COPENHAGEN – DNSSEC Workshop -- Part II
Wednesday, March 15, 2017 – 11:00 to 12:45 CET
ICANN58 | Copenhagen, Denmark

DAN YORK: …Paul [inaudible] is here to talk a little bit about what he is doing, or what they are doing there within Comcast. So, Paul go ahead. For the remote attendees, I would just mention that this is intended to be a discussion, and so we don't necessarily have a great number of slides.

So, you are welcome as well to participate and ask questions in the chat room. We have Kathy and Julie who are here monitoring the chat room, and are able to relay any questions that you have. So, I do know we have some remote folks.

So, go ahead Paul. Tell us a little bit about, what is Comcast doing to be prepared? And what advise do they have for other ISPs?

PAUL: Thanks, Dan. So, we have actually two infrastructures that I support. We support, I think the latest number is 26 million homes on the customer side, plus three or four million small businesses. But we also have the corporate side and IT DNS, and we're doing DNSSEC validation for both of them.

Because of that, we have, by the time this key rollover happens, I'm going to have somewhere in the neighborhood of 300 recursive servers on the public side, and somewhere in the 50 to 60 server range on the internal side.

So, we have pretty much decided that even though we are using [inaudible] machines for performance reasons, we treat them like VMs. Everything is completely automated. We just stomp the OS, shovel packages, and configure for the type of resolver we have. So, for us, 5011 and automated really wasn't a valid method, because it actually confuses all of our automation and our sanity checks that we have, did the push work correctly, and all the signatures and check sums correct.

So, basically what we will be doing is getting the key, validating it, testing it in the lab. Checking it to get, and then just doing an automation run. And pushing it out from there. So, once it works in the labs, we just shovel it out everywhere. And that's pretty much, I think, in our case, be the plan.

My guess right now is that most of enterprises that are using AWS and other things, and running resolvers on virtual machines, are going to be doing something similar. So to summarize, get the new key, stick it in, and push it to everything out there.

UNKNOWN SPEAKER: Press button, go boom. [Laughter]

UNKNOWN SPEAKER: There you have it. A very simple automation strategy. Matt, did you capture that for a slide for your next KSK presentation?

And now Dan, this is why I didn't bother with slides. If I couldn't basically do it in about one bullet point on one slide, it's not operationally sane for me.

UNKNOWN SPEAKER: Okay, well that's a good one. Anyone have any questions for Comcast on their KSK rollover strategy?

All right. [Laughter] All right. Next up, we have [Tobin?] from [inaudible].

[TOBIN]: Hello. I hope you can understand my Swin-Lish today. And I got up 4:00 this morning, so I'm a little bit tired now. Yes [inaudible] is my name. And I feel a little small sitting behind Comcast here.

Next slide. Yes, the explanation of what I am doing with DNSSEC. I'm the co-founder and owner of the company [inaudible], and some of you have maybe seen my maps I've done for [inaudible]…

And the little green area in the middle of Sweden, I live somewhere there, you understand. So, I helped about 50 municipalities to sign their domains. And almost every Swedish municipality own their own DNS, more or less. You can take next slide. So, I'm responsible for, I feel very small, 30,000 subscribers.

[Inaudible] I'm responsible for the DNS resolvers, and we will trust RFC 50-11 on that. And they only have two resolvers, one master and one slave. So, I hope it will function. When I got invited to this conference, I trust, [inaudible]… So, I hope it will work for me. Next slide.

But we also have setup several validating resolvers for the enterprise. I'm not sure how many we have done it on, but we have used the [inaudible] there also, that's only for performance. I think DNS is, I don't know.

So, that's my case for the KSK rollover. And I hope it will function for me.

Yes, I think there is one more page. Yes, some problems. Some of you maybe have heard that the [inaudible] for 10 years ago, I was the one who signed the domain then. You can read this later, it's not about validation. Yes, I can say before the root were signed, we have some KSK key problems when dot [FC?]

rolled over KSK, and so but after the root were assigned, we had never had some issue with that.

Sometimes, I heard about people were worried about the size of the keys, double keys, and so, we have some municipalities, since we have more than 100 broken keys. And we can [steal sold?] them correctly, so I'm not worried about that. So, I'm finished.

Yes, almost.

UNKNOWN SPEAKER: And we should notice, [inaudible] is wearing a shirt that says, DNSSEC, been there, done that. All right, well, so any questions for [inaudible]? Yes. Sorry.

UNKNOWN SPEAKER: Thank you. So, [foreign language]. Every version from 2011, will deal with your problem, with the KSK rollover. So, I think in the past six years, you probably installed a recent version from 2011 or later. You will be in good shape. And I think also your role small [inaudible] will be able, it's either 50-11 or with [inaudible] anchor, who try to find an alternative way, or has a procedure to find an alternative way to download the new trust anchor from the ICANN website.

UNKNOWN SPEAKER: I will check some of my resolvers that will do the K.

DAN YORK: Any questions for [inaudible]? No? Wow, we're kind of moving along here quickly on this. I guess the answer is, we didn't need this panel, because it's just like going, it's simple, done, all right. Which is good. That's the good answer we want to here. But maybe, let's make it a little bit more complex, and we're going to ask Andre to talk about his experience and his connections within the IXP market, and the space that's there.

ANDRE: Thank you very much. You know, the ISPs never concentrate on DNS, right? That's just a service that transport them, they don't pay much attention to that. So, I believe it's kind of role of the institution that does somehow involve in the internet infrastructure to push developments. So, I think in the previous point, we develop [inaudible] that checks whether the resolver supports ECDSA.

Unfortunately, you can't find any way to say whether the resolver is proper converted and support 50-11. If there is any, please let me know, because it would be awesome to add this function to some kind of legitimate. I think without any special tricks like signing some special record in advance in the root zone, you cannot achieve that.

So, that's a problem. So, that's why we are trying to communicate as much as possible with the ISP community, we have some advantage because the check zone was signed before the root zone was signed. So, actually those ISPs first put check zone as a trust anchor, and then they convert it to root zone.

So, there is sort of went through a trust anchor change, so they are, might happen from time to time. So, and we still also have contacts to them, so we speak directly to them. We, you know, have conferences and we talk about the ratio, and also, we are quite closely, we have a good relationship with the local internet exchange point, which sort of makes the role of network operators group.

So, we, if there is a meeting of the ISP, we you know, present that, we warn them about the new things that happens in DNS, and that's probably the worst, the best way how to address it. I think if they don't use any [inaudible], they have good [inaudible] distribution with proper installed resolvers is nothing should happen.

And that's how the measurement of them works, some of them have some different solutions. So with them, we especially kind of talk that they should be ready, that they should check that the solution [inaudible] is okay. I think that's going to be successful, so I'm not afraid from the October 11th.

DAN YORK: Okay. So, I guess, nobody is concerned that they… I guess we're all good and happy with October 11th. So, Matt, you can stop your presentations. I think we're good, we're done. It's all baked.

Warren is scared, next to me, okay. So, let's hear from Irwin. Irwin, are you going to be equally as short?

IRWIN: Of course. What's going to happen? How hard could it be? So yes, I can say a little bit the same what Andre is saying, about at least [inaudible] the ISP that I know that have quite good technical people, they know what they're doing. So, we just have to make sure they know it's going to happen, and that's beforehand.

They probably have good software, that's 50-11, just make sure a couple of days ahead of October 11 that they check that the new key is actually in there. By coincidence, tomorrow is the yearly meeting of the Danish Network Operators group. [Inaudible] will be there, and make sure that it's mentioned, so that people will know and they can come to us if they have any questions.

The other outreach is quite important, is the software projects. I know, [unbound] is anywhere [inaudible] probably know as well, but also downstream, we have to make sure that is integrated in the software packages, to make sure we reach out to the Linux, and [inaudible], and other projects that they make sure they upgrade their packages. And especially, the operating systems that have include validation in their operating system themselves.

They have to find that way to make sure they use the operator ahead of time, by router notice, or whatever it is, their mechanism is, to make sure they use this upgrade. So, with that [inaudible] I do have one area that I am worried about, and those are the black boxes.

The enterprise to buy a black box that might actually [inaudible] validation that they actually don't know about, because they just bought a box that does DNS, and it just works. And suddenly one day, it stops working, because they just bought it, stick it in the basement, there is no consulting [inaudible], and they don't know what it's doing.

That's the one area I'm really worried about. They don't even know that DNS exists, let alone DNSSEC.

