COPENHAGEN – DNSSEC Workshop -- Part 1
Wednesday, March 15, 2017 – 09:00 to 10:30 CET
ICANN58 | Copenhagen, Denmark

UNKNOWN SPEAKER: …that people should listen to, especially if you want lunch. So, you should, at your seat, have your ticket. If you don't have one, let Kathy or I know. And that ticket has a map on the back that you may or may not want to follow. You can probably do a better job than I did.

So, or just find somebody else who knows where they're going. Anyway, it's kind of across the hall from where we are, and kind of down around a corner. But also, you'll note that there is an optional break, 10:30 to 11. We are going to go through the break, just because we have that much content to cover, but you're welcome to get up, really, any time and go get coffee or whatever.

And you know, but if you want to take a break at that time, that's fine as well. So, I want to go ahead and just turn things over to Dan York, who is going to start us out. Thank you.

DAN YORK: Good morning. How is everyone doing? Good morning. There we go! All right, come on, it is the morning here. We've got to get going a little bit with that, and I'm going to see if I can actually, probably not going to be on the cameras. Watch, they're trying to find me. Where am I? Nope, turn it the other way, and I'll try to stay over here on this side, and then you can see.

Look, watch, the camera is coming around to me. No, it can't do 360 degrees. It's looking up, up, up, high, there, hello remote folks. I know we do have some people coming in there remotely.

So, good morning. We've got a very packed day for you today. As Julie said, we did go across the breaks, so… Is Matt Larson here yet? No, sorry, Matt is the victim of that break. So, if you do want to get up during that time, if you already heard about the case, K-rollover… How many people have heard about the case, K-rollover? All right, all right, okay.

Well, Matt, we did talk yesterday. He might try to bring some new things to that, to make something that you've may not have seen before, but I see we've got a good number of folks. How many people have never been to this DNSSEC workshop before?

Okay, a few people. Welcome. Good, good to see you here. Yeah, [inaudible], you don't count. Okay. Let's go and talk and see what we're doing here. This session was brought to you by a program committee. How many program committee members are here in the room? I see a number, okay, you can blame all of these folks, if you wish to let them know. Or also, if you're interested. We will be doing another one of these in an abbreviated form, at the policy forum in Johannesburg.

The current plan is it will probably be merged with Tech Day like it was last time. So, if you're interested in showing your research to the community, and having it out there, and letting people know, we'll be looking for, we'll be doing a call for proposals soon after this, asking for that.

And then we will again, have a full day session at the Abu Dhabi event in November. November, October, whenever it is, at the end of the year, though. So, these are the folks that have been working. We have a weekly call. We want to also very much thank these three companies.

Let's see, I see Jim from Afilias, all right. Jacques from [inaudible], and Christian sitting right next to him from SIDN. We want to thank these folks. Let's give them a round.

They are the reason why we'll be able to have lunch here, and be able to continue our networking and discussions that we have then. So, thank you very much for them. I will also say, I am looking for a fourth sponsor to help continue this for the next two. If you're interested, please see me. It's a very small sum to help. All right? Let us know. Talk to me.

This is a picture of last night. We want to thank Irwin. Where is Irwin? There is Irwin. Irwin and DK host master, let's give them a round of applause.

Sadly, we only thought about taking the picture at the very end, when the majority of people had left, and it was suddenly like, oh, wait. We need a picture for the slides. So, imagine that times about four, and that was the number of people. There were about 30 people, 30, 40 people there, something like that. All there.

It was a very good discussion. Very good things were happening. So, thank you to Irwin for putting it on. I'll also put in a plug that when we go to Johannesburg, we will be looking for somebody to sponsor that evening down there, and also Abu Dhabi. So, if you're interested in either of those events, it's a great night to do some networking and connect with some people there.

All right. This is an activity supported by the security and stability advisory committee, or SSAC, along with the Internet Society Deploy 360 program, so both of those are part of what, the groups that help bring this together. And my clicker.

Where am I going? Clicker stopped. All right. Just hit the button, there we go. So, here is our program. You've got a copy of this on all of your sheets, you should see that. But you do see, we've got this great panel coming up on what's happening with

DNSSEC in Europe. I'm going to give a brief update on what's happening at the IETF lately, in case you haven't been paying attention and about the upcoming meeting happening there.

Then we're going have Matt talking about the root key rollover. And then we've got this panel that's talking about, what are we doing with validation in ISPs related to the root key rollover, and some discussion we want to have there about, what can ISPs do to prepare? And then we've got a demo from Paul [inaudible], who is going to do… We've got some secure email stuff happening in the afternoon here, with Paul doing one.

And then a little bit later, we've got [inaudible] talking about open exchange and the work there, in between there. Roland is going to do some discussion about ECDSA, deployment and what's there. Roland moved. You changed man, you were there. So, when I pointed, okay, Roland over there, is going to talk about ECDSA. Oliver is appropriately wearing, let's see his shirt there, will work for algorithm 13, which is ECDSA, if you don't know what that is.

And then we're going… And then Wes, is Wes here yet? Okay. I know he had some other meetings around here today. Wes is going to be the MC for the great DNSSEC quiz. Warren, of course, as I sat down next to Warren [inaudible] over there said, should we just fill out this form right now with answers? Because that's about as well as we may do on some of the quizzes, but you're all invited to participate and have fun.

Wes will be here for doing that. And then we will wrap-up with another demo, which I don't actually know anything about, other than it's about secure and encrypted email again. So, we'll have some interesting times here to talk about. There is Paul. All right. Let's go and see what's next.

So, is this now working or are you going to have to push the buttons? Okay, here, we'll do a quick… Oh wait, it's working, it's working. I don't know, something is happening. It could be operator error. Okay, so first of all, I want to talk about the deployment stats. How many of you have seen the state of DNSSEC deployment report? Okay, a number of folks there.

It's a good report. We put together a number of folks, in this room, who put together statistics around where we are with DNSSEC deployment. So, I'm going to show you some maps, but if you want a longer description in pieces like that, I would encourage you to go take a look at this report, because we tried to look at what is the, you know, draw a line and say, here is where we're at with DNSSEC deployment now.

My organization, the Internet Society, is committed to doing a 2017 update where we'll look at, and we're trying to get that done for the Abu Dhabi event, where we'll be able to say this is where we're at in 2017. What's the growth we've seen? What are we going on from there?

So, please take a look at that. Maybe I have to be here. Maybe I need to be closer. Okay. So, let's take a look at where we are at with some of the stats that are there. Okay, here is Jeff Houston's map of DNSSEC validation that he maintains that the APNIC stats. We've been holding fairly steady at this, if you look. We're still around 14, 15% has been kind of where we've been at globally. That changes in different parts. Because we're here in Europe, I did pull up the chart on what it looks like, this is the global notice of this.

And if you look at where some of the global validation is happening, the trick to reading this into Jeff's map, as far as the trick to me is, if you look in the first column, that's the percentage of validation he's seeing, that's happening in those regions. And the part over here, where it says use Google's PDNS, that's the percentage it's using Google's public DNS.

So, in some countries where there is a high percentage of that, which we'll see in another minute, it means that the local ISPs aren't doing validation, they're just outsourcing all their DNS to Google. But in countries, or in areas like we see here for Western Europe, where the use for Google public DNS is only around 7%, that is showing that a lot of the ISPs are, in fact, doing validation locally themselves, which is actually what we want to see because we'd like to see local ISPs doing that in some form.

So, this is what we're looking at globally, and if we look at the Europe picture, all right, just hit the next button. There we go. I'm back up. All right. So, here we are. The [inaudible] Islands, which someone needs to tell me, I know it's off the coast up in like near Iceland, right? No, keep going north?

[SPEAKER OFF MICROPHONE]

We lost a soccer game against them. Okay, well that's the important part here, okay. So, they actually come in the top of Jeff Houston's stats here, coming in at 86% of all DNS queries coming out of that, of the islands. I don't know how many of them there were, all right? But, that's the stats that they were there percentage wise, is there.

You can see Denmark is right in there. So, good to see there. And again, we're seeing the statistic there, generally low on Google public DNS usage, which indicates that the ISPs themselves in that region are doing a lot of the validation, which is kind of what we want to see.

