BARCELONA – DNSSEC Workshop (1 of 3)
Wednesday, October 24, 2018 – 09:00 to 10:15 CEST
ICANN63 | Barcelona, Spain

UNIDENTIFIED FEMALE: October 24, DNSSEC Workshop, Part 1, 9:00-10:15, Room 113.

RUSS MUNDY: Good morning, everyone. It's not quite 9:00 yet, but our first panel is quite large, and hopefully I've been catching people as they came in the room. But I may have missed someone because the first panel is very large. There are nine people on it. So if there anyone in the room who is on the first panel who I haven't snagged yet, the chairs at the table here are where we'd like the panel members to sit. We'll begin here in a short bit, but before we actually begin – and I'll probably try to say again – the lunch arrangements that you see over there are NOT for the DNSSEC workshop. Our lunch will be upstairs, two flights of stairs upstairs. This is for a different group, so at lunch time we'll all have to clear out.

STEVE CROCKER: Hi, this is Steve Crocker.

RUSS MUNDY: Oh, and now Steve is on the phone with us. Good morning, Steve. This is Russ and you are in the room with us.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

STEVE CROCKER: Thank you.

RUSS MUNDY: Okay, let's see how we're doing on our panel members. Okay, it is 9:00 now, and I think we have almost everybody on our nine-person opening panel. I'm Russ Mundy and I'd like to welcome everybody to the DNSSEC Workshop at ICANN 63. We have a very full program today. I won't do very much of an introduction other than to point out yet one more time the lunch set up over there is not for the DNSSEC Workshop. We go out at lunchtime, up two layers of stairs, and it's a nice banquet hall Kathy tells me. Anyway, we do have to all leave the room at noontime for the lunch break and then come back afterwards.

So with that, we'll get underway. The first person who is going to be doing the presentations for us is Erwin – I never can remember how to say Erwin's last name, so I will let him say it.

ERWIN LANSING: Oh, I don't live in Holland anymore so I don't remember myself. Now I've got this microphone, so I might as well stand up. Welcome, everybody. So first of all, have we all finished our collective sigh of relief? Not yet?

UNIDENTIFIED MALE: [We have.]

ERWIN LANSING: We have? Great. We rolled the key, and the Internet did not break. We did not break the Internet.

So for today, [is everybody on the program ready]? Raise your hands. Just a few. Next slide.

Thanks our sponsors for lunch: SIDN, CIRA, and Afilias. Thank you. Next slide.

The workshop was organized by SSAC and the Internet Society Deploy360 Programme. Dan cannot be here today, otherwise he would be standing here doing the introduction. These are his slides though. Next slide.

We have a packed program.

UNIDENTIFIED FEMALE: Very packed.

ERWIN LANSING: Yes, so let's go on to the next slide, and next slide. We have a lot of numbers, and I'll give some more numbers about Denmark later. But these are the numbers for the whole world. These are based by the work Geoff has been doing for APNIC on collecting DNSSEC validation statistics through Google Ads, and it's still increasing slightly. That's about 14% for the whole world. We definitely want that to be higher, right? Next slide.

Some of the regions. You can see some of the regions are using a lot of Google. Google, of course, does their open resolver that does DNSSEC validation. Number one, Micronesia is 62% Google. Having a lower percentage of the Google statistics, of course, means having better support of the local community, of the local ISPs doing the resolving. Next slide.

These are some of the numbers on the signed domains. Christian, is this number right for Holland, [62,000]?

UNIDENTIFIED MALE: We don't know because we can't read.

ERWIN LANSING: I can. It says 62,240.

UNIDENTIFIED MALE: [inaudible]

ERWIN LANSING: Signed domains? Yes, so I'm not sure how Dan actually collected these numbers. But .com number one, .se number two, .nu, .net, .nl, .cz. I was wondering about Holland. That should be more. Next slide.

On the TLDs or at least the ccTLDs being signed, the Deploy360 Programme does a lot of work collecting who is actually signing the domain names or have signed [their] TLD. There are five levels. It starts with experimental, doing internal experiments. There's nothing in the

zone yet. They yellow one is for announcing to the world that they are going to look into it and start doing something. The blue ones have signed the zone but do not put the DS in the root, which means that the validation is not working yet. The light green is the DS into the root, but then not accepting DS records for second-level domains yet. And then the dark green is fully operational with signed second-level domains as well. So the full validation chain works through the hierarchy. Next slide.

We've got the whole world, which is getting more and more green which is looking good. We do have some white spots. I think the next slide is Africa which is quite white, having a few countries doing the signing but we still need a little work there. The next slide.

Yep, so southern Africa is doing well, but middle Africa is still quite white in this case. Next slide.

Asia getting greener. A few little holdouts in the Middle East primarily. Next slide.

Almost all green. Good luck, Europe. Well done. It looks like Belarus and Italy are now operational, as you want. Next slide.

Latin America looking good as well, getting there. Next slide.

Greenland coming, [not that many] TLDs in North America. Next slide.