DAN YORK: Paul, you look like you wanted to comment on that.

PAUL: Yeah. I think in the US, the biggest problem for that one, dot gov, when they had the DNSSEC mandate, they bought a lot of appliance space DNS, and considering the budget slashes that have happened, a number of people are probably running without support on those boxes is probably high. I know that in terms that we put negative trust anchors into overcome DNSSEC validations right now, dot gov is worlds above everybody else that we have.

DAN YORK: Anyone else? All right. Roland, I know you want to talk about some measurements you've done.

ROLAND: No, that's later. I'm going to talk about some measurements I want to do.

DAN YORK: Oh, okay.

ROLAND: So, next slide please. The operator actions fit on one slide, it's just that we're going to trust un-bounding. We already applied 161 on our, all of our resolvers, that includes the new root trust anchor tag in the un-bound anchor. And on K day, I've started calling it K day because I think July 11 is the important date, because that's when the first, it's the first time the key will appear.

And on K day, and I'm hoping to learn the time at which I need to start monitoring this file, I'm going to be checking the trust anchor repositories on our resolvers router. I'm going to have engineers, just to make sure that it gets picked up, and like what was said before, I trust the software to do it, but we want to make sure that there is no, sort of, read only places on the [inaudible] system that unbound can write to.

We are also going to be talking to separate operators in our constituencies. Surfnet is the national research and education network in the Midlands, and it means that we have lots of universities, research institutes. They all run their own infrastructure, some of them forward the traffic to us. Some of them do their own traffic, and we need to tell these people that they need to pay attention. We do have some appliance users in our constituency.

There is some people that run ICANN systems that do DNSSEC system resolution for them. And it will be interesting to see whether those devices pick up the new key. Next slide please. What I actually want to talk to you about is an idea I had which I bounced around, I talked to some people about this, for example, Roy [inaudible] at ICANN, which is to measure the KSK rollover and I've tried to find a nice picture of a canary in a coalmine.

Who knows what these were used for before? Whose familiar with the term canary in a coalmine? Okay. So, it's not everyone. That's interesting. But in the days when we still dug up coal and didn't have green energy, the… [Laughter] The miners used to take a canary in a little cage, into the mine with them. And the idea is that the canary is really sensitive to gasses in the environment, and if the canary starts acting weird, or rather drops dead, that is the sign that you should be evacuating the mine, because something bad is happening.

And what I would like to see if we could get this setup is to get something similar for the root case K rollover. Next slide please. So, I want to put a canary in a virtual coalmine, and the goal of that would be to track the operational impact of the root case K rollover. And I also want it to act as an early, well not as an early warning, but as a warning signal that validating resolvers are failing to validate with a new key.

And I have an ulterior motive, right? Because I'm also an academic, and I want to sort of write a nice paper about this, so I also want to collect this data and a measure the validation during the KSK rollover to learn from a global perspective, what happens during this type of event. Next slide please.

So, the idea is to use four perspectives, which is to use [inaudible] probes, use something called [inaudible]. Who here tries to watch Netflix from somewhere on the planet, and they want to watch US content and then use one of these unblocker services? Come on. Raise your hand. You know you're all doing it.

So, some of these companies offer some sort of peer to peer VPN service. And if you use it for free, you're basically giving them your machine as an exit node for VPN connections. And somebody at northeastern university in the US worked out EPUs to do measurements, which is really cool because it gives you visibility into residential networks, which RIPE Atlas maybe does, but it only gives you visibility into geek residential networks.

So, I want to go and talk to them and see if we could use their methodology to do measurements of validation from within these nodes, and they have almost a global presence in lots and lots of different residential networks. So, that's a really interesting vantage point. Equally, I want to seduce the good folks at APNIC, who are continuously doing these nice measurements, to somehow include this kind of measurement in their setup. And probably from what they're already doing, we can already pick this up in some way.

We can already work this out from the day that they're collecting. And then finally, of course, it's worth also to look at traffic to root name servers. And I know that some people are already planning to do this. To look at whether people are doing fetches of the keys, etc.

Now, what I want to do is establish a baseline of validation before K day. So we want to sort of get a signal and the noise ratio as well, right? So if we do these measurements, they're going to be intermittent, some data that validate, some data they don't validate resolvers, that you probably want to know of before the new key starts appearing.

And my basic idea right now is to do this measurement on a daily basis, but maybe to increase the frequency, if that is feasible, and/or desirable, and I'm guessing that the closer we get to October 11, it might actually be desirable, at least in some of the bigger residential providers, especially to sort of up the frequency. Next slide please.

And then, hopefully we can take action, right? If the canary starts to sing, or if it dies, there is an operator having trouble in validating a resolver, and we, as a community, can reach out to these folks and tell them, hey, this is serious. You need to take action now. Fix this. Lots of us have contacts all over the operator community.

And if we can somehow make this a community effort, we can make sure that this KSK rollover doesn't turn into a disaster, but it is the success that we're all thinking it's going to be. Next slide please.

My plan is to start the fourth week of April, to sort of start assessing what data we want to collect and how we want to collect that. Your input is more than welcome. I registered root canary dot org. I haven't had time to set anything up there yet, but at some point, I hope to put up, as Matt put it, a well-designed, graphically appealing website.

UNKNOWN SPEAKER: So, is it not a DNSSEC signed?

ROLAND: Root canary dot org is not DNSSEC signed, on purpose. I think that's my last slide. Can we check? Yes, it is. Okay, so if there are any questions, suggestions, feel free to ask, shout, give comment, or email me.

DAN YORK: I think we will have some. I've heard some questions. I also want to ask my own. So, the [inaudible] service, it's a VPN service, so if you use it for free, it literally is turning all of your end note into…

ROLAND: Yeah. I think the free offerings called [inaudible], and it just, if you… You know the things you never read where you click, okay I accept? That gives them the rights to use your machine as an exit note.

DAN YORK: Wow, that's awesome. Okay. I don't use that service, but it's good to know. All right. We have some questions forming. I see, let me go for Warren and then Roy here.

WARREN: So, can you go back two slides? Yup. So, the APNIC DNSSEC thing, Jeff Houston and George [inaudible] are planning to do a big one of this as the key roll happens through each, and I think are providing data straight back to ICANN. [CROSSTALK]

Normally it takes a day for them to analyze, they're going to try and do it faster for stuff like that. I believe the root servers are also going to be doing one of the digital type runs during the specific times, to make that available. And then can you go forward a slide?

ROLAND: Can I just comment before you go forward? What I didn't explain was why we want to do this from multiple perspectives, right? Because if you just look at APNIC, you get some visibility, but the problem with the APNIC measurement is that you can't reproduce measurements in the same location, reliably, right? You're dependent on the ad network.

So, it gives you great visibility, but it doesn't give you reproducibility. [Inaudible] allows you to pick the exit nodes, so you can get a much better sort of reproducibility, but it costs way more money to do than the APNIC measurement. So, we're trying to get multiple vantage points to get as good a view as we can of this.

WARREN: And then, next slide. So, what I've seen, the likely failure mode, is simply that validation stops completely, and if you're doing validation that means all DNS resolution stops completely. So, presumably, operators are going to notice that [LAUGHTER] because nothing will work.

So, hopefully… And that's sort of… Do we do general questions now as well? So that's sort of a general question as well, as for [inaudible] like Comcast. Presumably you have a population behind you, who is simply forwarding queries to you, and is doing validation. And you know what that population is? Because even though you might be working, if they're validating, they're going to go boom and they're going to call.

And there are a bunch of reasons this is going to happen, right? People running their name server in [inaudible], and so they don't really have a persistent file system, or they have a read only file system, or because Dan, and Julie, and Steve have been doing such a good DNSSEC for beginners thing, people who configure trusted keys and never moved managed keys, and appliances, and things.

So, for folk who are running validating resolvers, or just any old resolvers, do you have in place to try and figure out what percentage of users are doing validation? You know, because they said, you possibly see that, and also have you spoke to your tech support people? So that they have a script ready, so when it says my internet broke, they've got a whole, you know, this is how you do your DNSSEC troubleshooting and turn it off.

UNKNOWN SPEAKER: So, we don't have a good way of knowing if we are in a resolver chain. Unfortunately, almost everything these days says the DO bit by default for everything, everywhere, whether they actually do anything with it or not. So, that makes things a bit more complex. We have a pretty good idea of other folks running resolvers within our enterprise. We actually go through and do things like n-map and scans, and various other things, to watch for that.