All right, that's the validation side. Let's move on and talk about signing. This is Rick Lamb's… Is Rick here? I haven't seen him, okay. Well Rick, when you see him later, you can thank him for doing this great report that's here. Oh, I'm on translation and I'm talking too fast. So, I'm probably cause… Yeah, I see nodding heads back there. They're like, okay.

So, we will talk slowly, no, not that slow. This report shows that the number of domains that have been signed, and that big jump, of course, is with all of the new gTLDs that have been signed on there. So, let's go on to the next one. This is showing the numerical number of domains that are signed on there. And from Rick's latest statistics, SIDN, here, still has… Christian, what is this? I go to point at people and they disappear.

Well, Christian, who was sitting right next to Jacques, all right, well yeah, all the Dutch people who are here, okay? You know, all of the Dutch people moving around. Dot NL is still with the highest number of domains that we see out there, with over 2.5 million around there. Brazil next. You can see the other ones. Dot SE, dot CZ, where is Andre? There he is, okay.

He hasn't moved. But you can get these numbers from Rick's site, and they show a nice way… Now, if you want to get that nice thing that I have here, sorted this way, you need to go to the right side of Rick's thing where it says sign slash total, and you click on that total once, and then click on it again, and it will sort it this way. But you can see that.

If you look at that chart, and you find that your country is not represented in there, then you can send Rick an email, and maybe he'll work with you to incorporate it in there, but Rick is looking to add more statistics in there to be able to show the results that are there. Let's go on to the next one.

This was the new gTLDs. We like to provide this statistic just to show where the new gTLDs are with regard to DNSSEC. The top one, the top number of signed domains continues to be dot OVH, which is a hosting provider that also goes and signs its domains and has been very security conscious in general. So, that's one that's there. Let's go on.

So, I want to talk through our maps that we have here. And that maps that we do, for those that are not familiar, break things down into these areas. The statistics that we are aware of are, whether some things are experimental, whether it has been announced, whether they've started the work with it, or whether it's deployed in some fashion. So, let's go on.

This is what the overall world looks like right now, in terms of ccTLDs. All right? And in general, we can see that we're doing pretty well, you know, with the exception of Africa, most regions of the world are getting pretty signed in many different areas. You know, we have, certainly, Africa and South America and some parts of Asia still need a bit. Let's go on to the next one.

This is what Africa is looking like right now. The good news is, since the last meeting, we did have South Africa. Anybody from South Africa here? Anybody? Nope, okay. They've been working for a while to get to the point to sign, and they did in December. So, that one has been signed.

We also have workshops going on. I know Rick Lamb is going to be in several of these countries there this year, working with the local ccTLDs to get those signed. Let's go on to the next one. In Asia-Pacific, we had a couple of recent signatories. Hong Kong and Vietnam both signed in December, and Soma signed in January. So, let's go on.

Europe has been pretty similar, since it was the last time. Not much there. Next one. And Latin America has continued to move along, but let's go on, next one there. And North America is the same. Keep going. We're boring.

So, these maps are available. You can subscribe to them every Monday morning, they get issues, and you're welcome to join in and look at that. Let's go on. I mentioned this already. Let's go on from there. And we do have this history project. I'm still looking for people who would like to volunteer and contribute on that. Go ahead, next one. I think that's it. That's all I have for the morning.

Any questions or thoughts about this? Yes.

MARK: Good morning. Mark [inaudible], Global Village. I noticed that you have dot EG on the map, right? Did I notice that correctly?

DAN YORK: Dot EG.

MARK: Egypt.

DAN YORK: Egypt, yes?

MARK: Yes, I was wondering what that means, because actually, we are a dot EG registrar, but they don't allow access to the API for us, and I was wondering how DNSSEC works under those circumstances.

As far as I know, they do run [inaudible], but they don't have direct access to that service, so it goes through front-end or our contacts at the EG registry.

DAN YORK: So, you ask an excellent question, which is that the maps track whether the ccTLD is signed, it doesn't necessarily indicate whether people like yourselves can work with the registry to upload DS records. That's actually the distinction.

If we go back to the Egypt map, or the Africa map, is Egypt in the operational stage? I don't know actually know. Was it light green or dark green?

See, okay, so it's light green, which means the DS has been signed and put into root. It has not yet, we don't put it in the dark green, the operational stage, until we can verify that people like you can upload DS records.

MARK: Okay. It's only, when it's operational, that registrars can access…

DAN YORK: Yeah. And some of that, and I will say this too, if you see a country there in green, in light green, that you know you can upload DS records to, do get in touch with me because some of the switching it from the DS and root to the operational, a lot of that is, we have to reach out to people, or find out from people, that it is able to work that way.

So, we haven't switched Egypt there because we don't know that. From an operational point of view, we can know when there is a DS in root, but that's about it.

Okay, well I will leave you to the next regional panel, correct? Are we getting all of the people up here? Okay. For those who are new, this is an informal kind of session. We do like to have questions, so if you do have a question, please do feel free to come up to the microphone right there and ask questions. We don't bite, or other things like that. Most of the time.

I'm the moderator for this too, right. Okay.

All right, I'm going to come over here and sit down, because you don't want to see me standing up there in front of this. So, when we do these DNSSEC workshops, we like to have a panel that brings together people from around the area that we're in, to talk about what's happening with DNSSEC.

And we have the panelists sitting right up in front of you. Some of them who are there. And so, I'm going to begin by letting Andre speak about what's happening in the Czech Republic.

ANDRE: Thank you very much. My name is Andre [inaudible], and I'm from [inaudible] registry, dot CZ. And a little bit about the update, what's happening in Czech Republic. Next slide please.

So, I think it was said already, we have more than half of the registered domains signed, so you know, this number can remain quite quickly, because you need to find some way how to kind of force registers to sign domain, and because roughly however of them is also, you know, hosted on the DNS servers, that's the easier part.

The more complicated part is to commence the second half of the domains. So, we are really working on that, working hard, but it's not an easy job. Mainly, we are trying to pick up some high profile sites, like newspapers, banks. We're trying to explain why it's so important and why they should do it.

So, we are now growing, but I'm sure the growth will not be as quick as it used to be. We are also kind of lobbying inside the country to help to spread the word about DNSSEC. So, we are quite successful into getting a paragraph into DNSSEC into governmental strategy, digital [inaudible] two zero, and also DNSSEC part of the international cybersecurity strategy.

So, that means the government, the institution, should sign their domain. And actually the percentage of signed domains in the governmental site is higher than normal sites. So, quite good. And also, DNSSEC validation is, was put into the standards for connections for, for example, schools and some public institutions. So, currently we can say DNSSEC is semi-mandatory in the country, at least it's highly recommended.

And another good activity, interesting activities, is tied to the local exchange point, nic CZ. This exchange point, has a group of ISPs that have higher security standards. So, those ISPs have a special V-lan inside the exchange point. They exchange security information, and for you to be able to join the club, you must fulfill a few requirements, and DNSSEC is one of them. DNSSEC validation in signing your domain, so also, in such clubs that grow inside the country, DNSSEC is kind of mandatory. Next slide, please.

So, the validation, according to [inaudible] measurement, we are almost in the 50% of resolvers, the numbers changes it relays, so it's a little bit, but again, we are trying to talk to local ISPs. We are quite active in events that are organized by the local exchange point, because there is no NOG, but we usually have meetings related to the exchange point events.

So, we try to educate the ISPs and trying, you know, sort of convince them to start a DNSSEC validation. The good thing, for example, all the mobile operators validate, so the big guys do validate. Next slide, please. We produce quite a lot of software, open source software, and a few of them is also related to DNS.

So, one of them is called not DNS, it's [inaudible] to the DNS server, pretty stable. Run by some root server operators and some TLDs. Just to let you know what's going to happen this year, we would like to add support for EDDSA algorithms, this depends on the new TLD library which we use for the implementation, so as soon as it's new TLS, we will add this feature into, not DNS.

And also, we would like to add KSK rollover support, including CDS and CDN key, you know, currently, we have a mechanism to automatically send [inaudible] including the ZSK rollover while KSK rollover is not yet supported. So, that's the plan for this year. Next slide, please.

Second part of, second software which is DNS related, it's not resolvable. For this year, we have, we would like, again, some interesting feature related to DNSSEC. And to help somehow the root as well. So, one of them is implementation of RFC 7706, which basically says that you should run a copy of a root zone on the [inaudible], and then you know, you can serve some of the [inaudible] to the [inaudible] much quicker, so that would decrease the load to the zone.

