and others. This is the Program Committee, some of whom will be speaking today. You can see them from Mark Elkins, Jean Robert from Africa, Jacques Latour from CIRA and Canada, Russ Mundy, Ondřej Filip, Yoshiro, Fred Baker, myself, and Andrew McConachie and Kathy Schnitt. Steve Crocker has also been involved with the program as well. Next slide, please.

And you will see that in this. This is organized as an activity of the ICANN Security and Stability Advisory Committee (SSAC) with additional assistance from the Internet Society. Next, please.

The agenda, which is super hard to read on that screen as I look at that there, but maybe if you could reduce the notes here at the bottom of the screen, that might help a little bit there, too. You can see a bit about what we're going to do. I mentioned that there were three sections to this day today. The first one is what I'm going to begin with talking about, about where we're at with deployment statistics, and then we'll have a panel around where things are with some of the TLD deployments and the pieces that are going on. And you can see some of the speakers there: Moritz, Suzanne, Wes, Pablo. We'll have a short break then. It's an ICANN-mandated break in the schedule for half an hour. We'll come back to the same Zoom URL. So you will not have to change, you will be able to just stay at the same Zoom URL for the day.

And then in the second session, we have a panel discussion around automation of DS updates. This is really one of the big things we've seen over the time is that it's great that people sign their domains and do all of that, but one of the challenges is keeping the domains updated. I had this happened to myself. Recently, one of my domains, suddenly somebody said, "I can't reach your site," and I looked and, lo and behold, my KSK, my Key Signing Key, had expired. I had not provided the DS update to the TLD and the chain of trust was broken. It's to prevent things like that that a lot of the work we're doing now is around DS automation and how do we go and do that.

Steve Crocker has assembled and Shumon Huque have assembled a panel where we will be talking about the various aspects of this—where we're at, what we're doing, how we're working with this in some different ways and forms. That is pretty much the bulk of that

second session, with a brief presentation at the end from Matthijs around that.

We'll then have another break and we'll come back to have a session at the end where Willem from NLnet Labs will be talking a bit about the current state of DNS resolvers and the RPKI protection pieces. I've got some presentations from him around some the latest work he and others there have been around that. That is our session today. Next slide.

And that's where we'll be talking about that. So I want to first give you a little bit of a sense around where we're at today in terms of deployment. This picture here shows the validation rates. This is coming from APNIC Labs that has one of the ongoing statistics we've been watching. And this is the number of ISPs that are checking that are operating or, I should say, the number of networks where you can do DNSSEC validation, number of queries that are coming to various different sites and pieces, and we're seeing about 25% of that globally doing DNSSEC validation. You can see it's been a growth curve over time and it continues to grow. It's heading in the right direction. Of course, we'd love more, but it's also patchy in different spots of the world. You'll see that some of the validation is up around 60, 80, even 90% in some areas, in some countries, but then it's also down at 10% or even less in some other areas. So it's patchy all over. Next slide, please.

This was a list of some of the regions of the world where you can see from the APNIC Labs statistics that some parts of Oceania, some parts

there are significantly doing a significant number, almost two-thirds or more of the DNS queries are being validated, and so it's taking a height of the checking. Next slide, please.

This is just good to see where this is happening around there, going down to the other parts where it's not. This is a view from the DNSSEC tools, which is maintained by Wes Hardaker, Viktor Dukhovni, and others. We're seeing that the growth of DS records overall continues to climb. And so this is the other side, the signing side. So next slide, please.

This shows us really where we're going. This is some work that, again, Wes and Viktor have been tracking around the growth of DANE records, which is TLS records used—a lot of this is for e-mail, and this is primarily what we're seeing here in this chart is the signed e-mail. The DANE records provided TLS, MX records providing that security as well. Go on, please.

The RPKI which is the Resource Public Key Infrastructure, which is used for signing resource, ROAs for signing routing security records, we're also seeing that growth continue going on from there. Next slide, please.

You can see here the great growth we're seeing all around the world early in the number of signed prefixes that are being covered by this. We'll talk about this particularly at the end. We'll talk a bit about RPKI deployment, but this is another part of what we're looking at is how do we secure the routing infrastructure of the Internet. Next slide, please.

Okay. This is the other one. We've been maintaining these [maps] for years and we can see again that we're increasingly seeing it signed around the rest of the world and some numbers here. Let's go on to the next.

Here are some resources that are out there that you can be able to look at. You'll have access to the slides afterwards. You can be able to look at that from there. And let's go on from there and that's it. So I will turn it over to my colleague, Russ, to talk to you next about some of the deployment in various regions. All of us in the Program Committee will be around during this time. Feel free to ask questions using the Q&A pod or post a message in chat, pieces like that, and we will be glad to interact with you. So, over to you, Russ.

RUSS MUNDY: Great. Thank you very much, Dan. So we have a good collection of folks today. And this panel is really focused on activities that are, as Dan said, illustrating some of some of the deployment to functions that are going on. So I was scrambling around here to get my local copy of the other program back on the screen. I didn't quite get it up so I do not have the agenda in front of me, but I will try to get it up so I'm not quite so awkward here. Anyway, if we could go ahead and bring our first speaker's slides up, Kathy.

KATHY SCHNITT: Moritz has just been promoted to co-host. So he's actually going to share his own slide deck.

RUSS MUNDY: Oh, that's great. Okay. So our first speaker, here we go. It's some information about algorithm agility, which, for those of us that have been involved in DNSSEC for a while, it's something that we've seen some progress in. We've seen a number of changes within TLDs, two different algorithms. And so we're going to hear a little bit about the study that Moritz has done. So, please go ahead, Moritz.

MORITZ MÜLLER: Yes. Thank you. Do you see my full screen now, or do you just see the application window?

RUSS MUNDY: Well, I'm seeing the application window. It looks like it's Adobe and you're still getting the sidebar.

MORITZ MÜLLER: I think it's not full screen but I think that should be all right.

RUSS MUNDY: It looks good.

MORITZ MÜLLER: Okay. Thank you. Thanks for having me. My name is Moritz Müller. I work for SIDN Labs, which is the research agency .nl TLD. This research was together with folks from NLnet Labs, Virginia Tech, and University

of Twente. And the goal was to study what are the main barriers, but also success factors for introducing new algorithms in DNSSEC and also deprecating other ones, such that we can prepare DNSSEC for the challenges to come.

As you all know, DNSSEC brings integrity to the DNS, but it therefore heavily relies on the security of its signing algorithms. In the past, multiple different algorithms have been deprecated, and then were not considered secure enough anymore for DNSSEC, but others were introduced as well that had beneficial attributes like better performance, better security, smaller signatures and so forth.

All of these algorithms have in common, however, that they could be rendered insecure as soon as we've seen powerful quantum computers. And these powerful quantum computers, together with short algorithm, could break all of these algorithms. It is not clear yet when these quantum computers exist. However, we think it's still necessary to learn from the lessons in the past, from algorithm transitions in the past, to make sure that we can transition to quantum safe algorithms as fast as possible in the future.