So these maps are updated weekly. You can find out more on that link if you want to [come to it as well] because these are manually by Dan. I think that's the last slide. No.

Yes, that's the report the Deploy360 Programme did in 2016. It's a bit old but still a good report. I put in a lot of numbers there, did a lot of work, so go look it up. I think that's the last slide. Yes.

So with that, I think we will turn it over to the first panel.

RUSS MUNDY: Okay, because our first panel is so packed, we're not going to take questions after the maps section as we usually do. But thank you, Erwin, very much for helping us do that intro and doing the Dan maps.

With that, we will move right into our panel. Our first presenter on the panel is Erwin for what's going on in DK.

ERWIN LANSING: Hello again. Erwin Lansing, .dk. These are the numbers for .dk. It's increasing slowly up to about 24,000 domains signed, which is almost 2% I think out of 1.3 million domains. We keep working on convincing our hosting providers and registrars to do the signing. I'm not sure about the green number, but the blue number here is Algorithm 13 which looks interesting because everybody things people are using Algorithm 8. But a lot of our registrars moved to signing quite recently, in the last year or two, so they went straight through [inaudible] algorithms, which I think is good. I think the little one there in the middle that' a couple of domains signed by Algorithm 5. Want to get rid of those.

And the validation, I showed you the number for the world was about 14%. Denmark is doing quite well with 64% which is four out of five of the major ISPs doing the signing. This is also based on the APNIC numbers.

My last slide is our plans for the future. We have a unique system where all name servers have to be registered in the registry, which also means that all name server operators do have a login to our [self-service]. That means we can use that for allowing them to update the [inaudible] records on behalf of the registrant directly from the name server operator also going even if the name server operator is not a registrar.

We've had a proprietary protocol for that I think since 2010 when we signed the first time just after the root, which you can see in the bottom it's basically [an http] post command where you [send in] your login and they [key] information so you can update these automatically even when you're not doing [EPP] or want to use a self-service [inaudible] device.

It serves us well, but by now we do have the CDS/CDNSKEY protocol, so [I] probably want to look into that. However, looking into the zone and seeing how many CDS and [CDNSKEY] records there are of zones publishing them, it's hard to [validate] getting resources in our developing department with only 1200 domains doing CDS. So that's something we should look into. But those are plans for the future, to make the signing easier for our operators.

And that's my numbers for .dk.

RUSS MUNDY: Thank you very much, Erwin. We really appreciate that. Next, we will hear from Michael Hausding from SWITCH and .ch. Go ahead, Michael.

MICHAEL HAUSDING: Okay. I will give you some updates on numbers but [most likely] what we are doing to promote DNSSEC. Next slide.

The first one is the numbers of DNSSEC signed domain names. As of today, we have 57,000 signed .ch domain names. That's nearly 3%. This is a graph we also publish on our website. It started one year ago, and you can see from 2017 there's a rise in DNSSEC signed domain names. The main reason for that is that one of the registrars signs now by default if a domain name is newly registered. You'll see a small flat plateau on the top. That's why he forgot to sign. He made some changes and because there was not even a button to turn it on or off he made some changes and then he forgot to sign the domain names. But we realized and he changed it. Next slide, please.

We think that numbers are important, and that's why we publish something called the .ch Resilience Dashboard. Next please. We did together with Hardenize. That's Ivan Ristic who founded SSL Labs and he has a new project called Hardenize where he measures the implementation of security standards for web and for e-mail. Next slide, please.

We took the top 1,000 .ch domains and gave them to Hardenize, and they made a dashboard how good are these domains regarding

security. You can see we have 91% of HTTPS. Also, STARTTLS for e-mail is quite good. But if you go to the next slide, you will see that DNSSEC only has 3% within the top 1,000 .ch domains. But we think that it's important to give it visibility so people see how they're doing. Next slide, please.

We do some more to promote DNSSEC. This year we did DNSSEC training. In the beginning, we planned three DNSSEC trainings. They were free one-day trainings where you would learn basics about DNSSEC and how to sign your zone with PowerDNS. Within 24 hours, they were all three booked and we had to run two additional ones. So that was a success and we know that [there are] some registrars and some hosters [could] assigning their domain names. Next slide, please.

We also gave away a DNSSEC award – next slide – to the registrar that signs with DNSSEC by default. That's infomaniak. He's in the French part of Switzerland. So far they have about 38,000 out of 57,000 domains. So they have a market share on signed domain names that is more than 60%. Next slide, please.

We started CDS in the beginning of October. It's opt in until the end of the year, and then it's turned on for everyone. And we already have the first registrar who opted in, and currently we are doing 27 – we will sign 27 domain names I think tomorrow that we [found in] CDS. I will talk later about that. Next slide, please.

We will do an algorithm rollover with the annual key rollover from Algorithm 8 to 13. And last but not least, next slide please, we are very happy that our federal government signed the domain used by the

federal government. That's admin.ch. It was planned for years is what I know, and luckily this year was a question in the parliament if the federal government uses DNSSEC. And the minister wasn't aware of what it is and he said, "Sure, we do." But by that time, they didn't do it. But then the pressure rose and finally they signed it.