And the largest group that actually haven't started just using our normal any case and running their own, have the same thing we do, they do automation. So, once we tell them, put this trust anchor into your get, or whatever it is, that takes care of those. The population that actually concerns me, and it's the ISP complaining about CPE and updates, we did get DNS mask DNSSEC capable. We got the code in. By the way, Roland, if you're looking for funding for [inaudible] stuff, talk to me later, we have, yeah.

So, we have no way of controlling the config file that turns it on. We're pretty sure that most of the folks that have CPEs that have that capable, that the only ones that have turned it on, are the ones that we control the code for ourselves, and we have deliberately done it. And for those we own, that we own the updates.

So, I will have to coordinate with the folks that own the XP3s, and the various other CPE devices. We have not yet started talking to our frontline folks, that's going to be an interesting challenge anyway. DNSSEC in general has been mildly problematic. Sadly what happens is it just simple bleeds over, as it seems like it's DNS and it falls to my group.

And we just cope with it. So, that is sort of where we are, [inaudible].

UNKNOWN SPEAKER: So, just to note things like the tomato firmware for [inaudible] routers, there is a lot of [inaudible] you know, if you install tomato, click this button and you get the DNSSEC. So, there are other DNS mask type things.

UNKNOWN SPEAKER: I understand, but this is more of the, we don't have the visibility or any way of doing… At a certain point, what's going to happen is much like with our CPUs, if you pick your own, in theory, you are now on the hook, have that vendor support it, which is actually going to be ugly. It's getting vendors to do updates. Like I said, ISP, CBE, [inaudible], yeah, same old.

UNKNOWN SPEAKER: Roland, did you want to respond?

ROLAND: Yeah, so two comments to… Warren said, rightly, that really large operators are, the failure mode is probably going to be that the resolution completely stops, right? Like, what we've seen with the validation problems with some of the TLDs, where they had glitches where wrong keys were published, or an algorithm roll over failed, and everything below the TLD disappeared, and I guess what you're saying is that if that happens to the root, everything below the root disappears.

Which I guess is fair, although Olivier is shaking his head, so he has some ideas about maybe that won't happen. So, there are two other things that could be causing problems, because at some point during the root case K rollover, there is going to be this time when the DNS key set is very large.

And that may lead to really interesting failure modes. That don't necessarily mean that resolution completely stops all of the time. And the other issue is all of those Linux distributions, and freebies, [inaudible] that have now, by default, if you deploy the latest and greatest version, they have a resolver in there, or all of those things going to function correctly, because I've been sort of dabbling with some measurements on the authoritative name server side to work out where growth is, in terms of DNSSEC validation.

And there is a huge number of resolvers that only serve a very small client population, but the number of resolvers is increasing very, very rapidly. And those folks are also interesting to monitor.

DAN YORK: I've got Roy, [inaudible], and Oliver in the queue. So, Roy.

ROY: Thank you. I think this is a wonderful idea. I've, I'm sorry. This is [inaudible] for Canary. I think it's a wonderful idea. I saw the proposal a few weeks ago, for the first time, and immediately all of us in our team at ICANN, we jumped enthusiastically towards this. We will support this. We have our own data, which we will, the L root data, for instance, which we collect, we all look at that.

What I really like is the longitudinal aspect of this study. This is not incidental. This is not, for instance, like [inaudible], which is very good as well, but this was two days, this is for the entire period of the DNS key roll over. So, yeah, you [inaudible]. Thank you.

UNKNOWN SPEAKER: [Inaudible]. So, it's not exactly a question from me, but it's more repeating a question asked the KSK roll over panel yesterday. What do these things go wrong if the automated update don't work, etc., should there be some…? And a question to the operators and also At-Large.

Should it be kind of a publication or some information, how to repair by hand, or actually more…? Should it be more precise place, where this kind of information notify operators that they do need to take action?

Should it be one place where everybody can point to? So if you run your imbalance, your knot resolver, your [inaudible], your bind, these things that work, you can try using these steps, or they contain pointers to the [knot?] resolver website with specific instructions, or to the unbound? And this is more questions, not a suggestion.

I don't want to generate for others, but a question to the panel.

UNKNOWN SPEAKER: I think that's a good idea. I mean, that makes sense. The worry then is going to be if people are able to reset [inaudible] if their validation is filled, but that's another matter. And as Paul, he stepped out, but as Paul rightly remarked, you probably need to do that on a domain that's not signed.

I think it's a good idea to do that. And that could also be a community effort, right? That all the people that produce open source packages just have… These are four easy steps to fix your resolver.

UNKNOWN SPEAKER: I can't speak for Matt, is he…? Matt, are you back there? I think part of what… Or as Ed… I know that the folks at ICANN were talking about, you know, getting some of these things, you know, things are [bind?] and then not, making them available in some space, tutorials about how to go and make sure that your thing worked.

Although to your point, yeah, we may want to consider about making sure those are available at an unsigned domain. That is a good point too. There is Paul [inaudible].

PAUL: Hello? Okay. Yeah, I'm still here. I was actually sort of jokingly wondering, there is one IP address that everybody in the world knows where you can run a website on, that would actually work when all of DNS fails. So, Warren, why don't you run a nice informational page on 8888?

[Laughter]

UNKNOWN SPEAKER: For those who are remote, Warren is from Google who operates those, and there is Ed. Ed is coming up to the mic.

ED LEWIS: Ed Lewis. At the risk of going into solutioning a problem right now, one thing I'll point out is, if you have a bad trust anchor in your resolver, you'll resolve nothing out there, not even unsigned domains. So, the problem is a bit, it's not just where to put something, we've got to consider that too.

So, we thought about that. We don't know where to put the warning sign.

UNKNOWN SPEAKER: The warning side of the internet. This is bad. Go fix it somewhere here.

UNKNOWN SPEAKER: It will be even worse, it won't even resolve your resolver's IP address to log into and fix it.

UNKNOWN SPEAKER: All right, good points, all right. So, we'll just keep thinking about the [inaudible]. All right, Roland.

ROLAND: May I add some more doom to that? If you have configured your SSH team to do reverse DNS lookups, and block anything that doesn't have a reverse DNS entry, you can't even log into that machine.

DAN YORK: Awesome. Okay. Next, I have Oliver and then I see [inaudible].

OLIVER: Thank you, Dan. So, on Roland, the failure is going to be a little bit rolling, so hopefully people are going to be looking at [inaudible] going up. You may open, operate two, three resolvers. I think Paul operates a few more than that. So, if something starts going wrong there, it would only affect a small population of his, and in many cases, the end client will try again when they get [inaudible], hopefully get to another box.

But I think your idea about monitoring this, and trying to do it from a global perspective and all of the things, is a wonderful one. I would like to support it. So, I suggest you create an invitation only mailing list of people who are willing to discuss this and talk to you about it.

So, while certain information can be shared, but others could be shared. And to [inaudible] point, we have this wonderful communications channel for if things go wrong, it's called Twitter. [Laughter] So, why don't we create a hashtag, KSK roll over notice. Not call it failure, but notice, or something like that.

So, everybody can monitor that.

UNKNOWN SPEAKER: As can all the trolls and spammers. Or K Day. Hey Matt, can we, is K Day, can that be the official name of July 11th?

[Laughter]

All right. Any other questions? Yeah [inaudible].

UNKNOWN SPEAKER: My question is to Roland. So, you are [inaudible] dot org seems to be really important for the operators. So, I'd like to introduce your website to [inaudible] but, is it possible, because if the operators see something happen, then they will [inaudible] to the root operators dot org, and it will be some kind of DDOS attack.

So, I'm very worried about that. So, the information is important, but how can we distribute the information to the operators? I'm going to look at Olivier here and see if he can help me with some cloud [inaudible] to make sure that doesn't happen.

DAN YORK: Yeah, there might be a few people here who might have access to large scale CDNs and you know, things like that, that maybe could get involved.

Warren?

WARREN: Yes, I mean, one of the big things in a number of the SSAC documents like SSAC 63 and 73, was that there should be a lot of outreach to reach the sort of people who normally don't participate. I think one of the issues is actually, we've been too successful with the DNSSEC push, right? We've done a lot, if you want to turn on DNSSEC, there is a lot of deploy 360 stuff, which is, it's so awesome, let's go do it now.

