MARRAKECH – DNSsec Workshop
Wednesday, March 09, 2016 – 09:00 to 15:15 WET
ICANN55 | Marrakech, Morocco

UNIDENTIFIED FEMALE: .ca, Canada.

UNIDENTIFIED MALE: Thank you. [inaudible] I come from, live in the U.S., done DNSsec since last millennium.

UNIDENTIFIED FEMALE: [inaudible], U.S.

UNIDENTIFIED MALE: Hi, [inaudible] from .tr ccTLD.

VICKY RISK: Vicky Risk from ISC and we've been doing DNSsec since 2006, and I don't believe you were doing it in the last millennium.

RAO NAVEED BIN RAIS: Naveed Bin Rais, Pakistan Capital University.

NEIL: [Neil Gins] from [inaudible] UAE and we've been protecting keys since 1960s.

JOHN CHAND: John Chand from Fiji. ICANN Fellow.

WILLIAM STUCKE: William Stucke, South Africa. ICANN at DNS Africa Study.

UNIDENTIFIED MALE: Okay, good. We've got some more folks over here.

[BEN]: Ben [inaudible] Labs.

UNIDENTIFIED MALE: [inaudible], Labs. DNSsec before it got standardized.

UNIDENTIFIED MALE: [inaudible] from [inaudible] Zambia.

SIMON BALTHAZAR: Simon Balthazar, .tz, Tanzania.

SONAM KEBA: Hello, everyone. I am Sonam from Bhutan, and I came here to from my DNSsec because we have never implemented DNSsec in my country, so I'd like to come to learn something. Thank you.

RAJEEWA ABEYGUNARATHNA: I'm Rajeewa from Sri Lanka. ICANN Fellow. Yeah.

UNIDENTIFIED MALE: [inaudible] [Zechariah] from Morocco.

UNIDENTIFIED MALE: [inaudible] [Muhammad] from Morocco.

UNIDENTIFIED MALE: Excellent. Anybody else? Do you want to just yell your name? Here.

UNIDENTIFIED MALE: I didn't run this morning.

UNIDENTIFIED MALE: [inaudible] .ru.

UNIDENTIFIED MALE: Okay. Anybody else?

UNIDENTIFIED MALE: Oh, here we go.

JOSE URZUA: Jose Urzua from .cl.

UNIDENTIFIED MALE: .cz? C, okay. What?

UNIDENTIFIED MALE: [inaudible] from .in registry [inaudible] India.

UNIDENTIFIED MALE: Oh, great. Anybody else we missed. Oh, Dani.

DANI GRANT: What is the prompt?

UNIDENTIFIED MALE: Who are you and where do you come from?

DANI GRANT: Who am I? I'm Dani. I come from CloudFlare.

UNIDENTIFIED MALE: Anyone else? Oh, hey. Say hello and where are you from.

SARA MONTEIRO: I'm Sara. I'm from .pt, Portugal.

UNIDENTIFIED MALE: Excellent. Anybody else we missed?

BRAM FUDZULANI: I'm Bram Fudzulani from Malawi.

UNIDENTIFIED MALE: Great. We should do that more often. That was kind of good. We should do that. Oh, and Robert's here. Oh, hey, Robert.

ROBERT MARTIN-LEGENE: Present myself. I'm Robert Martin-Legene from Packet Clearing House.

UNIDENTIFIED MALE: Okay, let's go. Would like you to say hello? Introduce yourself? No. Okay.

UNIDENTIFIED MALE: All right. Well welcome, everyone, to the DNSsec workshop. That was actually good timing that we were needing to do that. That was actually good. Julie, we should build in some time for that next time, too. So if I can borrow this from Kathy, I was about to write something useful.

You should see one of these Andrew's bringing around. For those who are new to the DNSsec Workshop, you have now committed to stay in this hot room until 2:15 this afternoon. Six-plus hours of really – no. Actually, you're not. You can get up and leave. This shows the order of when we're going to have our presentations and what we're doing. You're welcome to stay for as much or as little of the event as you're interested in. And Julie wants to say something.

JULIE HEDLUND: I'll just let you know for lunch, you should have received a luncheon ticket that has a map on the back. Lunch is not going to be in here, which you'll be glad to know. It will be outside and it will be in a nice place, but it's not real nearby. So we're giving you about 10 minutes or so to get to lunch, the map will show you how to do that. There will be friendly, helpful ushers and signs along the way. But you must have your ticket. So keep that ticket even if you decide to go someplace else this morning. If you want lunch, keep your ticket. Thank you.

DAN YORK: So I will also just point out for speakers, Russ Mundy is playing our hook over here. He's got his little iPad with a timing clock on it. So we are trying to keep us on time as we go through this with the caveat that, of course, we've already started 15 minutes late. But we'll just ask people to speak quicker or something.

So I'm just going to run through a couple quick slides here. My name, again, is Dan York. I am part of the Program Committee that is – the slides are not working so. Well it's not – here. Why don't we just push buttons or something. Is this thing on? Oh, hey, look. Power button. Woohoo. Let's try this again.

Okay. How do you translate woohoo? No, he's shaking his head. Okay. Here, put it in mode, in – oh, yeah, here. Yeah. We'll just go up to the view menu [inaudible]. I'll just go. Okay. So let's see if this works. Here we go. No. All right. So let's just use the slides. Let's just go ahead. Next slide.

So in theory, the slides and audio streams are at that link. In theory, we're supposed to have these live video streams on YouTube. We're still confirming whether they are actually up there. But are they? It's streaming on Adobe Connect, so the YouTube streams are not there. Okay. Gentleman says it's streaming on Adobe. It's not on. Yes, but do we have these two YouTube links? Oh, no. Okay. We don't have the YouTube links.

Never mind. They must have been left over from – oh, okay. All right. We've had a disconnect. That was from 54 in Dublin where we threw those up quickly. So you can get this through the Adobe Connect room, ignore those YouTube links. Let's go on.

There is a Program Committee that is part of this. How many members of the Program Committee are here? Just raise your hand or something. Okay. A number of the folks who are part of this have been involved with what's going on.

So we're the ones who put this together, the program is here, we will also, shortly after this, be looking for presentations for next time in whichever the location is formally announced. So for ICANN 56. Yeah, the location formally known as Panama. So next slide.

We are very grateful to our sponsors that have brought this together. I think Afilias, do we have anyone from Afilias in the room? No. Jim will be here, maybe he'll be here at some point. Sara, we've got Jacques and what? Amanda, yes, who is here. Dyn isn't, I don't think anybody from here is from Dyn but an SIDN, I know Christian was around. Yeah, there he is, right there.

So if you get a chance, say, "Thank you," to these people because they are the people who helped provide us with lunch. Okay. So, and if you'll [inaudible].

UNIDENTIFIED MALE: [inaudible] wait until after the lunch [inaudible].

DAN YORK: Well I'm going to thank them right now, so. Okay, next. We also want to thank Afilias for coming through and helping with the DNSsec implementers gathering. A number of people were here. Who was there. A number of people who are here. Okay. For future knowledge, as well, the Monday night of every ICANN meeting we have a gathering. Next slide, please.

Here is a nice little picture. Oh, this isn't the set of slides. Uh oh. Yeah. Okay. Okay.

UNIDENTIFIED MALE: Yes. Next time, I think on the B meeting, tech day and DNSsec will work closer together, so we'll see whether we can pull out some of the per diems that put that into the [inaudible].

DAN YORK: Sounds good. And also, I would like to just say, too, by the way, Dr. Eberhard Lisse is here, who organizes the tech day. I'd encourage you to go back and look at the archives for it, if you can, because the gentleman over here from dot TR, Attila, gave an excellent presentation about the DDoS attack that happened

in Turkey. It's not directly DNSsec related but it was an excellent presentation. So go ahead.

UNIDENTIFIED MALE: It was my boss. I am not the one making the presentation.

DAN YORK: Oh, I'm sorry. I'm confusing you.

UNIDENTIFIED MALE: He's very [inaudible] than me.

DAN YORK: Okay, I'm sorry. Okay. Anyway. It was a great presentation from dot TR. Go look it up. It was good. Also, the gentleman back here from Tanzania gave a good – He's like, "What?" At the Africa DNS Forum, gave a great talk about what he's doing to implement DNSsec and other technologies in where he is, so that's a good one, too. We should get those links. Okay. Let's go on to the next picture.

This workshop is brought to us by the ICANN SSAC with the additional assistance from the Internet Society Deploy 360 program, which is how I wind up being involved with some of this. So it's good things to have. Let's go on.

This is our agenda, and you should have one printed right in front of you, which will give you a bit better to, perhaps, read with that. The essence of it is that we've got Vicky coming up first to give us an update about the DLV, we've also got then a great panel I'm looking forward to, and many of the people already here talking about DNSsec in Africa.

Then we will have a presentation from Alain about the DNSsec switchover or sign or switchover. We've got Dani here to talk about CloudFlare's efforts to do DNSsec at scale. And then for those who have not participated, we do have the great DNSsec quiz, and it will challenge you this time. Roy Arends has done it and you will get the ever-dying fame, right? Because who won it at 54? Do we remember? I don't remember. Who won it? I don't know. [inaudible] you'll get fame in some world.

After lunch, we will have a panel of folks who are going to be talking about how do we upgrade the cryptography in DNSsec, and we've got some great presentations there talking about that. And we're going to round out the day with a discussion around the KSK rollover and what needs to happen there.

So next slide, please. And next slide. Oh, Julie is saying something. Oh, no. Okay. Okay. So we'll standby for a moment while we get the correct pictures, because we're not going to

show you the right things on the screen, and so that will be bad. You don't want to do that. So tap dancer team.

Okay. So anybody want to talk about anything else? Robert, what's great going on in – no. Yeah, yeah, I know. I guess we're in Africa so our room needs to be hot. Usually, we're cold in here, right? Okay. I apologize for those YouTube links, Julie. I know where those came from. That was me last time in Dublin because we had no camera, so I threw up a quick camera. And then you were so efficient.

Julie is amazingly efficient with all this, and so she updated it with the links to this thing, but I didn't realize that that was links that were me, that that wasn't really me. So I've been advertising the wrong links. Sorry about that, for anybody listening remotely. Okay.

It does, yeah. What happened last time was we wound up in a whacky room on the fourth floor of the Dublin Convention Center that was wide open, and there were no cameras. And so we wound up, we had no way to show video. And so what we did was I threw up a camera really quickly and threw it on to the Internet Society's YouTube account, and we were streaming out with that.

Today, we actually do have a camera, although it's a laptop there streaming out the video, so they can actually see us this

time. Okay. Here we go. Oh, well then let's show the picture. We should show the picture. So let's go through here. Here we go.

Oh, and wait, back up one slide. I knew this was. There we go. So we are, and because Christian's got his new logo in here, all right? And this is an important thing. All right? SIDN is a new logo, all right? So we do also, we are looking for a fifth sponsor, a company that would be willing to help fund these events as we go through here. You get the opportunity to be listed on here and on the lunch tickets and other pieces. You also help, you get the undying gratitude of this community for helping fund lunch.

It'll be $2,000 for the rest of this year and U.S. dollars. I'd love to talk to anybody who'd be interested in doing it. We greatly appreciate the sponsors, but we'd like to have a fifth one because sometimes when you go to places, it costs a good chunk of money to be able to get the room and the lunches and everything else that we want to do.

So let's go on to the next one and the next one where we have our picture. There were some of the people. All right. And we had a great conversation, a great time to talk about people. Projects have been developed out of these gatherings. We've also just had a lot of fun talking to each other. So let's go on. Next one.

Okay, next. Next. And here we go. Next one. So we want to talk about statistics about DNSsec and maps and some of the pieces

that are here about this. We're going to remind people that when we talk about this, there's two sides to DNSsec, right? There's the signing side and there's the validation side. And one of those is creating the signatures, one is checking them. So let's look through these.

And so let's look at this and we've got, first up, from Geoff Huston, who's sitting in corner there. We've got his great maps, and these slides are available up on the ICANN site, and so you can see them and you can also look at the URLs I provided for where they are. But Geoff's map is showing the continued growth in DNSsec validation globally. So we're seeing an increased rise in the amount of validation happening.

That big drop in the middle there in September, so was when Google redid the way that they do ads and stuff, which is what Geoff using for counting this. And so there was a drop in that, which, but it's all good. We're back on the trend. Okay? Next slide, please.

Here was a list, which it's really hard to read from this view where I'm at. I guess I need a new eye prescription. But one of the things that's interesting is this is the overall view of the world of where validation is happening. And what's interesting is if you look up at the top of that, the regions of some of the regions of the world that have the highest level of DNSsec

validation are actually in Africa, for reasons we'll dive into in another moment.

But you could see the kind of areas of where we're seeing a higher level, about 30, what's that? 34% on the top of that. Okay. Let's go on to the next slide. Here was the overall world perspective on DNSsec validation, and notice that Africa is slightly higher.

Now if you start to get into it a little bit, you could see that it's also a higher usage of Google's public DNS server, the 8.8.8 and associated with IPv4 and IPv6, and that's a bit of what goes on. If we look at the next picture, oh, that's unreadable from here. Okay. So never mind that.

But if you go to that URL and look at Geoff's slides, or Geoff's stats, you'll see that what's happening is some of the countries that are in there, they have a high percentage of validation, but part of that is because they have a high use of Google public DNS.

The fourth one down there, though, Madagascar, notice it only has about 8% use of public DNS, of Google's DNS, which means the other 92% is DNSsec validation happening within the local ISPs there in Madagascar, so that's huge, that's a great thing to see. We love seeing that kind of stuff happening.

So good news is that's going on. Let's talk at the signing side. Here's Rick Lamb's deployment report showing the percentage of overall TLDs that are signed. We're now way up over 80%. Of course, most of that is the New gTLDs that are coming in, sign by default, but still good to see. Let's go on. Next one.

Okay. I can't read that from here, so note to myself for next time, I'll make it a little bit bigger for me to read from 50 feet away. I could get closer. I have a mic in my hand, Robert's telling me. So yes, we can read this, thank you, Robert, for pointing out the obvious. The heat's getting to me, perhaps.

So you could see up here on top, .NL is coming in at the top here with about 44% of their domain signed, over 2 million, so kudos to the .NL folks. Are they in here? Yeah. They should be here. You guys are here. Good job. All right?

Brazil is also in here with a large number. What I've done here on Rick's side is if you click on the, it's not intuitive. Rick will tell you he's not a user experience designer, but if you click on the signed total, if you click on that twice, you'll get it sorted that way and you can see what's in there.

And it's also in here we see se.com has a large number, although the percentage is tiny. So we're starting to see some good pickup and we're starting to see some metrics around the percentage of sites that are there. Next slide, please.

Want to get into our maps and for those who are not aware, we rate them on five stages from experimental, which is basically we know they're playing around with DNSsec in some way. Announce, they've said they're going to do it. Partial, the zone's signed but there's not a DS in root, and then the DS is in the root and then it's operational. Next slide, please.

The one detail I would say is some of you have said to me, "Hey, why is our map still showing DS in root but not operational?" And the answer is because I don't actually have an easy way to know unless you tell me that you're accepting it. So if you see yourself in a bright green DS in root but you're accepting DS records, let me know. Next slide, please.

So here's our overall view of the map. We're getting a lot more green except for over here. We'll see that. Yeah, little detail. We'll get there. Next slide, please.

So here's what Africa looks like. Now there's one other addition that we should put on here to the folks in Morocco, congratulations. You signed your .ma domain but it was signed after I did these maps. But it'll be in the next round of things that are there. Botswana also signed down here, as well, so we're seeing some growth of this, but obviously, this is a big area where we could see more growth and I know Alain will talk about, or well, Alain over here is very involved with the program,

which is at DNSsec-Africa.org, which is doing a lot to help expand the signing here. Let's go on. Next one.

Asia-Pacific, in the general region, the Middle East, the one change since last time is Azerbaijan signed the .az or AZ. Next one. Europe has not changed since last time. Next one. Neither has LAC. It's been continuing to go on there. Next, please. And North America, oh there you are. Next, please.

So these maps do come out every Monday morning. We update them and they're there. You can subscribe. Next, please. We also have an events calendar we've been trying to update with DNSsec events. You're welcome to send me suggestions, if you've got that. Next, please.

I'll mention that there is a hack-a-thon. We've had these that the IETF has been doing on the weekend before the IETF. And it happens, started a couple of times ago, and there's a group of people who get together in that weekend and work on DNSsec DANE, DNS privacy, and our group has actually won top of show awards for the last two hack-a-thons. We've had a group there.

And so there's another group that will be gathering. If you're going to be going to IETF, you know developers who are going, and they want to code and work on DNS-related security projects. We'd love to have you. You can follow links. Next slide, please.

And last piece is there's a DNSsec history project that we're continuing to look for feedback and input, and that's all I'm going to say. And we'll get going right away with Julie saying something.

JULIE HEDLUND: We have two questions in the chatroom. The first is from Marcus from Global Village. He has a question, I think it was concerning some of the statistics that you had up. His question is, "How can Mayot have a DNSsec validation rate of 95% and a Google usage rate of 96%?"

DAN YORK: Geoff, do you want to answer that?

GEOFF HUSTON: Sure. It's slightly higher than Google because, actually, so one or two of the local ISPs might well be running validation, as well.

DAN YORK: I think it was the other way.

GEOFF HUSTON: Oh, if it's lower. Oh, okay. So sometimes folk put more than one resolver in their local config, and [inaudible].com. And it's often

the case that the ISP might well list Google and, perhaps, one other resolver. Now the issue about DNSsec is that when you go to a domain that is badly signed, and my test has one, it doesn't say, "That's badly signed."

The answer that the DNS returns is, "The server failed." And so if you have more than one resolver, when the server fails, you think, "Ah, I should try the other resolver." And if that resolver does not validate the answer, you're going to be misled and you're going to go to a domain that really was badly signed.

So in this case, there must be a number of folk using a local resolver in addition to Google. When Google says, "I can't go there because it's badly signed server fail," that's more number of folk go, "I have a better answer, I'll take the lying answer." That's a really stupid thing to do but people do that.

DAN YORK: All right. Thank you, Geoff.

GEOFF HUSTON: Geoff.

DAN YORK: Second question, Julie.

JULIE HEDLUND: Actually, that person found the answer that he was looking for, so we're set.

DAN YORK: Awesome. We love those kind of questions. Okay, well welcome, everyone, to the DNSsec Workshop. Please feel free, as you've seen already for newcomers, you're certainly welcome to ask questions at any point in time. We're a kind crowd to questions. We don't bite too much. And we'll be glad to talk to you all in any way, shape, or form. Please do ask away.

And with that, Vicky, you can either sit here or you can use the mic, whatever you want to do. Well yeah. We don't have a clicker, so Kathy's the. Yeah. Whatever. We'll figure out the clicker working at some point here.

VICKY RISK: Hi. I'm Vicky Risk from ISC. For those of you who don't know, we're the publishers of the open source BIND DNS system. But today, I'm going to talk about the DLV. Go ahead.

So the DLV, it stands for the DNSsec Lookaside Validator. It's something that ISC established back in 2006. And the idea was that people who wanted to use DNSsec before the root and the top-level domains were signed could use the DLV as kind of like a foster parent.

At this point, as you just heard from Dan, large percentage of the top-level domains are signed and the root, of course, is signed. And so there is a sense that the DLV has already accomplished what it could to assist with early adoption.

I think also there are people who think that continuing to have this alternative path to validate your DNSsec possibly is discouraging the remaining adopters. So a year ago, actually, at this first ICANN meeting of 2015, we announced, ISC announced that we plan to turn off the DLV by the end of 2017. Go ahead.

I apologize for the small type again. So we announced this back at ICANN in Singapore last February. We also updated the main homepage for the DLV site, we put it up on our own website, we sent it to some Internet mailing lists, we contacted the BIND packagers, the operating system packagers of BIND software. We announced it at NANOG, we've announced it at a couple of other conferences, and we sent an e-mail to every user in the DLV.

Obviously, we want to make sure that everyone is aware that we are planning to decommission this before we turn it off. So our plan was first, to start what we expect will be an extended process of discouraging people from querying the DLV, so discouraging people from setting their resolvers to query the

DLV. And then to start gradually removing the zones and the DLV over time.

Our plan is that we will continue answering the queries in the DLV indefinitely because it's better for the resolver to get a quick negative answer than to not get an answer and, perhaps, retry multiple times. Sorry, go ahead.

So this is just one example of the e-mail that we sent out. We sent this last June. We went into our system and checked to see for each user what zones they had, whether or not they were working, whether or not they could validate without the DLV, and we sent them information on their zones and asked them to remove them if possible. Go ahead.

So I'm going to show you a couple of the responses that we got, and these are, I think, representative. This one, actually, I know who this is from. This particular individual is very committed to DNSsec, but does not have any other way to get the reverse zone signed. Plenty of people, depending on where you are, don't really have a choice of ISP, and this user doesn't have another way to get their reverse zone signed. Going to the next one.

This is another person who does have a path to get signed, but they cannot get their parent zone to accept DS records. And these two are very common responses.