Thank you.

RUSS MUNDY: Thank you very much. Appreciate that. Our next presenter is Peter Koch from .de.

PETER KOCH: Yeah, thanks, Russ. Good morning. This is me at the other end of the horseshoe. I'll share some numbers and some graphs with you for DNSSEC regarding DNSSEC development or DNSSEC growth in .de, mostly since the beginning of the year. Next slide, please.

Just to remind everyone about the sizes so that the number of DNSSEC domains don't look so impressive, we have 16.2 million domains in total. We have 300 members which are all registrars. Some of them have resellers or chains of resellers. And for the registrars to submit DNSSEC key material, there's no sign up procedure necessary in our registration system. They just submit things and no tests in front of that and no nothing.

The top three registrars hold roughly 50% of all the signed domains. There is some concentration, of course, as everywhere. In those cases,

it is that the registrar also is the DNS operator for almost all of these domains. So they have a one-stop shopping with themselves submitting key material, taking that out of their own operations.

This is a model that also is true for smaller registrars or registrars with smaller numbers and the party that Michael mentioned from Switzerland is definitely also a known contributor to DNSSEC in .de.

As I just mentioned and again just for completeness, we are working on the DNSKEY records. So registrars submit the DNSKEY record. That goes into the registry, and we calculate the DS records and only use [inaudible] Algorithm 2 for that.

We do have pre-delegation checks for normal registrations, and if a registrar submits key material, we will also apply additional checks to the DNSSEC key material and that checks multiple validations so the SOA must validate with [this]. They can submit keys that aren't in the zone, and we will accept those at least as long as there is – I'm sorry. It's so early in the morning, so I'll start over. We will accept keys that are not present in the zone only if there is at least one that fully validates the SOA record. So that is to assist with key rollovers or standby keys.

We do have some 100,000 (sometimes 200,000) domains that are authoritatively served from within the .de zone. And, of course, they are naturally signed by our own ZSK. We usually do not count them in the statistics in terms of truth in advertising.

It's still early in the morning, but there's one topic that needs to go through every meeting this week. Next slide, please. So 25 May had a

big influence. Guess what happened on 25 May. Any takers? Somebody said GDPR. Well, next slide, please. Can you shift that to the left a bit? No, that is one too far. Go one slide back, please. Yeah, that's the one. Okay, great.

So, of course, it had nothing to do with the GDPR. There was a dent in the number of domains with DNSSEC, and that coincidentally happened on 25 May. We can now argue [that the] registrar was so busy with DNSSEC that they didn't notice they deleted they keys for so-and-so many domains. With the help of one other registry, we got to the registrar and they noticed their mistake and then resubmitted the keys for all these domains.

If we proceed one slide, please, you still see that little dent in May. Unfortunately, the axis is gone but believe me that one is in May. I show this not only out of curiosity or for the fun of 25 May but to signal that some of the registrars have processes that still need a bit more monitoring maybe. But manual intervention helped in that case.

I have two more slides. If you look at the submitted material, you will see that we started with 80,000 domains signed in January. That was 0.5%, and we are at 100,000 at the moment. So we have 25% growth without any promotion activity. Next slide, please.

We'll skip that one. Next slide talking about the algorithms. Just looking at the algorithms, dominant is Algorithm 8-RSASHA256 and still Algorithm 7 in red, but we also have 9% ECDSA and the rest is the others, including one GOST and one DSA because some people like testing. Shouldn't be too different from others.

Thank you so much.

RUSS MUNDY: Thank you very much, Peter. We appreciate that. Next on the agenda is Brett Carr from Nominet. Go ahead, Brett.

BRETT CARR: Good morning, everybody. I've got the clicker, so maybe it will be more efficient. When I originally talked to Jack about giving a presentation in this group, he mentioned that normally it's a raft of people going around talking about statistics. So I decided to not do that and do something a bit different to try and break up the stats a bit. So I hope that's okay. So that slide if you could see it would say "NO STATS."

I wanted to talk a little bit about how we simplified DNSSEC a little bit at Nominet recently. I'll start off with a potted history of some things we've done in the past.

In 2009, we signed .uk. Some of you in the room, probably most of you in the room, will remember we had a small issue in 2011 where we started using a new key without doing the relevant pre-publishing. That was due to a combination of a hardware failure and some human error. I'm reminded about this event every year because this picture that's on the screen pops up in my Facebook feed. You can't see the text probably, but it was posted by my wife at the time when I was trying to fix this issue. It says, "Helping Daddy fix the Internet or something." It's a picture of me looking quite stressed with my one-year older daughter

[inaudible]. We did fix it, obviously. Then in 2014, we also started signing gTLDs as well.