And, you know, DNSSEC for everybody, and things like that. What scares me is the number of people who have turned this on because we've suggested that it is the right thing to do. And then wondered off, or quit the company and worked somewhere else. And so a lot of un-managed boxes which, you know, are not going be, anybody around who know what it is, who turned it on, how you turned it off.

Following on something somebody said, ISC actually has a webpage up on, you know, what the KSK roll means for you, and possibly what you do if it hurts and how to turn it off. I suspect, unfortunately when things go bad, people aren't going to bother fixing the key. They're just going to turn off validation, because that's the easy fast thing, and once you've done that, the pain stops and people go away. So, oh well.

DAN YORK: I suspect you're right, Warren.

UNKNOWN SPEAKER: Yeah, my experience with validation failures where we reach out to the zone owner, and in most cases, if it's not a key rollover, it's they've taken out either the DS or taken out the signatures, because they didn't know they had a signed zone. And almost universally, when you explain what they need to do to fix it, or you can take it out, they will just disable DNSSEC.

UNKNOWN SPEAKER: Nice try. [Inaudible]. Warren just inspired me to suggest a DNSSEC spring cleaning. So, when people are putting the hands in their resolver conflict anyway, to either enable automatic rollover or installed a new key, I would install the new key, would I?

They could actually not only should [inaudible] be destroyed, as always, the [resolver?] should be switched off, right? That's a nice opportunity to do the right thing, two right things at the same time.

UNKNOWN SPEAKER: And disable DLV.

DAN YORK: One question, though. So, how many people, and this is the wrong room to ask this question, but how many people have actually gone in and change the configuration for the DNS resolver any time in the last six months? Yeah, all right. It's the wrong room to ask this question.

All right. Let me ask a question. If we were to poll the general population outside this room here at ICANN, how people think that the average person out there has changed, or has even looked at their DNS configuration in the last year?

[SPEAKER OFF MICROPHONE]

Exactly, yes.

[SPEAKER OFF MICROPHONE]

UNKNOWN SPEAKER: And I think you might slightly be, a slightly overcomplicated topic. Or, could rephrase the question and get more responses, because you know that everybody raised their hand, even when you haven't given any timeline anyway, so people are living with their hands in the resolver conflict, obviously.

Seriously, upgrading the software somehow, to rely on defaults would achieve the same, and people won't notice, so quote, quote, dumb down, and I hope the ombudsman is not coming after me, but dumb down this to the end user level, might be helpful.

DAN YORK: Yeah, I mean, I think [inaudible] is a real one, you know, I know that… I mean, it's a question when people buy that box in the United States where I'm from, you know, they go to Best Buy, or they do something, and they get their home wi-fi router because that's what they, because many of the ISPs in the United States, anyway, are encouraging people to go get their own device and put it in there, which is awesome, except for the fact that then it just sits there and they never upgrade it.

And so, they are several years old and some of the configurations and that kind of thing. You guys wanted to… All right, go ahead.

UNKNOWN SPEAKER: One thing I'm wondering now is, are there any ends into the large software companies. I know that Paul is here from Red Hat, but for instance [CROSSTALK]… The reason I'm asking the question is, I recently had an exchange with one of our [inaudible] that were trying to deploy DNSSEC, and they had, they were using one of our authoritative servers as a secondary.

And it was keeping copies of old signatures, and I was really surprised. I've never seen that behavior before. It turned out it's a bug in Windows Server 2012 that got resolved, but they hadn't deployed the full chain of dependencies that they needed to deploy this fix. And I'm worrying that this is true for things to do with validation as well.

And the good thing is that, I'm guessing if you are a legitimate Windows user, that Microsoft probably knows which fixes you have deployed and which you haven't, because it's associated with the license that you have. And I'm wondering whether this is true for other big software platforms such as Red Hat, or Umbtu, or whatever, whether they have some sort of visibility into how many people at least downloaded the packages that they can be sure of, have the right behavior to deal with this.

DAN YORK: Well, as it happens, the person standing at the microphone might be able to answer, maybe, I don't know. But Paul.

PAUL: Hi. Paul [inaudible] with Red Hat. We do have some statistics, but since a lot of people around like clusters behind proxy servers, we don't really know the statistics of people who upgrade. However, in our case, the solution is even simpler. There is no newer package for you to upgrade to, since the last whatever year or so, because nobody is filing bugs at Red Hat saying, our DNS software is too old. We need newer software.

We are missing these features. We are missing these bug fixes. We run by these bugs. So, the standard policy of Red Hat, and that's why you all love Red Hat so much, is it's really stable and it doesn't change. So, if you want to change something, please file bug reports and say, the DNS software is too old for my use. I need newer DNS software.

Because I've been trying to push internally, and as long as there are no customers asking for this, I am not getting traction. So, file bug reports, if you have a real license, so we can move this to newer versions.

DAN YORK: All right. Other questions for our panel?

Come on. Anybody else sitting out there? Anybody else from an ISP out there who is thinking about this? What have you done? Go ahead.

UNKNOWN SPEAKER: Just one other comment, and this is actually, probably for the ICANN folks to watch as well. I know one of the concerns is the size of the keys. My comment on that is, actually it's not an issue any more than anything else is right now, but I think anybody who is doing DNSSEC validation has discovered that getting large UDP packets in general, is problematic all of the time.

After zone, or key roll over failures in DNSSEC, my biggest DNSSEC problem is not DNSSEC, but is just largely UDP packets. So, that's the thing to continually watch while we're doing this.

DAN YORK: When did you want to…? Oh, you looked like you had wanted to say something.

UNKNOWN SPEAKER: I was just going to say, if you do buy your own CP [inaudible] you would make sure you would find a trustworthy vendor. Mine is actually sitting three places from me, so I know if my [inaudible] goes boom, I know where to find him. I also, Warren just mentioned the SSAC reports. I think we should all thank SSAC, Warren, [inaudible], and others for making an excellent report.

DAN YORK: Indeed, we should. And I see a gentleman standing there.

BERT: Yes, hello. This is [inaudible]. I'd like to add a few small notes. One, at power DNS, we can actually see what versions of software people are running, which will enable us to more selectively warn more important deployments, which is something that we'll be doing, especially since we did not implement RFC 5011. So, it's really important that you get it right.

The other thing, as a data point, as I'm sort of a little bit like Paul, a proxy for the operator community. Because I actually do speak to people with large resolver firms, and how they run them. And the situation out there is quite depressing. And I echo the sentiments that people will turn off DNSSEC validation, at the first hint of trouble, and they may turn it back on again.

My suggestion would be, therefore, not only to tell everyone how extremely important it is, because we're doomed if we do not put the upgrade beforehand, but also provide a readymade materials for the people that somehow did not listen to us. And say look, this is the page you need to go, this has cut and paste instructions that will make it go boom, sorry, make it go zoom again.

That would be my suggestion because to finalize this story, I would estimate that the average, very large scale European service provider has 0.4 people working on the DNS resolver, and they also have other things to do. So, that's ends my little bit of input.

DAN YORK: Great points. And I should also just thank you, Bert, since you're here, for all of the work you've been doing over the years on power DNS, and all of the work you've done with DNSSEC and statistics and all of that, so thank you for all of your work in this.

BERT: You're welcome. [Applause]

DAN YORK: Anybody want to react to what Bert said or anything?

UNKNOWN SPEAKER: Just out of curiosity, which parts of RFC 5011 did you hate most that made you not implement it?

BERT: I'm here to dispel the myth that power DNS exists of me exclusively, we're now seven people. And those seven people have very strong opinions, and I listen to them, and I will relay your concern to them, because I really don't know.

UNKNOWN SPEAKER: I look forward to the Tweet.

MATT LARSON: Matt Larson, ICANN. One document that I've realized that we need to produce is the one that Alberto has described, something specifically targeted at operators. We have presentation materials that we're going to be going around with between now and the KSK rollover, targeted operates, telling them what to do. But we need that in prose form, not the slide form that's it in now. So, that's going to appear on a webpage soon, and that will be an URL where people can point to.

DAN YORK: Yeah, and Matt, I was thinking, we should collectively all talk about how we can help make that a really simple site somewhere, something. Maybe we spin up a little micro site or something, just to focus kind of, like a root canary type, and something just DNSSEC is broken, here is what you need to do to fix it type of thing, or something.