The reason I'm bringing this presentation here is I'm aware that many of you here in the room have some influence on improving the situation for these users who are committed to DNSsec, some of whom have been signing their zones since 2006, who are facing the prospect of going insecure when we turn off the DLV. Go ahead.

So far, since we started asking people to remove their delegations if they could, we have removed about 800 zones, 800 working zones. There were many more zones in there that were nonworking. I think a lot of people were using the DLV as a training tool. The problem is that the remaining 2,000-plus may have no other option to maintain their DNSsec security.

We have already kind of extended the timeframe when we plan to purge zones that could validate without the DLV. At the moment, where you see the blue line, that's where we are now. We're getting ready to discontinue registration of any new zones that could validate without the DLV. And as you see, the endpoint on here, July 2017, that's when we plan to remove the remaining existing DLV records. That will be a two-year notice for those people whose records are removed, but at this point, from what I can see, I think that we will be basically forcing people to go insecure who may not have another path.

So even two years notice is not necessarily enough, apparently. So we talked about the records in the DLV. Now let's talk about the resolver queries to the DLV. These are resolvers that are trying to validate the DNSsec. Querying the DLV puts extra burden on those validating resolvers, particularly since there are not actually a large number of zones in there, and it's desirable to minimize these queries going forward.

Of course, after 2017, there won't be any zones at all in the DLV, so it is completely useless for resolvers to query it, so we'd like to discourage that. Paul [inaudible] isn't here. Oh, okay, great. Well anyway, one of the folks that helped us out with this, the Red Hat folks, removed the queries to the DLV from the default configuration, resolver configuration in their distribution. Some of the other packagers have done the same. The unbound development team also removed it from their default configuration, and I think put a note in the documentation recommending that you not query the DLV. Go ahead.

So right now, we're seeing about half as many queries as we were a year ago. Again, I mentioned that the shutdown process will be complete in 2017, but we do expect that there will continue to be some queries to the DLV after that, so we're going to leave the service running.

So in summary, ISC created the DLV to encourage more use of DNSsec. At this point, we think it has probably served its purpose. It is not a solution for the systemic problem of nonsupport for DNSsec across the industry, and so once again, we're planning on discontinuing it. I think I'm done.

Oh, I just wanted to thank Afilias, I believe, for the duration of this project. Afilias has been providing secondary service for the DLV and they actually get more queries than ISC does. That's it.

DAN YORK: Vicky, one question for you. So as of July 2017, will DLV still be running or will it?

VICKY RISK: It will be answering queries but it will not any zones in it, so.

DAN YORK: There will be no more zones in DLV, okay.

VICKY RISK: Right. We're going to keep answering queries just because it will enable the resolvers to move on a little faster.

DAN YORK: Okay. But effectively, the DLV service will be closed as of July 2017.

VICKY RISK: Yes.

DAN YORK: Thank you. Are there questions for folks? Okay. Russ and then Alain.

RUSS MUNDY: Thanks, Vicky, for this presentation. I really appreciate it. One of the things I'd like to emphasize here to everyone in the room and if you've certainly been to the beginner's session, you've heard me talk about it, and that is people in the room, regardless of what you're doing with DNSsec, keep asking for more and more DNSsec support, whether it's from your registrars, your registries, your vendors.

Because as Vicky says, there are a number of activities that won't be able to do validation. And the best way to get broader usage of DNSsec throughout the industry is to have all of the supporters of the various functions involved in DNS doing the proper things to make sure DNS is available or DNSsec is

available to anyone that wants to use it. So ask, ask, ask. Thank you.

VICKY RISK: So actually, just to underscore that, I would love to be able to refer these people to an operator, an ISP who could help them to maintain their DNSsec chain of trust after we turn down the DLV, and some of them have come asking us for those references. It occurs to me now, of course, that hindsight is great that if we had been charging people money for this service all along, then they could take that money somewhere else and create a market for this, but it's probably late for that.

DAN YORK: Alain? Oh. I saw Alain first.

ALIAN AINA: Okay, sure. Thank ISC for providing these services because during the initial discussion, I think it was not easy even to get consensus in the technical community to go for DLV. And I hope we have people in this room who can remember the discussion on DNSOP DNS Extension mailing list. So but I think it was useful, very helpful, and thank you, ISC, and probably say, "Hello," to Paul Vixie for [inaudible].

VICKY RISK: Thank you for that, yeah. I wasn't at ISC at the time, but I have been told it was very contentious.

DAN YORK: Robert.

ROBERT MARTIN-LEGENE: Yeah. I think it's good that you're winding down the DLV. For the users that are very happy with the DLV, the technology still remains inside of various software, as far as I know. So people could do their own DLV if they really want to, as far as I understand.

But do you have any idea about what's actually remaining in there? Is it why it's still there? Is it a lot of .com registries and so is it some countries that don't support DNSsec at all or what?

VICKY RISK: There are a fair number of reverse zones. I've talked to folks from DE. There were a lot of folks in education and – it's really all over the map, honestly. I'm not sure I can characterize exactly what's in there. There are people that use it as a transition mechanism when they're moving from one provider to another, and they don't have cooperation.

But mostly, I think, the delegations in there are not actually temporary, but it's not any one thing. It's not obvious. I mean, there are a few people who manage quite a number of delegations in there, but mostly they're onesy twosy. [inaudible].

DAN YORK: Anyone else?

VICKY RISK: Yeah. Andre.

ANDRE: Just kill the thing already. Well my question is you are afraid that it will happen if you just turn it off. Because the number of queries just to K is really low number, so not many users use it. There are not many zones in there. And what would happen if you just turn it tomorrow? I think nothing. So I think you are free to turn off DLV while according to your plan.

But my real question is, why we are still talking about it? What you are afraid that will happen when you turn off the DLV? I don't think there will be any, well, damaging your reputation, which is the only thing that might happen. And I don't think that will happen, so I think you are free to just kill it.

VICKY RISK: Well I have to tell you we haven't gotten any love letters over this. The people that are in the DLV are pretty unhappy about it.

DAN YORK: Any other questions?

ANDRE: I think the people are happy that you're killing it, they already left.

VICKY RISK: Yeah, right.

DAN YORK: And if there's anybody behind this, whoever is doing this, and you want to speak, please just jump around, shout, raise your hand, do something. We do have a portable mic.

Okay. Well I would just like to say, "Thank you." I would like to echo Alain's words and say, "Thank you," to Vicky in ISC for running this. It was a very extremely necessary tool during the transition, so thank you.

Okay. Next up, we need our regional panel up here, please. So come up to the front and join us, and I will turn this to Mark, who is going to be the moderator.

MARK ELKINS: Good morning, everybody. My name is Mark Elkins. I'm the moderator for the next session. Our first panelist is moving slowly up to the front. If we do it from the front, then everyone can see your beautiful face on the camera. So our first presenter, we have four presenters including myself.

Our first presenter, Alain Aina, very active in the technical community in Africa, has run his own companies. He's certainly very involved in AFNOG, which is the training organization, Africa Network Operator Group. He was also, for a number of years, since November, the Special Projects Manager at AFRINIC. And spent a lot of time in Mauritius doing various DNSsec-y things. So, for example, the whole of AFRINIC does have DNSsec for reverse, including v6 and including legacy, which I'm very happy about. And, essentially, is working as an ICANN consultant on the DNSsec Roadshow Project, which I think is what he's going to talk about.

ALAIN AINA: Yes. Thank you, Mark. So what I speak to French. Okay, no, let me [inaudible], no, but not many people here have the, it's okay.

MARK ELKINS: We can get headsets, if you wish. If you're more comfortable, we can –

ALAIN AINA: Okay. Let me just speak English. Yeah. Thank you, Mark. And as you said, I'm speaking here as an ICANN consultant for the [inaudible] DNSsec Roadshow in Africa. And from what then show in the map, you could see that Africa is lagging behind in term of ccTLDs DNSsec adoption.

And I must say that what you saw in 2015 is better than what it was in 2013 when we started these things, but we still have a long way to go. So the roadshow, the DNSsec Roadshow is one of the inner city part of the African ICANN African strategy. And then we are trying to help the ccTLDs in Africa to understand what is DNSsec, how DNSsec can improve their services to the community, etc. etc.

But it's not easy. It's not easy at all because we all know that DNSsec brings some kind of complexity to DNS, and when you don't have a reliable DNS or let's say resist the operation, it's difficult to add the DNSsec liaise.

So if you go to DNSsec-Africa.org, you'll see we maintain a website. We have tools which daily trying to see how the African cc are doing and we are trying to build a history. So we check and see the first time we see DNS key for a cc, we put a date. Then we also track when the first time we see a DS in the root zone for the cc. Okay. That's what you'll see.

But we keep tracking the change in the key IDs and we keep tracking the algorithm. Okay? So, and we have nine cc on the main continent, which have signed their [by] zone. But as [inaudible] then said, signing is only is one thing. But being operational, which mean accepting DS, where DS recall from your registrants is something else. So in term of how many of them are operational, then the different story, the different story, and I think soon we're going to hear from Dr. Lisse about the [any we'll see] how is NA doing, for example, in term of how many DS record we have since NA has been signed in 2009, etc. etc.

So we have three cc currently as DNS key, [inaudible] signed zone without DS recording the root zone. The letters to come is Sierra Leone. So we are watching closely. But for the DNS Roadshow itself, what we do is we visit countries and we have a three days event. And the first day is get together. We ask our host to invite all the players because the DNSsec is not only about signing, it's also about validation.

So we ask for our host to invite ISPs, all stakeholder interested in DNSsec, then we discuss. We present the benefit, what is DNSsec, etc., and then including now the specific things. And then the second day, we have a tech day, where we show people you can deploy DNSsec, especially how do you validate, etc. etc.

And then the last day, we sit with the cc in the room, okay? And then we look at show me your registry system, okay? And then we look at how can you deploy DNSsec, and we come up with a plan. Okay? And the plan and we trying to follow up, but it's not easy. What we find out is much of the time, the same thing. The registry operation not reliable, not ready, okay? No monitoring tools, no full, no dedicated staff, etc. etc. So it is same thing.

So you end up saying, "Okay. Okay, let's work on fixing your registry. Okay?" And then we add DNSsec, so what you are saying, what then you show is, yeah. This is the reason of why we are there, and we hope, so we hope we can improve. We can improve the adoption in Africa.

And last year, I think, everybody hear about the two DNSsec incident. Say you are engaging people, pushing people to adopt DNSsec, but unfortunately, last year, we have two DNSsec incident. KE and at the end of the year, we have another incident, Botswana.

And these two incidents show that we need to go back and also help people work in how you manage the incident, business continuity, and disaster recovery. So at ICANN, then we add in this aspect to the Roadshow, okay? Helping out people. We had a call a few months ago with the cc to discuss the incent management plan, business continuity, etc. etc. So I will just stop there, Mark. So if there any questions about [inaudible].

MARK ELKINS: I think what we'll do is we'll hold the questions until the end of the four sessions, if that's fine with everyone. So please do write down your questions for later on. Thank you very much, Alain. I've known Alain for years and years and years, and if you go to an AFRINIC event and he's not there, then it's not an AFRINIC event. Thank you.

Okay. So the next speaker is myself. We're going according to the agenda here. So I'm going to give a very brief report back about actually what is happening in South Africa. South Africa. We have been giving DNS training for the last ten years now, ever since after ICANN in Cape Town, the first ICANN we had in South Africa. And that's been happening twice yearly.

That's both intro course and an advanced course, which means people have been taught what DNSsec is. And I believe we've been seeing the fruits of that. Personally, I've been running

DNSsec for seven years using the ISC DLV system. Please don't take it away. I was going to answer some of the asked questions about that in the presentation from Victoria, but I didn't.

And I've also done a project called Rollover in the process. One should note that the [Zeda EPP] systems have the DNSsec extensions, and I've been playing and rolling DS keys in the CO.za domain name space for the last three years. The reason that ZA is more one of political-ness rather than anything else. And the proof of that is that the three gTLD cities, Durban, Cape Town, and Joburg are signed and are running just fine.

The fact that when I looked at the Joburg zone recently, it's only got one signed domain and I happen to be the person that put that one in is neither here nor there. So like I said, there has been fruit from all of this training. So I can say that Telkom South Africa, who, as much as they don't peer with anyone and seem to really try and do everything themselves and don't talk to the community, they do come on the training courses because they're free. And they run DNSsec aware resolvers, which accounts for, I believe, about 15% of the queries in South Africa. Or there's a 15% figure hanging around that of all lookups.

I'd also like to claim credit for the increase in East Africa, because I had Andrew O'Steen sitting with me at the last DNS Africa forum, and together we put DNSsec validation into his

resolvers at that time. And I'm quite pleased to see that that's sort of showing up quite nicely now.

So South Africa should be signed soon. It's simply not happening. The .za itself. Like I said, the facilitates to put stuff into the zone is, it's the majority of zones is there. So that would include all the ZACR-run zones like COZA net .za [inaudible] .zaorg, .zalaw, .za.

Interestingly enough, also, a couple of the other domains in South Africa, everything was not run by a central organization initially, but given out to different people to do different second levels. So there is a little bit of confusion there, perhaps.

So I'd personally look after edu.za and someone else, a friend of mine, looks after non.za. Both of those are signed and both of those have DLV lookaside records. So technically, they are there, although the number of domains actually signed, well, those are two very, very small domains.

From an African point of view, from my point of view, all the reverses are there and has been there for a long time. So you should never see anyone from Africa complaining that they cannot do reverse DNSsec as such.

And then changing the topic very, very slightly. ICANN put out an RFP for a DNS African study. Myself and a gentleman by the

name of William Stucke down at the bottom there, are in the room today. There's a group of another 10-15 people who are also doing the same study or involved in that study.

The study includes looking at DNSsec records to see if things are signed. So there is, that is happening. But if you also happen to be here because you're an Africa ccTLD manager, or registrant, or registrar, then this study will be hitting your mailbox as soon. Please help us. It's only by looking and picking up the numbers that people can do these sorts of presentations, or it certainly helps from the future point of view.

And I think I will call that quits. Enough about me. Our third panelist this morning. Our third panelist this morning is Sara.

SARA MONTEIRO: Yes.

MARK ELKINS: And she actually did give me a CV eventually, didn't she? Degree in Computer Science from University of Lisbon. She's Portuguese. Member of the Infrastructure Team at DNS .pt since 2006. Responsible for the management of the ccTLD in Portugal, and served various roles in the technical area doing various things, and it would appear activities within the DNSsec extensions are included in that.

And you're going to speak in English?

SARA MONTEIRO: Yes.

MARK ELKINS: Oh, cool. Thank you, Sara. Over to you.

SARA MONTEIRO: Good morning, everyone. As Mark said, I am a member of the Portuguese ccTLD, .pt. I'm on the technical team but today, I'm here on behalf of some African ccTLDs where the DNS .pt is assigned as a technical contact at IANA. So next slide, please.

So before I start speaking specifically on some ccTLDs, I want just to tell you about LusNIC, that is a Portuguese language ccTLD association that was created last year. So its mission is to promote and to collaborate in the defense of the [inter soft] Portuguese language ccTLDs. So we believe that with this association, we'll be able to help some ccTLDs especially in Africa, and other ccTLDs. So the main role is to help and to cooperate among all the ccTLDs. Next slide, please.

So LusNIC, as I said, the main purpose is the sharing of knowledge in the areas of the intervention regarding technical, security, legal matters, good practices. So the mission is to

conceive the joint actions and to advance this sustained growth of Portuguese language top-level domains, especially .br from Brazil, .cv, Cape Verde, .gw Guinea-Bissau, .pt Portugal, .st, St. Tome and Principe, and .ao, Angola.

So right now, these are the ones that are signed and are members of the association. But we are looking for it for new members and the sharing of all this experience. Next slide, please.

So talking specifically, .ao from Angola. Since DNS .pt has succeeded to have [inaudible] in the management of the top-level domain of Portugal in 2013. In consequence, it also succeeded in other responsibilities. So we are helping .ao from Angola. We, in the end of 2015, had 364 domain names registered. And in the matters of DNSsec, we held one-week training, DNS training, where we try to share our knowledge in the matters of DNS in Lisbon in our DNS .pt site.

So, and we also, we did propose to improve their DNS and DNSsec knowledge. We had given them a hands-on workshop, and we had six participants in total from two different entities. Next slide, please.

Regarding .cv, Cape Verde. In 2010, DNS .pt, that's have been managed the primary [inaudible] for .cv, was able to transfer other roles and responsibilities to ANAC, the National Agency of

Telecommunications, and they start assuming that this role independently.

So in the same year, we host workshop and to local entities where we try to promote their cc top-level domain. And in 2013, again, we hold a hands-on onsite where we invited ANAC technical staff. We analyzed all the CV infrastructure, and we created the report in order to help them to configure all the necessary adjustments to adopt DNSsec. So I think they are prepared to adopt it. I don't know why they didn't. I think they feel more comfortable if we help them, so they are trying to arrange a date to where they can come to Portugal again to continue the deployment or maybe we will be going there to help them, so I don't know. We are looking forward.

So we also, in this matter, offered and installed name server in ANAC's facilities, as I said, to help them to technically manage their ccTLD by their own. And we also had given our previous .pt management system rights and software in order to help them to manage a system as independent as possible. Next slide, please.

And the last one, it's .gw for Guinea-Bissau. In July of 2014, our RN is held responsible for mentioning .gw. The top-level domain by IANA and the registration and management of [inaudible] returns to the area of Guinea-Bissau. So right now, DNS .pt is

being assuming the technical and the administrative operations and legal management of the Domain Names Registry and .gw by IRN request. But we are looking forward to transferring all these roles to this entity. But we will be able to do that after intensive training and the setup of a proper network and [inaudible] technical infrastructures. And next slide, please.

Okay. We can share with you that in a cumulative analysis between the data, it's validation, and the end of the 2015 .gw had reached 2,200 domain names. So we believe that this evolution was possible because the NSPT was able to count on Portuguese registrars to embrace this new ccTLD on their business. And also some international registrants had joined. And in a total so far, all 15 registrars. Next slide.

Regarding to the DNSsec, in February of 2015, we had, since we are managing the zone entirely, we had signed it with DNSsec. We are still remaining to submit DNS record in the root zone by political matters, but it's a question of time.

And in May of the same year, again, we are, had hosted the workshop. This time, we went to Guinea-Bissau and with the proper of giving an overview of the Internet, particularly on the DNS matters and on the cybersecurity and DNSsec matters, we were able to give them a presentation at the total of 42

participants. So I think that's all the information I got, so I hope it's useful for you, so thank you.

MARK ELKINS: Thank you very much, Sara. I didn't realize there were quite so many Portuguese-speaking countries in Africa. But now that you put it there, I understand, yes. My last speaker for this morning from my panel, a gentleman that I've known for an awful long time, Dr. [Elise] Lisse, Eberhard.

He is well-known in this community from running Tech Day. I'm going to spoil something now. His favorite party trick at ICANN is to ask people what is his occupation, daytime occupation, because it's got absolutely nothing to do with running a ccTLD registry. He's a gynecologist.

And yet, being more serious, he's been absolutely fantastic from a personal point of view in doing things like women and children protection in Namibia. They're actually changing the law, making it easier for women to be women in Namibia. So he really has a soft heart somewhere. You don't see it, I know, but he definitely has a soft heart in there somewhere.

Anyway, now that I'm – please continue. No, Warren, we were not laughing at you as you entered the – well, some of us were, but most of us were not.

EBERHARD LISSE: Oh, I'm on. Oh. I always say I used to have a day job, which is gynecologist, and then I also said I have a night job, which is obstetrician, but due to some the fact that the malpractice insurance have reached us, I don't have to do this anymore, so I get much more sleep.

But this profession has taught me a few things that, for example, can we have the next slide? That a patient doesn't really matter, isn't really concerned about a number of visits to the doctor, but whether I can fix their problem. And I am very critical about a few things. I'm very happy to see that [inaudible] foreign countries sort of get adopted by the former colonial master to assist them a little bit, but I think that's the wrong approach in the long run and it's the wrong approach in the short run, as well.

The DNS, I haven't been able to find out how much the DNS Roadshow spends in money, and I was hoping that this would be said at the presentation, but I will dig it up with Xavier, the Financial Manager. He's used to my e-mails now.

This is what's supposed to be, the DNS Roadshow is to do [inaudible] around a lot and it's supposed to promote the adoption of the DNSsec. But if I can have the next slide, as we

see in 2013, that was the picture there, and now we can have the picture, the next picture.

It didn't really change anything, so we waste a lot of money in traveling around business class or whatever, doing nice little workshops, and look at what we all know that the ccTLD managers are inherently too lazy to do the job. And, obviously, if they can't do the basic job, then they won't figure out something that a simple gynecologist can figure out in six week when he was booked sick after surgery, which I did in 2009. BIND is not that difficult.

It is really a shame that only two countries are operational, and that's Tanzania and maybe the other six are all not visible because they're small little islands and they're running on other platforms. If a little island runs on the .org platform, it doesn't count. If Guinea-Bissau was ccTLD gets to run on the .pt platform, it doesn't count. It's not intrinsic, it's not rocket science, never mind that we have our own human resources. We send people to universities to get master's degrees in computer science but we simply are not able to do simple stuff like this. So next slide, please.