Over the years, the that we've used for DNSSEC, we started off in 2009 using SCA6000 Sun PCI-based [inaudible]. They were fairly reliable, but they were the initial cause of the issue we had in 2011. Although we probably could have recovered from that issue without causing a problem if it had not been for human error as well. The thing that killed those off in Nominet was the fact that Oracle bought Sun and then the price went through the roof.

So in 2013 we moved Thales network-based HSMs and OpenDNSSEC. We found both of those solutions quite complex and difficult to support. The Thales stuff was really reliable but fairly complicated to manage. And the combination of it being really reliable but complicated meant when it did go wrong, the relevant people had forgotten how it worked to any extent. And then we'd have to open support cases and the complication of having to deal with support both with Thales and with [inaudible] for OpenDNSSEC was not easy.

So in 2016 we came up with a simpler solution. We now use no HSM at all. All our signing is done on a geographically replicated virtual machine with BIND. Obviously, now if we have issues, we only deal with ISC. We've had a few issues but nothing major. And anything that we've had has not been impacted production, but the support from ISC has been very good for when we have had problems.

Our keys are stored in an encrypted partition which is protected by a split password. What I mean by a split password is the password is X

amount of characters long and half of the password is given to the engineering team and the other half of the password is given to a group of security officers. So to do any kind of work on the machine requires two groups of people to come together. And we have a fairly strict change management policy as well, which means that somebody has got to open a change, detail exactly what they want to do. And then the security officer and the engineering person come together. The security officer monitors that what they do is what they say they're going to do [inaudible].

In normal operations, access to that machine is XFR in and out only. There is no ssh connection to the machine. There's no external orchestration or anything like that. The only access to the machine to do any work on it is via the console, which as I said both the password for the encrypted partition and the console login are both protected by split password. And like I already mentioned, all change is done by the engineer monitored by a security officer.

So that has led to 2018, me looking a lot less stressed and my one-year old daughter looking a lot older than she did then.

RUSS MUNDY: Great. Thank you very much, Brett. We appreciate the update from .uk. Next is Patrik Faltstrom from .se.

PATRIK FALTSTROM: Patrik Faltstrom from Netnod, not from .se. But there was an interest in having an update from Sweden, and even though I've seen .se people

here, there seemed to be some issues of getting hold of them. So I promised to give an update to them. They're a customer of ours just like others in here. But as you know, just to be clear, this is not an update from them. It's from me. I don't have any slides. I do like Amazon. No PowerPoint. On the other hand, I noticed just like a few seconds ago that maybe it would have been good if I had some slides. So let's see how this works.

The first thing is we were the first TLD that was signed, and we did this long before the root was signed just like some other ccTLDs. One of the things that we noticed which I would like to emphasize, we had noticed very early that one way of getting zones signed is by starting to push validation. We are still trying to push validation in Sweden quite hard, and that is something I strongly recommend. There are too many people that just look at DNSSEC deployment in the form of signing zones. Our experience since ten years back, that does not work. You have to start with validation.

Today, according to the measurements that Geoff used and is doing, we have about 74.5% validation in Sweden. It's not the best one in the world anymore, but we're just before Norway and that's very important for us. About 0.1% before Norway. Yeah, we have that kind of game between the Scandinavian countries. No one beats our sibling except myself. If you try to attack my sibling, I'll come and beat you up. Anyways, between us we have this friendly nagging.

Anyways, some more numbers. At the moment, it's 1.77 million domains in .se. Out of those, 800,000 are signed. So as you do some

simple math and have some memory, there's about one million that are not signed. This means that we have succeeded somewhat in the validation, but it's much easier to sell the "please sign your zone" concept when there is actually validation going on. Because of this, of course, we were a little bit – we talked quite carefully about the KSK rollover in Sweden because we had so much validation going on. But on the other hand, we had already rolled the key, so we knew what kind of impact that could be. So we were not nervous and, no, there were no traces of any kind of problems whatsoever. Another number that could be interesting is that we have 86,000 IDN domains.

One interesting thing that is happening in Sweden at the moment was something that was supposed to happen yesterday but is postponed to today. That is a change of the key and the algorithm change that is happen for .se from RSASHA1-NSEC3-SHA1 to ECDSA Curve P-256 with SHA-256. I just got an e-mail this morning whether it was sent. Yes, I read it this morning. It was sent yesterday probably, that the algorithm change was postponed to today. I haven't got any more technical information why that was postponed but, anyways, it's happening.

You can go – and this is why I wanted to have a slide – there are two URLs that I will try to feed into the material afterwards. If you go to iis.se/se-tech/rolling-rolling-rolling, that's the information about the key roll algorithm change.

Another thing that we have in Sweden is we have one crazy guy that among other thing has made these t-shirts. He also has a website which is dnssecandipv6.se. What he has a map of various countries in

Scandinavia and other countries also if you want to participate, and he measures whether municipalities and organizations and entities have properly signed their zone, use IPv6, have MX records set up correctly. So it's a blame and shame thing for organizations. That is actually very, very useful. And as we heard before, it's actually pretty good when politicians that have absolutely no idea about the technical stuff are very proud. Yes, we are participating. They see the map, and they see that their city is red. That works.