In our paper, which will be published next week by the way, we've looked at the whole life cycle of the algorithm standardization starting from the standardization in the IETF, and then continuing on with the algorithm support and software, and the registration channel, and following by the deployment at domain names but also at resolvers, and finally, looking into the deprecation of insecure algorithms and the adoption of new ones as well.

In our research, we look at different parts of the algorithms in the different stages of the life cycle. For the first two stages, we look at all the algorithms. For the deployment section, we mostly look at ECDSA for signing, and ED25519 and ED448 for validation. And in the deprecation section, we look mostly at RSASHA-1-NSEC3, but also at the other algorithms that should not be used anymore.

Just to give you a general overview at what we are right now—these numbers are from a few months ago—but what we can see here is the domains that were signed in the different TLDs and with which algorithms that were signed. And as you can see here, RSASHA256 is still the most common used algorithm in the zones that we discussed in our research, but ECDSA is luckily already second, which is, I think, quite a good sign. However, RSASHA-1-NSEC3 is still hanging around in most zones.

Okay. So let's first start with the standardization of a new algorithm. As you might know, this usually starts in the IETF by an individual, going to the DNS Working Group and proposing a new algorithm for DNSSEC. And if there's enough interest then the draft will be adopted by the working group, and the working group will then work together on this draft and discuss the details. At some point in time, when the draft is mature enough, there will be usually a last call. And when no other issues are raised during this last call then we will probably see that this algorithm gets standardized at some point.

Okay, this is unfortunate. Probably my PDF didn't export very well. So let me briefly jump to PowerPoint. Excuse me for that. You should now see PowerPoint, I think.

DAN YORK: We do.

MORITZ MÜLLER: Okay. Let's say from here. I'm sorry. So this slide here shows the time it took until new algorithms were standardized in the IETF for DNSSEC, from the whole time period when it was first proposed until it was standardized. And these are the algorithms that were standardized after DNSSEC itself was standardized. What we can see here is that standardization can take between one and four years, which is quite a wide range. It's kind of hard to draw more general conclusions.

Why this is the case? For example, in the early days, we've seen some more protocol-related issues in the standardization of algorithm. Like for example, in the case of RSASHA256, people thought that it was not the right time to already standardize new algorithms but focus on the deployment in general and, therefore, also the standardization of RSASHA256 was stalled in a way. Also later on, there were discussions about NSEC and whether or not they should be included in the algorithm standardization, which was also then hindering its deployment. Overall, we can see, however, that new algorithms that should be standardized should advance the current algorithms by, for

example, having smaller signatures or better performance or any other way and they should be supported in software sufficiently.

And this last step here, that brings us already to the support and software, and the support and the registration channel. Unfortunately, standardization is not enough to get an algorithm deployed as we will see.

Most of the DNS software that is currently out today is not implementing the cryptographic functions themselves, but they rely on third party libraries. Most of them rely on OpenSSL and [inaudible] TLS and it is therefore very, very important that these libraries also support the new algorithm.

Many operators also do not install and update these libraries and DNS software themselves, but they rely on the operating system. The operating system provides the updates or the operating systems are shipped with the most recent software. And this process can also take some time. So in the example of Ubuntu 18.04 and the resolver unbound, together with OpenSSL, it took more than two-and-a-half years after ED25519 was standardized, after all the necessary updates rolled in such that a resolve that would run on Ubuntu 18.04 with unbound would also be able to validate ED25519 successfully.

Next to the software part, we also require support at the registries and registrars. DNS is a hierarchical protocol, which means that if I sign a domain name like example.com then I also have to share the information about this new key with my parents, so .com in this case. This then requires that my parents, .com, the registry needs to support

the key, but also my registrar and, in some cases, that DNS operator as well.

This figure here shows the number of algorithms that are supported by 15 European ccTLDs where we carried out a survey. And this graph already here shows that on the very right, the most recent algorithms, ED25519 and ED448, are not supported by all the registries in our survey yet. This algorithm is older than two years. On the other side, we can see also that many registries still support insecure on deprecated algorithms, which is probably also not such a good sign for deprecating algorithms because people might still be able to use these algorithms in the future.

We reached out to some of the registries and asked them, "Okay. Why is this picture so diverse?" One registry just said, "Yeah, we have a very little policy with what we accept in our zone. So we also do not want to restrict the algorithms that our second-level domain names have." At the same time, other registries said, "Okay. We really want to make sure that the second-level domain names [inaudible] can form algorithms and, therefore, we restrict the number of algorithms to the secure ones."

We get a similar picture if we look at the algorithm support at the top 20 registries and registrars. There we again can see that the number of operators that support ED25519 is still very, very low. At the same time, support for deprecated algorithms is still quite high. And note also here that on the very right, you can see that some of the top operators still do not support DNSSEC at all.

So from that we can conclude that we still have to go through quite a lot of barriers before we can deploy an algorithm wide. But if we finally reach the stage, we can now sign domain names on a larger scale and also upgrade our resolvers, and this is something which we want to look now.

The deployment stage, we want to look as ECDSA for signing and ED25519 for validation. This figure here shows the total number of domain names that were signed with ECDSA starting from the point in time where the draft for ECDSA was submitted to the IETF in 2011. What we can see here is that's right after the standardization, some of the popular DNS software already supported this algorithm but its support didn't have any effects on the deployment of ECDSA at domain names.

Only after Cloudflare started to sign their domain names with ECDSA we do see a small growth here. Nevertheless, it took more than four and a half years after the algorithm was standardized that the first 100,000 domain names were signed with ECDSA.

In this figure here, we can also see some jumps here and there. For example—here I think you can see my cursor—where usually larger DNS operators and registrars then sign all the domain names with ECDSA. Two jumps that stand out. It happened in .se. Here again, these are two operators that sign all the domain names with ECDSA but this time it's not a coincidence. As you might know, .se gives out financial incentives for signing domain names with DNSSEC. But at that point in time, they announced that they would now require also

this usage of certain secure algorithms or versions of secure algorithms, and not just give you money if you would sign your domain name with DNSSEC. This seems to have quite a nice effect on the signing of .se domain names with ECDSA. I believe there will be also some people from .se in the panel later so maybe they can tell you more about that as well.

In general, however, we see even though larger breaks, of course, drive adoption in large numbers. We see that the early adopters were actually small operators. Also what we've seen is that many of the domain names that are signed now with ECDSA have not been signed before at all with DNSSEC or they have already registered, and this is probably not such a good sign for moving to more secure algorithms.

If we now look at the validation site then, in this case, we took more than 11,000 [inaudible] which are measurement points that you can use to start your own measurements, and they're deployed mostly in the U.S. but in Europe, but also in other places of the world. And this is actually data where—then we'll talk about partially I think later on in this workshop.