Another thing is, RFC 8020, plus draft aggressive use of DNSSEC validated identification. Again, that basically means if there is, if you got to the [inaudible] some know that means that everything belong the note is also non-existent, that's RFC 8020, and aggressive use of DNS [inaudible] is the way, how you can, again, decrease the load to the root zone by [inaudible] responses to the clients.

And last, we implemented already DNS over TLS. I mean, that's meant for clients, so if I'm a client, I can use TLS to communicate with the [inaudible] resolver, and would also like to [inaudible] function for the outgoing DNS or TLS, it means from resolve to its upstream resolver. So, that's going to be added next year.

Next slide please. And, that's a typo, I apologize. We are preparing for [inaudible], you know, roughly 30,000 domains in dot CZ zone is currently signed by ECSA. We would like to sign dot CZ as well. We would like to do second algorithm rollover. We performed the first one, I think, four years ago.

So, we are preparing the community for that. We communicate for the ISPs, as I said, during the exchange point meetings. We also do some conferences, seminars. But currently, you cannot do that. The main problem that is IANA hasn't implemented the feature in their APIs, so we are waiting for that, and we are trying to provide, say IANA, that we are waiting, that would be great if IANA can implement.

There is one thing, just to be sure that all of the validation chain is okay. We created a [inaudible], and it started as actually an

IPv6, it was just indicating the eyeballs that the connection supports IPv6, then we added DNSSEC functionality, and this year, we added another functionality that says whether it's validating, both [inaudible] meaning RSA and also ECDSA.

So, if your DNS server validates, but doesn't support ECDSA, you will see, you know, the button, not green, but, and not red, but something between that says, [inaudible] DNSSEC but not ECDSA. And it's on our webpage, so that's also the way we plan to spread the information that we would like to move to new algorithms.

So, next slide please. I believe that's all. Thank you very much.

[Applause]

DAN YORK: Thanks Andre. I actually had two questions. One, could you clarify on… Is the issue on the IANA that they don't support algorithm 13?

ANDRE: Yeah, you cannot submit DNS records with 13, so.

DAN YORK: Okay. Good to know. We need to fix that. Second question, you mentioned the digital check 2.0. Is that something that's out now, or is that in development?

ANDRE: Actually, yeah, it's a national strategy for digital things. So, I think it's four years old, it's quite [inaudible]…

DAN YORK: Okay. So, that's part of the plan, that's there? All right. Any questions for Andre? Go ahead.

KIM DAVIES: Hi. Since you're talking about IANA, I just thought I'd say that we are working on trying to do what we can for support for ECDSA, [inaudible] EDDSA. Essentially we're trying to get a mature implementations that is support by the root management partners. As you know, we work with Verisign as well, [inaudible] implemented in their systems.

We need to implement it now. So, I'm happy to talk to you in more detail about what we're running into, but it's a work in progress.

ANDRE: Do you have some outlook as to approximately…? I completely understand that it's important thing. You should make it, you know, in good quality, but quicker. So, it's fine, take your time, but do you have some…

KIM DAVIES: I don't have a date I can give you today. Trust me, if I did, it would be all over my slide decks I'm giving, but until that point, I don't have a date I can commit to.

DAN YORK: Thank you very much. You want to introduce yourself?

KIM DAVIES: Kim Davies, IANA.

DAN YORK: There we go. All right, nice to have the people in the room when we have questions like that. So, thank you Kim, for standing up and saying that. All right. So next up on our order, we have asked Peter Koch to talk about DENIC and dot DE.

PETER KOCH: Thanks Dan. And I'd like to thank the programming committee for the invitation to give yet another update on what happened to and with DNSSEC in Germany, or in the DE top level domain in particular. So, next slide please.

Just to give a bit of historic background. So, we started full deployment of DNSSEC for DE in 2011, so we are on our sixth anniversary right now. We operate on the registration of DNS key records, so registrars or registrants don't submit DS records.

We receive DNS key records, that's similar to what the Dutch and the Czech colleagues do. We accept up to five keys. Actually, most of the time, people submit one key or two when they're in rollover. We've had one instance, somebody submitted five keys, and we went after them asking, hey, what are you doing? This sounds interesting. And it turned out that oh yeah, we made a mistake in our submission system.

So, on the other hand, that means we are safe on that limitation. We do apply validation checks at registration time, similar to what Kim just explained for the root, which is in line with our general non-DNSSEC pre-delegation checks. And what we basically do is we check that the chain to the SOA records will be validated by at least one key that is submitted.

So, it supports all kinds of KSK rollover, and [inaudible] by keys and so on and so forth. And we will generate the DNS record for [inaudible] to only, because we don't see any point in supporting algorithm from the DNS record itself.

Also, there is one [inaudible] number that hasn't been mentioned yet, that is RC 18 63, which is EPP key relay, and that is based on a document that a colleague from SIDN and another colleague of mine, and myself wrote a couple of years ago, explaining how to do operator change without going through insecure.

This is supported by our registration system out of the box, basically because we are not EPP based, and the intrinsic of our system, if you're interested in the details, come talk to me afterwards. We've actually witnessed very few of these operator changes going secure, and most of them appear to be test cases.

But I'll probably come back to that later. On the registrar side, there is no accreditation process, and we don't require any sign-up for registrars to support DNSSEC. They just do it. Again, that is probably very much related to properties of our registration system, because we usually operate on the whole domain object.

That means somebody submits a domain object with DNSSEC information in it in there. If there is a registrar change and the gaining registrar doesn't support DNSSEC, they would just not submit the DNSSEC information, and then the domain goes unsigned. But hopefully, in a registrar change, that is happening with the customer's consent, or at least their knowledge. Next slide please.

So, this is the numbers. And since we're all talking so much about signed domains, this is what we have. This goes back to 2011 when we started. And you see two colors, actually. The light blue one on the bottom is the number of zones with registered keys, or as we say colloquially, the signed domains, or signed delegations, and we are up to like 64,000 at the end of February, and it's more or less 65,000 as of 10 minutes ago.

And yeah, there is steady growth. If you look to the right side, the right end of the graph, and you have a bit of a fantasy and optimism, you see that the growth is actually accelerating, or has been accelerating, over the last five to six months. We don't have a particular explanation for that, it's just that the breadth is increasing. We'll see that in one of the upcoming slides, that more registrars are working on this, and bigger registrars and resellers are participating.

There is one step, and I guess I had a previous opportunity to explain that one, in mid-2015, when we had a DNSSEC day in cooperation with the Federal Institute of Information Security Information [inaudible], one of the major [inaudible] use portals.

And a couple of registrars took that as the incentive to actually sign all of the domains, and that explains that jump up there.

Now, the interesting part to us, except for the others and the growth, one interesting thing that I wanted to point out here is the red bars. And this is the number of domains that are signed, where we find key material in the zone, but has just not yet been registered with us.

And in part, this is, of course, natural, because when you go sign your domain portfolio, you would first sign and then do some tests and register afterwards. But we are carrying over part of this, and have been carrying this over, for a month, talking to registrars. And it turns out that sometimes, it's larger resellers doing DNSSEC for one or another reason, and then waiting to talk to the registrar and so on and so forth.

We are in the process to encourage those people to submit their key material, and so far, we haven't heard any like technical hurdle, or procedural hurdles, is maybe people are just too shy, we just don't know.

Exactly. Next slide please.

DAN YORK: That's like 20,000 dot DE domains, or so, that are signed, but there is no DS record [CROSSTALK]…

PETER KOCH: That is roughly another 20,000, which is a third compared to what actually is there. Anyway. So, latest activities and observations. Last year, 2016, we changed our HSM, for both the KSK and the zone signing key. We, as many of you at the table, and maybe as some in the back actually, we use the then very cheap and good [inaudible] 6000 cards, but they're no longer supported, and so it was safe to migrate.

We chose the Luna Safe Net, and meanwhile, acquired by [inaudible] systems, and also have migrated from PCI cards to dedicated network appliances, at least for the ZSK. That implied, actually, a KSK rollover and a ZSK anyway, and we did that in August 2016. Anything…? Excuse me?

Anything else we kept, so we stayed with RSA and we stayed with the key sizes. We stayed with the RSA especially because we thought we'd rather wait for the real elliptic curves, and give others a chance to run ahead. I'm interested in the number of registrations. There is one specialty again. We also have a feature that you can have authoritative data in the DE zone immediately, up to five records per domain.