Basically at the moment, and I am pleased would ask the people from .cz not to start hyperventilating just yet. We are coming to that. That's an in joke. There's two ways, when I wrote this

presentation, there were two ways of doing DNSsec. DNSsec is simple but it's not easy.

What we want, we want on the one hand to give [Tarlis], to have [Tarlis] give us this hardware for relatively cheap. Yeah? We need three of them. Each ccTLD needs three of them, and I fortunately I hear you can change the battery in a [Tarlis] so you don't have to replace them all the time. But we need to get them at a reasonable price.

So what we actually need to look at, we need to look at something where we can do it for 20 bucks. Soft HSM is an answer, and BIND is simple to do. If it's BIND, it's simple to do in software, but BIND does not support a $20 soft HSM, at least not out of the box. [inaudible] has written a patch, but the problem is whenever BIND is updated, you have to reapply the patch, and that doesn't scale, and that cannot be done.

If that were happening that I can just update with the package manager and it would work, write your conscripts do all the error catching that you want, and be done with it.

OpenDNSSEC is complicated to set up. It's difficult to debug. It does support soft HSM, but on Ubuntu, this card requires a library, and this library has the annoying habit of dying but still running. And OpenDNSSEC has the annoying habit of ceasing to

work and ceasing to sign without telling you. So that's not really a simple way of doing this. Could we have the next slide?

OpenDNSSEC was involved in several crises of ccTLDs in one way or another. It's difficult to debug. What I am doing is I sign lisse.na with this soft HSM card. I have to kill the [inaudible] daemon three or four times a day so that it fires up again and then resigns within a day or so, but that's not good way of running a railway.

So when I was writing this presentation, I was thinking we should, instead of maybe wasting more money on traveling on the DNSsec Travel Show, but take some of that funding and have a look at what works, like the extra signing of the DNSsec, and write standalone programs that you can run on a command line. That would make it easier to debug. Once you get the hang of it, you can put it in shell scripts, run it on [inaudible] under [inaudible] and it would work. And that's what a costing is supposed to. Could we have the next slide, please?

In the meantime, Andre [inaudible], who spoke on Tech Day on Monday, mentioned over lunch that not DNS, which is bound to take over the world, can actually talk to this soft HSM card. So I'm going to work with them to see that we can find method that works on Ubuntu out of the box so that even if given a special [inaudible] the way that we can do the updates on the packet

manager, and if that works, that might be a way where we can get a hardware-based solution, which increases the security and we don't have to go through this expensive machine.

It's a little card. It's a little chip card costs $20, you buy, it cost 20 euro, you buy it in Germany, and if you buy five and you're from a developing country, they give you six for the same price. And it has a little chip, which actually does the signing in the chip. It can do about five signing per second.

Can I finish my presentation, please? Anthony [inaudible], somebody who I do not hold very dear, and he knows that, recently got himself made available for ultimate employment and he posted on a website that he got fired, and he basically said for the [inaudible] market to have five sort of registries. Two don't really reply to us and in decreasing order, a supermarket approach is what some ccTLDs are trying to do is selling a large amount of domains for very little profit.

Whether that works, I don't think so. ICANN would like registry to be a purely technical function only interested in infrastructure and service level, and what's working for us very well is a small business, keeps the cost down, build the business over time, look for nice or ongoing income. We basically say we want to have a higher renewal rate and my view and the next slide, please is that we should have the best of these two.

In summary, the hardware is very expensive if we have to pay 20,000 to 30,000 euro for one machine, it's simply out of order. We cannot do it. Soft HSM is still not ready for primetime. One thing it's very easy to do and I really don't understand why not many ccTLD are using is setting up a secure way of pushing the zone to PCH. They will sign it in a really absolutely secure fashion and either push it back to you or act as one of the authority name servers since they were ours, we do this for the second level domains already.

Accepting DNS records [inaudible] tools, which is in wide use in Africa, a later version, everything from middle of last year except DNS record. DS records, Mark and I, we were playing with this. I didn't really come here to show how many clients we have. We have virtually clients who are taking this up.

If you go to the bank and try to explain [inaudible] yeah, but we have got https that works for us. Never mind that they always forget to renew the certificate and I can guarantee Standard Bank on the 22nd of December this year is going to fail because the certificate expires.

The take-home message is build it and they will come. If you can build a system, which is relatively cheap, cheap, which is function. Eventually, clients will start figuring this out. Our government wants to mandate DNSsec. We told them not to do

this just yet until we can audit from the top down through hardware.

I don't really think it's a difficult problem to get them to sign. If I tell my registrars, who are also the connectivity providers, unless you put validating resolvers, we'll give you a little premium on your registrations or we give you a discount if you do it, they will start doing this quickly if it becomes a business population.

I think that's the last slide. Thank you very much.

MARK ELKINS: Thank you very much. He really does have a heart in their somewhere. Okay. So we have about ten minutes' worth of questions. Just a quick definition. If I look at what HSMs are, etc. HSM hardware security module. To me, there is a soft HSM, which would be the piece of software that Richard Belkin in Sweden wrote, by definition. Well, okay.

UNIDENTIFIED MALE: Yes. As part of the DNSsec project, indeed, but it's maintained by [inaudible] sponsored by ServNet graciously.

MARK ELKINS: Okay. I was quickly going over the definitions. The HSM thing that Eberhard was talking about to me is a, it looks like a credit

card with a smart card with a little gold module in it. Yeah, yeah, okay, PKC [inaudible]. And the nice thing about them is they are really cheap, they are really, really cheap, they're great for doing preconfiguring a whole bunch of signatures and stuff, and then at the other end of the scale, you've got the other HSMs like the tallies, like the cypher machines that the root is signed with, etc. And they come at megabucks.

So there are, from my point of view, three types. Do you want to clarify and let Dan? Okay. I was also going to fire off one quick question first to get the ball rolling, but it looks like going to happen. Alain. 54 countries in Africa. How many do you still have to do and how much longer do you think it's going to take?

ALAIN AINA: What we do is we resell to people and we only visit those who already, who want us to come. So we are not just going. We are [inaudible], we resold and we discuss, we see where people are, and see if they are willing to host an event. So it's not moving to places. We're not visiting each ccTLD, so this is all I can tell you how many because right now, I don't know when I'm going next. So it depend on people who are ready and who want to host.

MARK ELKINS: That was actually my question for Alain was to ask. So if there are countries here in the room from other parts and they would like to bring the roadshow to there to go and work with that. And I've had great feedback from others about what you've done in those areas. How would they go about doing that?

ALAIN AINA: Two ways, talking to me or talking to Pierre or the ICANN Africa Bureau people, or even Internet Society, or talking to ICANN DNS people like [inaudible]. You use various way to the same [inaudible], so.

MARK ELKINS: Okay. I would also just say I think it's great that you've added the part about disaster recovery and preparedness. It's an excellent thing around that. While I have the mic for a moment, I would also just encourage everybody to join in with what that DNS study Mark was talking about. We need, as you saw in the beginning when I talked about the metrics and stuff, we need more data about the usage, the deployment, all of that. So please do help with that study when it comes out.

JULIE HEDLUND: I'll just note. Please do state your name and your affiliation. We also need that for the folks who are joining us remotely. I do

know some of you, so I've been putting that in the chat, but I don't know everybody. And also, if you have a question and you're not sitting at a mic, Kathy Schnitt here is graciously going to walk around with a mic. So be sure to ask your question with a microphone or the folks who are joining remote will not be able to hear you.

And then just for your reference, Mark, I do have a question in the chat, if you'd add it to your queue, please.

MARK ELKINS: I see no other questions immediately. Would you like to read that question? Oh, sorry. Victoria.

VICKY RISK: I just have a comment. Eberhard, I know you've been looking for support for these credit card soft HSMs and BIND, and if Rick wants to submit a patch, as long as we have a test for it and a little bit of documentation, we'd be happy to make it more readily available to other BIND users. That, of course, is ideally how open source works. So in fact, even if you want to give a presentation to other folks interested in using this soft HSM, I'd be happy to sponsor a webinar or something like that.

EBERHARD LISSE: So let me just get this. Is this a change in view by ISC on this? Because I had prior correspondence with the implementer. He wasn't interested.

VICKY RISK: We have our crypto expert has a mixed opinion of the FIPS certifiability of the soft HSM card and so on and so forth. There's a big difference between recommending a solution as being the cryptographic pinnacle of excellence and enabling people who are trying to run DNSsec. I'm sure we can find a compromise as particularly if you have a working patch, sure.

EBERHARD LISSE: This is great news. I will get together with Rick and we'll communicate with you and we'll see what we can do.

MARK ELKINS: I hear that as a call to arms. I've actually wrote that down to Victoria for ISC to include some form of standard support for card-based HSMs, standard. Can we have the remote question, please?

JULIE HEDLUND: Thank you, Mark. The remote question is from Marcus from Global Village. His question is, "Will the African registries use

standard EPP DNSsec extension or will they use the .pt style DNSsec record pickup?"

SARA MONTEIRO: I think that question is for me. So regarding the Africa registry, that's DNS PT is helping. They don't have EPP extensions implemented yet, but I believe the DNS .pt will not apply the same techniques that we apply on .pt because we are not trying to copy what we do to others; we are just helping others to set up their own system and trying to, with their own knowledge and technicals to improve what they have and to be able to do it.

So for now, you can submit DNSsec information in plain text or something, but in the future, I think they will decide that not .pt for sure. So I don't know.

MARK ELKINS: Any ccTLD registry or gTLD registry that uses [inaudible] tools from a version later than June or May 2015 can accept DS records by standard EPP. It works out of the box for any ICANN-accredited registrar. And, of course, they can put it into the GUI or they can send it for e-mail, but as Mark Elkins and I, we had a problem, we couldn't get it to work. Eventually they fixed it and now it's working standard state out of the box.

MARK ELKINS: Next question.

ROBERT MARTIN-LEGENE: Robert from PCH. No. I was just to what Eberhard said and his presentation about PCH signing TLDs. PCH will happily take on TLDs and sign them for free, and hand back with [inaudible]. You don't need to go to any other services that we have, but you are very welcome to. If you want Anycast or DNSsec or whatever, come talk to us.

RUSS MUNDY: Well I want to thank the panel for this fine set of presentations. This is Russ Mundy from SSAC. And really am very pleased to see the amount of progress from this continent over the last five years, basically; it's been huge. One of the things that I found very interesting in the set of presentation is when Eberhard mentioned that the government was thinking about mandating the use of DNSsec, which itself is an extremely positive progress that one of the governments are thinking about doing this.

And I really had two questions. First, are there other governments in Africa that are thinking about taking a similar step? Mandating, for some segment or some part of the community, the use of DNSsec. And secondly, a somewhat very

separate question, does the registrar function still present significant challenges to making DNSsec work right in the whole in Africa?

EBERHARD LISSE: Registrant can only submit DS records in two ways, EPP or e-mail or, if you use [inaudible] tools, then a third way is possible with the graphical user interface. But there is no demand. You can go to bank and explain to them how this work, and they tell you, "No. We have got SSL certificates and it's good, that protects our users." They just don't understand it. You can explain them 1,000 times, you can explain them very politely, you can do it easily, you can go do it more complicated. You can. They write really nice apps. The banking app from the one bank that is the most difficult is the best I've ever seen in the world, but they just not interested.

And I am a strong believer that you shouldn't push the demand from the seller side. We provide the service, we build it. If they come, they come. If they don't come, they don't come. We would tell our government that they should mandate any of the placement resolver must be validated.

MARK ELKINS: Thank you, Eberhard. I'm just looking at the clock there. I've also seen AFRINIC use SSL website to upload DS records, and it works just fine. Dan, you have a question.

DAN YORK: Real quick for Sara. Actually, I hate Robert. I want to talk to her. Stop. I want to talk to her. So first of all, I would like to just say thank you to Sara for coming here and talking about what LusNIC is doing. I join Mark in – I did not know there were that many Portuguese-speaking countries in Africa until the last time you presented this, which blew my mind. So thank you for doing that and continuing to do that.

One question. You mentioned with .gw, they're signed, they're ready to go, but it's political delays or it's just delays in that space, or could you speak a bit to that or something?

SARA MONTEIRO: It started at technical delays and since we need to have, when we submitted the information in IANA, we need to have everyone's approval, and they are not very – it's not very user-friendly for people that never use it. I believe so, I don't know. But the problem, it's not like a problem, but .pt is in 2015 also had shift from old infrastructure to a new infrastructure. So also, the name servers that actually are delegated will change, so we

are trying to do the same change at once, and this way, it would be easier for everyone for the management entities and the technical ones.

But we are working hard on it, and we believe in 2016, we'll be able to do it, so.

DAN YORK: Okay, well thank you. Thanks.

MARK ELKINS: Last question, [inaudible].

UNIDENTIFIED MALE: I would like to add to what Vicky said. We are also implemented to begin CS [inaudible] support in DNS and we are now testing with different HSMs. So if you have HSM that you would like to be added into our product, we would, and if you can give us remote access of the HSM to test it, we would be happy to have the support there, because if you implement the [inaudible] CS-11 support, it doesn't mean it supports all HSMs. Everyone is different, unfortunately.

MARK ELKINS: Thank you very much. Add tallies, please. Wrap up. 30 seconds per person. Alain.

ALAIN AINA: Yes. I wish I could travel business class but we are not traveling in business calls for the DNSsec Roadshow, and part of the Roadshow is also to provide some resources. So if you go to the website, you see we have material, therefore, people. And I think the Roadshow is not only looking at the technical side as Lisse said, we also need to engage the community to create the need for people to follow you.

Otherwise, the registry you signed is owned, but nobody follow you, so [inaudible].

MARK ELKINS: Thank you. 30 seconds up.

ALAIN AINA: Thank you.

MARK ELKINS: Sara.

SARA MONTEIRO: Sorry.

MARK ELKINS: 30 seconds wrap up.

SARA MONTEIRO: Okay. I think the main goal is to help the DNSsec deployment in every country and every ccTLD and gTLD. So we are trying to do it. And we are just sharing all the knowledge and best effort that we have, and we hope we will be able to help everyone.

MARK ELKINS: Thank you very much. Doctor.

EBERHARD LISSE: Yeah. Now I can count down the 29 seconds because I don't really have a good wrap up. My view is that we Africans are inherently lazy, we like to go – yes, yes I am. Even if you don't think I look like it. And so is Mark. And the point is I don't think doing this from top down is going to help, and creating an artificial demand is not going to help. We should sort of make available resources but the result will only come on the bottom up. We must basically not convince somebody to do it. If they want to do it, they will do it, and eventually it will work. We must just make the resources available in practice, not just by having to go to meetings.

MARK ELKINS: Thank you very much. Thank you, my panel. Great show. And applause.

JULIE HEDLUND: And also thanks to Mark. Thank you, Mark, very much. Excellent moderating.

MARK ELKINS: And we look forward to seeing that map further filled in next time we're in Africa.

JULIE HEDLUND: So we are supposed to have a break. We're also cognizant that we are about 15 minutes over, but I think we could probably make up the time. What do you think, Dan?

DAN YORK: Sure. I mean, so what's the breaks? What do we have?

JULIE HEDLUND: Pardon me?

DAN YORK: Yeah. I'm missing my schedule. By the way, if you are not going to be here for lunch, please leave the lunch tickets behind, if you could, for others that are there.

JULIE HEDLUND: Yes. So 15 minutes for a coffee break, please. Followed by Alain Aina on the OpenDNSsec signer switchover experience, and then Dani Grant on the DNSsec at scale, and then the quiz.

DAN YORK: All right, hey. Everyone, everyone, hey, we're already going to break. So let's take a break, but be quick about it, please, so we could come back as soon as possible, and let's not start any later than 15 minutes. Right?

JULIE HEDLUND: Yeah. We'll start without you.

DAN YORK: We will start and you want to hear Alain talk about his thing.

RUSS MUNDY: And clock applies to the break, also. If anyone wants to know, just come look at the clock.

DAN YORK: Five minutes, five minutes, folks. Get your drinks. Get your stuff. Come back. We want to get going.

Three minutes.

RUSS MUNDY: Two minutes in the break. Start moving back to your seats, please.

DAN YORK: So let's, as Russ just said, let's come back to our seats, if we can start moving that way. And if you were sitting in the back and you want to sit up at the table, you're welcome to do that, too. If there's a blank spot. So come on, folks. Let's come on back. We got another minute left, but come on. Let's get in here.

If you see a blank spot at the table and you'd like to join us, you're welcome to. There is one right here, if somebody wants to sit next to me, you're welcome to. Whatever. Come on back. Good. We're getting there. All right.

So why don't we – are we ready? Oh, no. Kathy, we're still, we're doing our thingy. What are we doing? All right. Ah, okay. So we're all good. All right. Well then. I will like to introduce, well, a gentleman who was just speaking, Alain, who is here to talk to us again. And I will turn it directly over to him. I'll be moderating

the questions, so if you do have questions, please feel free to get ready to ask about them. And here he is.

ALAIN AINA: Yes. This is Alain Aina from Africa. I want to just share experience of DNSsec switchover where we had at AFRINIC. So yes, now I'm [inaudible], I was AFRINIC before, and I did this with the team before I left. So [inaudible]. Yes. This switchover happened a AFRINIC and maybe I should explain that AFRINIC as the regional Internet registry manage the [inaudible] DNS for the v4 and v6 [inaudible] AFRINIC manage.

AFRINIC manage nine zones, six v4 and three v6 zones. And AFRINIC has been doing DNSsec since April 2012, suing OpenDNSsec, and we, for some reason, we have to switch, and this is what I'm going to present. So if you go to the first link, you'll learn about DNSsec at AFRINIC, and the second link show you exactly what I'm going to talk about.

So the context [inaudible] AFRINIC use OpenDNSsec to sign the nine zones. Key in soft HSM use [inaudible] SEC. [inaudible] 56 and the OpenDNSsec we're using at that time was with SQLite database. And along the way, we faced some issues, zone signing issues, so they signed time to time just phrase. And we then, in this case, some delays in a zone publication, and we, what we did is to put some work around, which was to restart, to

reload the standard every, I think every hours to, yeah, to get the engine up and running again. So that was the workaround until we moved to this.

So yes, as I said, motivation is to move to a new [inaudible], which still based on OpenDNSsec, changing the database to also allow us to add more zones. We, AFRINIC manage also a normal DNS and many names for the continent, and AFRINIC was also planning to start signing for members. So we decided that we should move to a database to [inaudible] of the SQLite.

A new version of the software system, we want to keep the key in the software system, same algorithm, same sign-in policy. Next. So our strategy, because we're keeping the key in the software system, the strategy was no private key export, no fresh start. And you have to keep the validation state of all zone, all time, so this is, yeah, this is what we have, too. We have decided we are not going to exposure the private key.

We cannot do with fresh start because of the third plan. We are in production and we have members who has sign zone, then we have to keep the validation state at all times. So then what you do then, you migrate with a key rollover. This is the [inaudible]. On side, we see the old [inaudible], and the system is based on getting the zone from a hidden master through zone transfer.

[inaudible] and push to the public master and then the public master through zone transfer to the public secondary name service [inaudible]. So this is what we did. You could see these big publishing the DNS key and [inaudible], so you pick on the key, we took the [inaudible] and KSK from the new [inaudible], then to the old [inaudible], pre-publish. Okay? And we also put the DS of the new key at the IP [inaudible] and we also exposure the public key from the old [Sonya] then to the new [Sonya] [inaudible] call pre-publishing the DNS key and [inaudible] sign in.

And then at some point, following the timing, you stop from the old [Sonya] and we switch to the new [Sonya]. So this is before the switchover. You could see that we have the DS from the old pointing to DS for the old key pointing to the old key, which used to sign both the old and new key. Okay? Next.

Then after the switchover, then we, this is what from our side you see, you see the two keys, assigned the two KSK being used to sign both the old ZSK and new ZSK, so you have two keys with one [inaudible]. So when we're doing this, the system was rolling from ZSK, so some ZSK rollover was [inaudible] the two keys you see over there with [inaudible] point.

So we advertise switchover for some time, we had the old KSK and the new KSK sign in the two sign in the two ZSK, you could

see the cross. Then after some time, this [inaudible] what you see, then we remove the old key, and then the final stage was to remove the DS from the DS for the old key from IP [inaudible] zones. Next.

And so this thing require careful reconsideration of the planning and planning, and timing. You need to be careful on the sign in signature, let time, the TTM, looking at the keys, the state of the keys, etc. etc. And carefully manage when do you switch because remember that we said we want to keep the validation state or time. So there's no room to go and validate and valid for some time. So you need really to be careful. So it work out very well, no crash, no alert. Next.

So the good experience and I think this also can even apply if you were moving from BIND sign in to OpenDNSSEC or BIND OpenDNSSEC I think is the same thing apply because I think it's about managing the key, okay, to I think this experience [inaudible] also apply for moving from BIND to open the other way around. So it will have been a different story for the key is in the SSM in the hardware security, so maybe we will not go for no private key export, for example, so if we had the hardware security modem, maybe one option could be just build a new one and make it talk to a key [inaudible] in the SSM.