What we can see here is how many resolvers support ED25519 after it was standardized in 2017. What we can see here is that roughly 60% of the results in our dataset today are able to validate ED25519. We also see that ED448 support is lower, but this is something that we expect because ED25519 is the expected standard in the future.

In 2019, an updated RFC was also published that redefines which algorithms should be used for signing and which should not be used

for signing anymore, but also which are should be considered secure by resolvers. It seems that this updated RFC, which now also says that ED25519 should be supportive for validation, had some small impact on adoption. Here we also see that adoption in general is driven by large operators, which seemed to upgrade their resolvers to support new algorithms faster than other ones.

So to conclude the deployment stage, we can see that deployment of new algorithms, especially at the signing side, can take multiple years. If you look at the resolver side then this seems to go a bit faster, but still we talk about multiple years, and so we see a good number of resolvers supporting the algorithm. And with that, we want to move on to the last stage of the life cycle, the deprecation and replacement of insecure algorithms.

As an example here, I have picked RSA-SHA1-NSEC3-SHA1. This graph again shows the total number of domain names in the different TLDs that are signed with this algorithm. As you can see here, until a year ago or so, the total number of domain names that are signed with this algorithm is still on the rise. We can also see here that even though multiple attacks have been published on SHA1, these didn't have any major effect. Only after the recent RFC was published again we do see some decline. However, if we look at the share of signed domain names that uses algorithm that, from the beginning of a measurement, the shares dropping by 35%, which is probably quite a quite a good sign. However, if you look at the domain names that were signed with this algorithm at its peak but now not anymore, then we see that the majority of the domains have either turned off DNSSEC

altogether or they're not registered anymore and only 1% of them actually rolled to a more secure algorithm. Also if you look at who's responsible for these domain names, then we can see that 90% of these domain names are operated by only three registrars. So if these three registrars would move away from this algorithm then we will see probably quite a big decline.

Now, let's look at the validation side again. RSA-SHA1 can still be considered secure by resolvers, and this is something also what we can see here. Almost 100% of the resolvers in our dataset still support this algorithm or consider it secure. It only seems to decrease in the last few months.

The other algorithms here—RSAMD5, DSA, ECC-GOST—they should not be considered secure anymore by resolvers and we also see that the share of resolvers that consider them secure is dropping or is declining slowly. Here again it seems that the publication of this new RFC recommending against the use of these algorithms has some impact.

Basically, in the observations we asked ourselves, has DNSSEC now achieved algorithm agility? There's an RFC–I forgot its number right now—which defines a protocol has achieved algorithm agility if we can transition from one algorithm to another algorithm over time easily. Based on our measurements and observations, we think that DNSSEC only has achieved algorithm agility partially.

Standardization, support and widespread deployment still takes a decade or decades, but DNSSEC on the other side is really the problem it seems. We think that lack of support in software and in the

registration channel still are the large barriers here. Also we think that the complexity of algorithm rollovers are an issue. We have seen that not many domains rolled to some more secure algorithms. We've seen that, for example, also operators turn off DNSSEC signing before moving to a more secure algorithm. So I think there's still some room for improvement. Improvement in the DS deployment might help DS more.

So with that, we can look maybe a bit further with a potential threat of quantum computing on the rise. And here we've seen that already transitioning to current or algorithms that no one use take a lot of time. And here also the Root still not has rolled its algorithm yet.

So we think that we should assess quantum safe algorithms as early as possible, find an adequate algorithm as soon as these tests decided on which might be useful or not. There also take barriers into account that's come into play. So we make sure that we can transition to new algorithms as fast as possible if it becomes necessary.

With that, thank you for your attention. And as I mentioned, the paper will be published next week. Way more information is in the paper. With that, maybe we have time for questions.

RUSS MUNDY: Thanks a lot, Moritz. Yes. In fact, we do have about three minutes for questions. There is one in the Q&A module. Are you where you can see the Q&A module? I don't know exactly.

MORITZ MÜLLER: Yes. I think from Matthijs I see a question. Should I read that aloud?

RUSS MUNDY: Yes. If you would, please.

MORITZ MÜLLER: Okay. Matthijs says, "Moritz mentioned that it took four years after the standard was published before zone started to use ECDSA algorithm. This specific period during algorithm rollovers was still tricky. Not many implementation support automated algorithms. Now that software has improved on the subjects, do you expect that the transition period will be shorter or do you expect that other barriers exist that will prevent operators from moving to new algorithms?"

Yeah, I think this is definitely the case. I think algorithm rollovers were still very, very tricky back in the days. This improved software that can automate algorithm rollovers to some extent can help a lot. We've seen in the past I think that also this also is not perfect. But I think it can address one of the barriers of transitioning to new algorithms. Other barriers like lack of support at registrars and registries, it's still something that we have to address.

RUSS MUNDY: There's one more question, I believe. So let's go ahead and do one more. We certainly have time for polls. Go ahead, Moritz.

MORITZ MÜLLER: Yeah. Okay. "Are there any registries you've come across that are already experimenting with post quantum algorithms for signing their zones?" That's a good question. I am not aware of that. We, coincidentally, have a paper that will hopefully be published also this month— NCCR if you're interested—where we look into the different attributes of post-quantum crypto algorithms that are currently still [inaudible] this and see if we can fit these algorithms into DNSSEC. This is the only research I'm aware of right now at the moment. I'm not aware of other registries experimenting. We're actually signing their zones.

RUSS MUNDY: I think Viktor Dukhovni just made a comment in the Question pod about .br just rolled over 300,000 domains from algorithm 5 to 13.

Thank you very much. And we do have a couple more questions popping up. So if you would be so kind to answer them in the question pod, that would be wonderful. Let's try to make good use of our technology here. We will go on to our next presentation, which is going to be done by Suzanne Woolf and it was prepared jointly by her and Joe Abley. So, Suzanne, over to you.

SUZANNE WOOLF: Thank you very much, Russ. Kathy or Kimberly, can I have a sound check? Can you see me? Can you hear me?

KATHY SCHNITT: Hi, Suzanne. We can see you and hear you.

SUZANNE WOOLF: Great. Thanks. I am Suzanne Woolf. I work for PIR, the registry for .org and I'll be talking today about what we wanted to do about DNSSEC maintenance in .org this year, and what we actually have done. First, to acknowledge, Joe Abley, he and I have been trading off different versions of this plan and this talk for most of the year. Also the Ops team at PIR and the DNS team from our registry services provider, Afilias. Next slide, please.

Just to start with a quick history. It's worth noting the .org was signed in 2009 and the first signed gTLD, one of the earliest TLDs signed and a signed zone before the Root was. And the signing parameters chosen then timeouts, key sizes, algorithms were carefully analyzed and worked without a problem for those 11 years. But part of the effective operational deployment of any technology is maintenance. Every once in a while, you want to go back and review and maybe update what you're doing.