Thank you.

RUSS MUNDY: Thank you very much, Patrik. Next we hear from Arianna from Italy, .it.

ARIANNA DEL SOLDATO: Good morning. I am Arianna Del Soldato from the registry .it, a recent DNSSEC registry. We are not able to see all the slides. Sorry.

DNSSEC for us is the result of a long process. Starting in 2014, we collaborated with the Swedish registry and Netnod to consolidate the technological knowledge already existing in the .it registry. In 2016, there was a setting up a joint working group between the registry and the registrar. And they decided to develop the [inaudible]. In the same year, just a few months later in 2016, a test platform was made accessible to all .it registrars.

This is our test platform. That is a platform replicating the real registration platform. We have an EPP test server [inaudible]. We use

BIND to sign the zone. As it is a different zone from the one in production, we have replicated also with the [slave] [inaudible] server and a special test resolver that the [registrar] can use in order to test their operation made with the EPP server and to query the database.

Our choices between the two possibilities, we have chosen the DS data interface. We have no web interface in order to manage the DS server, but we have manage the DS server only via EPP [command]. But we have developed a DNS validator that has a web interface and the [registrar] can use prior to register the domain name, [the signed] domain name.

DNSSEC for us is not mandatory, but the registrar must pass an accreditation test in order to be able to register [signed] domain names. Accredited registrars are identified by a specific logo in our website. This logo can be used by them in their website in order to show that they are accredited.

The accreditation test enables them to book the test and receive some specification that they have to use in order to pass the test, like the domain name, the machine to use, and the algorithm to use in order to sign the zone. They have to register [a not signed] domain name and create a key signing key and zone signing key and then transmit the DS record. There are no time limits to pass the test, but the duration of each test is 90 minutes. In case of failure, you have to wait one week before to perform the other test.

This is our current status. In 2016, the DNSSEC test platform was made available. In 2017 we [had the] signed it. zone so the [inaudible]. This

August, there was the publication of the new technical guidelines that includes the DNSSEC specifications. One month later in September, we opened our accreditation test for the [registrars]. Finally, this September, we had the first registrar accreditation and the first signed domain name.

Current numbers, now here we have a surprise. I will have to change the smiley face because yesterday had six accredited registrars but 1,384 signed domain names. Only one day because [a registrar] decided to send us [inaudible] record for 1,300 domain names.

In the meantime, we organized a training course on the subject of DNSSEC [in the context] of the training course that we made for the registrars and also [in the context] of cybersecurity master organized by the registry and the department of engineering of the University of Pisa.

Thanks.

RUSS MUNDY: Thank you very much, Arianna. That was a great increase in the number just before the program. Thank you. That's good news.

Next, we have Jose Lopez from .es to tell us what's going on around here.

JOSE LOPEZ: Good morning. I'm going to talk about DNSSEC at .es registry. Let's start with a bit of the history. In 2006 we created the testbed just to know more about DNSSEC, how did it work, how to implement, and so on.

Then in 2013 we included DNSSEC into our registry system software, and we activated it in July 2014.

Some info about our platform. We are using BIND through OpenDNSSEC. It was a couple of servers, HSM servers. Concerning the signing policy, we are doing rollover of the KSK every two years and the ZSK every three months. The platform has been very stable. We just had one issue this year. In January this year, we got wrong NSEC3 signatures errors. It took us awhile to find out where was the error. We found out it was caused by the HSM server, one of them. To find out the origin, we want to thank you some [registries] you helped us like the [SWITCH] registry, the [Swedish], the [inaudible] and the [inaudible]. Finally, we found out the origin.

And the numbers. The numbers of domains signed is [coming in] slowly. Right now we are 17,000 domains signed out of 1.9 million domains overall. As you may know, the registrars are very important. The top five registrars signing domains are managing 95% domains signed. This year, we expected to have an increase between 70% and 80% at the end of the year.

Challenges, we have taken some challenges and initiatives. Challenges, we have less than 1% of domains signed. We want to increase this number, of course. Also, we want have more local registrars involved to have DNSSEC as [activate] and also to identify more drivers to growth.

The initiatives were on the professional side we are migrating our HSM service to put FIPS level 4. Also we have collaborated with INCIBE, the national cybersecurity agency, to create a guide to help people to

implement DNSSEC. Also, we have some awareness activities with ESNOG, the national Spanish networking operator group.

That's all. Thank you.

RUSS MUNDY: Thank you. That was excellent timing here and a great presentation.

Next we'll hear from Jaromir from the CZNIC on what's going on in Czech Republic.

JAROMIR TALIR: Thank you, Russ. I will give you a quick update about the situation in .cz. We are slowly climbing to the mark of 700,000 signed domains. It's roughly 53%. Recently, we have crossed the line of getting over the 50% of signed domains, which is quite important for us because since that we can actually say that to have DNSSEC it is normal. It's a good marketing thing for DNSSEC. However, over the last few years we could see stagnation that the climb is not as big as it was before.