And a lot of people use that, and it's also used by one of our registry features, so we have another 200,000 something domains in the DE zone, and then they get accidently signed, so to speak. So, if we want to pimp up the numbers, that's almost 300,000 now, but truth in advertising, the delegations are 64,000.

And again, that's .4% of the overall number of domains. Mostly this is driven by registrars, or I should say, by the DNS operator within the registrar. So, we see in batches of hundreds or few thousands domain coming up over the course of a couple of weeks, being signed usually infrastructure that is run by the registrar.

And we know that sometimes the customer knows, sometimes the customer has to check a box, and meanwhile, we have a very large registrar with a high number, multiple 10,000s. We started migrating to the DNSSEC, so we expect the numbers to grow a bit steeper even, until the end of the year.

Still, even though it's all dominated or driven by the registrars and the DNS operator, for some reason, there is still a KSK ZSK split, although in that particular scenario, a single key could even be easier. Anyway. Next slide please. Speaking of algorithms, the majority uses RSA in the two flavors of RSA [inaudible] three, which is algorithm number seven on the top in the circle, and [inaudible] 256.

We also see 5% of the algorithm 13. This is not [inaudible]. There is at least one other registrar who falls in that category, sign all my domains, and then used elliptic curve algorithm 13 pillar on the right. To the very bottom, you see zero percent, that is a handful of domains with algorithm 14. You see algorithm 5 RSA, and algorithm 10 RSA [inaudible] 512, with 1%.

And we do support [inaudible], and we still do support algorithm 3DSA. There is one registered [inaudible] domain, and truly this is a test of domain of our own. And this one or two DSOA domains, but the name of the domain suggests that someone is testing that as well, so that doesn't have any particular purpose.

Similar to what Kim said, since we do the validation, we need to explicitly support the algorithm in our validation software, which means that even though algorithm 15 and 16 have been standardized right now. There is no implementation yet.

No implementation on our side, so we can't support this, but we're well aware, especially ED 25519, will come up and that is on our radar. So, maybe next time. Next slide please.

Numbers again, from bottom to top. In like 2013, we had roughly 300 registrars. 42 of them had at least one domain under management that was signed and registered. We are still in the range of 300 odd registrars, and you see a fraction of registrars that supports DNSSEC is steadily growing.

109 now. Next slide please. And when I said at least one domain under management, this is shown here, in this graph, please

note, at the Y axis, it's a logarithmic scale, so it goes up to, what is that? 16,900 or something, is the top registrar. And then it goes down to the bottom, and to the very right, the 20 pillars that you don't see are the ones that have a single domain under management.

And then you also can recognize from the left side of the graft, that there are a handful of contributing the most of the numbers, and then there is a wide distribution in numbers of domains, which is hopefully in line and inconsistent with what I said before, that this is registrar driven and it goes, and more and more registrars, one-third right now, as I said, is supporting DNSSEC.

And I guess, next slide please, that was all I had to say. Any questions?

DAN YORK: Questions for Peter. Come on, you can't let him off this easy. [Foreign language]

PETER KOCH: [Foreign language]

UNKNOWN SPEAKER: One question. You talked about the one ECBSA supporting registrar that wasn't [Oliver]. Where they by any chance, Norwegian?

PETER KOCH: Honestly, I don't know.

UNKNOWN SPEAKER: Okay, we'll talk later.

PETER KOCH: We can talk later. I don't know off the top of my head. Oh yeah, but, yeah, speaking about [foreign language], I should say though that, most of the registrars that support DNSSEC are actually Dutch registrars. So, credit where credit is due, we understand that most of this growth is probably a fall out or side effect of SDIN's initiative to convince their own registrars.

So, yeah. Thank you for that question.

UNKNOWN SPEAKER: You're welcome.

UNKNOWN SPEAKER: One last question. So, if you add the EPP, do you think you have more registration?

PETER KOCH: If you want a response, you need to [inaudible]. Okay. You mean, more than 16 million domains? No, we don't believe that, but that was probably not your question.

No, we haven't… It is not that anyone would have expressed interest to register domains either on the customer, end customer side, or on the registrar side, given any reason that would stop them, except no interest, no time, nothing, but nothing that we're aware of, we could influence.

DAN YORK: All right. Thank you very much, Peter. [Applause]

Next up, we're going to bring up our host of the implementers gathering last night, in our local natives and [inaudible]… Well, okay. Local country, I'm looking at Erwin, I realize this. And so, for Denmark, talking about DK, Erwin Lansing.

ERWIN LANSING: I'll be happy to do it in Dutch as well.

DAN YORK: Please English for us. Thank you.

ERWIN LANSING: So, welcome to Copenhagen everyone. Next slide please. We started doing DNSSEC back in 2010, just I think two months after the [inaudible], so after six years, it was time to change some things. So, we had a little theme last year, where we did a lot of minor things throughout the year. And there is a long list. I will just go to the next slide please.

One thing that… I have to thank Jack, actually, from [inaudible] for the idea, is that we allow our registrants to go directly to us through our self-service portal. And instead of having them copy paste long hashes and make all kinds of mistakes there, we added a new feature we call import DNS keys, which means we go out, we know the name servers, we look them up in our [inaudible] database, [inaudible] TCP, fixed the key, calculate the DS, and then next slide.

Just present the user with, we found these keys, which one do you want? Much easier, much less chance for typos, [inaudible] breaks, or whatever your keys. Next slide. We also, when we released our new [inaudible] portal, we changed our terms and conditions on a lot of levels, also for DNSSEC.

We have this little quirk in our registry system that all name servers have to be registered with us, which means we know the operator of the name server, which funnily enough is called NSA. And then we change our terms and conditions that the registrant allows the name operator to handle DNS keys on their behalf by default.

They can disable that [inaudible] if you want later on, but the default operators allowed to have the DNSSEC keys on behalf of the registrant, without having to go through a registrar. Next slide.

We started [inaudible], this was a lot of fun because the journalist thought he would change my wording a little bit and make some click bait. So, this is actually says, Danish hosting provider is neglecting DNS security. Under 1% of DNS [inaudible] signed with DNSSEC. They were not happy, but we did get a lot of attention, so [inaudible] does work. Next slide please.

We added newer algorithms after a lot of encouragement from certain people in this room. So, we now support 13 or 14, and we have plans for 15 or 16 [inaudible] this year. Next slide.

First, [inaudible] implementation was kind of low on features. Our registrars are really just registering new domains, so they were only commands that we implemented in the first release. We extended our EPP release this year, in autumn, I guess, and one of the features there is, of course, that we can add DNS keys and delete them in there as well.

Next slide. Not by actual planning, but it turns out that we actually have a DNSSEC workshop every second year. This was the third time. We have around 30 people turning up every year. It's a full day workshop with hands-on, it's a technical workshop so that we both teach [inaudible] DNSSEC, and it's hands on with opening SSAC to actually do signed zones, and [inaudible] at the end of the day.

Next slide. Statistics. We all love statistics. This is different from [inaudible], because most of our algorithms are actually [inaudible] 13, and again, this is not [inaudible]. It's very nasty. They keep finding bugs in our system.

We are working with him, hopefully, later in a couple of weeks. But the reason for that is, on the next slide, and that's because all of the technical implementations we did, we started talking to registrars about finding all of their zones. So, you can see that most of the domains are signed recently in the last couple of months, and those registrars are using algorithm 13.

We're now just crossing 5% of signed domains. I think we are the largest CC that does not have a monetary incentive, which I think is quite unique. Most of the registrars are spoiled. When we talk to them, they say, give us money. And we go like, well, you already have your implementation, why don't you just do it because it's good for your users?

So, we did find some smaller registrars that are doing it. So, we're about 5% and we keep talking with everybody else decided not to do a monetary incentive. I just hope they are going to do it at the [inaudible] house. Also with you, Peter, I'm going to recommend people to look at our domains, their users.

I also found a small registrar with a couple of thousand domains that are signed, but we don't have the keys to them, so we're also talking to them to submit them there now. And I guess that's my last slide. Any questions?

DAN YORK: Any questions for Erwin? Everybody likes Copenhagen, so they don't want to irritate the local folks. Come on, you've got to give Erwin some questions here? Anything about what he is saying?