We decided early in 2020 that it was more than time to review our DNSSEC deployment in .org and update if that seemed what it was. Largely but not entirely prompted by the increasing velocity of deprecation of SHA-1 in various applications, we needed to move on. But we wanted to review and update the whole thing. Next slide, please.

So what was the situation we found ourselves in? There was a large DNSKEY RRSet associated with .org. This had been noted by our technology community, various conferences, not just Jeff, but we needed to take a look at a smaller key set .Org is signed with algorithm 7 SHA-1 and there's a long list of reasons and documentation that was more than time to revisit. And we had signed originally with NSEC3 but the reasons for that seemed less important. Opt-out, it was making an aggressive negative caching difficult. In addition, NSEC3, we had noted complicated provisioning since the zone size depends on DNSSEC uptake in children and NSEC was going to be more controllable. Next, please.

So what are we going to do about these things? We're going to identify incomplete KSK rolls, if any, and make sure that were completed. Review the pre-publication parameters for unused keys. Start lab testing different signer parameters to find out what else we could improve on. Changing algorithms either 8 or 13. It will be critical to go to 13. That will help with the DNSKEY response size. Let's do that. We're willing to take a big step and make sure we've done lab testing and find the performance implications of 7 versus 8 versus 13.

Org is signed using NSEC3. Okay. NSEC is operationally less complicated, we're fairly concerned. We're fairly convinced that the reasons for that are less salient now. However, with 10 million delegations, most of which are insecure, adding NSEC and RRSIG to each one means something like 20 million additional resource records. So let's start lab testing to find the performance implications of

signing the all those NSECs. Start reviewing the edge capacity forecasts for memory. Next, please.

A key feature of our initial approach was outreach and community engagement. Around PIR, we like to remind each other that part of our mission is to meet exemplary registry. And for us, that includes sharing our experience openly with other technologists where possible. This lets us learn from other people. It lets our experience be a resource for others. So we identified particular technical communities that we wanted to make sure we talked to early in the process. We want to make sure resolver operators are aware of our plans. Let's review the relative differences in the validator population when it comes to 8 versus 13. We should do a bunch of lab testing.

We thought there might be research opportunities in people being able to observe the change we were making. Org might have a more widespread base of dependent validators in the ccTLDs that have rolled to 13. Perhaps there are interesting differences we didn't know. We wanted to find out. We wanted to engage researchers in taking a look at that. We don't know for sure, but we think that possibly there hasn't been a production roll to TLD roll from NSEC3 to NSEC. Again, not clear what the implications of that are for research, but we wanted to make sure that people had a chance to study a production change of this kind.

So we started talking with the folks at DNS-OARC about our plans. Keith and Matt offered to host the mailing list for outreach. We started talking about how we might contribute funds to help with data

collection if researchers suggested they were interested in data. Next, please.

So in early 2020, we had it all figured. We announced the DNSSEC refresh in the .org zone. We're gathering perspectives. We had a lively discussion at an actual microphone in a room full of people. We started the conversations with researchers and TLD operators and resolver operators to talk about these questions we were posing, and then of course everything stopped. Next, please.

We discovered several issues, so obviously we had to reconsider our plans. We discovered several issues and exactly one of them was purely technical. It was substantial but purely technical. The thing was everything else changed, too. The purely technical issue was a significant performance impact of algorithm 3 on existing signers. The signing platform and use for .org has not yet gotten to optimize support for ECDSA. The new signing platform under development for other TLDs would very likely not have this problem still, but still is under development.

But there were also all those other issues. No travel. Setting up a lab with new hardware is suddenly much harder. Crossing borders to increase edge capacity, memory footprints, etc., suddenly seems difficult. Changes to key management, well, there's the problem of handling credentials and sometimes people need to be in the same room, at least as a backup plan, and you can't count on that. The research angle suddenly became more challenging. Universities all over the planet start closing down. We all have vivid memories of this

time. Campuses close, research plans disrupted. Everybody's challenged.

But also everybody suddenly depends on the DNS even more than they used to because everybody's depending on the Internet more than they used to, more than they expected, more than they wanted. This would be a particularly terrible time for anything to go wrong. A large TLD is critical, critical infrastructure, and part of maintenance is making sure you're doing it but also part of maintenance is doing it as responsibly as you can, as carefully. It's an area where conservatism is very, very wise. And what conservatism meant suddenly got a lot more constrained. Next, please.

We did have to think, though, for a while before we fully realized that we were dealing with a longer term situation than perhaps seemed initially obvious. Next, please.

So somewhere around March 50th we started thinking about what could we do within the new constraints. So we can review relevant parameters in the existing signers like key pre-publication, signature lifetimes, TTLs, ZSK rollovers. We can do some testing on the performance implications of a roll to algorithm 8. More incremental step than we'd wanted, but it gets us away from SHA-1. We can test the robustness of algorithm rollover and the current signer. We could run even public testing. We can do initial changes and test those out in some smaller TLDs. We would take full precautions with any TLD, no matter how small. But the impact of a problem in a smaller TLD is easier to mitigate and would affect fewer end-users. And we can do

some amount of the original plan for communications outreach coordination with researchers. So we proceeded on what we could do next.

So here we are, and suddenly it's March 235th. I counted. What did we end up actually doing? We did do a lot of outreach to various audiences. Joe and I have sort of been taking turns with the various groups and conferences and meetings that have continued online. We have gotten very familiar. We did spend a fair amount of time on prep work that we originally expect with our backend registry services provider. Roll from 7 to 8 was going to be reasonable, even with the lower risk tolerance of the new world. And again, it gets us away from SHA-1. Successful lab testing have a roll from 7 to 8 using the same signer platform showed no major concerns. And then doing a production roll from 7 to 8 for a different and smaller new gTLD also proceeded without any unforeseen challenges.

We published the plans that we had made, the detailed timelines and so on, and finalized details of the incremental steps, with dates, over the summer. What we ended up with was a less ambitious plan for a less forgiving time because now is not the time to mess around and now has continued. We're trying to regard it as a dress rehearsal for a future time when there's more room for bigger changes. Next, please.

So the schedule and the steps we ended up with, end of September, the new KSKs and ZSKs were added. The DNSKEY RRSet was signed by both algorithms. A couple weeks ago, the old algorithm 7 KSK record was removed from the RRSet. The DNSKEY RRSet no longer signed by

that key. Last week, the old algorithm 7 ZSK record was removed. The superfluous ZSK-based RRSIG on the DNSKEY RRSet has been removed.

Current state: per the diagram in RFC 6781, .org remains in the DNSKEY Removal step. What it says here is next week, but in fact I was corrected offline. It's tomorrow—fingers crossed—the old algorithm 7 based zone RRSIGs will be removed, which will complete the algorithm roll. So we've got this. No big global problems in the remainder of 2020, right? Fingers crossed. All told, this routine maintenance event has taken 11 years, or 8 months, or 5 weeks, depending on how you count. I think looking at all of it in one place, the main lesson for DNSSEC deployment is maintenance is important. It does need to continue. The main lesson here is: proceed cautiously but proceed. Because the new normal is not what anybody ordered, but the world is counting on us to keep the Internet going. We do need to do what we can, including responsibly maintaining the technology we already have under the conditions we're actually in.