We also publish statistics about the algorithm support in the .cz zone. We can see that there is quite a big uptake of the ECDSA algorithm thanks to our biggest registrars. The three big registrars are responsible for the situation that ECDSA or Algorithm 13 is the most used DNSSEC algorithm in the Czech zone. We have also the two smaller registrars that migrated to Algorithm 14, which is not quite usual.

With such a support for ECDSA, you could expect that some ECDSA domains will appear in the root zone also. So there are currently two

TLDs, .cz and .br, we have rolled the key to ECDSA in June and we are in August I think that I [saw in the presentation] later today about their role.

Some information about the software that we are developing, our open source registry FRED which is used by some more TLDs as well. Recently, we have developed a DNSSEC algorithm check. Before that, we haven't checked algorithm any way, so any algorithm could be put in the registry. Right now we still allow to put any algorithm in the registry, but at least it is possible now to configure if you want to, for example, not allow some old algorithm to get into the registry. So it's up to the registry how to configure that. Last year, we have implemented the CDS/CDNSKEY [skinner], and [Andrea] will talk about it later today. He will show you some statistics.

Our DNS software Knot Resolver, there is a new version we released recently. It supports aggressive NSEC3 caching. The previous version only supported NSEC records. There's some polishing of implementation of KSK sentinel based off the new drafts.

Authoritative DNS server, right now we are implementing support for offline KSK, which is something that is new. It actually should help us with using it in our own scenario where we have the split management of zone signing keys and key signing keys where we pre-generate zone signing keys in advance and sign them offline. So hopefully this scenario will be also supported in [inaudible] DNS soon. So anyone who is using this scenario, I would like to hear if this is something that can be an interest for you.

That's it. Thank you.

RUSS MUNDY: Thank you very much. And now we'll hear from Paul Ebersman from Neustar who will give us some updates on what they're doing.

PAUL EBERSMAN: Thank you. Neustar is a commercial company. We run registry and registrar. We have an open recursive resolver service, and we also do run as a DNS operator for various folks' zones. So I'll break through the various pieces of that and where we are with DNSSEC.

Starting with the good news, our resolver service has been validating for a number of years. We do DNSSEC validation on every query. We do about 10 billion queries a day, and we have had no reported incidents according to my [NOC] in the last year. So the whole DNSSEC is a little bit fragile seems to fall by the wayside with that argument.

We are unfortunately a commercial company and we support mostly enterprise. So our signed zone story is a little less stellar. We have had a fairly fixed percentage of our zones signed. The number of zones we serve has gone up at a steady curve, but we have remained at about 30% signed. Of those, I think it was 29 and change that were all secondaries where someone else is signing the zone and we're merely serving the data. The vast majority of that is a data center and hosting provider in Sweden.

Part of the challenge, which is what I hear a lot when I talk to commercial customers also, is we do most of the stupid DNS tricks. We do load balancing. We do GeoIP. We have some form of CNAME at apex. And they're much more interested in those stupid DNS tricks than in DNSSEC working. When we have gone to management in the past – I'm relatively new, but this is according to the folks who were there – new features have won over doing DNSSEC for correctness.

We are, however, going through. We write all of our own software, so we have our own recursive resolver, our own authoritative server. They are not open source. But we are in the midst of doing a fairly major redesign of that code. And one of the things we are looking at is actually being able to do signing on the fly, which will allow us to do an awful lot more of those stupid DNS tricks but still have DNSSEC signed.

As far as other usage, we seem to be also in the middle of the conservative curve. Algorithm is almost exclusively Algorithm 8. We've seen a few folks doing ECDSA, but the biggest folks pushing for it to be honest have been us internally just due to the response sizes on our authoritatives.

Registry, we are looking at some of the initiatives that are going on with CDS. And assuming that ICANN doesn't speak negatively or do anything to make life more complicated, that's another that's being put into our roadmap and I'm hoping to have that in 2019.

Any questions from anyone?

RUSS MUNDY: Well, thank you, Paul. We actually do have about five minutes for questions for the panel. But before we take questions, let me thank the panel for a group of wonderful presentations.

Now we will open it up for questions for anyone on the panel. Yes, over here.

RAED ALFAYEZ: Yes. Hello, my name is Raed Alfayez. I am from SaudiNIC. My question is regarding as a registry operator, do you believe that we need to check the [inaudible] that have been uploaded by the registrant, is it valid or not? Or do we just leave it for the registrant to upload whatever he wants and maybe he will damage [the] zone file or the resolvers? What do you think? Thank you.

JAROMIR TALIR: For .cz, we just implemented the CDS and we read the CDS and then we actually check if the zone validates with the CDS key that is used. So you cannot break it by publishing a wrong CDS record. We think that helps to prevent mistakes and errors.

RAED ALFAYEZ: But the problem here is that a client will ask you why you haven't uploaded the new [inaudible] and these kind of things and keep having tickets and calls.