So next time, I would do it, same thing except pre-publishing the KSK. We did publish the KSK with .DS, which was not really needed because we could just do this with the [dub] DS but we decide that to also pre-publish the KSK to avoid any issue, but next time I think we should do it without pre-publishing the KSK, pre-publish the ZSK, and do [dub] DS. Yeah. Thank you. I think that was the last slide. Thank you.

DAN YORK: Okay. We have time for some questions and I'll begin with could you run that through of why you would not pre-publish the KSK?

ALAIN AINA: So, no. It's not needed. Okay? Because by doing the [dub] DS, so that mean you have the DS of the new key already published at the [inaudible], so no need to pre-publish the KSK. Okay. Because when you have the. Okay. It's like doing KSK rollover. If you want to do KSK rollover, you can do [dub] signing, or you can do [dub] DS.

But what we did here is we did [dub] DS and [dub] sign in by pre-publishing the key [inaudible] the KSK.

DAN YORK: Okay. I need a whiteboard to think that through in my brain or something. We have some questions already, and one is I see from Robert. And if you, Robert and [inaudible] I see in the queue. Anybody else? Okay. Let me know if you are interested. Go ahead, Robert.

ROBERT MARTIN-LEGENE: Hi. This is Robert from PCH. Ben and I agree that you might not be correct. But the whiteboard, again, about the pre-publish. Well the thing is when you pre-publish the KSK, you have a signature set on the DNS key resource record set, and that might be cached somewhere. And that's where you might actually experience problems.

But if nobody picked it up, that's good. My question was during this exercise of rolling the keys, were you consulting any of the RFC out for DNSsec best practice or something about how to do the timers and everything? There's an RFC out about how to do DNSsec. And that also, they also have some sections about how to actually perform this operation. Were you consulting that for how long to wait before each step and stuff like that?

ALAIN AINA: Yeah, definitely as I said. Managing the timing in DNSsec is very critical. So yeah, we did look at the RFC and also some

documentation of [inaudible] someone also did something like this and published some resources, but we – yes, as I said. Because this we need to keep the chain of trust [inaudible] the trust then we had to really look at our policies, sign in policy, the timing, and design the system to match our need exactly. But yes, we did use the best practices from the RFC. Yeah.

[BEN]: [Ben] [inaudible] Labs. Well one of the maintainer of OpenDNSSEC. So thank you very much for this presentation, sharing your experience. We always eager to learn about the good, the bad, and the ugly. This kind of feedback is very useful, and also what could be improved, of course.

What I. So about the timing indeed, so [inaudible] I'm curious to know. I think it's better to be one-on-one. What's your [inaudible]? What's your policies? The OpenDNSSEC 2.0 is near or a public release, and there you have more flexible way of specifying your policies and enforcing these policies on the key rollover.

ALAIN AINA: So yes, there is I saw on the [inaudible] second slide, we published some information about this on AFRINIC blog, the [inaudible] we have, if you, on the first link that direct you to a

DNSsec at AFRINIC where you could see the DPS, and the second line URL take you to the block. But if you need more information, we can, yeah, I can, yeah.

DAN YORK: Geoff, I saw you.

GEOFF HUSTON: Yeah. I think you'll find that RFC 6781 is the document you're looking for. And indeed, if you look at it 6781, it actually analyzes a whole bunch of ways in which you can do this key rollover. Basically, if you do double signing and do a period where both keys are active, you increase the size of the zone, you increase the size of responses. That may increase the size of your DNS responses that may be a problem.

You can do this in a staged way that doesn't involve double signing, but there are compromises, as well. It's not for the faint of heart. 6781 is written for folk who understand DNSsec. But if you're going to start rolling keys, you probably need to understand DNSsec. So 6781 is really compulsory reading. Don't roll your keys until you understand the RFC, and then you'll be fine. Thanks.

ALAIN AINA: Thank you, Geoff.

DAN YORK: Are there other questions for us?

RUSS MUNDY: Thanks, Dan. Thanks, Alain. Very useful presentation. Two questions. One, earlier in the African Regional Panel, there was a fair bit of discussion about the slowness of uptake of validation and actual use of the signed zones. And I was curious if you had established any way of measuring or in some way collecting data with respect to at least close to end users? And how you examined whether or not there were breakages or slowdowns or if there were problems with response sizes. In sort of the predominant areas, which these zones are used, could you talk a little bit about what you did in that area?

ALAIN AINA: Are you talking about during this key rollover or in general? No.

RUSS MUNDY: During the key rollover in particular, if there were measurements you looked or various places you worked with to collect data.

ALAIN AINA: Yeah, okay. During this key rollover, we, okay, we used the DNS [inaudible] most of the time, but also some resolver from, for example, I did this remotely. So I was in Togo, then I was following this using my resolver in Togo, then our operation is in South Africa. Then we also had a view from Mauritius plus what we got from DNS view. So this is how we follow this key rollover to make sure that we nothing, yeah, nothing break. Yeah. Nothing break.

RUSS MUNDY: Great, thank you. And you'll hear this again probably from Dan and I later on. Measurement, measurement, measurement, collect data, because that's really important. We don't have that much data and we really want to have more collected.

ALAIN AINA: Yeah, yeah, no. Definitely.

DAN YORK: And I would also just echo, I'll channel my inner Julie and ask that people do say their names and affiliations when they do speak at the microphone for the folks who are there. And with that, I'm going to turn it to the person next to me. Go ahead.

WAFA DAHMANI ZAAFOURI: Wafa from Tunisia. I just wanted to say a comment for Alain. You know, Alain, thanks to your support and the support of AFRINIC today to [inaudible] assign it, so it's a sense [inaudible]. But we have to do other work further, the steps after. We have now to sign all the zones and we have many work with the registrars. I just want to add something. You are one of the best DNSsec trainer ever.

ALAIN AINA: Can I comment on a comment?

DAN YORK: Sure.

ALAIN AINA: No, no, no. [inaudible] she worked for ATI and ATI is [inaudible]. If you look at the statistic from the reverse zone at AFRINIC, ATI and [inaudible] added two people who have signed and then pushed the DS to turn to [inaudible] and they really helped me to show to see what AFRINIC that I was doing something.

DAN YORK: Anyone else? Behind me? Anybody? Okay. All right. I want to say thank you, Alain, for bringing this kind of example. One of the things we've often asked about. And I'll put a tip out there, for

the next session at ICANN 56, we're always looking for these kind of case studies or things that people talk about what did they do. What would they have done differently? What would they do? How would they make that work?

So please, if you're doing this, and you would like to come and present and talk, you can see that we don't ask too tough questions. We don't eat people alive. Some of us might, but we really appreciate this. So thank you, Alain.

Next up, we have a new presenter among us, who we're glad to have here to speak. Many of us have been aware that CloudFlare made big waves over the past year by announcing that they were going to enable signing for their millions of domains that were there. And Olafur, who is often here, but sometimes is – he also has – but he's often here.

He's come and talked to us before about what they were going to do and the steps they were going to make and Olafur and Jacques, who's sitting over, or was over here. Where's Jacques? Oh, he also left. All right, well so the people left. They've been working on how to automate some of that but Dani Grant is here to talk to us about what CloudFlare has been doing, and how to do large scale DNSsec signing for millions of domains. So here you are.

DANI GRANT: Hi, everyone. I'm Dani, I am the Product Manager of DNS. That's like so much of your ego you have to lower. Okay. I'm the Product Manager of DNSsec CloudFlare. CloudFlare is authoritative for about 4 million domains. Every day we answer 43 billion DNS queries across 76 locations. And about four months ago, we launched DNSsec for any domain for free.

At our scale, this was a challenge. We had to be very creative in our implementation, and I want to share with you the steps that we took to make universal DNSsec happen. Next slide. Namely, how we chose our signature algorithm, how we save compute cycles on negative answers, and what we're learning about registrar and registry support for the protocol. Next slide and the next one.

CloudFlare's core competency is DDoS mitigation. CloudFlare often mitigates attacks as large as 400 million packets per second. For reference, the attack on L-root in November was only 5 million packets per second, so 1/80th of the size.

One way that attackers DDoS websites is by repeatedly doing DNS queries that have small query sizes but large answers. The attackers then spoof their IP addresses so that these large answers are sent to the server that they are attacking. Go back.

Zones with DNSsec, because of some of these answer sizes, are usually ripe for this type of abuse. Just last month, Akamai

published a security report about how some of their .gov domains are being used for this type of amplification attack. Imagine if every domain with DNSsec on CloudFlare could be used for this type of amplification, we would essentially be making ourselves a target.

So for this reason, we took precaution, next slide, to make sure that every DNS answer we send fits into a packet that is under 512 bytes, even with DNSsec. One of the key ways that we do this is by using the Elliptic Curve Signature Algorithm, ECDSA, which is DNSsec algorithm 13, which lets us use small keys and smaller signatures. Next slide.

There is a Dutch mathematician, Ajren Lenstra, who famously talks about cryptography in terms of energy. He takes the amount of energy required to break a cryptographic cipher and compares that with the amount of water that energy could boil. Next slide.

So to break a 228-bit RSA key, it takes about the amount of energy to boil a teaspoon of water. Compare that with, next slide, an ECDSA key, the same size ECDSA key. To break that would take enough energy to boil all the water on earth. So using ECDSA allows us to use smaller keys with similar security. So we use a 256-bit ECDSA key, which is equivalent in strength

with a 3,100-bit RSA key. Most RSA keys are 1,024 or 2,048 bits. Next slide.

So you can see what that does for our packet size. Next slide. There's another benefit to ECDSA, which is that it's fast. CloudFlare now generates 57 billion signatures a day, so care a lot about the cost of computing. Next slide.

So we thought ECDSA was fast and then one of our engineers, Vlas Krasnov, implemented it natively in Go and got a speed up of 21 times. This is actually now part of the Go crypto library as of Go 1.6, and now takes CloudFlare a split of a second, literally 0.0001 of a second to sign a DNS record. Cool, next slide.

Okay, negative answers. Next slide. There are two problems with negative answers. The first is that it requires the authoritative server to return the previous and next name. For CloudFlare, this is computationally expensive and it can leak information about a zone. The second problem is that it requires two [NSEC] records and two subsequent signatures to authenticate the nonexistence of one missing name.

So I'll talk first about the previous and next name. Here's a little bit of background on our DNS. CloudFlare uses a custom DNS server written in Go called RRDNS that actually stands for Ray Ray DNS after Ray Bejjani, who was a Systems Engineer at CloudFlare and one of the original engineers on the project.

I'm going too fast, apparently. What's unique about RRDNS is that there's no concept of a zone file. Instead.

DAN YORK: Dani, if it helps you. I have the same exact problem. Okay? And when I started going out here, people just told me, "Dan, kick it back a lot." So no worries. You're in good company.

DANI GRANT: I've been challenged to go even faster. Okay. Okay, okay. So RRDNS. What's unique about our DNS server is that we have no concept of a zone file. Instead, what we have is a SQL database that is flat, and holds all of the DNS records for every zone on CloudFlare. When we receive a DNS query for record, then we just go to the database and we pick out the record that we need.

Another unique aspect of RRDNS is that a lot of our business logic is handled in the DNS. CloudFlare often dynamically generates answers on the fly, so we don't always know how we are going to respond before we do. Next slide.

Another problem – okay. Traditionally with negative answers, the authoritative server needs to return the previous and next name. For CloudFlare, without full view of the zone file, we would have to ask the data to do a sorted search just to find the previous and next names. And with our dynamic answers, it

would be so difficult for us to know even what the previous and next names would be without previously computing all of the possible outputs.

The second problem with previous and next name is that it can expose zone information. It exposes what names exist on a zone. The common solution to this is NSEC3, but even that can be cracked with a dictionary attack. Next slide.

There is a proposed solution to previous and next names, which is RFC 4470, dubbed White Lies. White Lies says, “Ah, DNS operators can randomly generate the previous and next names by finding something that’s just canonically slightly before and after the missing name.” So this is great. This helps prevent zone walking and prevents the extra database lookups. But still, it’s two separately signed NSEC records to say one thing. Next slide.

At CloudFlare we decided to take lying to its fullest extent. Instead of White Lies, CloudFlare does Black Lies. Here’s an example of what we do for no data. When the name does exist but not in the type asked for, we say, “Oh, every type does exist, just not the type you asked for.” So if you asked for TXT, we say, “Yes, oh, you have such bad luck. We have every single type, just not TXT.” And then when you ask for MX, we’ll say, “You missed it again. We have every single type, including TXT, but not just MX.” Next slide.

This is what this does to our packet size. So our negative answers are at about 300 bytes. For comparison, the negative answers for IETF.org and ICANN.org, the first uses NSEC and the latter uses NSEC3, are a little bit over 1,000 bytes, so we are 1/3 of the packet size, which is really neat. It also saves us the database lookups and especially since so many attacks are just feeding off of random negative answers, this is very computationally efficient for us. Next slide.

Okay. Beyond the technical challenges of DNSsec, one major consideration for a large scale DNSsec deployment is the support cost of having to explain to registrants why sometimes they can't go and add their DS at the registrar if the registrar or registry has not added support for DNSsec or Algorithm 13, which is our signature algorithm choice. Next slide. Next one.

I want to show you some of the things that registrars are – okay. So often, this is what's kind of interesting here. So often, when the users go to their registrars, they're kind of met with support teams that have never heard of DNSsec or give them incorrect information. So what I want to do is show you some of that incorrect information that our users receive from the registrars.

So this first one is from a very large registrar. And there's some confusion here about who can add the DS. The registrar tells our user, "In order to enable the DNSsec, the domain name must be

under the registrar's DNS management, which means the domain will need to be moved to our servers. The changes have not been completed and this request has been closed." This, of course, is not correct. They can add the DS even if the user is using third party name servers. Next slide.

Here's another one. A user told us, "I talked to support at the registrar and they said that I would need to enter the DS record with you since my DNS is hosted here." Again, this is not correct. The next one is my favorite.

This is a chat with a registrar. The registrar support says, "The DNSsec option is not yet operational. We still don't provide support for it." And the registrant clarifies, "So if I add my DS record and it says, 'DNSsec active,' DNSsec won't really be active?" And support says, "Exactly."

We've had customers who have been sent PDFs to fill out to get a DS record added. One customer was even sent a Perl script to run, which was great. But this is kind of the state of the world. Next slide.

There are also really good cases. Tons of registrars and registries have added support for DNSsec or for Algorithm 13 since we've launched. Next slide.

.no is even incentivizing DNSsec support for registrars by providing a discount on signed domains. So this is a huge inefficiency and this manual copy and paste of the DS into a registrar's portal is something that can and should be automated. We at CloudFlare would love to be able to send DS records automatically to the registrar or registry, but ICANN rules are really strict about which organizations can talk to which other organizations and domain names. So a registrar can talk to a registry, but a DNS operator like CloudFlare cannot. Go down two slides.

Alongside Rightside, Sara, and Red Hat, we've published an Internet draft proposing a way to automate DS, to automate sending DS to registrars and registries. Already a few registrars and registries are onboard, which means by next year, we'll be able to enable DNSsec automatically for a few hundred thousand domains. Next slide.

Are there any questions?

DAN YORK: I suspect there will be. Not least of which maybe from the translators trying to figure out. But no, I see a queue going on here, and Julie is telling me, what, we've got remote? Okay, well I saw [Dmitry] first largely because he's sitting next to Dani, so go ahead, Dmitry.

DMITRY: Well I must be lucky. Well first of all, a comment then. In UAV implemented 13 actually we had a test [inaudible] in CloudFlare [inaudible] the feature was launched thanks to Martin Levy, who supported that. It's a test URL, we can even test it. If you want accent dash dash MQA [inaudible].

But the second comment that in order is one more thing, which again, using my privilege, I can show you that on the screen. You can look at this right here. This is [inaudible] interface. Well, as you cannot see, but I can provide you [inaudible] copy to anybody who wants. The dropdown of the S type record in [inaudible] management database does not have the type 13. It has three, five, six, seven, eight, and ten. So if one hand knows that, another one doesn't, and actually spoke to Kim Davis about that I think at least two years ago.

Anyway, still pending implementation. Maybe the new contract would include that feature.

DAN YORK: Standby for the talk at 1:15, where we talk about all [inaudible].

[DMITRY]: Yeah. I'm sure it will be resolved once. That's pretty much it. And thanks for excellent work.

DAN YORK: Okay. Remote. Want to go to the remote?

JULIE HEDLUND: Yeah. This is Julie Hedlund from ICANN staff reading a remote question, and I'll just remind everybody here. Please do state your name and also your affiliation when you're speaking. This is a question from Marcus from Global Village. He says, "I understand that elliptic crypto algorithms are vulnerable to quantum computing attacks, if quantum computers are to become a reality, whereas RSA algs are not. Do you consider that a problem?"

DANI GRANT: If quantum computers are to become a reality.

DAN YORK: If we would have one to test. I mean, we're having going to have a session this afternoon talking about elliptic curve cryptography in specific, so I would encourage the gentleman to hang on and listen to that because we'll be talking about this,

and he can raise that question certainly then. Olafur, you want to answer?

OLAFUR GUOMUNDSSON: RSA is also vulnerable.

DAN YORK: Yeah, okay. I've seen Lars over here and I saw Mark down there, and Robert, too. Okay. So Lars, oh. But you don't go remote. So in the meantime, let me jump to Robert. Oh, okay. Go ahead.

LARS-JOHAN LIMAN: I can use this. I'm Lars Liman from Netnod. I was a bit curious about the Black Lies, and I should probably talk to Olafur offline. But if you lie yb leaving out the exact record type that's asked for, is there any risk that the client catches that information?

DANI GRANT: Negative answers have the lowest TTL value possible for that reason. There's also the way that we justify it is the zone could have changed in the amount of time between which you asked.

DAN YORK: Loosely coherent. Okay. Mark.

MARK ELKINS: Yeah. I love those Black Lies. The case where you put a DS record into the zone and it says, "DNSsec signed yes," but it's not. That actually exactly what we do at [inaudible] and that's simply because you can put the DS key in, DS records in, and yes, it's not signed. And that's really what is happening.

DANI GRANT: That's interesting. I think best case is you add the DS, it gets propagated to the parent, and everything is signed. Best case.

DAN YORK: Okay. I've got Robert.

ROBERT MARTIN-LEGENE: Yeah. This is Robert from PCH. I like that you use elliptic curve because nobody else seems to be doing a lot of that. Do you have any idea about how much, if anyone actually has problems validating that? Do you have kind of measuring that?

DAN YORK: Standby for the 1:15 talk from Geoff Huston.

DANI GRANT: I can give a quick answer to that. When we started developing on DNSsec Algorithm 13, there was one resolver that still did not

have support, but since then, Google Public DNS has added support.

ROBERT MARTIN-LEGENE: Okay. One more comment. One more comment about the Black Lies. Maybe you should call it Spooky Lies because that is freaking us out a bit, I think.

DANI GRANT: We have a suggestion box in our office.

DAN YORK: Okay. We have a remote.

JULIE HEDLUND: Thank you, Dan. This is a remote question from Antoine [inaudible]. He [inaudible], he lists it as a comment but it actually ends in a question. It says, "DNS operators not being able to talk to registries is not only a technical issue but a mistake on ICANN's model and ICANN's model. What is being done to convince the ICANN community to change the model to increase security and stability?"

DANI GRANT: Okay. On the comment, yes, we agree. And the answer to the question, what is being done? Is proof of concept. So right now, we're working with a few registries and a few registrars to adopt this Internet draft, and then I think the only way forward is to show that it works and that it's safe.

DAN YORK: Other question. Olafur?

OLAFUR GUOMUNDSSON: This is Olafur Guomundsson from CloudFlare. We are doing these experiments and proof of concepts in ccTLDs and we would be happy to work with any ccTLDs to show this as it works and it works well, so talk to us afterwards or send us e-mail later.

DAN YORK: Okay, over here.

UNIDENTIFIED MALE: [inaudible] .dk. [inaudible] in Dublin on your talk there, and since then, we did change our [inaudible] so are allowed to talk to us directly. I'm now working on Algorithm 13. Standby.

DAN YORK: I saw Geoff down there.

JULIE HEDLUND: We have a roving mic for those who don't have mics. It's probably not a good idea to [inaudible] break, you know.

DAN YORK: Geoff, I'm sorry. No?

GEOFF HUSTON: No.

DAN YORK: Okay. Anyone else? Well I would like to thank you, Dani. This is fascinating on this, and we've been a fan, I think, of CloudFlare's efforts to push on this on a couple of levels. One is getting more of the large scale CDNs and hosting providers to do this, and also for the push on elliptic curve. So it's a huge step forward on that. So thank you for all this and thank you for presenting.

So somehow, we seem to have done something, which is interesting. It might be because of – maybe it was Dani's speed. It might have been. We're actually running ten minutes ahead of time, which is okay because we have much longer to walk to the – oh, no. Julie's saying something.