So that was all we had. If there are questions, comments. Joe is also here so we can answer any questions people have.

RUSS MUNDY: Thank you very much, Suzanne. A very interesting analysis of the results of real-world implications and activities. Folks, please go ahead and use the Q&A pod. I think we have one hand up. I believe that is Viktor from the last session but I'm not certain. Can I get a little

help from the staff to tell me if this is a new hand or if this is a hand that's been up before?

KATHY SCHNITT: Viktor, you can talk now if you'd like. Just unmute your phone. Viktor, you need to just unmute your phone.

VIKTOR DUKHOVNI: Okay. Can you hear me now?

KATHY SCHNITT: You're a little faint.

VIKTOR DUKHOVNI: Okay. I'll do my best.

KATHY SCHNITT: That's better, Viktor. Thank you.

VIKTOR DUKHOVNI: Okay. I just wanted to mention that similar migrations have recently been talked about by AFNIC with their domain portfolio. They've rolled most of them to 13 now, but they're still holding back on .fr for reasons similar to what was mentioned here, in that their signing software has some sort of performance issues that they haven't yet been able to upgrade through. So it seems to be a somewhat common problem that existing large scale systems still have some older

software and some of the tools may not be sufficiently current to make a go.

On the other hand, some others like the .br, that I've mentioned earlier, have just rolled over 300,000 domains for .com, .br and others from 5 to 13, skipping 7 and 8. It took two weeks and they're done. So there's some good news, I think, for algorithm rollovers going forward. It's really starting to happen. Broader than what was mentioned in the earlier talk, the algorithm 7 numbers really are starting to drop noticeably and very recently over the last month or two. So I think this is the time to do it.

SUZANNE WOOLF: Yeah. It's just a matter of, as we said, just being super conservative about possible risks. It's not that they're not controllable, only that we just have to be even more careful than we would have been before. It's okay if it takes a while. We've started the process, we've laid the groundwork. Starting with something easier, a smaller step has allowed us to make sure the communications are in place, make sure the procedures are in place. It's okay if it takes a while, we'll get there.

RUSS MUNDY: Suzanne, did you see there is a question from Steve Crocker in the chat room? Why is zone walking no longer an issue?

JOE ABLEY: I can speak to that if you like?

SUZANNE WOOLF: Joe, if you would.

JOE ABLEY: There's a couple problems with NSEC3 and NSEC. So there's this sort of both sides of it. One side is when we sign with opt-out, we end up with a zone whose size in terms of distribution and the operational sort of complexities of just transferring it around the place to odd corners of the world scales with the amount of DNSSEC deployment. In other words, the more DNSSEC deployment we get, the more DNS records there are. The heart of the zone is to transport around the place. Now, we don't expect this to be a big problem, .org is not that big. However, it is something we haven't tested in production because the zone hasn't been that big.

So I think one of the core reasons to do this, in addition to the things that Suzanne has talked about with complexity of NSEC3, is that we really want our operational actual mechanics of shifting the zone around the planet every time there's an update every minute, to be reflective of the fact that everything could be signed. We don't want to have to sort of find out that when two or three big registrars start signing everything, that the zone inflates in size and we suddenly have an operational problem. NSEC gets around that because we have so many more NSECs and RRSIGs that the infrastructure already has to scale to be able to handle it.

So your actual question, Steve, why is zone walking no longer an issue? Because this is the other side. This was the original motivation to have NSEC3 in the first time to obscure the chain of owner names. We think that there's enough opportunities to get hold of the ORG zone right now, that people don't need to walk the zone. It's much simpler to sign up with a throwaway identity to seize ideas or to obtain passive DNS data or just to exchange a copy of the org zone from some other mechanism that came from one of those things. That if you are not interested in obeying the legal agreements that you sign up to, for example, CZDS, because you're a criminal and you have bad intent, then it's not difficult to get the zone anyway. So we don't think we're actually preventing people from accessing the contents of the ORG zone by using NSEC3. So what we're left with is NSEC3 basically only has negative connotations at that point. We're running out of benefits and it looks like all risk.

RUSS MUNDY: Okay. Thank you, Joe, and thank you, Suzanne, both of you for this very interesting presentation. If we have time at the end, we may do a few more questions, but it's pretty packed agenda here.

The next person on the schedule for giving a presentation is Wes Hardaker. Wes is with USC ISI and he's going to show us some information about DNSSEC and DANE. So Wes, over to you.

WES HARDAKER: Thanks very much. Kathy, am I able to share screen?

KATHY SCHNITT: Yes, you are. Yes. You can share.

WES HARDAKER: Now it says, “Host has disabled screen sharing.”

KATHY SCHNITT: You are a co-host. Give me just one second, let me check with tech.

WES HARDAKER: Somebody else did it so –

KATHY SCHNITT: Yes, you should have the right to share.

WES HARDAKER: Uh-oh. You may have had a technical glitch. Why don’t you share my slides then and I’ll walk you through it? I think that’s probably the only way forward easily.

KATHY SCHNITT: Just one second here, Wes.

WES HARDAKER: I can quit and restart but I think that’s probably not working.

KATHY SCHNITT: All right.

WES HARDAKER: Great. As a word of warning, we're going to go to a web browser in the middle of this so I apologize for that, too. But I can walk you through it.

I'm going to talk today about the DNSSEC DANE survey. I've talked about this a bunch in the past. I want you to go ahead and go on to the next slide.

This is joint work between Viktor Dukhovni who does all of the hard stuff, and then I just sort of present it both on the web and in presentations. We've talked about it in Puerto Rico and Barcelona and Panama and all those wonderful places that we've been in the past.

In the past, we've concentrated a lot on the data. We've shown pretty graphs and things like that. Today, we're actually going to be talking most about the presentation of it and updates that have happened since the previous times. Specifically, we've done a few things, we moved the scanning site, we've updated the website statistics in how they look, as well as there's a new data exploration site which we're going to demo today as well. Next slide.

Kathy, your screen just went blank. There we go.

First off, the scanning site has actually been moved. It was running previously out of Viktor's apartment in New York. I decided to sort of donate some hardware to the cause, and so now it's actually being run

out of ISI's network. Viktor still controls it, runs it all, but we're now running out of the university. That was probably has some benefits from actually being scanned out of university, people are probably a little bit more pleased about that. Although Viktor does a lot of the scanning work and, as you know, he's here today and can answer questions as well, there's tons of participants that have helped us, either from giving us data sources or we make use of a ton of upstream resolvers as well that Viktor carefully watches every day to load balance between a bunch of upstream resolvers in order to scan 10 million plus domains a day. Next.