JAROMIR TALIR: We have something called a status portal where you can see what DS you have in your CDS record. It will tell you if and we implement it into the parent zone. So we try to answer this question upfront. I will talk later in the CDS panel about that.

RUSS MUNDY: Do we have responses from anybody else? Yes, go ahead.

UNIDENTIFIED MALE: [inaudible] different approach. We allow the registrar to upload anything into the registry. It's not just about DNSSEC. It's about name servers who can upload [to invite] name servers. What we actually do is that we do technical checks later on. We are regularly scanning the validity and we are informing the registrant that they are doing something wrong. But it's up to them to fix it. So that's for a [liberal] approach, I would say.

RUSS MUNDY: Okay, any other thoughts? Okay, Peter, yes?

PETER KOCH: Thanks, Russ. Obviously, we are a bit biased because we've been running pre-delegation checks ever since and we decided to apply those to DNSSEC as well. The reason behind that is less to protect the registrant or the registrar from their own errors but especially in the case of DNSSEC to avoid a negative perception of DNSSEC as a whole.

So it's more the quality of the overall namespace than preventing people from making their mistakes.

PATRIK FALTSTROM: I think if it is the case that you implement a policy, you need to be very careful in a situation where registrars have uploaded multiple DSs. Because you don't really know if they are new ones incoming or if they're old ones. So you should be very, very careful before you start policing there.

I think just like word from some other people in the room, it also might impact who has the ultimate responsibility of the working zone in relation to the customer, whether it's the [registry or] registrar. And who has the greatest responsibility depends. It differs very much between different ccTLDs in the world. We heard from Denmark has one approach and others have other approaches. And you should do something that fits your environment.

UNIDENTIFIED MALE: Yeah, just to add on to that, if it's DS for an existing DNS key and if they inputted the wrong information, you should let them know that it's incorrect at that time.

RUSS MUNDY: Okay, I think that we are basically out of time and we need to move to our next panel. But again, thank you for all the presenters. And any other questions, catch up with people afterwards because this

community has been very good about answering individual questions and working one-on-one with people. Thank you, panelists.

Next we have Frederico Neves from .br who has recently been engaged in an algorithm rollover, and he's going to give us an overview of how that went.

FREDERICO NEVES: Good morning, everyone. As Russ said, I'm Frederico Neves. I work for NIC.br. In the last ten months we have been working on an algorithm rollover for .br. I will give a brief presentation talking a little bit about what went on.

This is the executive summary. Ten months of preparation, a lot of tests and software writing. We went from RSA-SHA1 to ECDSAP256. It was executed from August 20-23. It went very smoothly, no issues reported or detected.

A little bit of introduction: .br was signed in 2007. We have 128+ child zones. About 90% of all the domains are below com.br a third-level domain, a second-level zone, with third-level delegations. It was signed with RSA-SHA1.

During this period, we had two KSK rollovers, regular ones in 2010 just before the root was signed and in 2015. During those two KSK rolls, we increased the size of the key, the KSK, from 1280to 1536 for the KSK. And the CSK that we use for the second-level zones and the ZSK for the .br zone we increased from 1024 to 1280. So those are the sizes of the

keys that we had before the algorithm roll, 1280 for the ZSK and 1536 for the KSK.

The motivation was to improve security, mainly being prepared for the algorithm rollover. Because we use our own signer, we didn't have a support for algorithm rollovers on the software. So we decided to be prepared in a regular rollover or during a time that we didn't have to do an algorithm rollover in a rush.

Reduce DNS response size, that was another motivation. At least from the key set and RRSIGs we have a 60% reduction in the size. So less network usage and much less TCP fallback. We will see a little bit of numbers [of that].

Other motivation, the stat that was provisioning the DNS was written in 2004. A little bit dated. We had some maintainability issues with the code, deficiencies in memory management that imposed some operational restrictions to us and we were moving the registry to another stack.

We had a dilemma on how to do the algorithm rollover. We had already presented. I will not go in details here, but we decided to test both methods, the conservative and the liberal. So finally we picked the liberal mode. That's basically a [double] signing. It's much simpler. The problem actually reported by RIPE in the past, it was only affecting old version of Unbound.

But anyway, we did the tests. Probes with [inaudible] RIPE Atlas. So we measured no significant difference between both methods. The

reference in the back slides of the presentation, we have all the measurements done on the RIPE Atlas platform.

The algorithm rollover, we went from RSASHA1 with those key sizes to ECDSA. We now have a single CSK. And for the second-level ones from RSASHA1 and RSASHA1NSEC3 for some zones. And now we have a single key for the second levels, the CSK. Both are ECDSA and a split key for .br.

The execution, preliminary we had to do a lot of upgrades on the provisioning system. Besides the software, we upgraded the software on the HSMs to add support to ECDSA. All the generation of the key and the export to the four HSMs that we have in two different sites, this took a little bit of time, but it was done on a separate ceremony three weeks before the roll.