UNKNOWN SPEAKER: It's very nice, Erwin, as rollover, that you are offering us to upload the keys, though we're not the registrar in the case. Thank you, and I wish others were to follow your good example.

ERWIN LANSING: Thank you.

UNKNOWN SPEAKER: So, question [inaudible]. How are the ISPs in Denmark doing in terms of DNSSEC validation?

ERWIN LANSING: We have three major ISPs in Denmark. Two of them are now validating, the third is not. We are talking to them. So, we are just about 50%.

UNKNOWN SPEAKER: That's interesting. So, the situation is kind of the other way around in the Netherlands, where we have a large number of signed domain names, but not many, i.e. no, ISPs are validating yet. Interesting.

UNKNOWN SPEAKER: Do you want to correct me on that?

UNKNOWN SPEAKER: I'm not an ISP, so.

DAN YORK: For those who are remote, that was an exchange between two Dutch people from the opposite sides of the table. In English, yes, okay. So Christian, there are no ISPs in the Netherlands who are natively validated?

CHRISTIAN: Not yet. There is some rumors that a major ISP will be starting to do that in this year somewhere, so if they do, then it would be very good news, and we were hoping that this will lead to other ISPs following their example.

DAN YORK: Very good. Go ahead, Erwin.

ERWIN LANSING: I just have one closing remark. We, unfortunately, ran out of men's t-shirt, but if you want to bring a t-shirt home for your other half, we do have a lot of ladies t-shirt [inaudible] and a booth.

DAN YORK: So, if you want a woman's t-shirt about algorithm 13, you can go to the DK Host master booth, and they will give you a t-shirt in a woman's size. Oh, okay. For those who are remote, Erwin is now showing us the t-shirt which says, we love dot DK. Yes.

ERWIN LANSING: We have several themes.

DAN YORK: Oh, okay, there are themes there. We should put in a promotion that if you go to the [inaudible] booth, you can get a DNS scarf, appropriate for the cold. Jacques is going to correct me.

JACQUES: We're almost ran out.

DAN YORK: We're almost out, okay. So, you know, the swag is getting low here. Okay, on that note, let's move along to another country here that is going to speak about this, and we have Alex to talk about DNSSEC in Austria.

ALEXANDER MAYRHOFER: Thanks Dan. Good morning everybody. If we look at the format of the slides, you are going to notice that they didn't change a lot between the last time I did this, which was in 2014, which shows that I have to admit that we are… I will put it in a positive way. We are one of the registries doing organic [inaudible] from DNSSEC, so we love having a lot of activities in that way.

But let me give you a little bit more detail about that. Next slide please. So, in what areas do we actually provide DNSSEC services? Obviously, we run the ccTLD dot AT. And we have DNSSEC in production since February 2012.

We use open DNSSEC for that, and we actually offer our registrars to upload the DNS key, DS [inaudible] and EPP extension. I understand that APP extension. We also operate a product that's called registry in a box, and that is a registry back end service for nine new gTLDs that we operate.

As you probably all know, DNSSEC is mandatory for the new gTLDs, so we run open DNSSEC for those TLDs as well, and we allow upload of DS records. Something that we also operate, we run our own any cast network, that we also offer to customers. If you haven't seen our video, America First, [inaudible] secondary, it's highly recommended, yeah.

And what we do there, we offer a bump in the wire signing for our customers, and we [inaudible] for that. Don't ask me why, that's why our engineering department decided to do. So, it's like free and included in the service, and some of our registrars actually signed up with us, because they were too lazy to implement DNSSEC signing themselves, so they went for that service.

Next slide please. Yeah, that's just a brief recap of the timeline. Like everybody else, we did a test bed and we had a deliberately unresolvable AT zone. So anyway, and then we had the DS in the root and we started EPP a couple of weeks later. Next one please.

Registrar statistics. We, as of March 2017, we have 405 registrars. We lost a couple of registrars since 2014, mainly because we introduced a minimum fee on registrars, which put off some really smaller ones. What's a little bit special about us, we ask our registrars to indicate whether or not they support DNSSEC.

And what happens actually, we could argue for this for like a couple of beer evenings, when we see a transfer to a registrar that doesn't have DNSSEC turned on, we actually remove the DS record from that zone. That was a policy decision that we took in 2012, so we probably need to revisit that again.

So, out of the good news is that out of our 405 registrars, about 20 more decided to click that yes, we support DNSSEC, switch in their internal registry registrar panel, and actually 43 out of them, which is, yeah, I'm going for marketing stuff here. It's almost as many as 2014, actually have at least one DNSSEC enabled domain.

Next one please. So, as I said, we never really gave registrars any kind of incentive as to monetary incentive to actually enable DNSSEC. So, we have like very few signed domain names. But, looking at the figures from 2014, we almost quite [inaudible] so that's good news. Next slide please. That gives a little bit of a timeline, again, funny thing here.

Credit where credit is due. The jump in DNSSEC enabled domains in 2015, seems to coincide with the German DNSSEC day, and that actually makes sense because a lot of our bigger registrars are actually based in Germany. Yeah, so it seems like [inaudible] did a good job for us in terms of like increasing the number of DNSSEC domains about actually, by 50% in a single month, by a single [inaudible]. Thank you very much [inaudible] sponsoring it next time.

Thanks to this idea. Yeah. We also see, interestingly enough, a little like hint of a hockey stick figure at the very end of the chart, actually look closer at that, whether we see an accelerated growth in terms of registrations. Next one please. Registrars, that's not linear scales, not a logarithmic one.

So, I think like you've seen everybody else's presentations, DNSSEC domain [inaudible] is dominated by a few bigger ones. And there are quite a few out there, just test domains or they have that one geek who loves to add DNSSEC to his domain. But the majority of registrations comes from the top five, six, six, yeah. Next one please.

So, what did we do recently? We removed [inaudible] DS record from the root zone. We did a couple of KSK rollovers, obviously, and we enabled support for [inaudible] 13 and 14 in EPP quite recently, I think a couple of weeks ago. What I might think about doing is like do like a local DNSSEC folks beer evening, or something like that, just a local operator to like figure whether they're aware of the KSK key roll over in the root zone.

Yeah, but that's something that came to my mind only recently, so it's not on the slides. Next one please. Last one. Thank you for your time. That's it.

DAN YORK: Thank you for that view into what's happening in Austria. So, any questions for Alexander?

UNKNOWN SPEAKER: When exactly did you enable algorithm 13 slash 14?

ALEXANDER MAYRHOFER: I need to look it up. A couple of weeks ago, I think.

UNKNOWN SPEAKER: Okay, thanks.

DAN YORK: Any other questions? Oh come on people. All right, questions for the entire panel? I have one if nobody else does, so come on, somebody save them from me for something. Anybody? Phil, you must have a question. No? Phil, no? Anybody else?

So, my question was basically, if you think about all of the presentations here, I guess I do have a general question. What do you think are some of the things that can be done to enable more registrars to get into the designing side of things? What advice do you have for others? Or what have you seen from your space?

UNKNOWN SPEAKER: So, what we found out here in Denmark with all of the initiatives that we took last year, is to talk to the registrars and talk about the hurdles that might be technical, [inaudible] wanted it in EPP. We had a different service called DS upload, [inaudible], which is a very simple API with post-string.

You just post the string and say, this is my key, nothing else. Now we have EPP, registrars said we want EPP. It might be a simple API, but it's a different API, so we had an EPP. It might be other things. It might be policy, like we changed the terms and conditions, talk to the registrars, find out what the hurdles are from a technical policy side, and then talk to them about starting doing it.

Just make it easy for them.

UNKNOWN SPEAKER: The funniest thing is that when I talk to registrars, very often it's not a technical decision. What happens in some cases is that, take out, they got in front in marketing, that there is another competitor out there, who has like for their, we're posting… He has a lot of checkmark at [inaudible] that's called DNSSEC. And the marketing department [inaudible] engineers there and says, we don't have that in our product description.

What's it? And the engineers go like, okay, okay. And that's when they come to us and talk to us, for example, to sign up [inaudible] aware signing. So, it's sometimes hard to convince them that there is really a technical advantage that wades off the administrative burden. That still has to happen, I guess, especially since there is, as we talk like for ages before.

The end doesn't seem to be the [inaudible] product yet. So, in most cases, it's marketing driven, funnily enough. Yeah. It's another checkmark, yeah.