On the infrastructure side of things, all of this is housed at stats.dnssec-tools.org. But basically, the way the operation runs is daily there's a list of all the signed zones that we know about that we've gathered either from our data sources or through some mechanism that ends up in our list. They all have to be registered on the Public Suffix List. One question that we occasionally get is, "Why isn't my site there?" And if your site is a subdomain of an existing site, anything under ISI, for example, isi.edu, it wouldn't count as a separate domain. We're only doing stuff with the Public Suffix List breakpoint. We collect all the DNS records for each of those zones, specifically, the DNS records that we actually want to care about measure because we can't do them all. But we look for DNS keys, we look for DNS records, we look for MX records, and then TLSA records for each of the MX records for a domain.

Then Viktor actually opens an SMTP connection to each mail host that is listed for a domain to test their TLS connection and their

capabilities as well as collect all the certificates. There's a lot of number crunching that goes on behind the scenes after the daily run is done. It takes often up to five or six hours in order to complete. Then the results are updated and displayed daily on our website. Next.

Recently the website has had a complete overhaul. We will demo it in a little bit. I finished it about nine hours ago. What could go wrong with a live demo and something that was just pushed nine hours ago? There's also a new data explorer website. This has actually been there for about a month, but probably most people haven't noticed it yet so this is sort of the official announcement for it. The goal of this new website is to allow easy access to the exploration results per zone so that you can see what data was actually collected for a zone. And more importantly, as Viktor and I were talking a couple of months ago, we realized that we could create an API that would actually allow you to look at the issues that were identified. So the end result is there's actually a huge list of issues which we'll see on the next slide. Wait one sec, though. It'll warn you about—we don't send notifications so you have to kind of go and look, generally, but it's an easy way to explore, how does my zone look today and what's the most recent scan you needed to find anything in particular with my zone. This complements many of the existing sites, dane.sys4.de and dnsviz.net or the very popular ones. We actually even provide links to those at the bottom of our exploration site per zone so that you can jump around between the various websites that help you diagnose and debug DNSSEC-related issues. Next.

So the new explorer page actually has a huge list of things that we look for. We look for errors associated with MX lookups, whether their address or looking at the MX record themselves, when they fail, you'll get a warning about that. When there are invalid entries for MX hosts, you shouldn't have an IP address as your MX name record. And unfortunately, some people actually do that. When there's failures in SMTP connections, either because bad certificates or just TCP is failing or whatever it might be, those are logged.

DNSKEY lookups sometimes fail as well for some zones. We actually warn you about deprecated algorithms and, as we look at the data, we'll note that a large number of zones are still using algorithm 5, which is RSA-SHA1. That really should be rolled out. As even a lot of people have discussed earlier today, that's beginning to roll out so newer algorithms are being selected. I've just done that myself for a lot of my own zones. That's the most common warning. It's actually a deprecated algorithm.

DANE TLSA records sometimes fail to validate the SMTP certificates. So when the DANE TLSA record does not match the SMTP certificate, you'll get a nice red dialog box. Then sometimes the TLSA records themselves fail to be looked up and then sometimes MX hosts actually don't have a TLSA record. That is actually true for a couple of my own zones because I don't control my secondary MX and it's harder to get a TLSA record working for them. Next.

So now we're going to go into a demo time. I apologize, Kathy, but this is going to be a little bit of typing for you, if you don't mind. Can you open a web browser?

KATHY SCHNITT: Sure. Okay.

WES HARDAKER: Okay, so you're going to go to stats.dnssec-tools.org. Dash tools, not dot tools.

KATHY SCHNITT: I'm sorry. Say that again.

WES HARDAKER: stats.dnssec-tools. You misspelled DNSSEC. There we go. Excellent.

This is the brand new, shiny, spiffy new version of our webpage. It's part of the DNSSEC tools project but it's sort of a side project of the DNSSEC tools. Lots of information about it. If you scroll down a little bit.

To the next section, you will see that there are summary statistics about how many zones that we've actually explored. Then there's an explorer dialog box on the right. Don't click on that yet, but we're going to do that in a minute. If we go down to DANE Trend Graphs, everybody remembers this webpage used to be super long. It was sort

of hard to see the information that you were particularly looking at. So now, everything's sort of housed into tabs.

This first one is the DNSSEC deployment growth and you can see that we're upwards of over 101,250,000 DS records that we're collecting, again, under Public Suffix List points. If you click on the second tab, the signed MX records, you'll see that this is the growth of the number of mail servers that are actually making use of DNSSEC and DANE. Again, continuing the growth, make a huge jump. Those huge jumps result from individual mail servers that are actually serving a whole ton numbers. The first big jump was actually from one.com signing, for example, all of the zones that they host.

If you go to the next tab. Then there's the actual number of zones that actually ramp upwards in terms of ... Actually not zones, mail servers that actually are deploying new TLSA records. So there's a good linear growth of mail servers individually that are slowly deploying DNSSEC and DANE, which is fantastic. It also shows the breadth of how many mail servers are actually supporting a huge number of other zones. You saw in the previous graph that there was a large volume of zones that are actually being served by a smaller number of mail servers. Scroll down further, Kathy.

Down further, we have the DNSSEC parameter frequency analysis graphs. There's a whole bunch of them where we actually—algorithm KSK—we graph independently the various algorithms that are in use. You can see 8 and 13 and 7 are still popular algorithms and that's slowly shifting. If you go to the third tab, RSA key, KSK sizes. I won't go

through all of these tabs today, but it gives you a note of what the average KSK key size is. 2,048 is the most common. One of the nice things about tabs is if you click on the next one, when we go to this zone signing key, you'll see that there's a sudden shift where it goes to 1,024. So you can quickly jump back and forth and compare what key sizes people are using. And of course, all the counts are right there as well. Go down to the next section, Kathy. Thank you.

So this is the graph—and Viktor and I were actually talking about this yesterday. Of all of the TLDs—scroll down just a little bit more so that we can get the words. They're kind of jumbled. We're actually sort of graphing the top 100 most successful TLDs in terms of DNSSEC deployment and getting all of their zones actually correct underneath. Okay. Scroll up just a little bit and we'll go to the second tab.

All right, so this is now the Details List which actually shows that realty is 99.99% working page .br. Br has to be given a lot of credit, because having that many working zones and having almost all of them working in 99.96 is truly a impressive feat. The smaller ones, of course, it's great that they have working too, but keeping track as the numbers grow, it gets harder and harder to keep track of making sure that all of your subdomains are actually working. So kudos to the .br. It's a rather large TLD.

Then finally, on the rightmost tab, I will be honest that TLD graphs needs the most work. This is going to roll out and be improved. Actually, this is what I was just working on last night. If you click on the Select button and then pick a random domain like bank, it would be

great. It'll actually show you the details per TLD. So it shows you the number of records for bank. There's a lot of TLDs so the Select button needs some work on making it usability. But if you start scrolling down, you'll see that we both have the signed subdomain count over time, as well as the percentage of working domains and how well things are working over time. You can get individual details, especially if you're a TLD operator, as many of you might be at ICANN, this is a great way to sort of explore how is my TLD working.