We reduced the TTL of some records one hour to speed up the rollover and we could achieve a seven-hour rollover time for the CSK, especially for com.br that is a very large zone.

The CSK rollover for .br, it started at 12:00 UTC on 20 August. It was double signed. We wait for five TTLs mainly for the new key to propagate and be completely sure that everybody was already with the new key set. At 17:00 we changed the DS on the parent zone, on .br, and the old CSK was removed two hours later.

The KSK rollover started at the same time, and at 17:00 we asked IANA to change the DS, made all the confirmations. And luckily and thank IANA they did it very fast and we basically finished at least the transition

on the zone on the same day, and three days later we could withdraw the old key on the .br zone.

The trust chain CSK rollover went very smoothly, as you can see here. Those are the seven hours of the rollover. The blue line is the secure resolutions measured by the RIPE Atlas probes. As you can see, there is no perceptible difference from one algorithm to the other. The insecure ones kept basically on the same percentage, roughly a little bit less than 40%.

So those are the message size of the key set for before the rollover, 638 bytes, and after it 289 bytes. The response sizes, those are [inaudible] of the positive and negative responses. The upper one is a month earlier. I guess it was in July. The below one is after the rollover. As you can see, we had peaks of negative [answers] around 1,200 bytes before the rollover, and now it's around 800. So it was a large reduction.

Here we have the [inaudible] of the responses before and after the rollover. The blue one is the RSA. The green one is the ECDSA after the rollover. As you can see on the 512 bytes response before we had 42% of the responses below this threshold and after 65%. And 99% of the responses now are below 850 bytes and before it was below 1,200. So it was a good change.

This is the percentage of TCP queries. Again, the blue line is in July, and then we were having – this is through I guess a 24-hour period. We had peaks of 3.5% of TCP [transport], and now we are roughly 0.7%. So it was a very good reduction.

Those are the references for the RIPE Atlas if anyone is interested. It's a lot of data.

So that was what I have. We have four minutes if anyone has any question.

RUSS MUNDY: Thanks very much, Frederico. Are there questions? Geoff?

GEOFF HUSTON: Do I get this right that you were getting truncated [inaudible] buffer sizes of less than 1,200 and you were giving truncated answers under RSA, which seems an awfully small number to me.

FREDERICO NEVES: We had some responses above 1,280 but, yes, we had higher TCP query rates before the roll.

RUSS MUNDY: More questions?

FREDERICO NEVES: If you look at the graph just before the CSK roll for [inaudible], it dropped just after we dropped the old keys. And actually during the roll, I have not shown the graph. I had another one that shows the seven-hour period and the three-day period for the .br roll. It raised the volume of TCP queries for 4.5%. But at that time, we had a key set

roughly with 1,600 bytes size. But the graph is one month before this graph that I show the blue one. That was a regular .br situation.

And another comment is that we do regular CSK rolls on a monthly basis. So before that during a week we had a [pre-publishing] and a key set a little bit bigger anyway.

RUSS MUNDY: Yes, go ahead, Duane.

DUANE WESSELS: First of all, congratulations. That was very nicely done. Love all the data. This is not really related to your talk, but can you explain a little bit about why you use a combined signing key for your second-level zones?

FREDERICO NEVES: The ZSK for .br and the combined key for the second levels, we use [an] online signer for that. And as we control everything and the stack is completely integrated, it's much simpler to have a single key on the second level. So we have a smaller key set and it's the same software that does the regular rolls. It was easier to use the combined key.

DUANE WESSELS: Thanks.

RUSS MUNDY: I have one question for you, Frederico. I noticed you dropped the TTLs as part of this. Were you also monitoring load on your servers to where you could see any difference, a higher load or it stayed the same, during this [low TTL period]?

FREDERICO NEVES: Actually, we dropped the TTL of the DS delegations and even for the NS delegations two months before. We used to have NS delegations of 24 hours and DS delegations of 6 hours, I guess. And we reduced to one hour, and this increased our query load by 30%. So we used to have a lower number of queries and this increased for 30%. But now we kept it in one hour, and it was good for customers and this reduced support calls regarding especially NS changes.

RUSS MUNDY: Okay. Thank you very much. One real quick.

UNIDENTIFIED MALE: Yeah, just maybe a follow up question on what Duane said. Have you thought maybe about using the CSK for the TLD? I know that there is the issue with uploading the key frequently to IANA, which is not automated. But if there [would] be such a case that maybe?

FREDERICO NEVES: For the KSK, we use a HSM [inaudible]. And there is the problem of managing the relationship with the parent. So I guess it would not be possible to use the CSK for .br.

RUSS MUNDY: Okay, thank you very much, Frederico. Very interesting.

We are now at our break time. There should be coffee break and so forth out in the area. And we will start again promptly at 10:30. And as we come back in, if our 10:30 panel members would join us at the table at the front, that would be appreciated. Enjoy your coffee break. Thanks.

[END OF TRANSCRIPTION]