JULIE HEDLUND: Well given that our lunch is scheduled at noon, the ushers will be expecting us to be going over at noon. But I will also note. As some of you have noticed, there was a sort of a lunch set up that was going on in this room that was not meant to be. It's meant to be in a different room. They all sort of have similar names around here. So we have taken care of that. We are very definitely in [inaudible], which is a much more comfortable and nice place to have lunch.

DAN YORK: Okay. So I'm going to get up here and talk. All right. Handheld, yep, oh, okay, good. Check, one two. So you all get to experience this grand thing. There are papers coming around. What is a piece of paper? Yes. You might need to have a pen. There are these old concepts. I realize we're in the electronic age, but somebody gave these out. How long did it take you, by the way, to figure out that the pen that was in the bag was also a flashlight? Also. Okay. Oh, you mean it's a pen, oh, yes. Here, we're in luck, you could do that. Oh, it's a pen.

Oh, man. All right. So here's the deal. We have a little bit of fun here, and for people who are new to this, this is the DNSsec quiz. It's actually great, we call it the great DNSsec quiz, but some of this relates to DNS, as well. So you all will have a nice piece of paper, and what you're going to do.

The reason why we have a name slot on here is to prevent cheating. We have you fill it out and then give it to a person next to you for correcting. Okay? All right. We want to get through this so we can go to lunch, so one. All right.

So these questions are not mine. Okay. So Roy Arends from Nominet. No, no, no, no, no. Roy Arends from ICANN. Sorry, Roy was a Nominet employee for a long time coming to these things and doing this stuff, so he has recently shifted to ICANN, where recently as a couple of meetings ago or whatever, but anyway.

And Paul Wouters also did some of these and Warren did some of these and other people did some of these. So here we go with what Roy has done. So you'll get an answer or a question that's posed up here. I will warn you that in some cases, there may be multiple answers. Okay? Multiple correct answers. And yes, when we go back to it, we can dispute these, but in the event of a dispute, I'm right.

Oh, here we go. Use the back. Oh, no. Use the form. You could form a group or play on your own. Put your name on the form. Yeah, okay, we're going to do that. Okay. Here we go. Sometimes more answers are correct. The points scored for each correct answer, no points are scored if there's a wrong answer.

Which of these top-level domains does not deploy DNSsec? Is it A, EC? B, MA? C, TV? D, MX? You can write down on that piece A,

B, C, or D. Yes, this is the level of questions we're getting to, folks who are new. No questions in here.

UNIDENTIFIED MALE: Just to quote Clinton, what does deployment of DNSsec mean?

DAN YORK: Oh, it's signed. Come on. Which one of these is not signed. Okay? All right. What did – that could be part of that. What did TPC and TPC.INT stand for? The Transition Policy Center, the Technical Program Committee, the Transpacific Cable, or The Phone Company? It doesn't relate to DNSsec. It's the DNSsec/DNS. Here's a tip. If you'd like to help improve these questions, Roy would love them for the next one. So if you don't like this, help out.

So and if you have no clue, which INT domain does not currently exist? IPv4.int or IPv6.int, eurofish.int, or cto.int? I don't know where Roy comes up with these from. Okay? Here's an easier one. What does the do bit do stand from in a DNS query? DNSsec off, DNSsec on, DNSsec out, or DNSsec okay? We're not going to dispute these. Go back to the RFCs. All right.

What does 257 indicate in a DNS key record? A, zone key and secure entry point. B, DNSsec zone signing key. C, Algorithm 257. Or D, CCLVII. That could be correct in a DNS context. Okay.

Number six. What are valid NSEC3 hash algorithms? [inaudible] one. [inaudible] 256. [inaudible] 384. Or Ghost R 34.11-94. And there could be multiple answers, remember. Roy, if you're listening. All right. What does the CD bit stand for in a DNS query? Choice A, compact disc. B, checking disabled. C, cryptographic device. Or D, for all the Windows fans out there, and Unix fans and Linux fans and everybody else, change directory. Computer fans, yes.

And I will admit that if I were taking this test, I'm not sure how well I'd do on some of these. But I have the answers. I have some answers. I have Roy's answers. Okay. What does the KSK stand for? Is it the Key Signing Key. The Kill Switch Key. The Key Switch Key. Okay. For the people who are listening remote, it was pointed out that Roy does not say, "What does it mean in DNSsec?" We'll have to –

It is the DNSsec quiz, so the last choice, of course, is Kappa Sigma Kappa, which I think we're talking about. All right. Are we ready? How many different root server addresses are there? Choice A, 12. Choice B, 13. Choice C, 24. Choice D, 26. I see people. I see people looking around. How many DNS root server addresses are there? Not how many nodes are there. How many root addresses are there?

Yeah. No looking on your computers. Okay? Computers closed. No going in there. Come on. No. Which country code top-level domain was the first to deploy DNSsec? A, Puerto Rico. B, Sweden. C, Denmark. D, Germany. And if I know Roy, there's probably some trick related to this. When you say deploy, I'm going to say when it's signed. Okay?

UNIDENTIFIED MALE: Those names are not ccTLDs.

DAN YORK: Okay. So if I read that precisely, notice it says, "Which country with code domain in parenthesis, was the first?" So which country, and actually, if we're honest, Puerto Rico is not a country. So. Okay. How are we doing? Ready? That's it. Make sure you put your name on the form. Oh, did you do that? You just did that. Okay. I was looking at it and I thought I. Thank you. Okay. All right. So remember, you get one point for each correct answer. All right. So, this one, our choices, which of these TLDs does not deploy DNSsec? What's the answer? Eh. Eh. A. Ecuador has not deployed DNSsec.

B, choice B, MA, Morocco. Who's from Morocco here. Yes. February 16th they put their DS in root. Woohoo. Our newest signatory. Yes. Oh, it does. Well but they have their sign, but they

don't have a DS record, right? They don't have a DNS key? They have a DNS key. I've known that. Hey, all right, guys. Come on. We want to get to lunch. There's lunch coming up. All right? So I rule, okay? And so the answer is A. Go figure out digging from somewhere else.

Oh, good, look. They figured out. It does have it. How long have you been working with DNS? Didn't you write some software? Okay. That's Ondrej Sury from, he's done a lot with this. Yeah [inaudible] no excuse there, okay. All right. Come. Okay. Wait we got to get going here, folks, or else we're never going to get the lunch. Okay.

What did TPC and TPC.INT? Does anyone know what? Was anyone around when TPC.INT was? Yeah, okay, all right, okay. Oh, you ran it. Well then what's the answer? What? D. The phone company. I would have got this one wrong, too. Okay? I have no idea about this. This predated me. Okay.

Which INT domain does not currently exist? What do you think? A. What do you think? D? The answer is B, ip6.int does not currently exist. Apparently eurofish.int is real. Blame Roy, okay? Next. What does the do bit stand for? Oh, I can't wait for this one. Answer is? How many people say A? B? C? D? Answer is D. DNSsec okay. Look it up in the RFC if you don't believe me. Okay.

Next choice. All right? What does 257 indicate in a DNS key record? A. Correct. It is in fact that, the zone key and the secure siding point. What are valid NSEC3 hash algorithms? Well. So Roy says only A. Olafur says he's right. I guess well Olafur wrote the RFC on NSEC3, so if Olafur says that, I guess that's pretty definitive. So the answer is A. Could I go back a slide?

Yeah. Okay. But this choice was only A. Yeah. Okay. Let's go on here. Number seven, what does the CD bit stand for in a DNS query? Answer is? What? B. Yes. Checking disabled. That is the correct answer. What does a KSK stand for in DNSsec? What does it stand for? That would be wishing in some other parts of the venue here today, right? Okay. In our venue, there is no such thing. It is the Key Signing Key. Choice A.

All right. How many different root servers are there? I can't wait for this one. C? C? D? All right. How many people think A? All right. How many people think B? How many people think C? Oh, look at. A lot of those. How many people think D? All right. We had a bunch of root signing operators. The RSSAC folks in here. So why is it C? Correct. There are 13 that have IPv4 addresses and only 11 of those have IPv6 addresses. What, Jim?

Oh. So what? So are you telling me the actual answer? So you're telling me the actual answer is 25? Oh, they kept the old one.

LARS-JOHAN LIMAN: Then it would be 27 because [inaudible] is still [inaudible]. Indeed.

DAN YORK: For everybody new here, we are this geeky, yes. Okay. Well so I'm going to go with 24. 24 is correct, and now. Okay, it's 26, right? Because of the. Okay. We're going with Roy's answer, blame Roy, he's not here. It's 24, okay? I'm taking choice C. If you have a dispute, bring it up with Roy. Right, exactly. So which country, which country was the first to deploy DNSsec? Puerto Rico, Sweden, Denmark, or Germany? And I see, I gave it away a bit, okay. What's the answer? B. Sweden.

UNIDENTIFIED MALE: Sorry. Isn't Denmark, Denmark?

DAN YORK: What? Oh, that was an attempt at a joke, got it. Okay. All right. Let's go back. So how many people, let's start out with this. How many people, add them all up, we should have a total of ten points this time. Actually, we did not have any multiple answers. Roy was slacking a little bit. Okay. Okay. Let's go quickly because we want to get to lunch. So how many people got one right? Or only one right? No, no. Let's start at the top. Anybody.

No, I don't want to start at the top. Let's start at five. How many people got five right? At least five. At least five. How many people got six right? Seven? Eight? Nine? I guess we have a tie between Ondrej and Olafur. Well all right. Well thank you, everyone. We will thank Roy for doing this, and if you would like to help with the next quiz, we're looking for people to help with that, as well. Roy loves input.

Okay, with that, we need to head over to lunch. Julie?

JULIE HEDLUND: Yeah. So just a reminder again, bring your tickets. You need a ticket for lunch. There is actually only one entrance into the lunch area. Well the other three sides are surrounded by water, so I suppose you could swim, but then your ticket would get kind of wet and probably wouldn't be legible.

DAN YORK: And if you did not get a ticket, if you came later and did not get one, but you want to join us for lunch, you can see Andrew and there are a few more.

JULIE HEDLUND: But ideally, you should have been here all the whole time since this morning so that you earned lunch. So do follow the map on

the other side of your ticket, and there will also be ushers, but at any rate, good luck. We'll see you soon.

DAN YORK: Just a note. This room will not be locked, so you probably do want to bring your gear with you, etc.

As the crowds rejoice over there as Paul says I don't need my sweater, so this is good. So panelists, which would be who? Dan, that's me. Geoff Huston, Jim Galvin, Olafur, and Ondrej. Why don't you come up here and sit in the front? So if you want to sit, you can either sit next to me, Olafur, or you can sit over there. But I'm looking for, yeah, sit over there because then we can.

Julie's next to Kathy, but then who's down there? I don't know. Well Eberhard can move. Yes. And Geoff, if you want to come up here, you can come up here and join us, too. You can sit. There you go. Right wherever that nice bag is. I'm not sure whose that is.

No, no, no. We'll put Ondrej when Ondrej come back. We'll have him sit where Sara was sitting. That's mine, Robert. That's mine, but you can move it if you wish. Well because I'm not going to sit here all this time, but you can move that. That's all good. You get your arms worked out if you do that. You get a nice coat out of

the deal. Oh, you could have sat over there. We didn't know who it was, so we kicked you out.

All right. Good afternoon for the afternoon session here at the DNSsec Workshop. As we're all filing back in. If you are sitting in a chair against the wall or at the other place, you are welcome to come and join us at the table. You are welcome. You can do that. The side benefit of joining at the table is that you get a plug that you can be able to use, if you'd like, for power. You also get nice little microphones like this one that you can use if you wish to weigh in on the kind of issues that are here.

Although I'm told by my fellow panelists that we will have a fight between the two large gentlemen to my left here. And given that they are both very tall, large men, this could be interesting. We might put them in the middle here, give them each a chainsaw, and see what happens.

Warren will start to take bets. Okay. I'm not sure if – do we have anybody from Morocco who could tell us? Are chainsaws allowed here? Is combat? No. Swords, maybe. I don't know. What do we? I'm not sure. Daggers. Daggers, yes. We'll go down to the sook and see what we can pick up. Okay.

Seriously. Thank you all for coming here. We also want to give a big round of applause and thanks to Afilias, Sara, SIDN. No, I said Sara. Afilias, Sara, SIDN, Dyn. Dyn. I should parity thank Kyle York

at Dyn, who was the one who arranged, who did all that. He is their Chief Marketing Officer, etc. there and so he arranged that. But no relation to me, even though we're both in New Hampshire. Strange world. Here we go.

I'm just waiting for slides to come up in the Adobe room. Okay. We are all good. So I want to begin this session. This session is all about DNSsec and elliptic curve cryptography, and we've got a couple of different pieces around here. And I see the fight that we're going to talk about a little bit here. And some of this, I'm going to just set up a little bit and actually Dani Grant did a little bit of that in the beginning. So let's go to the first slide.

The reasons what we use DNSsec algorithms for, because I know we have some folks who are newer in here, as we think about them, as we use them to generate the keys for signing, we use them in DNS signatures, we use them in the DS records to create the global chain of trust, and we use them in validation. These are the points that we have to touch when we look at changing DNSsec algorithms. Next slide.

So if we look at the current IANA registry, there's a whole range of existing algorithms. As Geoff Huston may get into when he talks about a very small percentage of these are actually used. In fact, it's really only just a very small percentage that are actually

used. But these are these algorithms that are available now. Next slide, please.

There are two that are newer in the, and if you extend the definition of newer to go back about five years, or six years, I guess, if we are close to that, the two being ECDSA and Ghost. Now ECDSA had very little adoption until about four months ago, when CloudFlare turned it on and lit it up for their records that were there. But next slide. We're going to talk about the other ones in a moment.

So the reasons we care about them are some of what Dani talked about earlier. Faster, conceivably much faster in the signing and conceivably in the validation. It depends and we can have arguments about which ones. Smaller keys and signatures. And better cryptography. And I'll mention this last one is a particular pain point for me.

Part of you know that my charge with the Internet Society is to help accelerate the adoption of DNSsec and work on the advocacy side of trying to get people to use it. And one particular pain point we have right now is that there's a significant part of the security community that is looking at how do we move away from 1,024-bit RSA keys.

And in particular ,the browser, the Web browser community is looking at turning off all support of TLS certificates that are less

than 2,048 bits of RSA. Now we can argue with the Web browser community the way we do things is different, we have three-month ZSKs or one month ZSKs or other things like this. We can have arguments about why it's okay, but at the end of the day, there's a public perception that says 1,024-bit RSA is super bad, get rid of it, be gone. And from a security point of view, that's the argument that's made.

So for just evolving past that to making a more secure, more trusted DNS and DNSsec, we want to move away from those keys, and elliptic curve is currently the way we're looking on that. Next slide, please.

As we mentioned, there are these aspects that we get into with deploying new algorithms. We have to think about validation, we have to think about signing and the DNS hosting operators that do that. We have to think about the registries and accepting DS records. We have to do the registrars, developers, all of those. Next slide, please.

On the validation side, we've looked at this and said that the resolvers have to be updated with the new algorithms in order to perform validation. So as we look at rolling out new ones, we have to get that out into all of that software out there. We've heard already about libraries that were not updated, that don't have this. How do you go and do this?

One other piece that we've identified in the past, too, is that RFC 4035 clearly says that if the resolver doesn't support any of the algorithms, it should treat the zone as if it was unsigned. Some implementations will do that. And so effectively, just because we're using DNSsec with a different and more secure algorithm, we wind up with the zone being treated as if it were not secured by DNSsec at all. Next slide, please.

On the signing side, the software on the authoritative servers needs updates, of course. You can see the other pieces here. We have to update this, we have to go and change this. There can be impacts while we go through the role from one algorithm to another. There is some period of time. Next slide, please.

The registries, as we see here. Some only accept DS records with certain algorithms. We also ran into this challenge that we don't know, programmatically, what algorithms registries will accept. There's no way to know what algorithms they'll necessarily do when you're submitting keys in certain ways. One suggestion that we've had is the bullet item up here. I don't need – I'll read it since I'm here for the remote, but update the EPP feed. Is there some way we can go and update that?

There's also the ongoing question of why do registries need to check the algorithm type? And we've had some debates about

that in the past. Next slide, please. And we can get into discussions about that, but anyway.

The registrars, some of them have Web interfaces that they only accept certain algorithms. Here was the example of one registrar, which shall remain nameless, but might be Warren's employer. Okay. There was a, in all seriousness, this is Google Domains, they did the right thing. Here they were before somebody asked for ECDSA, there was just a list of a few algorithms, and then next slide.

After that, they had a whole bunch of algorithms in there. You'll also notice that they put the numbers next to the algorithms in this interface, which is another little bit of curiosity because we get cases where DNS hosting operators will generate DS records. And if the guy who wrote the DS records spec, blame him on the.

Anyway, they'll supply it to you with a number, but not the algorithm, and other ones will supply you the algorithm, but not the number. And so registrars, the smartest way to do it is to show both to make it less confusing for people. Longer discussion, which I know Olafur, Jacques, and others are looking at ways to get the user kind of out of the space of having to enter this in.

But anyway. Next step. So we, again, we've gone through this why do registrars need to do this. They should just accept the DS

records, but we know, we've had this discussion around it comes down to user interfaces, wanting to check to reduce support issues, all of those kind of questions. Next slide.

So with developers, the challenge, of course, is that if you tell somebody, if you give people a list of things to check, developers have been told to check boundaries, to check lists. So if it's not on a list, hey, go, do it. The challenge, of course, is that many times, as software gets written and they never update it when there are new additions to the algorithms. So as we look at adding new algorithms to the IANA list, many of the software out there that checks for the existing algorithms is not going to update that list until at some point we go and ask them.

So next slide. These are just kind of setting the stage for this discussion as we look at how do we add in new algorithms. How do we bring this about? We need to look at how do we help people understand? How do we help promote the value of these new algorithms? And how do we go and start making these changes take effect? And that's part of what we will be talking about here and coming out of here, this panel, as we talk about elliptic curve.

We want to go and see what we have to do to make this happen, to roll out an even more secure DNSsec. I think that's it for me. I

think I was going to suggest that Geoff talk a bit about what he has seen in the way of DNSsec next.

And if you have questions along the way, if there are specific points for the person presenting, please feel free to ask them and raise them. If there are longer questions, maybe we can wait until the panel is done. But if there's a specific clarifying question, we're glad to do it.

GEOFF HUSTON: No questions? Okay. I'll begin then. I'm Geoff Huston, I work in APNIC. I do a huge amount of work in measurement. And one of the aspects of measurement is actually measurement of DNSsec. And in this case, I want to look at the level of support in ECDSA on the resolver side. So I'm not looking at what algorithm you use to sign the zones and so on. That's not what I'm looking at.

I'm looking at resolvers. If you sign your zone with ECDSA P-256, which is crypto algorithm number 13, will folk be able to actually use that algorithm and figure out whether that zone is secure? Next slide.

So the beauty about this is as we've heard this morning, we're being told, and I have no reason not to believe it, the strength of ECC lies in the fact there's more computation and less bits. So I haven't done the drop of water plan out the size of the earth

business, but as far as I can see and been told, 256 bits of ECC is equivalent of 3,072 bits of RSA. It's certainly more dense in terms of its cryptographic capability.

This is important in the DNS because the original DNS specification said that once a DNS response gets over 512 bytes of payload, all bets are off. Now we go puh, we can do more than that. But interestingly, once you get up over 1,000 octets and head towards that magic number of 1,500, some resolvers cannot get the answer. And then you get into the whole issue of once you get over 1,500 octets, fragmentation of UDP occurs. And again, that's its own particular piece of nightmare.

And if you're running v6 and UDP fragmentation, then you have to invoke the deities because nothing else is going to help you. So there are real, real issues with fragmentation response size. So an algorithm that's smaller is preferred, all other things being equal. Next slide.

So here's the kind of example in ECDSA, exactly the same question signed with ECDSA, 527 octets. I'm almost underneath the magic 512, precisely the same thing, RSA 937. And that's pretty typical. Next.

So let's go to it, yeah? Not a problem. But I'm like I can go and sign things in ECDSA, but you're the person who's got to accept my signed zone. And so the real question is if I did this, would

you believe me? And so I'm kind of looking at if I signed using ECDSA, which resolvers will validate that signature? Who's capable of supporting that protocol? Next.

So we use Google Ads to measure the networking from the user side. So the ads are incredibly useful. They're very simple. They do what you normally do. They fetch a URL. Now that URL is kind of special because it has a DNS component and then a Web component. The DNS component is under my control. The name is absolutely unique and each name is used once and only once and Google are very nice. If you do an ad that's incredibly uninspiring and insipid and doesn't generate much revenue, Google give it more and more attention because they really, really, really want to get that ad presented up to get the client's bit of money. So the worse, the ad, the more times the ad gets impressed. Happy Geoff.

So in this case, what the ad does is have a tiny script inside that fetches five URLs. Totally unique name so every single time a user tries to resolve this, those queries hit my authority of name servers. I have a number of them over the globe. So as you see there, I'm trying to controls with tests. So the absolute control is no DNSsec signed at all. Can you resolve this name?