All right, so let's go all the way back to the top. We're going to dive a little bit down a little bit more. Hit that Explore button. This is the website that allows us to explore and see issues with zones and how they might be working. I will get a couple of quick demonstrations. Note that ietf.org is sort of the default. It shows us that the issues related to ietf.org, and these are all basically deprecated algorithms or a little bit old. As I said before, this is sort of the most common. If you scroll down, it allows us to see all of the data records that have been gathered. So the MX records, you can see that ietf.org has one MX record and it's for mail.ietf.org. If you click on the TLSA records tab, the second one, it'll show you all of the TLSA records.

If you click on the next tab, it will show you all the certificates that have been gathered. This actually gets kind of long. This is another place where the UI will improve over time. It shows you each address and all of the certificate records that were collected for what it's valid for. It even shows you all of your parent certificates. So if you have certificate tree, which has four or five parents long, you'll get all of the results from that.

Under DS records, you can see that we have the DS records that are used by ietf.org and there's both the SHA-1 and SHA256 under DNS key records. We will see that these are the actual keys. You can copy and paste them. They're really meant for human display, more than anything else, so we show all the details as well as how old they are. The 3 years and 22 hours in this case is actually I think related to how long Viktor's been running the collection mechanism. So the key in some cases is as old as the steps that we started collecting. But if you roll keys on a regular basis, you'll see a smaller age for that.

All right, if you scroll back to the top, Kathy. Instead of ietf.org, let's put in icann.org. Click Submit and it updates the page. You'll see that we have weak algorithms and now we actually see that the MX hosts have no TLSA records. And it says the e-mail to this domain is not DANE-protected and that's because ICANN hasn't actually rolled out TLSA records to protect incoming mail at this point yet. So that's the other type of warning you'll see. Go up again.

Let's see one more example. Let's go to otr.ie. So when DNSKEY lookups are failing, you'll see that we'll have far less information and will actually show when the last time we successfully queried those records as well, which is kind of useful.

And let's do one more, which is one.com. Again, I have to give kudos for one.com because they have been one of the largest jumps in providing SMTP support, and it's actually one of the few things with no issues found. They're using recent algorithms. They have no issues with any of the records that we're collecting. So you do get a nice

green check box when you've gone through all of our hoops. All right, let's go back to the slides. Kathy.

So do feel free to go around and play with it. It's statistics.dnssec-tools.org. If you go to the next page, one final sort of word of warning is that Let's Encrypt is about to roll their Certificate Authority certificates in September of next year. So a lot of people right now only have I think that first TLSA record as a DANE TLSA record for their zone. They should really have two because they have a backup CA, so you really want to support two. But more importantly, right now you really want all six because they're adding four more CAs that they will start using in September, and if you haven't updated your DANE TLSA records, if you're using type 211, which is saying, "I'm going to use my parents CA as a fingerprint," you have to start using all four—all six, really—until through September of next year, and then you can remove the first two. So word of warning for those of you that are using Let's Encrypt and using not a 311 TLSA record, which points to your own certificate, but rather a 211, which points to the Let's Encrypt CA or really type 2, make sure that you point to their newest certificates as well.

There's a link there that Viktor wrote up a post for all of the sites that are sort of going to have this issue. You can go look at it and there's instructions on what you must do in order to fix this problem. Go ahead and go on to the last slide.

So come out and play. Here's the links again. They're fun sites to just kind of browse around and see how things are going. They're updated

daily, I should say, the data is updated daily. Of course, you should sign your zone. I think I preached about that enough, and you should secure your e-mail as well. The growth of that is going but there's of course more to do, including icann.org, for example.

Then there's an e-mail address for anybody that wants to contact us. It'll get to both of us, regardless of whether you have website issues or scanning issues or you want to even opt out of scanning and things like that, we support that as well. Go ahead and reach out to us. Is there any questions?

RUSS MUNDY: Well, Wes, I'd love to be able to take questions verbally, but we have reached the end of our time. So if we could, there are questions in the Q&A pod, so if you could look at that and respond to those there, that would be just great.

WES HARDAKER: I will do that.

RUSS MUNDY: Thank you very, very much. And as usual, excellent timing. We're now on to our last presenter for this session and that's Pablo Rodriguez and he's going to give us some output of perceptions of DNSSEC by folks that are making decisions about whether or not to make use of DNSSEC. So, Pablo, if we could go over to you.

PABLO RODRIGUEZ: Thank you very much, Russ. Good time of day to all of you. Thank you for this opportunity. I would like to share with you the perceptions of those IT decisionmakers or whom we perceive that are IT decision makers on the use of DNSSEC in the Latin America and Caribbean region. Next slide, please.

The purpose of this is to understand what are they thinking about, what are the factors that may promote or impede the adoption of DNSSEC, and based on what we learned from this study, we want to develop a set of recommendations that can help us increase implementation of DNSSEC among the ccTLDs operators. Next slide, please.

The study involved interviews of about 24 operators in the lac region. We know there are around 47 ccTLD operators in Latin America, of which 26 of them have not implemented DNSSEC.

I was able to involve 24 to participate in my study, of which 12 of each category, implementors and non-implementors were interviewed. Next slide, please.

So this is not the entirety of all the findings, but these are very interesting ones. So one of the first things that I wanted to know was, do you believe that DNSSEC does what it's supposed to do? There is no question that every one of the participants do believe that DNSSEC performs as it's supposed to. However, the majority of those implementers of DNSSEC, it is their experience that it has not increased domain registrations. So that was an interesting finding. So if it's not increasing domain registrations, why else in addition of

security would you adopt DNSSEC? You'd think that because it could increase domain registrations, you would want to implement that, it would be a motivator. But it doesn't seem to be the case.

Another finding is that misconfigurations of DNSSEC are perceived as a risk because it is not a forgiving protocol. So if you make a mistake, you're out of the picture very quickly and these participants fear that very much so.

In addition to that, we also found that the majority of these participants believe that it does improve the cybersecurity. However, we come back to the same thing that has been mentioned in some of your presentations, complexity and difficulties, disadvantage. And thus prevents people, impedes some of these operators to adopt DNSSEC. It does. Many of those who have not implemented DNSSEC feel that it does provide a competitive advantage, and the cost of implementing is a disadvantage which is that that I was thinking that when participants talk about cost, you would think about hardware infrastructure ,but in reality, it has more to do with their concerns about training personnel, hiring additional personnel, sending them out of their country for training, per diem, travel, and increasing their payrolls in order to keep and retain these participants. It is something that although I will not go further here, we can discuss it online. Next slide, please.