MATT LARSON: Yeah, I don't have strong feelings on the branding for it, so it doesn't have to be on the [CROSSTALK]…

DAN YORK: I'm just thinking on both your site and my internet sites, we tend to wind up putting things on there that wind up getting these long, really ugly URLs that get buried and stuff, and so maybe we should collectively thing about how we can make that a simple thing somewhere. Okay?

Other questions or comments. Roland, I'll just reach too to your, the survey you're giving for K Day, I like that. Let's definitely talk too, because I'm working on the state of DNSSEC deployment

2017 report. If you're doing that stuff that's in the summer, you're going to, okay, because my goal is to publish that for ICANN 60, so it will be published for the end of that.

So, if you're doing stuff over the summer or somewhere there, let's talk and see, at least preliminary kind of info, what we can put into something like that, because it would be great data to add in there.

ROLAND: Yeah, sure.

DAN YORK: Okay. I think, do we have anything further for our ISP panel? All right. Let's give a round of applause of our folks here. [Applause]

So, with that, we are going to move into a demo. We're going to be brave and daring, and Paul [inaudible] is coming up to go and do this kind of thing. So, while he's getting set up, I should also mention [inaudible] didn't, we didn't fully acknowledge the fact that [inaudible] here, or [inaudible], is the man behind a number of different statistics sites that are out there for different sites.

And you mentioned it briefly, but we should have said that too. For DNSSEC and IPv6, and also we should note, I've actually always wanted to meet him, so I was glad to meet him here because he is the man who writes about the IPv6 goat that gets burned down in Sweden every year.

And if you don't know what I'm talking about, you can go to Circle ID dot com, and you can look there, and you can look up the stories that he has written about the IPv6 goat, or you could probably just search in that search engine, of course, and find the IPv6 goat stories.

UNKNOWN SPEAKER: Important. Christmas goat.

DAN YORK: The IPv6 Christmas goat, as compared to the Easter Goat or the, you know, fall goat, or whatever it may be, but yes, it is something that is there in Sweden, and it gets burned down every year, and for a brief while, it provides IPv6 statistics. These are the little factoids, and that's just me burning up time while Paul gets his demo ready.

UNKNOWN SPEAKER: I must comment. The last Christmas, it was about two hours before it was burnt down.

DAN YORK: And why the Swedes want to burn large wooden goats, I'm not quite sure, but these are the things that go on there. But he also does have some interesting statistics about IPv6 and DNSSEC for a variety of things, including counties in Texas, right? Was that…? Or, where was it in the US?

UNKNOWN SPEAKER: It was in Texas, but that site is broken now. [CROSSTALK] … [inaudible], and new PHP version, and I didn't have time to fix it.

DAN YORK: Okay. Well, I just always found it entertaining that an IPv6 advocate in Sweden, was providing information about counties in Texas that has IPv6. So, you know. There we go. All right, we now are at the stage of our presentation when we are seeing command lines up on our screen, which is always starting to get…

So, now we're going to see if Paul can make opportunistic IPSEC using DNSSEC actually exciting for a demo.

PAUL: That's a high bar. Okay. So, I am part of the [inaudible] project, that started out many, many, a decade and a half ago, I guess, by John Gilmmer, from the EFF. With the [inaudible] project, where the intension was to encrypt the entire internet all of the time for every packet of data that goes over using IPSEC. We're not doing it, but we keep rolling it.

And in fact, the reason that team got involved very much in the early days of DNSSEC was that they wanted to put public keys in DNS, so that you could pull those keys securely, and then use them to build secure connections to other machines. So, they were planning to use the DNS and hierarchal distributed secure database.

So, just a few slides to explain things. So, a typical VPN, when people think of VPN, this is one of two deployments. One is a side to side VPN, where you can see there are two VPN servers, and they're connecting two clouds or two subnets or offices, and they're connected. And the communication inside those clouds are all not encrypted, and so they're all in the clear, and indeed, the IPSEC servers that connect these two networks, that is encrypted and safe.

So, it's not the ideal situation, but this is a common setup. And we see now actually, strong push [inaudible], the Snowden and the NSA smiley slide. We see a lot of push to actually encrypt all of these individual node components as well. Of course, we also like to use IPSEC for that.

So, this is the other kind of VPN tunnel that people are really familiar with. It's the remote into your home or to your office, so we have your roaming device in IPSEC terms, we tend to call them war warriors, and they connect to a VPN server, and then they connect from the VPN server to the cloud. And this is the [inaudible] is also the model used by all our Netflix, I am not in the US people, that connect with their laptops.

And so, from their laptops to the IPSEC, it's all encrypted. But once it leaves the VPN server, it's all in the clear going further. Now what is opportunistic IPSEC? So, we needed a few features that we didn't have 15 years ago. So, with [inaudible] two, which is the [inaudible] keying exchange protocol that's used for IPSEC, so you negotiate the crypto-keys for the VPN tunnel, we didn't have asymmetric authentication where the client could remain anonymous.

And this is what the model is for TLS. If you go to a secure website, your connection is encrypted, you make sure that you identify the server and authenticate the server, but the server has no desire to authenticate you. They don't know who you are, you're completely anonymous. So finally, with IP 2, we were able to do this model as well, and this is very important because one of two reasons we failed a decade ago, was that for IPSEC, you needed to have an identity in a publicly yourself, and so your laptop would have to have some credentials, and then somehow you would have to publish these credentials.

And that was actually my charter problem to solve. The next item that we needed for this to deploy was DNSSEC on a local host. So now, I've forgot to say earlier that they saw a massive increase of [inaudible] first being used everywhere. That's actually great because that means people are running resolvers on their laptops and hopefully on their phones, and then soon they will have DNSSEC up until the end node on their machine.

So they don't, there is no insecure last mile in between. So, that was the important part. And that allows us to do DNSSEC based triggering. So, when we want to send a packet to a remote destination or a remote host, we know the name, we can look up the IPSEC key, install it in the kernel, get the tunnel up, and get the application going.

An additional problem, not so interested in the DNSSEC part, is that we needed to address the NAT problem. IPSEC builds up tunnels using the source IP on your device, and if you're behind NAT, the only IP you have is the [inaudible] 68 one dot one IP address.

And so, we needed to have a way to have multiple people connect to the same server without causing a conflict. And we came up with a nice idea. We wrote a draft that expired, that will probably wrap it up again, and a code, and Linux has improved that we can actually install that. So, this is all invisible done within the IPSEC subsystem.

So, there is no additional NAT rules for something that could conflict. So, this is how the packet flow works. You have an application, say Firefox, and they do a DNS lookup to connect to [inaudible] dot org. So, they sent this DNS lookup to the local DNS server. This could be unbound, [inaudible] anything.

And that local server will go and fax the A record, and do all of the proper DNSSEC validation, but in parallel, it will send an inquiry for the IPSEC key record as well. And only once it has an answer for both of these queries, will it then continue and in the next stop of the process.

If there is an IPSEC key, then it will first build up an IPSEC, and also it will give this information, the Q&A plus the A record, so the IP address, plus the IPSEC key, to the [inaudible] and then the [inaudible] will then setup an IPSEC tunnel, and everything will be encrypted.

And only then, will the DNS server return the A record to the application, so that when the application then has its, you know, it resolved its A record, they've got an IP address, and it will just send unencrypted information, it will be caught in the IPSEC get encrypted. And this is important. We call this opportunistic encryption. The user is not aware of this, we're just trying to blanket encryption everywhere, as securely as possible, and maybe even if we cannot authenticate it, we might want to do it unauthenticated, but it's just a raising the bar for mass eavesdropping.

This is not a replacement for a green address bar, or any other indication that you have authenticated another party. And with that said, I sort of tried to make a diagram of it, which I guess, might be displayed while I try and run the demo.

So, unfortunately my screen is a little smaller than I had hoped, so all of my carefully placed x-terms are overlapping, but we'll make do. So, first of all, this is [inaudible] machine in the middle, and I will just start at [inaudible] here, so that we can see what's happening.

So, if I go on the first server, and I will just… So, everything has been disabled at this point. So, nothing, this is just to get a baseline. So, if I run the ping, interesting. [Laughter]

That was fast. There we go. So we see the ping happening, and we see the plain text ICP. So, this is completely unencrypted. So, now we will… NAT has a short time out here.

Okay, there we go.

I'll just make sure, it starts with a clean state, and [inaudible] to see if there are any tunnels up. So, it tells us there is no tunnels up. So, now… So, we haven't integrated this yet into the DNS servers, we're working on that, and we would like some help too. So, this right now, is a standalone module that could sort of… The concept of this would go into the DNS server.