Next test, RSA-based signature. Will you get it? Third test, I'm really interested what happens if I give you something that's

deliberately broken. In other words, you should not trust this piece of DNS. The signature does not work. You should accept serve fail and live with it. This will not resolve. And I repeat those two tests using exactly the same mechanism, but this time with ECDSA P-256. Next.

So that's what the ad actually looks like in URL terms. There's some unique stuff up the front, and then there's, if you will, some sort of common labels that I can stitch it all together, and those are the five different URLs. So that's what, if you saw the ad, your browser would silently go and fetch and try and resolve those five distinct domain names in the background. Next.

Now the DNS is, there's the simple view and there's reality. So the simple view is really interesting, really easy. I give you a question, the forward is passed over to the server, the server gives back an answer. Yeah? One query, one response. With DNSsec validation, it's a little bit more work, but it's still simple, you ask me a question, I send you back a signed answer. You validate that by firstly, maybe the order's different, but you ask for the DS record from the parent, and then you ask for the zone key of the child, the DNS key record.

So what I should see is if you're validating your resolver, I should see those three queries rather than just one. Next. So that's what

I should be seeing, right? I send you this, I should see three queries for each of those three records. Next.

The DNS is a masterpiece of convolution. It is not engineered, it is random crap. Nothing is straightforward when you look at a DNS dump. There's slave farms, there's servers, there's replication of queries. Anything that could possibly happen will happen. There are probably query loops there, but they're still looping because there's no TTL on a query. So maybe half the DNS forwarders isn't talking to the other half of the DNS for whatever reasons. We don't know. So everything has their own independent timings. When you set off a question, the questions just reverberate. Next.

This is a very simple example of this reverberation. I set the client one question and the following five resolvers all asked me questions that I'd sent to the original single client. The first resolver looks to be something operated by that customer's ISP, and the fact that there was an A record, a DNS key query, and then a DS tends to say that it's validating. That next one is Google. And that's a Google slave engine. An A, a DS, DNS key, DS, DS. Didn't like the first DS. So this is a bit weird. There's a second slave two addresses away, 145, which seems to be working in league with the first slave because that's got the two missing DNS keys, hasn't it?

But then a second ISP resolver is also involved and it's asking a bunch of questions, and just for the hell of it, there's another Google resolver asking me for DS record. So unless I actually knew that those three Google addresses were all part of the same brain, that would look really, really weird. And unless I kind of knew those 200 resolvers were part of the same ISP, you'd be wondering what's going on here.

So instead of having three queries and three answers, as you see, there is 12 queries and 12 answers, and it's kind of difficult to understand, but it looks like it's validating. Next. That's a bit of reason, go and look at the slides. The reason why, by the way, there are so many queries, is that this is badly signed. And so when the first resolver, 25522468, sends back, I couldn't do this. It doesn't say I couldn't do this because there's no I couldn't do this in DNSsec.

It simply says, "Me, the server, failed." Which is an implicit message to try some more. And so the user tries Google. Google says, "Well I'm a serve fail," so it gets desperate. It says failure in DNSsec is unpleasant because it causes basically, it's not quite a query storm, but it causes a lot of queries. Next.

So ECDSA. How can we look at how many folk actually do this? The first one is actually really simple, and it's basically statistics. So I count the number of DS and DNS key queries I get for RSA,

and I count the same number of queries I get for ECC. Next. So this worked over 45 days, I tested 765 million people. These ads are amazing. Google get to a lot of people really quickly. So there's 765 million people, 27% with DNSsec validating in RSA. I saw these queries. That's a huge number. V6 would kill for those numbers, literally.

DAN YORK: So Geoff, we do need to keep.

GEOFF HUSTON: Keep going? Okay. ECDSA, 23%, so it's a bit lower. Next. I'm running over time, so I'll go a bit faster. So basically, what it seems that one in five who can do RSA won't do ECDSA. Next.

Now one in five is better than it was. In September 2004, one in three who could do RSA could not do ECDSA. So it looks like we're doing a bit better just based on stats. Next.

So now I'm actually going to go a little bit deeper and see if I can track this through. Next.

What I'm really looking at is that critical query that says, "This is ECDSA." And that comes off the DS record. Next.

So if you look at the words of the ancients. Next.

DAN YORK: Next.

GEOFF HUSTON: I'm still going fast. It's the DS record that's really important. Next.

So now, next, it's really the fact that when I see something in the DS I don't know, I abandon. Next.

So this gets me to the real answer. Using a much deeper level of involvement, one in six clients that use resolvers that support RSA will not support ECDSA. Next.

So that's the summary. Next.

Is it effective?

DAN YORK: You could have left at the summary up there a moment longer.

GEOFF HUSTON: No. That was the summary. Okay. So let me actually go to one thing. If you live in Dominica, 98% failure in ECDSA. That's really bad. If you live in New Zealand, a 70% failure on ECDSA versus RSA. That's really bad. If you live in South Africa, 75% failure. That's really bad.

So while there's a sort of smearing of one in six, it's not uniform, it depends. Next if we've got really to the end. Why is this going on? We're actually able to identify individual resolvers. And what we actually find is that the majority of resolvers that don't support ECDSA are run by telephone companies doing mobile data services.

What it appears is that that particular user sector gets stuff out of the box, takes off the shrink wrap, and turns it on. They have no idea of what's in the box. The resolvers that they run contribute to that failure rate. If we got that industry to actually understand IT, you'd probably have your problems solved. That's all I can say. Thank you.

DAN YORK: Thank you, Geoff.

GEOFF HUSTON: And sorry for running over by 4 minutes and 54 seconds.

DAN YORK: Thank you, Geoff. And that's – yeah. No, that was good that interesting about the telco side of that. Okay, Jim, do you want to talk about the registry side of this?

JIM GALVIN: So, yes. Thank you, Dan. Jim Galvin from Afilias, and where is everyone else here is probably going to be giving you some kind of bad news or news that you wish was different. I guess I'm here to give you some good news, I suppose.

From a registry point of view, we're obviously a critical player in this space for two reasons, and so there's two things to talk about. One is the registries themselves have to be a consumer of the technology. And in that respect, because we sign TLDs, we have to find. these solutions have to be available, but it's important to keep in mind that registries are driven by requirements and those requirements will come from two places. One is standards, which are obviously under development and requirements in that respect. We certainly have a list of valid algorithms.

And the other side of that is from as a registry and as a gTLD in particular, we are a contracted party to ICANN and so there are requirements that come out of policies out of ICANN, unfortunately, that one has to pay attention to. Okay? But outside of that, sometimes.

But all of that is good news. I think that those are all things, which are easily fixed, if you will, or easily made to meet the needs or the requirements of switching algorithms. And as a registry, and in particular for us as a significant registry provider,

and we have a lot of different customers. We're well over 100 now in terms of the TLDs that we support. We have an about need to want to be a generic service provider and provide services across the board.

The other half of the problem or the other half of the space that the registries contribute to is supporting registrants and supporting registrars, especially in the gTLD space. Because, again, you have a set of requirements, you're guided by those things from the ICANN side as a contracted party. There are rules about how things have to work, but we have to allow for registrants who have domain names, who have DNS servers, who want to support other algorithms besides just RSA today, the ability for them to get those DS records up into the TLD zone so that they're available in order for the rest of this, which we're going to find out, doesn't quite work but we'd like to work better to get there.

From our point of view, again, we have the advantage because we want to support a lot of TLDs and a lot of different TLDs. So for us, our restrictions are quite limited in terms of what the registrars required to do. We're willing to take in ourselves any algorithm. We actually will accept any of the valid listed algorithms in the technical standards because there are no requirements on the ICANN side, the policy requirements that restrict that.

There is a somewhat issue in terms of our interoperability with registrars in that we take DS records, not key records. Some registries prefer to take key records from the registrant so that they can turn it into the DS record to put in the TLD zone. So registrars make that an issue. But we just take what you give you and we stick it up there, as long as it is self-consistent and syntactically valid, we don't care. And that's the good news.

There are obviously registries for more focused or maybe singular kinds of TLDs or registry service providers that only support one TLD. They may have a variety of different kinds of restrictions on what they can do, and so they might not want to take the algorithm. But I think that you'll find in the gTLD space, especially for those that support most of them, you're not going to have a lot of those kinds of restrictions, the stuff will work fairly easily and fairly straightforwardly. And that's what works for us.

I think in summary, what I would say is we are driven by external requirements, not technological requirements. As long as the technology is there, we're in a place to support it. Right? But we are driven by standards and what they say should be done. And it's important to keep in mind that as a registry, our spot in this ecosystem is also driven by the policies that we are obligated to by our contractual relationship with ICANN in particular.

I think that all of those kinds of things are solvable problems, so that's the good news. And thus, we want to be a good player and a partner of all this with people. So I'll leave it to the rest of you to make this bad for the community. Thank you.

DAN YORK: All right. Thanks, Jim. So you heard me set the stage for kind of what we have to do to change algorithms. We've heard Geoff talk about the reality of what we're seeing on the validation side, that first part of that. And we've heard Jim say that the registries are, they're willing to do this if there's an external driver, if people go and change that in some way, and now we're going to have Olafur talk a bit about what he's seen in this process, and I should just then say that we're going to wrap it up with Ondrej, talking about, well, hey, this is all interesting, but I've got some new algorithms to get out there, so how do we do that?

And then we want to open this up to questions and to some conversation, and I've got some questions, but I'm looking forward to those from you all, too, so think about that as we go to Olafur now.

OLAFUR GUOMUNDSSON: Thank you, Dan. We had deployed a new DNSsec algorithm earlier this year, sorry, the last year. This has been a long year.

And this is about some of the things we have discovered. I apologize if my talk is not as entertaining as my coworkers, Dani's this morning, and we cannot all live up to her high standards.

DAN YORK: You'll balance each other out in speed, though.

OLAFUR GUOMUNDSSON: I'm trying to be polite to the translators. I got yelled at in Brazil for speaking too fast. Okay. So yeah, next slide.

DAN YORK: [inaudible] next slide.

OLAFUR GUOMUNDSSON: Okay. We are the first ones to do this on a massive scale. We are working very hard to making it others follow our lead because we think this is the right thing for various reasons that others have covered. And but the one big lesson we have taken from all of this is the ICANN registration model, which is copied by many of the TLDs, is broken, because DNS operators do not exist in that model, and they are the ones that should be able to feed this information instead of going through a key registrant channel. Next slide.

Well we can look at the really simplistic view of the DNS, which is probably more complicated than most of the policy people upstairs understand. There are [inaudible] servers that are resolvers and that are clients, and these all work perfectly together and have a big harmony between them. And there are no problems and there are no bugs, and there is absolutely no delay in any updates ever happening, and nobody cares about patents. Next slide.

Many of the systems that people use to publish information into the DNS are based on what is called provision systems. And they are not just the [inaudible] files that people used to use last century. There are all kinds of other ways to do it, and enumerating or finding out all the different hacks that are in use everywhere in the world is impossible.

So when something has to be published in the DNS, it's frequently left up to each enterprise or organization to have them update their own interfaces and tools to publish something new. This does not apply to DNSsec, this applies to new RR types and other stuff. So DNS is becoming, well, you'll see later what it is becoming. Next slide.

Well, Dan has mentioned many of these things, but why are people not using good algorithms like elliptic curve? Well there may be at the registry level a rule that says, "We allow these

algorithms." Where that rule came from? Well they read that list that Dan mentioned earlier. Well, the software that is doing the signing or servicing is not maintained anymore or the provisioning system or the user interface. And there are no developers.

The HSM because some people use HSM, so that is not supporting the new algorithm because the device is old. There may be also national policies that dictate what algorithms are used. Okay. Management of providing resources is a very common thing that we hear. Why is it? One unnamed registry took one year to support Algorithm 13 because of resource exhaustion. I'm not going to name them.

And in full fairness, it is really hard to explain to managers that there's a benefit to do this new things. They will ask, "Will this increase our revenue?" Answer is, "No". "Will this make us look better?" "Maybe." "Will this cause bugs." "Maybe." "Okay. Next topic." And everybody thinks it is not their problem.

Also, we have this interesting deployment problem for new crypto analogy. Assuming there is no patents involved, and we only have to deal with the academic community, agree that this new wonderful crypto technology is okay. I'm giving that about ten years, maybe seven years. There are going to be some eager

beavers who want to jump on the bandwagon earlier, or there may be some others that want to do it later. Okay.

So new algorithm is probably going to be defined, there's going to be ten years until the IETF standards standardizing it. It can show up in software libraries at various times in this, and that's totally independent.

DNSsec adopts it at some later point as the IETF does, could be one month, could be same time, could be few years later. Now we get into the release cycle. Nobody can release any software supporting this until they get the kids like the number 13 or 14 or 15 or whatever the new number is going to be. And, optimistically, for the major software we're looking at the release cycle from OS vendors of more than two years.

If we talk about enterprise software, we're maybe looking at six years. I am still seeing open binary softwares on the net that are red hot three. That was released almost last century, almost. Okay. Then it is the release cycle for all these enterprise level, organization level software. Yeah [inaudible] there is not. It is done when somebody pokes hard enough, long enough, and beats people into submission. Next slide.

So if we have to add the new algorithm, it is all about the advocates to do this one task, motivating the rest of the world to come along. And it's really hard to do it. And we cannot assume

that people know what they're doing, just like [inaudible] said. We have these telcos doing some shrink wrap installation. Do they know what's in there? Do they know that DNSsec validation is even going on in there? We have no idea.

And also, there are going to be lots of people saying this is never going to happen, this is never going to work. But it will. Next slide. So we can get people's attention once in a while. We can't be doing this all the time. So we have to have a really good reason why we introduce new algorithm. Going to much smaller signatures is a good reason. Going to much stronger algorithm is a good reason. Going to even faster algorithm with a same secure or better properties than ones we're using today is also a good reason. So we have to quantify what the reason is.

And more importantly, we have to educate people who are in the DNS industry or operate DNS, it's not status quo. Things will change once in a while. Until we can get cryptographers to invent unbreakable algorithms, we are going to be in this space. If somebody invents quantum computers, I'm going to retire. Next slide.

So there has to be a good reason, like I said, so we should not give out vanity algorithms just because somebody thinks their algorithm is better than Ondrej's or DJB's or whoever. We have to realize what the costs are, we have to retire the old ones, and

it would be really nice if Google removed the option of having the unspecified algorithm number four removed from the user interface.

And we need much better measurements than Geoff is doing and we need to be able to demonstrate that things are actually working. But it's going to be slow. Therefore, we are all working as James [inaudible].

DAN YORK: Is that it? Oh, okay. Well thank you, Olafur. All right, so now that we've heard from Olafur about why these things will take us forever and it'll be a glacially slow pace, and it'll pretty much never happen. Now we're going to have Ondrej tell us why we should make it happen.

OLAFUR GUOMUNDSSON: I don't think we are in disagreement [inaudible].

DAN YORK: Oh, man. I wanted to fight.

ONDREJ SURY: There will be no fight.

DAN YORK: Come on.

ONDREJ SURY: I am Ondrej Sury from cz.nic and I also have two drafts at IETF curdle working for the new curves in DNSsec. Next slide, please.

Sorry for the small letters. I can't see those myself. Anyway, there's a work by Daniel Bernstein, who is infamous in the DNS community because he was one of the people banned from name droppers. But this is kind of revenge for him to introduce his algorithm to DNSsec. So the SafeCurves, if you don't know, it's worked by him and Tanja Lange from some German university, and they basically showed that there's a difference between the [terithical] properties of the curve algorithm and the practical properties. And they might differ.

So they defined another set of requirements for elliptic-curve algorithm to be secure. If you are interested more in that, just look up the page. I'm not security researcher; I'm just security thinker. Just connect the pieces together. So next slide, please.

So there's another set of elliptic curve algorithms. It's Edwards curve this is different properties than ECDSA. So EdDSA has some high performance, not as high as the work in Go and CloudFlare did for ECDSA, but still, it's better than ECDSA algorithms. It doesn't require the unique numbering number for

each signature, which is good. It's most resilient for side channel attacks. It has small public keys for those I'm going to define in DNSsec.

And the formulas are strongly unified, so they are valid for all points on the curve, so there are no exceptions, because the exceptions might reveal some information about private key. And the algorithm is also collision resistant. Next slide, please.

So these are two curves that got adopted by Crypto Forum Research Group at IETF. It's Curve25519 and Curve448, also named Goldilocks. The first one was defined by Daniel Bernstein in 2006, so there was the years from your presentation. So ten years later, it was adopted by IETF, so you're good, we are on track. And it has 128-bit security target, which is roughly as [inaudible] 3K.

And the second curve was even faster because it was defined in 2014 by Mike Hamburg, and it's even stronger. So it's comparable to RSA 15K or something like that, just really high number. Next slide, please.

So there are two drafts for DNSsec, for DNS keys, and both of them. Well I just submitted the second one to you, [inaudible] working group, yesterday, so those slides are not updated. So both of them, they're adopted in the CURDLE Working Group, and for the first one for the ed25519, there is consensus to use in

DNSsec and I think it's almost complete, so please, if you have time, please for review to document.

And it's basically waiting for the drafted using by [inaudible] users and the draft IETF EDDSA. And the second draft was just submitted yesterday. And there's some opponents, well there's one opponent, Paul Hoffman, so if you feel strongly one or another way for using ed448 in DNSsec, please come to the CURDLE Working Group and say so, so we know what to do. Because there are possible options of dropping this.

Well having this as a standalone [inaudible] or just merging those two together. And I don't really care one way or another, but we need to have a decision at the end of the day. And there should be probably also a future draft as [inaudible] also mentioned something that will kill the old algorithm that should not be used anymore like DSA, for example. Next slide, please.

So I think most of it was already mentioned, so I will just say that we will have a similar workshop at the DNS-OARC in Buenos Aires, but well we will invite DNS vendors, as well. And we will continue to talk there. So you're all welcome to come and participate. And yeah, so I think we are basically in agreement before for that it takes a lot of time, so my aim is that when we roll the key in ten years, then the root key, we could perhaps use

this as an algorithm. Well I think that the ten years is optimistic target. Thank you.

DAN YORK: Thank you, Ondrej. And yes, the Russ can appreciate the dig for the next panel. We're going to talk about KSK as far as what timeframe will it actually be. Will it be 2026? Did you hear it here now? So I'd like to open it up for questions and I just would ask one question for Ondrej, when you say the workshop is going to be at DNS-OARC, could you speak a little bit more about that? What are you trying to do?

ONDREJ SURY: Well I'm going to, well, that was my idea and I am almost inviting the people from DNS vendors from the, well, operating system vendors like the Red Hat people, the Red Hat three, and we should talk more about the life cycles of the software, life cycle of the deployments, and I would like to continue the discussion. What can we do to make this faster? Because the [inaudible] people could do it, basically, and there's something wrong with DNS that we couldn't do that.

So I think it's a time to change the paradigm, which we are working on, and it will hurt to change the paradigm, as any paradigm change. But it needs to be done and we need to be

more flexible in terms of the algorithms in DNSsec to, well, make the things work in the future, and it really [inaudible] from the algorithm definition to deployment is really long time, and we need to make this much, much more shorter.

PAUL HOFFMAN: So I can respond briefly to that. So part of the problem is actually completely unrelated to all of this. It's related to the FIPS certifications and the process at NIST. And NIST is aware of this and there is a program that's recently been started to redo the entire method of a FIPS certification works. So with that, you will be able to go much faster in case of allowing your algorithms to be shipped in ROS and sending those updates out.

NIST itself is planning this reversed method of certification will be ready in two years.

DAN YORK: So Paul. So what you're saying is that is NIST the gating factor in getting software into [inaudible]?

PAUL HOFFMAN: Well there were two. There were two. The FIPS certification is one important one because we do send out regular updates on our OSes and we do support them for a long time. So the

updates for new algorithm is actually not a problem for us. So FIPS is the one that's a very important one.

And now I forgot what the other one was. I'll remember at some point.

DAN YORK: Okay. Well I think, and Ondrej, part of your answer, too, right? Is that browser vendors can iterate quicker because they can put up big honking warning signs that say, "Your browser will be out of date unless you might update now." Type of thing and they can do that and users will obey. But we have a harder way to do that with DNS.

ONDREJ SURY: So remember the other one. The other one is that lawyers actually do care, unfortunately. And if you are a big company, then the lawyers really do look at can we get sued or not and how much money is that going to cost?

DAN YORK: Warren, you looked at me funny when I said this. Warren is from Google.

WARREN KUMARI: Warren Kumari, Google. I thought you were going to propose putting out text messages saying, "Your algorithm is out of date. You should roll it soon in the next additional section of all records."

DAN YORK: Can we do that?

WARREN KUMARI: We can.

DAN YORK: Yes. Go for it. Queue is open.