This particular question had to do with the perception of the type of personnel that they need. Most of them agreed, especially the implementers believe that, implementers and non-implementers, that

highly trained personnel is needed to manage and maintain DNSSEC. However, as you can see in the area in bullet C, there is a scarcity of personnel, so we need to develop ways in which we can train more people on, again, lack of infrastructure, both technical and organizational, meaning the hardware as well as the personnel, and lack of budget for hiring, training and personnel retention are challenges that they continue to find.

Training and key signing ceremonies are challenges [inaudible] due to the coordination that is required in order to do this. And to reduce the workload that is required to adopt DNSSEC both from the operator as well as their corporate clients seems to be an impeding factor. Next slide, please.

So when I was looking at what are the influencers, who are those indivudals that you perceive that want you to use this protocol, we found several things. One of the questions had to do with who do you think should use DNSSEC, and it is an overwhelming response from both implementers and non-implementers at government, banking institutions and transactional websites should be using DNSSEC. Again, there is resounding support for the use of DNSSEC. No one questions that DNSSEC is effective. However, I found this very interesting, it seems that some participants on both implementers and non-implementers have found that some either superiors and/or stakeholders do not support this because they feel that perhaps it requires too much money of their budget, which they already mentioned they don't have it, or it may cause difficulties that they may not be trained for to handle if they were to occur.

On the implementer side, as we expected, they all believe that malicious actors are the ones that do not want them to have DNSSEC. Most of both implementers and non-implementers believe that ccTLDs will implement DNSSEC in the near future. And many of them—or at least those that made exclusive expressions about it—believe that either perceive that IETF, LACTLD, LACNIC, and/or ICANN wants them to use DNSSEC, which leads to the fact that you are influencers that have the ear of the ccTLD operators but there are other factors that are equally important and that need to be handled in order to increase this adoption. For example, the perception that registrars want them to use DNSSEC, but how can we get these registrars to adopt this implementation? Next slide, please.

So once again, we begin to see that lack of technical infrastructure and/or trained personnel are challenges that are impeding DNSSEC implementation in ccTLDs. And look at that bullet D, lack of institutional support. So we need to start working on workshops in which we can get these IT decision makers within each one of the ccTLDs to teach them and explain to them why is it important that they adopt DNSSEC. And we need to identify who are these IT decision makers? Are those the ones that come to ICANN, or are there other IT decision makers that are above those that are represented in ICANN?

In bullet E, we can find again infrastructure, hiring of additional personnel, training, and legal services. And when I talk about legal services, this has to do with the DNSSEC statement of practice. Many of them expressed that it was very difficult for them to develop this

type of documentation and they need help, and most of the time, they would need legal help in order to put this together.

So this is an opportunity for us in which we can help them out by developing some of this documentation. And again, institutional support seems to be a problem that needs to be overcome in order to increase these numbers, at least with the people that participated in this study. Next slide, please.

So again, we can see here that most of the participants in the study do not perceive that DNSSEC does not pose a risk. However, they have found that many of those who have implemented DNSSEC have set it up in such a way that they don't need to celebrate the key signing ceremony, and consequently, they do not have intentions to celebrate one anytime soon.

We can see, again, bullets N and O that we need to work to reduce the amount of work and effort that is required from corporate clients, and also from ccTLD operators. We need to increase ways in which we can facilitate for people for people to be able to sign their zones. And at the same time, we need to increase communication and education programs to teach how we can preserve the DNSSEC chain of trust. Next slide, please.

This is something that I found very interesting. The majority of the implementers of DNSSEC and non-implementers of DNSSEC perceive that implementing DNSSEC provides them with a reputational advantage. They are perceived as competent, trustworthy for implementing DNSSEC, trustworthy from the key signing ceremony.

So this is a very strong driver, and this is something that we should be able to use in order to get people to buy into the implementation of DNSSEC, because many of them feel, as I already mentioned, that it will provide them with a reputational advantage. Next slide, please.

So these are the perceptions of those implementers of DNSSEC. We are not seeing here the perceptions of those that have not implemented. And in their experience ,what they're telling me is that what's holding back their corporate clients from adopting DNSSEC is that they lack awareness, that there are technical challenges, the high cost, and again, as a corporate client, do I have the personnel and the infrastructure to implement DNSSEC? That's what those high costs refer to.

Enforcement. And we saw a little bit of that when Wes was talking about .br and how .br has achieved these great numbers. So, can we develop ways in which we can facilitate our registrants and our corporate clients to adopt DNSSEC? And that's something that we should continue to explore, because it seems to be working extremely well.

Some of these, more than half of the participants in the implementer side believe there is a tremendous lack of interest, and I find it very interesting, and this also confirms some of the findings that Moritz was mentioning, which was that promotional, financial incentives and education, and the reduction of effort to implement DNSSEC, will improve the adoption of DNSSEC. Next slide, please.

So these are some of the findings. Lack of budget to support both the organizational and technical part of the company and the concern of misconfigurations impede implementation of DNSSEC. Workshops are needed to provide didactive material such that it can have those at the decision, at the helm of these ccTLD operators to understand why this is important. There is a tremendous lack of knowledge among IT decision makers. Necessarily not those that are in front of the operation of the ccTLD but those who manage the budget.

And reputation is a major driver of technology adoption and we should take adoption of that. So, what are the recommendations? Next slide, please. We should develop workshops to increase institutional support and reduce DNSSEC's implementation difficulty. Develop workshops to explain to ccTLD operators the cost, minimum number of personnel needed, training and infrastructure. Let's try to find numbers that can help us identify how much it costs to do this, involving implementation and maintenance of DNSSEC. Develop interfaces to reduce the workload of corporate clients zone signing with the ccTLD.

Finally, integrate a warning system. I found this very interesting. Several participants made references to how SSL achieved great adoption numbers because people are aware whether a website has an SSL active or not. Can we have a warning system in browsers that can tell us whether DNSSEC is present or not? This is an interesting recommendation that should be explored. Next slide, please.

Finally, I want to thank you all for the opportunity. I am available at both—you can find the entire study at the link, and you can also visit rodriguez.pr or write to me at pablo@rodriguez.br. and I would be more than happy to share further thoughts. Thank you very much.

RUSS MUNDY: Thank you, Pablo. Very interesting presentation. One of the things, especially since we get an archive of the chat room, perhaps you can also put the URL from your slide into the chat room. it might be a little easier for people to find. That would be really helpful.

And I think we're a little bit into our mandated break time here, so I think we get to use the same Zoom room throughout the workshop, and I'll ask Kathy or Kim if she has any specific guidance for us. We will resume half past the hour, I think. Kathy, over to you.

KATHY SCHNITT: Thank you, Russ, and thank you to our panelists. Yes, that's correct, we're going to be in the same Zoom room for our next two sessions. You can disconnect or remain online, it's up to you. We're going to stop the recording. You may hear some chitchat on the panelist side. Of course, that's just us testing for part two. So we'll see you back at half past. Thank you. Please stop the recording.

[END OF TRANSCRIPTION]