Works better if I start IPSEC. Let's try this again. There we go. Okay, let me scroll back now because [inaudible] quickly. So, first you see, it got the A record. And this is just like some unbound Python code. So, we got the A record, it was protected by DNSSEC. We found an IPSEC key record. We dump the raw data.

For those DNSSEC implementers that have done any implementation of IPSEC key records, I am really sorry. If there was any comfort, I was doing this at 1 AM last night, so I feel your pain of the worst DNS record ever designed by IETF. Anyway, if you decode this properly, you get this basic defer blob, which is the actual RSA key of [inaudible] labels on the [inaudible].

So, we pulled this from DNSSEC. So then, we have an interface to push this key into the IPSEC server. Then let's see if I can fit it on one screen, with magical scrolling. There we go. So, basically, it's the equivalent of this connection, which here sounds like the left side, which is the client side, it's using no authentication.

It means it doesn't authenticate itself, because this is the laptop. Right? It found the IP address. It put it in the connection, and the rest are mostly sort of internal IPSEC terms. Very interesting to the DNS world. And then it loads the connection and initiates the connection, then you see here some parameters and negotiation as doing [inaudible], as agreeing on keys, sending up the tunnel. And then the tunnel has established.

And we can see here, we haven't done any bytes yet, so let me run the ping again.

And we see that everything is encrypted. So basically, we're sending up lots of IPSEC tunnels based on DNSSEC data of public keys pulled out of DNS. And so, we're hoping to speed this up and sort of enable this for default, so that we'll get [malware?] encryption on it by default. Okay, any questions?

DAN YORK: Seriously, that was it? No more questions? All right.

UNKNOWN SPEAKER: You only talked about A records. What about [inaudible]?

UNKNOWN SPEAKER: Feature creep? No, no, we'll do it [inaudible]. So, the [inaudible] will actually do both A and the [inaudible], and look up. There is actually more additional problems too, because for instance, if you have six A records returned, you have two choices, right? You can either try and setup six tunnels, or if you cannot, and let's say you have only one of the six A records that sets up a tunnel, then you have to decide, am I going to lie to the application and only return the one A record?

Or, what are we going to do? Those are some intriguing questions that we've sort of postponed answering for now.

DAN YORK: That was actually directed to you from [inaudible] here, that our local IPv6 advocate, who is suggest that. In the line here, I see, we've got a couple of people.

UNKNOWN SPEAKER: Yesterday [inaudible] I had to get around an intercepting firewall, and so I switched to my VPN home tunnel, which is the intercepting file that I control. The thing is, how do you want to survive next generation stuff that breaks into that, and your user sees a greenlight, but it's not green?

UNKNOWN SPEAKER: So the [inaudible] encryption part, so on purpose, we're not giving users feedback, because we're thinking of this as below the user level. We're just trying to raise the encryption on the internet without actually giving the user one specific authenticated website with a green address bar.

So, sure, if you do not agree with that feature and you would rather have plain text going on and on forever, then we can have that. You can bring this up to the application, and you can, just like, for instance, these [inaudible] people have done this to, with fake sets of [inaudible] options and get [inaudible] options, and then you can give the user feedback, but then inheritably, you'll get to the question, what if it doesn't work?

Or do you do a hard fit or soft fill? How are you going to talk to the user? We decided not to go there yet. I think, at first, we just need to raise the encryption for default on the internet at large. And if you want to do something authenticated on a website, and you would do a bank payment, then you need to be sure that, you know, from the application down, regardless of the transport, that you are encrypted and authenticated properly.

PHIL: So, Phil from the Network Startup Resource Center. I guess you didn't get many questions because everybody has been like, why haven't we had this for 25 years, right? We had skip… Just kidding. Now it's actually possible to do this, so this is great, and I think some of the questions that just came up, maybe our tied to what I'm about to ask.

What about the DNS to specify policy? Unless I miss something, and that was already talked about.

UNKNOWN SPEAKER: No, so, one of the failures of the [inaudible] project as well, was that they allowed gateways, and they used the reverse DNS to actually publish keys, and then they assumed that, you know, with the DNSSEC deployed, this would be great. So, you can say all of the traffic of this slash 24 goes to this one IP address.

But that really depends on having a secure reverse tree and signed with the DNSSEC. And as far as we can see, the reverse tree has never been accessible to users, and it's even happening less and less. I can't even mail Google because half of the time, my reverse IPv6 records are gone.

So, I don't see the reverse as a stable source of doing anything anymore. And so, we really wanted to move away from that. And so, when I came up with the idea of intercepting it at the DNS level, the problem then becomes is that you have only the forward DNS, and not the reverse. And so, you have no authority over any IP address, so I cannot make any statements, I cannot find any claims about IP address, and who owns them, and who could publish keys for them.

And maybe once RPKI and those efforts get further, and there is some interface to the end users that we can use that, we can look at that. But I've stayed away from RPKI because I already have enough problems with DNS people, and I didn't want to have all of the routing people to follow me too.

UNKNOWN SPEAKER: It will be interesting to figure out how do you start your BGP session when you're trying to do opportunistic IPSEC to set up RPKI.

UNKNOWN SPEAKER: Right. So, currently we do have different failure modes that we allow. So, there is no key found in DNS then we just allow plain text traffic. But you can actually have groups. You can have groups that you can mark, and that's more of a use case in the cloud where you actually do authentication, either by certificates or mutually authenticated with the DNSSEC records, is that you want to ensure that these are always encrypted, because those are under your control, and you do not expect a failure there.

So, you there you can actually hard fail and say only encrypted traffic is allow to this [inaudible] range. So, you know, 10 slash eight, encrypted. And then you can make exceptions, and like have some service in the clear. We had customers that said for legal reasons, they had to have some traffic in the clear, so make sure that happens.

And another problem we actually found was that, when you start deploying this in your internal network, half of your firewalls are becoming completely useless because you cannot see anything anymore, so that one of the first questions of one of the customers was, can you somehow expose the port number when you're encrypting it with IPSEC, so we can see what it is and then allow it to drop the traffic.

And then we sort of convince them after a while that, you know, if you do that, and it means that any attacker can also do that, and then your [inaudible] are kind of useless anyways, so your best bet is just move the firewalls onto the end node and distribute them with [inaudible] and other mechanism.

UNKNOWN SPEAKER: Cool, thanks. And when are we going to ship this in Red Hat?

Just kidding.

UNKNOWN SPEAKER: So, it first goes via Fedora into Red Hat, but in fact, I submitted the package for [inaudible] 7.4 also last night at about 1 AM, and that one will have, already has the opportunistic encryption capability for certificates. So, you can run this into your internal cloud, if you have one CA and certificates in all of your hosts, you can have this opportunistic initiated using certificates.

So, any hosts within your cloud will set up IPSEC, and almost any other host in your cloud.

DAN YORK: This is also the point where Paul would probably suggest that if you want this in Red Hat, Enterprise Linux, that you file a ticket or a bug report…

PAUL: We already have a bug report for this, it's fine. Like, the other feature request, it was an important customer. It's good, we're good.

DAN YORK: I was trying to help you out here, man. You're always asking us to fill out bug reports, you know?

PAUL: Just for DNS software. More bugs for DNS software. IPSEC is good.

DAN YORK: Okay. Carson, did you…? Okay. Anyone else questions for Paul? No? All right, I want to thank Paul for doing a live demo. [Applause]

As I just Tweeted, we are probably the only place at this entire conference that was having command lines on its screen at that time. So, not something, it's great to have that there. So, now moving from command lines to trend lines, or graph lines, yeah, okay that was a scratch.

We've got Roland here to talk to us a bit about ECDSA and what he has found in his work, and I'll turn it over to Roland.

ROLAND: Okay, thank you, Dan. Yes, but the first slide is missing, but the idea is that, thank you. This talk will be about ECDSA adoption in DNSSEC, and it gives you on three gTLDs, one special TLD, very special TLD, and seven ccTLDs, and this is work I did both as a researcher and as a servant employee, so it has both labels on it. Next slide, please.

So, I guess everybody is aware that the ECDSA is standardized in DNSSEC already in 2012, but nobody used it until Oliver came to an ICANN meeting and said, we're going to go and do DNSSEC at Cloud Flare, and we're going to use ECDSA. And there was no use, at all, until the end of 2015.