UNIDENTIFIED MALE: Okay. So different topic, just want to, if that's okay. All right. I want to respond to something that Olafur said and sort of repeat it and maybe [inaudible] why it's going to be here, I don't know, we'll see. I think that Olafur and I at least personally are in agreement, but the point here is just to emphasize because I know this workshop and this body has a preference to focus on technical issues. But it is occurring in the ICANN arena and it is important to repeat something, which we have said here before in this workshop and prior meetings, and Olafur has said it down

here in the end, and I just want to tease it out and emphasize it and say a little more about it.

And that is there is really a fundamental issue here in terms of support for anything related to DNSsec. And that is the fact that DNS service providers are not a recognized and separate entity in the ecosystem, at least not in the ICANN arena.

It's easy for me as a registry service provider to say, "Gee, we're the good news. I'm not going to get in your way as far as my organization is concerned." And most registries probably won't, either. There might be some that might, for any interesting legal reasons, just to leverage off the lawyer comment from before.

But even we might be seen as part of the problem to the extent that there are things that DNS service providers need and want that we simply can't provide. I mean, the policies in this ICANN arena simply don't allow them, and it's important to keep that in mind, and it's a driving force in some of the requirements and the ability to deploy these things independent of the technical issues going on.

So thank Olafur for bringing that up again. I just wanted to repeat it. You can look back through prior workshops. You'll see we've covered this particular issue in detail in other places, and see if Olafur wants to add to that. Thank you.

DAN YORK: Apparently not. Okay. So one-sided fight, but Geoff, you can be provocative. So here we go.

GEOFF HUSTON: You're right. Part of this issue, particularly about elliptical curve cryptography, and the real question is why do one in six users sit behind resolvers that don't accept elliptic curve cryptography? Now the observation is that in the world of cryptography, there is an awful lot of monocultures out there. And it's certainly true that a huge amount of software uses the OpenSSL library.

Now the thing about elliptical curve cryptography was that for a period of time, up until I think it was around about early 2000s, maybe mid-2000s, somewhere would know, there was an intellectual property right dispute a company called Certicom over who owned elliptical curve cryptography.

And the doubts about the intellectual property rights certainly prompted a number of distributors of packaged software to leave elliptical curve cryptography out of their package. And so what was going around in the world at that time in maybe it was Red Hat 3, I really don't know, but someone would, that those early versions did not include support for elliptical curve.

Now it's been in OpenSSL for more than ten years now. And we understand that if you got a package now, it would include elliptical curve cryptography. So why do one in six users sort of sit behind braindead things that don't understand it?

Because what's out there is sometimes extremely old. And that combination of the uncertainty over the rights of use of some of this intellectual property, which is a real problem for all of us, coupled with the extremely slow cycles, even after gone through all the standardization, the extremely long cycles of what folk do with their DNS resolvers.

It's certainly true in the operational environment that for many, many ISP operators, turning on a resolver is a once in a lifetime job. After that, they just leave it alone. So what happens is whatever weaknesses were around at the time, stay there and stick there.

DAN YORK: We can ask a question here. So how many people have a home router or a little home Wi-Fi router in their – it's not. What we call a router, okay? But it's not, I know in this audience it's one of those things, right? We all got those little boxes, right? At the edge of our network. Okay. Of those people who put their hands up, how many people have updated the software on it anytime recently? Oh, look at this. We're a really geeky crowd.

Oh, define recently. Okay. Within the last year.

UNIDENTIFIED MALE: Does buying a new one count?

DAN YORK: Buying a new one, okay. Okay. So let's ask another question. All of you probably have failsafe family, okay, who has them in their homes. How many think your family members have updated their software recently? Okay. Well yeah. Okay. You guys are giving them all tourist boxes, right? Okay. Yeah. For the newcomers, these are the cz.nic folks who have their nice little box that's all managed and so they pump down updates automatically and stuff like that. So of course they're going to update everybody.

For people outside of the Czech Republic or outside of Europe, okay? Who don't have tourist boxes, for everyone else, okay. I'm in the wrong crowd to ask that question. Other questions. I saw somebody. Robert. And then I saw Dani and anybody else? Okay.

ROBERT MARTIN-LEGENE: Okay. I'm an anonymous citizen. If you have an old installation of a server that you haven't updated since, well, four years ago,

maybe you don't deserve the validation that it gives if people run ECC.

DAN YORK: The unwashed masses of users don't deserve the extra security is what you're saying. Yeah, I don't think that works, Robert. Okay. Dani.

ROBERT MARTIN-LEGENE: Hey, I'm anonymous.

DAN YORK: Oh, sorry. Whoever you are. Oh, you want to respond?

UNIDENTIFIED MALE: I just want to respond to Geoff's comment that there are no IP intellectual property disputes over the ED algorithms defined in my drafts.

UNIDENTIFIED MALE: The patents expired in 2012, 13, and 14.

UNIDENTIFIED MALE: There you go. People know a lot more about it than me, but I, too, had heard that there are no residual disputes over the use

of this and today, there is, apart from Warren, there is [inaudible] use of it.

UNIDENTIFIED MALE: And I can't even talk about them through e-mail with my lawyers.

DAN YORK: Dani.

DANI GRANT: From the registrar and registry side, what is the reason for doing any validation on the algorithm number?

DAN YORK: Okay. Open religious war one.

UNIDENTIFIED MALE: You give people a list and validate.

DAN YORK: Anybody. Warren, you want to? Okay. I see Warren wants to chime in.

WARREN KUMARI: So it's because users are not always the swiftest, and so, I mean, Google public or the Google registrar end face now has a thing with one, three, blah, blah, blah, the numbers next to it. It's very hard just to get users to understand what those numbers mean. I know a bunch of people said, "Yeah, it's great you added the numbers." A bunch of users have no idea what that is, and when they see 13 ECDSA, they try and paste their ECDSA key 13 times and then become sad.

Or they think that they need 13 copies of it. It's really hard for people to understand. The sort of stuff that show up in these boxes, there's validation, but they have things like yes, please, I would like it, over the long term in the way you have a DS, place to put the DS.

So unfortunately, you need to do some sort of sanity checking, and I guess that it's just sanity checking has gone overboard somewhat.

DANI GRANT: From my take, this is a solvable problem, right? So you could say, in our UI, there's a limited set of choices, but if you use our

API, then you're free to use whatever. So really, the question still stands. You say, "Why should there be any validation at all?"

DAN YORK: Jim. I know you want to chime in.

JIM GALVIN: So yeah, we should separate a couple of issue here, and I think you just teased out one. There are, of this whole set of user interface issues and dealing with the user, and there's a variety of ways of dealing with that issue. From the registry side, I will observe for you that for us, we don't have any particular restrictions on what you do. So we let you do anything as long as it is a valid listed algorithm in the technical standards.

DANI GRANT: That's what I'm asking. Why do you need to validate that?

JIM GALVIN: You know, you're right. From a practical point of view, one really doesn't have to, but we do try to honor and respect the standards. So from our point of view, you should not be allowed to do something, which is not recognized in the community as a valid thing to do. You know, I mean, we don't let you do stupid things, shall we say? We do our best to prevent that. Okay?

So that's one level of wanting to check these kinds of things. We can certainly have a discussion about whether that's a fair thing to do or not at that level. Okay? The other side of, though, is that sometimes, if you are a registry, if you take the key and you're going to create the DS record on behalf of the user, there might be restrictions on what you can do there. All right?

And for that reason, you might have limits on what algorithms you're allowed to use and take from a user, and the relationship there, and you're going to enforce that. And so that's a limitation on that side. That's one of the reasons why we don't take keys, we only take the DSes, and we like to just let all that stuff pass through. We do a sanity check on it because we do happen to believe that that sanity check is appropriate.

DAN YORK: And we get into the situation that give developers a list and they will check it. We have a whole generation of Web developers in particular who have been beaten into their brains that they need to go and do this boundary checking for security.

JIM GALVIN: Okay, but I'm just saying that's the mantra, right? Thou shalt do boundary checking on whatever you can. So if you get a list, you check the list. That's what you do.

DAN YORK: [inaudible].

JIM GALVIN: Well one last thing to add in teasing out these set of validating things. The other thing, sadly, we do have to deal with these kinds of issues is sometimes, a particularly registry operator or maybe a nation state will have their own choices about what algorithms are allowed to use or not. Okay? And, I'm sorry, I mean, as a service provider, we have to honor that, too. We just have to live with those and we can't argue about that. Sorry.

DAN YORK: So I know you want to respond to this and then we do have a question in the chat, and then we'll need to wrap it up, but go for it.

[AARON LANSING]: 16 seconds, yes, I'll try. [Aaron Lansing], Denmark. I want to respond two ways one is we have customer service. So we don't allow customers to do really stupid stuff because that's just going to get us calls. The other thing is that we actually did open a new self-service we just released. We opened up our sanity checking is basically how many numbers did you put in? A to Z,

zero to ten, and it's the right number compared to the algorithm that you just played something along.

The other thing I wanted to say, and I want to [inaudible] on that, and it was from an idea from the [inaudible] with Olafur is that we also add a little button in our self-service that says, "Get my DS record." So then our sales service goes over, over TCP, of course, over the name servers we have in the WHOIS, we have the registry. Gets the key, calculates the DS records and says to the user, "Is this the DS record you want?" and the user just clicks okay, no copy paste.

That's UI. That's because we're a weird registry that actually talks to the registrants, and as operators.

DAN YORK: Very nice, okay. Now I see the question coming in. Go for it.

DANI GRANT: It's actually not question, it's a comment, but comments are also read out for the record. It's from [Antoine Gershwin]. He comments, "Some registries restrict algorithms because they want to be able to exclude old algorithms once they become insecure, not exclude better new algorithms, their goal is not make as much money by registering as many domains as

possible, and we don't care if they're broken. That's your own worry.

These registries may have a different goal like trust, security, and want to manage their domain's public image, and not zone image, but domain. There is no one policy that fits all TLDs, they're not all capitalistic, democratic, communist, or multi-stakeholder, pick your religion. That being said, I do think they should implement new better algorithms faster but there's no bad in disapproving insecure algorithms by the parents.

DAN YORK: Good point from [Antoine] in that it's okay. I mean, one point to restrict and phase out old ones. Okay, quickly. Robert and then Dani.

ROBERT MARTIN-LEGENE: How do you know if I'm?

DAN YORK: Whoever you are. Just look, time [inaudible].

ROBERT MARTIN-LEGENE: I'm not anonymous anymore. Robert from PCH. I'm just wondering if anyone had any experience with actually disallowing certain insecure DS algorithms and what they would

do. Would they just delete and go insecure for the customer or what?

DAN YORK: Yeah. Anybody? Nope.

UNIDENTIFIED MALE: I'll only say that as long as it's on the list. I mean, the IETF should remove it from the list and then we would take it off. I mean, we just feel an obligation to support the standards in that respect. We don't want to be seen as the cryptographers or security police of the world.

ROBERT MARTIN-LEGENE: But then you leave unsigned instead of weakly signed.

UNIDENTIFIED MALE: Okay. I think it's not [inaudible] thanks. I'll just say well that apart from the algorithms for encryption, there's also algorithms for hashing and actually yes, when we do get this type one and type two, in order to do a type one is just delete it, is just drop it. We had one registration that submitted both type two and type three, and I put them both in. I guess it's right thing to do. That's actually not the question I want to raise.

Do we feel like we should do multiple types if that make sense? But this is a long discussion, probably not for this room right now.

DAN YORK: You are absolutely correct because we are out of time and I need to bring up a new panel, but you had a final comment.

DANI GRANT: It's okay.

DAN YORK: It's okay. All right. Well so I don't know that we've resolved any things here, but we've talked about, I think we've talked about what the challenges are. This was good and I heard some good new thoughts out of this. And I think what I would encourage people to do is to look at the drafts that Ondrej has submitted that are out there because this does represent the good path to where we need to go to bring about stronger DNSsec in this regard.

And you've all heard the issues that have been raised here about how we deploy this, and I would love to hear thoughts about what we do. And I'd invite people to think for the next ICANN DNSsec workshop, are there things that we can bring in,

solutions we can bring to go and make this potentially work faster?

And let's talk to Ondrej if you want to be involved with the workshop at DNS-OARC right before Buenos Aires IETF. And with that, let's give a round of applause to the panelists and we'll bring in another panel in here.

RUSS MUNDY: Did anyone leave that jacket right there? Does anybody know that? Does anybody want a gray jacket?

UNIDENTIFIED MALE: It's a really nice one from Washington, D.C., apparently. Men's extra large, five bucks.

UNIDENTIFIED MALE: Hey. Your time's going down.

RUSS MUNDY: Well hopefully someone will claim the jacket here. Continuing our panel discussions, I'm Russ Mundy with the SSAC. Parsons is my employer. And we are going to have the last panel session of the today, talking about the root zone key rollover from a couple of perspectives. The first one, which I'll do shortly, will be related

to what the SSAC itself has published relative to the root key rollover.

Then we will have Geoff Huston tell us about the outputs of a design team that was formed last year, worked for several months, and the report was released Monday. Yeah. I think it was Monday. So it is out, it is publicly available at this point in time. And then Warren Kumari from Google will give us some perspectives of the impact and what some of the end user impact is expected to be from the root key rollover. And Warren is though he's not directly associated with the operation of the big validating Google resolver, is a really smart guy and he knows a lot, and will tell us good things.

UNIDENTIFIED MALE: So make it up on the fly, as people say.

RUSS MUNDY: Okay. So first the SSAC advisories and comments on the root key rollover. Next, please. There actually have been two that are related to it. The first one is SAC 63, it's called the Advisory on DNSsec Key Rollover in the Root Zone. Next.

There were actually a series of discussions that went on within the SSAC for about a year and a half. So the SSAC has considered this a very, very important topic for quite a number of years, and

we wanted to encourage the community to start taking steps even long before the approximate five-year time when the root key was intended to be rollover thereabouts before after at least close to that timeframe. So that's why we started work on this really in 2012, and it was published in 2013.

So in the document itself, it gives several areas of narrative text talking background and what the SSAC viewed as important things to think about and consider as part of this rollover. And the reason I mentioned that the timeframe is as time passes on the real chronological clock, some of the things that are important and that could have big impact will change.

And so from the document or the descriptions that we'll hear in this panel, this is the oldest document published in November 2013. So you can see the general topic areas and I'll just go next to the recommendations.

So the first recommendation is pointed heavily at the ICANN staff and the root zone management partners, who are at least. It is still in place that it is the NTIA, the U.S. Commerce Department, and Verisign, as well as ICANN. So it's three parties that they need to engage very heavily in a communications campaign throughout the world to make sure the world knows that this is going to happen. This is coming, folks, and get ready for whatever you need to do. Next, please.

And again, ICANN staff should lead and encourage and foster the development of testing and test beds to examine impacts of the rollover on middle boxes in particular or other devices that might be heavily impacted by this. There's a real history of DNS response sizes being large enough that some of, especially middle box type of devices tend to fall over, or at least be broken rather badly when these things hit them. Bless you.

So recommendation three is the ICANN staff needs to work closely with the community to figure out how to describe what breakage is and how to describe it. So it is definitely a concern on the part of the SSAC that there will be some problems of some nature caused in conjunction with the rollover. We didn't try to define what they were. We felt that was more appropriate to ask the ICANN staff and the community to generally develop what they were.

But it is something that is important to look at, and that way, if you have more than you're expecting, whatever that might be, you can take certain actions. Next, please.

Then the next, and it's really related to the last one. Should everything, in case things go terribly, horribly wrong. And what does wrong mean or how much breakage is there? You need to be prepared to roll back to the previous state. And you need to have the determination made in advance who would make

those decisions, what would the general parameters be that you'd use to make those decisions.

Because at this point, no one has ever really structured anything except to roll a key forward. And normally, that's all you're really particularly worried about because we've never done a key roll for the itself and so the possibility exists that you might have to roll it back and so all of the structure needs to be put in place in advance and planning to address that.

And then the last recommendation is that you need to collect as much information as possible, and that also includes figuring out what is the sensible information to collect in conjunction with this upcoming rollover so that you'll have at least some basis of data and information to use in comparing when the next rollover occurs. In other words, you need to gather what you need to help you learn and do it better next time.

So those are the five recommendations from the SSAC. So if we can go to the next slide, please. And then in SSAC report 73, we submitted comments on an early draft of public review timeframe draft of the design team report, which Geoff will be talking about shortly. Next, please.

And in there, we mentioned that the design team draft at that point did not really include much information or anything related to SAC 63, so here you have a group that's working on

the technical design for the root key rollover, you have another ICANN group, the SSAC, that's already said a number of things about the root key rollover, and there didn't seem to be any correlation. And so we noted that and suggested that it would be good to look at trying to incorporate those things and to also ask the Board again to give us an update on the state of what's happening with SAC 63.

So you can see there's been an ongoing set of things that the SSAC has been looking for. Next, Kathy, please. And there we'll go through the slides are up there. I want to just go ahead, pass on through quickly so we can keep on time here. So next.

And end at that we'll wait till the end of the panel presentations and then take questions at that point, so please write them down, and we'll next go to Geoff.

GEOFF HUSTON: Thanks, Russ. So I will be relatively brisk as I roll through this. Next. This is important because, quite frankly, we're now reached the point where approximately one in six users will not resolve a name if it is badly signed in DNSsec. So that normally means if you mark up your signatures in DNSsec, one in six folk will not see you anymore.

But if we mark up the root of validation, that's the number of folk who would be impacted. Next. So there's this thing that we're finally got this enormous sort of momentum of use of DNSsec to the point that if it's badly signed, a substantial amount of folk on the Internet will not be able to resolve that name, which is precisely what we wanted. Next.

So that's an important number because that's, if you will [inaudible] the folk that if we get this key roll wrong and strand these validating resolvers, that number of folk will have a problem with the DNS on that day. That would be a bad thing. Next.

So we go back to five years and nine months. And there was some coverage in the press because basically on 1 June of that year, 2010, things got signed. Next.

And here is a very critical document. It's actually the certificate the DNSsec practice statement published by ICANN over what they would do with this key. Now it's an important statement because without a practice statement, that public key is just a bunch of bits. And if the practice statement says, "We're going to take that private key and write it out and put it on the wall of every single door we can find," you probably shouldn't trust it.

The only reason why you should trust this key is that document. Because what that document is, is a commitment by ICANN on

the way they will manage this bunch of bits. And you should only trust those bunch of bits if ICANN fulfilled their commitment. And that commitment or set of commitments that ICANN made themselves, they weren't imposed upon them, is summarized. In fact, is enumerated in that practice statement. Important document.

And one part of this is actually circled there, and it basically says, "This will be rolled through." Geez, my reading. Let me get something closer. I need better glasses. Each root zone KSK will be scheduled to be rolled over through a key ceremony as required or after five years of operation. Next.

So sorry, back again. I thought there was another slide. After five years of operation means numerous things to numerous people. Certainly from where we sit in the design team, we actually felt it meant as close as reasonable to the fifth anniversary of the creation of the key. After five years, 2015.

And by the time we were formed in January 2015, it was pretty clear we were kind of slipping on this. But we felt there was a commitment there to make it happen within a reasonable period. It wasn't could delay it forever; it needed to work. Because that's the commitment of why you should trust this key. [inaudible] onto that, we've all got a problem. Next.

Quick bit of background. There are two keys out there in the root zone. We're not talking about the zone signing key. This zone signing key is actually rolled every quarter. So in the 1st of January, 1st of April, etc., that key is rolled and it's quite automatic in some ways. It just the new key is published for a period of ten days, the keys change over, and the old key is removed after a further ten days.

That key is basically managed by Verisign as part of the root management in day to day operation. Now the reason why they can do that is there's a key above it. The KSK. And that key is used to sign every new zone signing key, so that's why your resolvers magically track the zone signing key change. Nothing that you need to do. Next.

The key signing key is, of course, different. It's the apex. This is the thing that every single validating resolver keeps a local copy of. This is the thing that's inside your machine and my machine if your machine and my machine does DNSsec validation. So that's part of normally of config data. The real key, the private part of that key is kept offline in highly secure facilities. Next.

And they have floodlights and guard dogs and all kinds of things. Next. Except in California, where things are a bit more relaxed. Next. And we discovered this in Amsterdam. Next. So the actors. It's not just ICANN. ICANN are one. Currently under

arrangements, the NTIA is part of the U.S. Department of Commerce is one of the root zone management partners. And, of course, the operator, Verisign, is part of that partnership, as well.

We were formed last year as a design team with folk from each of those areas to help us to actually bring forward a design of how to roll this particular key. Next.

So there's a bit of a history to this, as you heard from Russ, there was initial consultations. Didn't involve the design team in 2012, an engineering study in '13, an SSAC review in '13, and this design team worked across most of '15. Next.

So if you break it down, a lot of work in the early part of the year of discussion, ponder, discussion, ponder, expiration, finding where the walls were, and why. You may have been seeing a public comment, a draft that came out in August with comments closing in October, which is our first part of this. And then from October through November, we prepared the final report. Next.

Now first of this is that rolling the key is important because everybody out there has a copy of the current key. So how do you automate all of those folk getting the new key and replacing the old key with the new key? There's nothing above this. There's no automated way of doing this where you just sort of rely on some other mechanism of trust.