DAN YORK: Those darned marketing communications people. Go ahead Peter.

PETER KOCH: I'm with Alex here. I think, I like the term organic growth. And I think that is what we see happening for DE as well. We have also withstood the temptation to retroactively assign financial incentives, even if at least one registrar asks for that. And quite frankly, that wouldn’t be supported by financial model, and governance model, and so on and so forth, so we just couldn’t.

But it also doesn’t make sense because others have already done that and that would punish them, and give them a disadvantage again. We also see that there is probably not so much a technical issue, especially given that we have these 20,000 domains already being signed, and what I didn’t say, forgot to say, was that sometimes these are in the hundreds of domains, sitting with the registrar that already has several thousand domains under management.

So, this is very often a communications topic to be very neutral between the registrars and resellers or enterprise customers. But things improve. Talking helps. We could like motivate people to talk to their specific customers [inaudible] but it takes time. Patience is also very helpful, and I regret to say that.

DAN YORK: Thanks, Peter. Anyone else?

UNKNOWN SPEAKER: Yeah, I have a question. For Peter mainly. The remark was just made that [inaudible] that people are thinking yet, but the

German BSI wrote these documents about making use of [inaudible] in the context of email, something that you should consider or should be mandatory for German Federal government agencies, that was my understanding of what the document says.

Have you seen any effects of that kind of standardization on your numbers? Because I know, in the Netherlands, the fact that the Dutch government put DNS [inaudible] on the explain list and has now done the same with DANE, is really a driving force. We're getting questions about hey, do you support this? Because we've seen it's on the complier explain list.

PETER KOCH: So, I don't think there is a similar thing like this list. There are for regulated sectors of the market. There are various requirements, but that would often enough only effect small numbers, however what we don't see here is the, quote, importance of the domain. If it is a domain of a major newspaper, or the domain of a major access provider, or somebody else.

This is counted the same like your and mine private domain. So, if we would… We can, of course, always adjust the measures to drive success, or at least made look at successful, but I think this is really important to understand that not all of these, like in our case, 16 million domain names, need to be signed to actually make the internet a safer place there.

There are domains that are very, very frequently resolved, and others that may be see one or two resolution requests an hour or even a day. And thanks for serving me another keyword here. I also did not mention, and partly because that was already in the report that Dan mentioned. And the BSI, the [inaudible] security indeed issued a recommendation for email service providers to support DANE and validation in that context.

Again, that would cover their email service. And on previous occasions, we need to discuss that this was a very interesting spot to deploy DANE on, because you explicitly don't have to affect your customers. You can do that in your mail department. And that then suggests that wouldn't affect the numbers, but we see this happening. We also know that the federal government itself has signed their domains.

We also have one larger cable provider doing validation, and exposing the customers to those validation results. And there is Google, of course, but the figures are usually what Jeff provides. There is some growth, it's not valid, immediately is reflected in the number of signed domains.

DAN YORK: I think it's interesting too, the growth on recommendations are on email both from the BSI and also from this to others, which I think has fed into the fact that when you look at our agenda today, we have a number of things about secure email services and looking at how DNSSEC and DANE can work together for that. We have a question back here. Yes?

UNKNOWN SPEAKER: One question, one remark. My name is [inaudible]. I work for a security company in Germany, [inaudible] advisory board for [inaudible]. Just to show my background. The first is a question to Peter and Alex. If you really show, if you look into the numbers and see what is the aspect of busy Dutch folks, can you see how much really, how many German registrars really go to DNSSEC?

So, do you think that this is still only the Dutch influence? Or do we really have respect for the numbers of German registrars doing DNSSEC?

UNKNOWN SPEAKER: I try to go first here. So, I guess that was the slide. I'm sorry, I can't look in your face and speak into the microphone at the same time. I have this 109 registrars on that slide, with the right hand at one domain, and the left side being the larger ones, I'm not completely sure. I think two of the five were German registrars that entered this scene after the DS IDN initiative.

But the ground had been set there, and we have lots of others. The situation is a bit complicated, assigning the domains to registrars and resellers because we only always see the registrar, but then we know according to, or can investigate according to the name servers used, and who is the operator? And then we find that it's probably a Dutch registrar slash name server operator going through some German based registrar, and which means the registrar supports DNSSEC in one way or another, also there are lots of registrars doing wholesale on the domain side and not necessarily supporting infrastructure, which complicates the picture a bit here.

This is also making it difficult for us to tell the end user, for example, this and that registrar supports DNSSEC, because what does it mean to support DNSSEC? And actually which product would the end customer have to choose? I'm not sure that answers the question.

UNKNOWN SPEAKER: That's okay. The other thing is, from the end point, from the end customer point of view, the only thing our customers tend to use DNSSEC is compliance. You see, this is the only thing. So, if we have [inaudible] insurance, of course they have 100% compliance and so they have DNSSEC.

So, we have strong data regulation stuff in Germany, we don't have any DNS security regulation, that's why. We don't have compliance that forces DNSSEC, and so DNSSEC will stay low until that day.

ALEXANDER MARHOFER: Alex Marhofer. The situation is pretty similar for us. From as far as I remember, I need to look that up [inaudible], but I think that out of the six larger registrars that had DNSSEC registrations with us, I think that at least three of them were picturing them and reseller [inaudible] in a way. I haven't looked at whether the domain name registrations itself are from the Netherlands in that case, or whether they are based.

We don't have that many registrations from the Netherlands. In either case, I would need to look it up. At least, I would say that the majority of DNSSEC registrations in our registry comes from the bigger, highly automated German reseller engine registrars. Yeah.

DAN YORK: Jacques, I saw that you had a question.

JACQUES: Well, we have five minutes left, right?

DAN YORK: We do.

JACQUES: So, not really relative to Europe, but with the DINE outage, a couple of months ago, I guess. It was kind of a sad day for DNSSEC, for registrar. There was a lot of registrar data, try to do emergency DNS operator change. And for those high profile domain that are DNSSEC enable, the cache, the DS was cache for 24 hours.

And they had a hard time transferring a domain over. And there were frantically trying to clear the DS records. So, that's perhaps a topic for another session. But we need to be able to [inaudible]… So in Canada, we already have a hard time getting registrar to do DNSSEC. And when we had an example of a large [inaudible] failure, so we need a solution to address this.

DAN YORK: All right. So, you're just completely hijacking the topic of the discussion here, but okay. No, that is a good topic to look at that, how do we do the automation of the secure key, and we have a number of proposals out there, or implementations that people are using. And I think that would be… You want to…? Go ahead, Erwin.

ERWIN LANSING: That's just one of the things we did three years ago, I think, is decrease the TTL for the DS records, to one or two hours, which is still too long in this kind of case, but leaves it shorter than one day, which is for the rest of the zone.

DAN YORK: And that would be an excellent topic if somebody wants to bring that to the DNSSEC workshops in either ICANN 59 or 60. So, if somebody wants to think about that, Jacques, I don't know… Somebody… It sounds like a good topic to have a conversation about if anybody is interested.

Well, I would like to… Let's give a round of applause for all of our speakers here from the region. [Applause]

Okay. I'm going to stand up, because I'm up to talk about the IETF. Anybody who is presenting, if you want to stand up like me, you're welcome to me. Or you can sit at the chair and hit the button.

JULIE HEDLUND: And this is Julie Hedlund. I'm sorry, I have to contradict that. It only works for PowerPoint slides, and we do generally ask people to provide their slides in PDF. So, your special, Dan.

DAN YORK: All right. I'm special. Special in some form. By the way, I want to thank the gentleman who asked the question about Egypt this morning, because in the way this works, of course, I was immediately corrected by somebody that EG is not signed. And in fact, when we looked in the database, we discovered that I actually have to check the map code that is used to generate those, which now makes me concerned, because there is no record in the database for dot EG either.

So, something is not quite right. If anyone has some cycles in the next little while, to dive into some Python code, I would, anybody who wants to do that, talk to me. I've got a database that needs to be checked on why there is no EG record, but yet EG was colored in. Anyway, I want to talk about DNSSEC activities at the IETF.

How many people have, are involved with the IETF in some way? Okay. And a good number of folks around the table here. I just want to talk quickly, you know, the IETF for those who are not involved with this, is the Internet Engineering Taskforce, which is the organization that creates the RFCs, or the request for comments, which are the standards that power the internet here.