I'll tell you a little bit more about the data sets that we use. We had less than 50 domains in our data sets signed with ECDSA. And then, in 2015, Cloud Flair announces universal DNSSEC. I don't know, you probably have to do this in a dark voice. Which is on the fly, DNSSEC signing ECDSA, and in 2016, the good folks at Power DNS, and I don't know if Bert is still here, yes he is, okay.

So, they make ECDSA the default algorithm, and this made me wonder, does that people actually start using it, and can we see that in our data sets? Next slide, please. So, just a quick recap, why would you want to use ECDSA? And if you're not already using it, why should you switch to it?

So, DNSSEC suffers from a rich ability problems because of fragmentation. Paul [inaudible] was referring to that, and unfortunately, yes, this is still a thing in 2017. And it's not going to go away, I'm afraid. And then the second problem is that the DNSSEC is abused for amplification attacks. This is sort of depends on whether DNS amplification is the attack de jure, or whether there is some other vulnerable protocol that people are abusing.

But there have been lots of reports that some of the bigger amplification attacks were using signed domains, although crafted domains made a comeback a couple of weeks ago as well. And then the common cause here is that large, that DNSSEC has large messages, and these are mostly large because of RSA signatures and RSA keys.

And an easy solution is to use [inaudible] curve crypto, because you get much smaller keys, you get much smaller signatures, and you get stronger cryptographic security. So, basically it's all the good stuff packaged in one algorithm. Next slide, please.

So, what we wanted to do is after we did a study of why making sort of a business case for using ECDSA, are people actually adopting it? And the data says that the we use were collected through a platform called Open Intel. There is an acknowledgement on the last slide. This is a project that Surfnet, SIDN Labs, and the University of Toronto run together.

Basically, it's a very large scale active DNS measurement platform. If you're interested, come talk to me. I can tell you a little bit more about it. And the data that we used is for three gTLDs, so it's for com, dot, and org, and we have data covering March 1, 2015 until February 14 of this year. For dot NL, we have data for about a year, and then for dot gov, a very special TLD, we have data for a single day, and we also looked at a single day of data for six ccTLDs, a few of which are actually from this region.

In this table, I mean, the slides are up on the ICANN website, and so in the table, you can see the stats. But you can see that there are varying degrees of DNSSEC adoption with dot NL having the highest number in sort of absolute numbers, and dot SC, the highest relative number of signed domains, at least in these data sets.

I think that the Norwegian ccTLD has a little bit higher percentage, but it's all sort of close to 50%. Next slide, please. So, what we wanted to do is look at adoption of ECDSA. So, we look at algorithm identifiers in the DS, DNS key, and RRSAC records. And then we distinguish between full and partial deployments.

And another thing, the figure is pretty self-explanatory. If there is a DNS key, and there are signatures, but there is no DS, we label this a partial deployment if all of the sort of essential ingredients for DNSSEC are there, we label this as a full deployment. Next slide, please. So, this is the graph for the three largest gTLDs. What you can see, the graph starts October 2015, because before that time, there was virtually no adoption.

And what it shows you is the date that Cloud Flare announces universal DNSSEC, is now available, and you can flip the switch and turn it on. And for almost a year, they are the only source of significant deployment of ECDSA for DNSSEC signing in com, net, and org. What is also interesting to note is that the darker blue are full deployments, the lighter blue are partial deployments.

So, the domain is signed but there is no secure delegation, so nobody can validate the signatures. Then from about April 2016, and it's very hard to see on this slide, but someone starts signing their domains with ECDSA, and this is a media company that publishes lots of local newspapers in the US, sort of world conquering publications like *The Sacramento Bee*.

And then things really start getting interesting from the middle of October last year, when [inaudible], which is a Norwegian company, and I asked for their permission to name them here, sort of assumed that Oliver was okay with this. And they turned on ECDSA for all the domains that they signed. I think they signed all of their domains by default if you use their DNS service, and they turned on ECDSA for all of them.

And interestingly, they did an algorithm roll over. So, they were signing with RSA before and they did a proper algorithm roll over, and I looked at the data and tracked it. They published signatures first, they published keys next, and had the two algorithms next to each other for about a month, and then switched completely to the ECDSA.

And what you can see is that they sort of now dwarf the deployment that Cloud Flare has. Next slide, please. So, I assumed a little bit on partial adoption, because partial adoption doesn't just occur for ECDSA, it also occurs for other algorithms. On the left side of the slide, you see the adoption of RSA [inaudible] one and six three, so that's algorithm seven.

And what you can see is that this is almost exclusively for deployment. If you look on the right, this is the adoption rate for RSA [inaudible] two six and six three, so algorithm eight, where the majority of deployments are actually partial deployments, so they are lots of people that signed their domain, but they don't have a secure delegation.

And we try to find out what are the causes for this, and sort of this varies. It can be because the registrar doesn't have support for secure delegations at all, or they don't support secure delegation for the particular algorithm, or registrants just simply forget to register a secure delegation. And all of these things appear to be happening.

So, hopefully with this new RFC for SDS CDS key use, this situation may change because there is actually a large reservoir of signed domains in TLDs such as dot com, that are currently cannot be validated, because there is no secure delegation, and this will significantly increase DNSSEC deployment in those TLDs.

Next slide, please. So, I Tweeted this picture as well. I plotted a graph of the algorithm distribution in dot com, and what you can see is that ECDSA PT56 is now, is about to overtake RSA [inaudible] 256. So, algorithm eight. Which is actually very interesting. And it appears that new deployments of DNSSEC are actually increasingly starting to use ECDSA, rather than RSA, from the get go.

A little bit more worrying is the huge percentage of people that are still using RSA [inaudible] one NSEC three, given the recent announcements about [inaudible] one. I heard, I don't know who said this, but there was going to be some discussion about this IETF in Chicago, is that correct?

DAN YORK: Roy? Somebody has a draft, right?

ROY: There are two drafts that are related to this. [Inaudible] Paul [inaudible] sitting next to me, and myself, we have a draft, two different drafts discussing [inaudible] one, [inaudible] 256, algorithm updates, etc.

DAN YORK: But I think the point of that would be to encourage people to move to [inaudible] right? To not use RSA one.

ROY: Yes.

ROLAND: Okay. So, next slide please. But we could make ECDSA, I couldn't resist, we could make it even greater. And we can make a huge by yes, yes, okay. You can hate me for this. We could make it huge, because if every Cloud Flare operated domain were to deploy their universal DNSSEC, this would more than double the number of signed domains in com, net, and org, and it would instantly overnight, make ECDSA the most used algorithm in com, net, and org.

So, I'll give Oliver some time to make a picture of this. I can give you the slide if you want. So, I'm guessing, I think Oliver commented that Cloud Flare has a policy that people have to make conscious decision to turn on DNSSEC rather than them turning it on for their customers, which I think this is a policy that we, and when I say we, I mean Surfnet, also have.

We don't force people to use it. We want this organic growth that people were also referring to, so we want people to switch it on themselves. But if everybody does that, and if they can be sort of stimulated to do that, then Cloud Fare could make ECDSA huge. Next slide, please.

So, we also look at adoption in the dot NL ccTLD, because dot NL has the largest absolutely number of signed domains. But also, dot NL didn't support ECDSA for secure delegations until March 1st of last year. So, we wanted to see if we could see some sort of effects from that in our data sets. And what you could see is that there were already dot NL domains signed with ECDSA through Cloud Fare, before secure delegations were possible.

And then if you look at sort of the arrows at the top, it says that more than 50% of those partial delegations that existed before secure delegations with this algorithm were possible, are still partial deployments at the end of the data set sort of this year. So, I guess the takeaway is that people forget about this.

They turn it on, and then they forget to make the secure delegation, because I checked the registrars through which these people have registered their domains, and they all support registering secure delegations. So, in principle, they could turn this into full deployments. And what you also see is that again, initially, only Cloud Fare operated domains use ECDSA, but then from the middle of June 2016, other operators start appearing that use ECDSA, and this is around the time that Power DNS for [inaudible] was released.

And they make ECDSA the default algorithm. And then you see a couple of local Dutch hosts enabling ECDSA, and each arrow points to a single operator on ECDSA for the domains that they signed. Now, good observers will see that on the left hand side, it says 8,000 domains signed with ECDSA, and if you think about the almost 2.6 million signed delegations in dot NL, that is still a very small number.