So that's the kind of problem and the issue is if we get it wrong, your validating resolver will have an old key. But the thing they're trying to validate against is signed with a different key. That's called serve fail, that's called going black.

It will not just give you an answer and say, "I couldn't validate it." Because it understands the protocol, it says, "Someone's playing with you. I will not give you an answer." So in this case, the fail is a fail hard, not soft. Next.

So what we actually do is use another trick in cryptography, and you're relying on the fact that no key ever gets compromised when you come around to roll it. This does not work if a key gets compromised. So we're kind of assuming right now that things are just fine and if things. And if things are just fine, the way you develop trust in the new key is to get it to be signed by the old key. If you trusted the old key, and the old key signs a new key, then the new key is good, right? Because the old key signed it.

And that's the mechanism that we use. It's actually documented in RFC 5011, but the way it works is you publish this new key and you include it in the root zone, but you sign that key with the old key. And you leave that for a while.

Now if your resolvers are on the ball, big if, and they're configured to track this automatic key roll, big if, they will see this new key signed by the old key and go, "Aha. I better load up

this new value and stash in my local cache beside the old one, and now both of these are trustable." And then we get to bullet three, we withdraw the old signature and the old key, and then finally, because it's really, really dangerous to leave old trust material lying around in your resolver.

Because if I come along five years later and crack the old key, and you trust it, you're toast. So what we actually have to do is the sort of the public cleanup is step four, revoke the old key. So we republish the old key once more, but this time there's a bit in the signature part that says, "If it's in your local cache, scrub it. This is crap. Do not use this key." Next.

So here are the stages in a diagrammatic form, and this takes all of three quarters, nine months. It's deliberately quite slow. Now on the top line, the zone signing key is rotating every quarter. So they publish the old key for further ten days, they then move the new zone key for 70 days, and then the next ten days, they publish the new zone signing key. So across the top, this is regular roll of the zone signing key.

Down the bottom is the process for the new key signing key. So for the first quarter on day ten, the new key is just introduced. It's not used, it's introduced. On the first day of the next quarter, all of a sudden the old key will disappear. [Am I] running over

time but deliberately. The old key will disappear, [thonk]. And all you'll have then is the new key, that's it.

If you haven't learned the new key by then, you've got a problem. We will run that for one complete quarter plus ten days, and then all going well, the plan is then to republish the old key and say, "Destroy your local copy. Get rid of it." Do that for further 80 days to make sure you got your message, and we're all done. Next.

So those are the three critical points. The preload, the critical switch, and the point of no return with revocation. Yes? Okay, next. So the assumption that this will work, right? If everyone does the right thing, so this RFC 5011 is supported in all resolvers. Everyone supports large DNS responses because the responses will get big, and everything will go without a hitch. Next.

This is, of course, nonsense. Next. So the first problem is that some resolvers say, "I'm managing my local trust keys manually." So it doesn't matter what you do in the root zone, it'll take a piece of configuration on a terminal to change the key. They've got a problem. Either they're paying attention or they're toast. One or the other. So that's the first problem.

The second problem is that these responses get larger. And the DNS certainly can handle large packets, but the network path

between the authoritative root name servers and your resolvers might not. You might not get the answer. The network might not actually carry those large responses. Next.

So the first of these technical concerns. Some of these resolvers don't support automatic key rollover. How many? We don't know. How many users? We don't know. What will they do if validation fails? Well if you're using an old resolver, it will go query thrashing, it'll just try and this year and try and try and try, I have evidence here of resolvers doing that. If you go to more new and more resolver, it'll just go, "No." That's it. Just no. There is no answer for any question. No.

What will users do when resolvers return this no? Well some of them go to a non-resolving, a non-validating resolver. We know this. 16% of the users today will not. No means no. It means black in this situation. Next.

So we can't test this in advance for you. We've tried all kinds of mechanisms to see how we could sneak in to see what's going on with you and your resolver. We cannot intrude in that conversation. We simply don't know. We will find out when it happens. Fine. That's the reality of the situation. Next.

There is a lot of DNSsec out there, so we're not talking little numbers. 87% of all queries have the DNSsec okay bit set. Remember from the quiz this morning? If a zone is signed, 87%

of all queries will give back the zone signature. That's a lot of DNSsec. 33% of all DNSsec okay queries attempt to validate. Again, those are really big numbers.

Basically, half of those folk, when they get back serve fail, will go and use the resolver that doesn't validate, but the other half will stick there and go, "No means no." Next. Large DNS responses. We all know that everything under 1,500 octets will work just fine. Won't it? Rubbish. It won't. in UDP, once you get to around 1,350 octets, things get very, very, very kooky. And what we actually observed in experiments, and we can experiment with this, is that around 6% of queries receive a truncate bit when they have 1,350 octet response, and they will be forced to use TCP.

Not all resolvers like using TCP. Firewalls resolver, policies, whatever, and there's a failure rate of around 1% to 2%; that's really bad. So these big responses will cause damage. .org, on the other hand, has been running a DNS key at 1,650 octets. I have no idea what their experience is, no one is saying, "My God, that was absolutely horrible. It failed miserably." So we've got this conflicting information that the experiments say, "1% to 2% of folk are going to die at 1,350. .org appeared to live at 1,650. This is the Internet, everything is possible all at once. Maybe Schrodinger's cat is at work here." Next.

We don't know how many folk are using 5011 and automated take-up. We're only going to see this when we roll. Next. So some things will fail. Some folk will switch over to a non-validating resolver, some validating resolvers might turn off validation. And a small number of folk will simply be left with nothing. Next.

These slides will put in a little bit before events changed. We're actually going to show you this report before it got published because I was a little bit annoyed with the fact that it hadn't been published, but ICANN, to give them credit, published this on Monday. So when I say publication is still forthcoming, that was Sunday's story. Monday's story is you can find this somewhere in the ICANN website. This is great.

Next. Here are the recommendations I was going to share with you. It's no longer a secret but they're still right. I'll leave you to read them, there are a lot, I'm not going to go through them. Next. There's a couple here that I just want to, next, just highlight. Next. Stop.

16. We're saying to ICANN, "Look, there's a metric of oh, my god, this problem's worse than we thought." And we're proposing that if we get more than 0.5% of the estimated Internet user population still dead three days after near those critical points, maybe it's time to think really hard about backing out immediately. That was our best shot at what was unacceptable

damage. So 0.5% of the estimated user population negatively impacted after three days.

You can argue with this, but it was really [inaudible] put a stake in the ground of going, "What's a metric of damage?" That seemed to be a reasonable metric. Next.

Right. And this is actually the timetable we're proposing at the time. It hadn't been published. 1 April looked really, really aggressive. 1 April is still about 18 days away or whatever. But nevertheless, it's not quite as hard as it looks. The first nine months is actually the key signing ceremonies and preparing the new key material. No changes to the root zone. No changes to the root zone. But there's nine months to actually open up the key, the normal ceremonies in those lock vaults, dig up the sand, whatever. Do that work and then change the keys over.

The real game starts on the 1st of January, the first change to the root would be on the 10th of January. Fascinatingly under this particular schedule, these slide in, slide out, there is no old key anymore will be on the 1st of April, 2017. That's just the way it worked, and the whole thing should conclude if everything goes well and there is no damage by basically in September of that year. Next.

What can you do? There is something you can do, and more to the point, there is something you must do. Next. If you see this in

your resolver config, go back to sleep. You're doing fine because your resolver is now managed keys. Things will work. Next. You've got a problem. If you see that, you got to pay attention. Because if you're not, you're going to die. This is nothing the rest of us can do about it. So those two slides are the real big slides that I wanted to say to you.

If you're using trusted keys, manually managed keys, pay deep attention over the next two years. If the timetable changes, you need to be aware because you said you're going to do manual management. If you're doing automated key management, you're okay. Things should just work. Next. There.

RUSS MUNDY: Thanks, Geoff. We'll move along quickly to Warren, but thank you for that great, indeed. You want to just go to questions? Okay. Warren says that Geoff covered everything he was going to say, so we'll go ahead and just go on to questions at this point. So Robert, you had your hand up first. Go ahead.

ROBERT MARTIN-LEGENE: Yeah. Thank you. Robert Martin-Legene, PCH. Well on the managed keys slide, it requires also that you [inaudible] log files because sometimes it says it needs a file to write the thing in.

And if you haven't configured that or you don't have write permissions, it's not going to work out anyway.

Can you go back, whoever has the thing? Back to the timetable slide with all of the nice colors? That's a lot of slides. Anyway, my concern was here at the beginning of quarter two, just start immediately. It doesn't say when you start signing with the key, it only says when you remove the first key.

GEOFF HUSTON: On the 1st of April, 2017, the DNS key resource record in the root zone will be signed by the new key, and the contents of that resource record will be at that day, the outgoing zone signing key, the incoming zone signing key, and the new key signing key. All of this is designed to effectively minimize the size of the response. This is the absolute minimal path that does not deliver redundant information in that DNS key response. This is as small as we can make it.

Even so, at the Q3 revocation. We need to sign the DNS key with two signatures. One is revoked, one is not. That point is 1,297 octets plus headers. That's going to be a problem.

ROBERT MARTIN-LEGENE: I'm thinking like TLD delegation. You have an [RSSAC] and that has a TTL in it. If you start immediately signing with a new KSK

and you remove the old KSK, like in Q2, I believe, won't you be having a cash problem?

GEOFF HUSTON: You will have loaded if you've got automated key management, the new key in your trusted keyset. Because it is in your trusted keyset, you will accept as valid the DNS key record at that point.

ROBERT MARTIN-LEGENE: Yeah, I agree, but I still have .uk with six hours of TTL in my cache.

GEOFF HUSTON: But .uk is signed by the zone signing key, da, da, da, da, da, da. You're okay.

ROBERT MARTIN-LEGENE: Maybe.

RUSS MUNDY: Thanks for the question, Robert. Yeah. This is one of the wonderful magics that was looked at in the 5011 structure that they. But separate offline conversations are highly encouraged here. Okay. I'm sure there's more questions, comments from

people. Yes? No? Oh, my. Oh, yes. Go ahead. Down there. Name, affiliation please.

UNIDENTIFIED MALE: My name is [inaudible], I am from Saudi Arabia, Saudi NIC. I have a question regarding the algorithm and the key length for the root. Are they going to change?

GEOFF HUSTON: Could you just move forward? I actually had some questions you should have asked. Keep going. Right near to the end. Stop. Sorry. Keep going, keep going, keep going. And I will give you an award because you asked one of them. Thank you very much. Next. This one. Right?

You asked this. Should we do an algorithm change, as well? It's certainly true that we would have less concerns if we used ECDSA because the big packet problem will disappear. Right? If we move to ECDSA, the responses will get a lot smaller.

We are juggling conservatism and changing one thing at a time, but encountering a large packet problem versus a more aggressive approach to change the protocol as well as change the key. This is the first time the world is experiencing a change of the KSK. The design team erred on the side of conservatism and erred on the side of larger responses. As long as everything

else remains the same, including the size of the zone signing key, which is critical, then the damage will be minimal but still okay, I think.

If the zone signing key gets bigger, the responses get bigger, we get into another problem. So yes, we thought about this, we felt that we can't ignore ECDSA, but we should roll the key first to at least get some experience of what it's like, and then have a successor group look at rolling the protocol. Thank you.

RUSS MUNDY: Yes. And just to add to Geoff's response there, the SSAC 63 included, we discussed it internally. No details specifically about that but the end result was there's a line or two in the report that says, "You should just do the key roll first." So more or less the same conclusion from SSAC as the design team that key roll later do the algorithm roll. One thing at a time.

UNIDENTIFIED MALE: What about the key length size of the key?

RUSS MUNDY: At that point in time, the SAC 63 point in time, that wasn't even addressed, so it wasn't really looked at, at all.

GEOFF HUSTON: The KSK is a 204 for 8-bit key. So we did not feel the advice we got from all the cryptography folk and that advice is in the report felt that there was any need to change the KSK key length at this point in time. There are some parallel discussions about the 1,024-bit ZSK, and this is this whole issue about which do you do first and why? And what are the implications if you change the ZSK and not the KSK, etc.?

RUSS MUNDY: Again, one of the very important issues is that the need for people watching and managing and monitoring their systems very carefully needs to get out to the world, and people need to be aware of the things they need to be watching. So Warren.

WARREN KUMARI: So yeah. I was one of the original authors with Russ on SAC 63. That was a cool ringtone. Thank you, thank you. And I think that I agree with all the recommendations there. It's worth mentioning, though, that a number of other documents have made very similar or almost identical recommendations to basically all of the SAC 63 ones. There've been at least two public comment periods, which said basically the same set of stuff.

There was an RZM meeting. The original version of the document from the design team said basically the same things. So I think that it's interesting to note that the technical folk all seem to be on the same page, which is largely saying this is important, we need to do it and move it along, and I think so far, everybody has all of the reports that I've seen have suggested that we just stick with RSA for now and 2,048.

RUSS MUNDY: Other questions. Okay. Oh, yes, Dan. Go ahead.

DAN YORK: I would just like to give a round of thanks to the KSK design team that has spent an awful lot of time and hours in putting together this document. So. Paul Wouters is here. Is there anyone here, Paul, that you remember from the design team? Ondrej left. He's out to savor the lights of Morocco, but yes, on behalf of myself, Paul, and Ondrej, thank you very much.

WARREN KUMARI: Well seeing as we still have some time, I'll play devil's advocate.

RUSS MUNDY: No, you don't.

WARREN KUMARI: So you say 16% of people won't be able to resolve invalid answers currently, if they get DNSsec failures. You've also got some stuff saying that there are a couple of large resolvers, which service a bunch of people. We hope that they will correctly do the key roll. But that still leaves a large number of people potentially at risk.

The design team says 0.5% after three days is acceptable. That sounds like a very large number of people who are not going to be able to get their DNS working. How did you come up with that? And I say, playing devil's advocate, instigating.

GEOFF HUSTON: Look, it would be really nice to say zero. Right? No damage after three days, just absolutely everything working properly or we back out. I don't think that's realistic within the technology and the variation we see out there. Even now, there's a certain amount of DNSsec damage that is going around. That wasn't reasonable.

We were, I suppose, just putting a stake in the ground, saying if we can measure this, it needs to be at a point that is measurably significantly. I'm not sure that we can measure the Internet at granularity at higher than 0.1%. Below that, it's kind of noise. It wouldn't be a reliable measurement. So that was sort of seen to

be something we could measure and see at a timeline that was reasonable.

Finger in the air, that was where it got to. If there is that level of damage, you really should be backing out. It was where we got to, but that's about as much as the science behind it.

RUSS MUNDY: I'd like to thank all the panelists here and also urge everybody in the room look at the URLs, grab the documents, at least look through them, and possibly read them in detail. There is some useful information and it's good for folks to be aware of what the content of these are. So thank you, Geoff. Thank you, Warren.

DAN YORK: We're good. Hey. All right. So we're in the final little bit for this. I'd like to thank you for all the people who sat here. Many of you I've seen since 9:00 this morning, so let's give ourselves a round of applause. So we want to just kind of wrap this up with a little bit about how you all can help, our suggestions, what we'd ask of everybody here, and Russ and I usually tag team this, and so I'll leave at the first one, but I'll say if you're a TLD operator, if you operate a ccTLD, we [inaudible] ask you to sign your TLD.

We've heard over the course of the day a number of different resources that are available, including if you're here in the Africa

region. You have the AFRINIC folks that are willing to come and travel and do a workshop at your session. If you're not in Africa, there are other resources from ICANN that will do the same kind of workshop that will be able to help with that.

We also ask people to accept DS records, to work with the registrars, and also to help us with statistics. You saw that chart up there earlier on with Rick Lamb's list of statistics about the number of domains versus signed. And we'd love to make sure that includes all of the relevant TLDs that are out there. So we'd ask ccTLD operators to do these steps. I guess, and Russ.

RUSS MUNDY: So other zone operators besides TLD operators. If you operated DNS authoritative server at all, look at doing DNSsec for it. It really isn't that hard. And like you've heard today, there is a huge amount of help and support and resources that you can take advantage of. And people in this community tend to be extremely helpful. So if you've run into something that is problematic, you can go back and look at these workshops and find out who talked about what, and I'll just about guarantee that if you send them an e-mail, you'll get a response and a lot of helpful information.

And again, statistics are important. We're really looking to gather more real actual data on what's going on out there in DNSsec land.

DAN YORK: If you're a network service provider, an ISP, we would please ask you to turn on validation. We'd like to see Geoff's graph go up even higher and higher. We'd like to see more and more validation. This is critical, in part, because we get some pushback by some of the companies out there when we talk to them about signing, and they say, "Well why should we sign? Because nobody's validating."

We then point them to Geoff's stats – thank you, Geoff – and we say, "Look, look at this chart. Look in your area at the amount of validation that is occurring. This is not some mythical beast. This is really real. This is real." So we need more of that. We want to go up from whatever we're at, 14%-15% now globally, we want to bring that even higher and higher and higher.

And this is a simple thing. You just have to enable, there's a couple of lines in your config file, but you also do have to be aware that you could cause people not to be able to get to websites, so you have to prepare your support staff, etc. to be able to support that, as I'm speeding up and I realize I need to slow down. My own victim there.

Other part is sign your zones and the other piece is we'd like you to promote the support of the DANE protocol, which we didn't really talk about here this time. But we are encouraging people to do that. Warren's smiling. Russ.

RUSS MUNDY: So if you're a website provider, and other content providers, look at signing all of your zones. If you're a website operator, there's a decent chance that if you're operating your website, you're also probably operating your DNS support. If you've outsourced your website operation to someone else, and just providing the content, go to the people that are actually operating the underlying machinery. Tell them you want all of this signed and you want to support DANE.

You want to see all of these things put in place and go to your vendors. Make sure your vendors are aware of the fact that you want to do it. Thank goodness over time this has gotten easier and easier because more and more vendors are supporting it. But one of the problems that we have had for a number of years is vendors would come back to us and say, "Nobody is asking us for this." Similar to the response when we got about doing validation, nobody's asking for validation well.

Nobody's asking for DNSsec signing. Asking for it from your vendors in all of your services that you're buying.

DAN YORK: So finally, what everyone can do. We ask you to use DNSsec yourself. Use validation if you can, if you can turn that on to sign your domains, do all of those things, whatever you can do in whatever capacity you have. And the important one we would ask you to share your lessons learned. We heard some great – share the lessons you learn out of your experiences. We've heard some great things here, we've heard them in tech day, we've heard them in other places. We'd like you to bring your ideas here.

The next session will be at ICANN 5, wherever that may be, and we will have another one later in the year at ICANN 57. And we will go on from here. Well yeah, we hear, yeah. But as Julie was saying, the official thing happens when the Board votes, but it may be in Finland. So anyway, wherever it may be.

We will have a regional panel, wherever the sessions are, and we would like to include people from the regional as we had people from Africa on this one, we'll have people from whatever continent we're on next time. And we'd like to include people in there. We also do want you to do this.

I also had a request today, somebody asked, "Well is there a way to stay up to date or connected to other people between times?" And I should mention, and I made a note to include this for the

next time, there is a mailing list, which we call the DNSsec coordination list, is DNSsec-coord, and you can join that list and share information with each other. We also have a monthly conference call on the first Thursday of every month except for this month when things are messed up.

But usually, most months, it's the first Thursday of each month when we get together on a conference call and talk about what these issues are, talk about how to accelerate the deployment, and do that. Anybody is welcome to join. You simply have to just join the mailing list so you find out about these things. You can find more of that out there.

I want to thank a couple of people again. I'd like to thank our sponsors for today, Afilias, [Sara], Dyn, and SIDN. And I want to thank them all and I'd like to give them a round of applause. On that note, I will mention we are again looking for one more sponsor just to help us for the rest of 2016. That would help us continue to do that. And we're also looking for a sponsor of the implementers gathering, the Monday night gathering at the venue that we have next. So think about that. Would your company be willing to help us continue these activities that are part of that?

And I also want to give a special thanks to Julie and Kathy, who have been helping make this all run as smoothly as it does. With

that, we will just end by saying if you'd like more information, here are some websites you can go to. DNSsec-deployment.org. The Internet Society, we never fixed this, .org/deploy360. Okay.

Program Committee, can we all agree we need to fix this? We always see this at the end of the session and you send – yeah, okay. So there is dot Internet Society. Okay?

UNIDENTIFIED MALE: For under $200,000, you.

DAN YORK: Sorry, no. It's internetsociety.org/deploy360. And then, also, the DNSsec-tools. And from that Deploy360 site, there is a link to the DNSsec community, where you'll find this mailing list and other pieces, and also statistics, resources, and more that's there. So I'd like to just say thank you all and –

RUSS MUNDY: One more big thank you to our tech staff here and our translators. Thank you very much.

DAN YORK: Yes. Thank you, translators. Yes. From acronyms and fast speakers and everything else, they've been through a lot today. Maybe they can go have a – anyway. Well with that, we do need

to wrap up and I think probably have to get out of this room fairly shortly. I don't know. 15 minutes. Okay. So we're all good. Thank you all. We'll see you at the next ICANN 56.

[END OF TRANSCRIPTION]