It is organized into working groups, WGs, working groups that are out there. There are 100 plus of them at any given time. They have a charter that goes for a certain period time. They are chartered to create certain standards. Warren and Oliver, for instance, are here who are part, who are the chairs of the DANE working group, that is there to create that.

There are also what are called birds of a feather sessions that go on through that. That are when we bring new work in, new areas there. And the nice thing is that anyone can participate in a working group. You can join a mailing list, you can become part of that, you can do that kind of thing. And anyone can submit an internet draft, as it's called, a document.

And the process that happens within the IETF, is that somebody creates an internet draft on some reason, something they think should be standardized. It goes through a process where the working group discusses this draft. They talk about it, they debate it, they endorse it, the approve it, they adopt it. And it goes on through this until eventually the internet draft is published as a RFC, or it's abandoned, or something like that, or it morphs into something like that.

But this is the general process that the IETF goes through for standards. Now, where this comes in with the DNS, oh, one other piece. The IETF primarily does all of its work through email lists. That's where things happen. That's where things get approved. All of that. But three times a year, people get together in different places of the world. It moves around so that it's equally convenient or inconvenient for people in different parts.

The next meeting where… How many people here will be at IETF 98 in Chicago? Depending upon my border guys. Well, outside of US border issues, but you can see a number of the folks who are here, will also be in Chicago. And what happens there is basically all of the engineers involved in different topics, that people get together to have face to face meetings where the most contiguous issues typically are discussed.

Things that cannot be solved simply on email get debated. You know, we've had all sorts of those kind of discussions in there about, you know, what are doing with different…? Gee, Warren, what are we going to do with special use domain names? Oh, and… [Laughter]

Time out, yes. We have lots of these kind of passionate discussions of things that happen in there. It's the work to move along what goes on. So, there is three this year. Chicago, Prague and then Singapore are where the meetings are held this year, and they'll be moving around from there.

So, some of the activity that's happened in the IETF that's DNS security related, the major group right now, where a lot of the DNSSEC activity happens is within the DNS operations group, or DNS OP. And actually, Susan Wolf, who many of you may see around here, ICANN Board, RSAC, other pieces like that, she is one of the co-chairs of that group as well, and they're doing a lot of, you know, DNSSEC is at the stage where the standards are well-defined.

It's now the process of getting it out there and deployed, and as we've heard about things, there are new changes, feedback that needs to be brought into the process about how do we do that better. One of the more recent RFCs is managing DS records with CDS and CDNS key. And I think, Wes, I see him there, is part of that, Oliver, others.

So, that was the way of automating providing a new DS record up to there. There is a draft about aggressive N-SEC caching, and some of the use that can have, which is currently in what's called last call for the final comments before it gets submitted for publication.

There is a number of other different documents that are going through that process, but if you're interested in where more of these standards are, DNS OP is probably the group to follow right now. I should say, there is a lot of other DNS operational activity that happens there beyond DNSSEC.

So, you can see that in the pages that are there. So, another group that has been very active is the DANE working group, which has been chaired by Warren and Olivier, that was charted to create the DANE standard and other associated standards. That group has moved along and is pretty far in completing its work, and really in the stages of looking at how is it closed down some of its activity and, right? You guys… Go ahead, you can say something.

UNKNOWN SPEAKER: Or a final document is at the ISG and we're just waiting for that to be published or rejected before we closed up.

DAN YORK: And his co-chair looks at him with funny eyes, saying, wait a minute, no. So, and this is part of the process. The IETF charters a group, develops standards, and then closes the group because its work is done. The standard is out there, it now needs to be deployed and done in some ways. The other group that's had a lot of activity recently, is the DNS privacy group, or DEPRIVE.

And this is a group looking at confidentiality. You know, we talk here about integrity, making sure the data coming out of DNS is the same info that was put into DNS. It's really, I mean, it's all of what DNSSEC is about. But this group is looking at the confidentiality of how do you know when you're going and sending queries to your local resolver, you know, how is that protected? So, somebody can't go and snoop that and learn all of the sites that you're going to and the pieces that are there.

And so, the primary, the mechanism being looked at there is, DNS over TLS. How do you…? You encrypt the connection between your stub resolver and your system, and your local recursive resolver that you're talking to, and you're doing that. That's where a lot of that work has happened. There have been two RFCs published lately.

As you see up there, there are 7858 for DNS over TLS, and RFC 1894, which is DNS over DTLS. So, those two of the… And that one was just like last month or two months ago, January I think it was published, the later one than that. There is still a good bit of ongoing work in that group, around different mechanisms to do that. It's also now starting to discuss whether the group should move on to talk about going from the recursive resolver, to the authoritative resolver, and looking at that next step of, do we protect the privacy between those two elements?

I will tell you, this has also been an interesting thing when I've been talking at enterprise customers, or enterprise conferences when I talk to people deploying this inside of, you know, DNS inside of enterprises, because they look at that and suddenly say, wait a minute. All of the DNS queries for my laptop to my, to the local resolver will be encrypted?

If that happens, then I can't do all of my monitoring and blocking and other pieces that I do inside my enterprise to prevent people from going to sports sites, or porn, or whatever other things they are doing inside of there. So, this was big news to some of the enterprises that the IETF was going off and standardizing this.

My response, of course, was well you control the computers, so you can turn this off inside your enterprise if that was really important to you, but you need to know that this kind of thing needs to be developed, because of the pervasive surveillance and everything else that we've seen on the internet out there in some way.

The other item of note that you should know is another group called [inaudible], there is a thing within IETF that you must have a cute name for your working group, is this is about elliptic curve cryptography, and how do we bring that into more protocols and things? And just recently, there was a standardization of a new RFC on ED DSA, the Edward's Curve for the cryptographic algorithm that's there.

And that has now been standardized as RFC 8080. And it is algorithm number 15? 15, 16? 15 and 16? And those through there, and Andre [inaudible], who is not here, was one of the authors of that, along with who else? Or was that just Andre? It was Andre and somebody. I don't remember. We got this. It's out there now.

So, we have a new crypto-algorithm that is available, and I know that there have been a number of people who have been looking at implications of that in some way, shape, or form. So, this is kind of the major activity that's happened in a bit. At IETF 98 coming up in just two weeks in Chicago, the kind of the DNS pieces that are going on there, will be there is an IETF 98 hack-a-thon that happens the week before.

There will be some more DNS activity there. We've been doing that the last several IETF events, where there is a hack-a-thon even in the two days' prior, and there are teams that have been there doing things. Ben, are you going to be there for that?

Okay. You want to say anything about what you're doing there? This is Ben [inaudible] from…

BEN: So, Ben [inaudible]. So, on Saturday, Sunday, I and a number of my team members, [inaudible] DNS, but also people from [inaudible] on the [inaudible] developers from IFC, well, we [inaudible] two tables, and we have a number of projects we want to work on. Sometimes, there is nice cross-overs of people from different projects collaborate on implementing, or interoperability of RFCs [inaudible].

And sometimes, for example, for the get DNS project, we are also focusing on our own project and put forward and get new features implemented and out there, and give back actually to the community. I think the interest for the IETF is that RFCs get implemented. You get sample codes, [inaudible] reference implementations. It's great fun.

DAN YORK: If you're in Chicago, or if you know people in Chicago, you might want to go and help, or if you're coming to IETF, and you come in early, you're welcome to go and hang out in a windowless room with a bunch of other DNS folks and work on code. It's quite fun.

BEN: Yeah, about 10 to 15 people hanging around. So, it's very, very good for exchanging ideas.

DAN YORK: The other area, DNS operations, the DNS OPT group is meeting on Monday this time, at the beginning of the week. The agenda has not yet been published. There are a number of different drafts up for discussion that are, there aren't too many DNSSEC related ones that I've seen on there. It has mostly been a lot of other DNS, some of the… RPZ is going to be a contiguous issue, I suspect.

And there will be a number of other different topics on there. I haven't seen as much. Warren, you guys seen much on the DNS OP? Not DNSSEC related, as much.

WARREN: No, it's mostly just straight DNS.

DAN YORK: Yeah. But it should be some interesting discussion there. Paul, you mentioned there might be one in the IPSEC group, don't know the agenda yet, but again about with email, right? Was the….

WARREN: No, this is about split DNS, so when you connect to a VPN, like you connect the [inaudible] from your internal network active on your device. So, you can do internal DNSSEC resolving, when you're connecting to your VPN.

DAN YORK: Okay. Well, that maybe discussed in the IPSEC group, right? Okay. And then in the security area group, there will be a, there is a draft about NSEC 5, the proposal for that, and that will have some discussion there. Go ahead, Warren.

WARREN: That's also in DNS OP as well. It's showing up in multiple place. There is also, Roy [inaudible] has a thing on doing [inaudible] 256 instead of [inaudible] one, which is going to be presenting, [inaudible] to implement instead of…

DAN YORK: Okay. All right. So, that's a bit about what's happening at the IETF. And on that, any questions?

Yes.

UNKNOWN SPEAKER: [Inaudible] I think we should not forgot also about the [inaudible] working group, which recently published [inaudible] about transferring keys, and there is all Jacque's draft about transfer of key material about [inaudible] registrar, registries. So, it's also important working group regarding DNSSEC.

DAN YORK: Thank you, very good. Jacques, do you know, is that going to be presented in Chicago at all?

JACQUES: We're on the agenda for the experimental track, the new team. So.

DAN YORK: Oh, okay. All right. Good to know. Yes, the registries extension group has been the group that's been looking at how… And that's actually for folks who are here at ICANN, for the registrars, registries, that's something, another good group to monitor, to work around that. Okay. That's all.

You can follow along at… If you go to the IETF website, you can follow along remotely if you would like to, to be able to see any of the things that are happening there, and you can participate. So, that's all from me, and I think we'll next bring up Matt to talk about the root KSK.

Do you want to speak with this, Matt? Can he do this with you hitting next slides? Yeah.

No, no, you don't have to. He doesn't have to use a clicker. Yeah, here you go.

MATT: Hello. If you have attended all of the DNSSEC sessions, you might be luckily enough that this is your third time in Copenhagen to hear me talking about the root KSK roll. So, I'll do the best I can to be entertaining, hearing the same thing three times.

So, I just want to give a quick update, since as I've said, you've probably heard this before, and may well be aware of it. Can I have the next slide please? This is the timetable for the root KSK roll. We generated the new key back in Q4 of 2016, that was in ICANN's east coast key management facility. The next quarter, we moved it to the west coast key management facility.

So, that the new key has been generated, and it has been in all of the right places, and it's what we consider operationally ready. So as of right now, we're in the phase of the project where we are telling people about the new key. I have shown it, not in this new presentation, I don't have it, but I've shown it in other presentations here.

It's not yet published in DNS, that will be on July 11th. But we're in the phase of the project between now and the actual role that we're communicating, mostly to operators. That's our target audience at this point, because if the operators don't update their trust anchors, then you know, bad things will happen.

So, that's the main focus of the communications right now, but certainly, we're happy to talk to anyone, and I appreciate the chance to talk to this audience, to let you know what's happening. So, the big date is October 11th. That is the date of the KSK roll, and that's the date that everyone has to be aware of.

Of course, especially if you operate DNSSEC validation infrastructure. And then after that, we will revoke the old KSK, and eventually securely delete it from the key management facilities. So that puts us in this time period between the key generation and the roll itself. And one of the important things that's going to happen is anyone who supports the automatic, rather, automated trust anchor update protocol, there is software, if it's operating correctly, will automatically update the trust anchor.

If you're not familiar with that protocol, it's pretty straightforward. The idea is that, if you already trust one key, and then you see a new key, that's signed by the key that you trust eventually, after 30 days, you'll trust the new key. Just transferring trust from one key to another, and so it's important that if you're relying on RFC5011, that it actually work, and there have been RFC5011 test beds before, that let you test your software, but they've been designed primarily for software developers, because RFC5011 has this 30 day ad hold on timer it's called.

It's very hard to test it in real time. You have to be patient and wait 30 days. So, from a software developer's perspective, what you can do is crank down a hold on timer, and use a test bed that operates in accelerated time, and does a key roll very fast. But what, at ICANN what we wanted to do was offer a test bed for people who could actually test, in real time, that there RFC5011 implementation worked correctly.

So, go to the next slide please. So, we announced this test bed just this week at the opening ceremony. So, we've created this test bed that's designed that potentially an operator on production infrastructure could use, because rather than rolling the actual root zone, it rolls zones deep within the DNS tree, that there is nothing else in that nobody would ever go to.

So, it's safe to configure these zones on a production resolver. And then the idea is that you can make sure that the resolver does a proper trust anchor will, with these zones, and hopefully it can successfully do that, then you're in good shape. And we're not trying to test here particular implementations that they've actually done it correctly.

You know, I'm not worried that [inaudible], I'm not worried about their code. It's more the packaging of that code. You know, can they write the key to the file system? Like, did somebody actually deploy this on, with a permissions problem, or on a read only file system, or something like that.

I realize that those things are probably are unlikely, and that the vast majority of people who think that they have RFC5011 support will do have proper 5011 support. Nevertheless, this was relatively straightforward to set up, it's not, it wasn't rocket science to do this test bed. And so, it's something easy that we can offer the community.

It basically is a mailing list. There are zones, a new zone every week that goes through a roll. So, every Sunday, we start a new zone through the role process, of the zone name you see there, 2717 [inaudible] five, that was actually last week's zone. This week zone is now 03-12, the Sunday was the 12th.

So, if you subscribe to the testbed, if you go to the testbed page, which is the bottom there, and could I have the next slide please, Julie? So, there is what it looks like. No expense was spared on graphic design for this webpage. You should have seen it before the coms people, [inaudible] what two engineers, it was the best of 1995 HTML.

So, really what's subscribing to the testbed, what joining the testbed means is subscribing to the mailing list for this week's zone. And then you get a few messages, one every week. I believe it's eight messages total, just telling you what's going on in the testbed that week, what to expect, it's very straightforward. It's a resource for operators or anyone who is interested.

So, that's the main thing I have to say just to let everybody know that the KSK is rolling, that the process is moving along just fine. To remind everyone, October 11, 2017 is the big day. And then I would just take any questions if anybody has any.

DAN YORK: Do we have any questions for Matt?

UNKNOWN SPEAKER: Well, if nobody has a question, apparently I need to ask what time a new key will appear in the zone?

MATT: Well, that's a good question, and that got asked yesterday at the session. Are you my plant in the audience? Oh, okay, all right.

So, we will announce to the community what time the actual time that the new root zone with the new key signing the key set for the first time, will be released.

We'll let people know in advance, so that you can be you know, you'll know the exact time to go into your bunker to prepare for the end of the internet.

UNKNOWN SPEAKER: Or get champagne.

MATT: Or get champagne, yes. Yes.

UNKNOWN SPEAKER: [Inaudible]. I've tried testbed, and I saw that there is a guide how to set up [inaudible] and bind. Would it be possible to include also not resolver?

MATT: Oh yes, thank you so much for mentioning that. I'm sorry. I just didn't get to not, just ran out of time. So, I would be very grateful to have text. If you submit text, we would update it immediately. Thank you very much.

DAN YORK: Anything else? Anyone else? Everybody prepared? You've got your trust anchors updated? Go ahead [inaudible].

UNKNOWN SPEAKER: Yeah, about testbeds. I know there is this, by… [Inaudible] contain trust anchor on the other side, which actually [inaudible] to get automatically the test anchor in. I come to test that as well.

MATT: I'm sorry [inaudible]. Can you say that again? I didn't hear.

UNKNOWN SPEAKER: The IANA site has trust anchor, and also [inaudible] in a signed block. Is this going to be part of this test as well?

MATT: No. we made the conscious decision not to exercise that part of the machinery, because that is specific to the root zone. So, yeah. We just declared that out of scope, basically, we're allowing people to test their 5011 implementation, but not what I know you've done an unbound anchor, for example, not exercising the ability to download the trust anchor file from the root, because that is, that is dedicated to the root.

That's machinery specifically around the rootzone key itself, as opposed to an arbitrary zone, trust anchor like the testbed does.

DAN YORK: Nobody else. Okay. Well, Matt, we'll give you, we'll let you step down, I guess. Thank you Matt. [Applause]

So, we do have a couple of minutes before we get our next panel up here. So, I will just mention that there is, there are snacks out there, some muffins, and some cheese, and such. And there are some…

[END OF TRANSCRIPTION]