But fortunately, the good people from domain names have shown that it is possible to do an algorithm rollover without breaking stuff, and I'll talk about this on the last slide that Surfnet will also be doing an algorithm rollover and blogging about it so people can learn from that.

Next slide, please. So then, we looked at six other ccTLDs, so for Austria, Canada, Denmark, Finland, I have no idea how to pronounce that, but it's a tiny island somewhere in the Pacific, and Sweden. And things are sort of all over the place. What you see is, for instance, Alexander from dot [inaudible] mentioned this morning that they've only recently started supporting secure delegation for ECDSA. And I guess that's reflected in the number of DNSSEC signed domains that have adopted ECDSA, and only 1%.

But then if you look at Finland, 75% in Denmark, 88% of domains that are DNSSEC signed, use ECDSA, so those are huge numbers. And it's probably because these are newer deployments. People are looking at all of the documentation there and thinking, okay I want to deploy DNSSEC, but I want to do it in sort of a modern way, so I'm going to take an algorithm that doesn't give my DNSSEC huge responses.

So, next slide please. Then we looked at dot gov. Federal agencies must sign their dot gov domains, right? There is this Presidential Directive from 2009 that says, thou shalt sign thy federal domain. And [inaudible] recommends that people use ECC, and they also recommend that if people do use RSA, that they use larger keys.

So, we asked ourselves the question, do dot gov use ECDSA, and the answer is no. Not a single one, zero. And some other fun facts…

UNKNOWN SPEAKER: There is no way to upload ECDSA keys, because of the registry.

ROLAND: Okay. I didn't know this, and that hurts any more. And some facts, 8% of dot gov domains exclusively 1024 bit RSA keys. Who was saying this about budget cuts and not replacing…? Yeah, Paul said that. Not replacing appliances. Six dot gov domains still use five 12 bit RSA. And almost 50% of dot gov domains use [inaudible] hashing, despite [inaudible] recommendations telling people to stop doing this in 2015.

[SPEAKER OFF MICROPHONE]

Paul says they still have card punchers.

UNKNOWN SPEAKER: Of course, this is all a problem because of their roll over tools not being easy, sexy, click, click, done.

ROLAND: Yeah. That's no excuse. So, where is dot gov? It's one of the first sort of serious efforts to get DNSSEC deployed in the government space. They are now seriously lagging behind, this is a real, real worry. And I don't know, I haven't asked Scott Rose how he feels about this, but I can't imagine he's happy about this.

DAN YORK: Probably we can ask him next week in Chicago if he's there, I don't know.

ROLAND: Okay. I'm not in Chicago, you ask him, please.

DAN YORK: If I see him, I will, and others here.

ROLAND: Yeah. And to be clear, I'm not trying to sort of shame dot gov, because it was a good effort in the original space, but this also shows you that you have to keep paying attention if you're doing DNSSEC. This was a new technology when they started deploying this, and it's, I would argue that with the use of things like ECDSA, the introduction of things like DANE, it's now much more mature technology, but you should keep updating if you're one of the pioneers.

DAN YORK: And I think to your point around that, as we talk about here, we have now new curves, all the EDDSA, which many people from a crypto point of view would like to see even more, just because that's, you know, a higher level of security tan ECDSA has been.

So, the question is, you know, yeah, getting those out will take even longer.

ROLAND: Yup. Okay, so next slide please. In some earlier work that we did, we showed that signing with a combined signing key, so that's a single key rather than having a KSK and a ZSK, has additional advantages to reduce fragmentation and amplification, because your DNS key responses are the most likely DNSSEC specific response to get fragmented, or to have large responses that can be abused for amplification, you want to reduce the size of that response.

Now, using ECDSA, or even EDDSA, once that becomes sort of available in implementation, will already reduce the size significantly, but using a single key will again, half the size of what you had before. So, we asked ourselves, do people actually use combined signing keys with ECDSA? And unfortunately, we couldn't find the key trend. It appears to be sort of all over the place.

And in some ccTLDs, there are significant numbers of domains that use combined signing keys, but in say com, net, and org, there is virtually no adoption of this at all. And this is something, if people haven't looked at this, I think that it's something that this should seriously consider. I'm going to look at Roberto again. I think that Power DNS, by default, uses ECDSA with a combined signing key. Is that correct?

Yeah, okay. So, Power DNS users who roll to ECDSA, will get this sort of scheme. Next slide, please. Of course, if you look at ECDSA, it's also interesting to look back into the past and see what developments there are on the RSA front. So, 1024 bit is generally now considered too weak, and people are sort of being now recommended to switch to larger keys, but are people actually switching?

If you look at the numbers for com, net, and org, in all three of these, 40% of the deployments that use RSA, have a 1024 bit KSK and a 1024 bit ZSK. So, those are significant numbers, and something needs to happen there.

What is also interesting is that people, for some reason, seem to think that RSA keys only come in powers of two. So, that means if you had 1024 before you should go to 24 [G eight?], and if you have 24 [G eight], you should go to 4096, which is the largest RSSAC size allowed in DNSSEC. So, we looked at how many people that use RSA, have a key size that is not a power of two, and in the sort of gTLDs, these are negligible numbers.

In dot NL, it's not negligible, but it's small. If, for some reason, you can't go to ECDSA, and you're stuck with RSA for a while, but you do need to upgrade your security, really software can deal with non-power of two RSA keys, and use something sensible rather than blowing up your responses and using 4096 bit RSA keys.

That's a really silly idea. Next slide, please. So, ECDSA was already mentioned. It's recently, very recently, been standardized with many thanks to Andre and Robert [inaudible], and it [inaudible] two new curves, ED 25519 and 256 bit curve, which offers under 28 bit security. I would say, this is highly attractive for use in DNSSEC. Because the key only requires 32 bites to store it in a DNS key record.

An ECDSA key is stored as the full representation of the curve point. That means that you need 64 bites in a DNS key record. But fortunately, ECDSA uses some sort of point compression that is not presented, so you can store it as a single part of the curve point representation, and that means that you can store even smaller keys in your DNS key record.

And then ED 448 was also standardized. This is like a high security of rock solid curve that you want to use if you have really high security requirements. I guess, I mean, 256 bit are fields for ECC are equivalent to 3,072 bit RSA roughly. If you're really paranoid, go for the 448 bit curve, but you're probably fine with the 256 bit curve for almost any application.

Next slide, please. So, because EDSA is new, it's virtually non-existent software. But there are good reasons to push for support. So, EDSA is much faster than ECDSA. It requires less space. It has better security properties. So, ECDSA has some security issues with it, the people that develop ECDSA [inaudible] and his colleagues, have a good list on safeguards of ca dot [inaudible] that tells you the differences between those curves in terms of security properties.

And so basically, what I want to do is call out to people to support their open source project to implement EDDSA, because that way, we're going to get that out there much quicker than we had with ECDSA. And we are actually jumping on this bandwagon as well.

We are renewing our DNS infrastructure. We're getting new [inaudible] in which we store our keys. And I'm pushing our vendor to support these curves in their HSM offering, and they claim to have put it on the roadmap, so hopefully there will be HSMs out there that will support this.

So, next slide please. So, to conclude, the graph shows you that ECDSA option is [inaudible] in some TLDs such as com, net, and org. We're actually seeing enough significant numbers of domains being signed with ECDSA, such that ECDSA is now overtaken some [inaudible]. But deployments are still traceable to only a handful of operators.

So, these are people that switch it on in bulk, and I think that, if I counted, it's about five bigger operators that have turned it on, but there are also lots of big operators that are still stuck with RSA, and in the case of com, net, and org, stuck with RSA 1024 bit.

Secure delegations through the RRR channel are blocking deployment of DNSSEC, I think that doesn't really need that much explanation. Really looking forward to seeing what would happen if people pick up on this CDS CNDS key, or see that was recently approved. Next slide, please.

So, maybe something actionable for the people in the room. If you are a DNSSEC operator, you're planning a new deployment, please use elliptic curve as your signing algorithm. And consider switching to ECDSA. We've already seen that although it isn't trivial to do, an algorithm roll over can really hurt you if you do it badly.

People have shown that it is definitely possible, and we're going to be doing it in 2017. If you're doing DNSSEC validation, check for support for ECDSA, Jeff Houston's number show around 82, 85% of validating resolvers support ECDSA. But that's not 100%. We want that at 100%. So, please check. Next slide, please.

So, what we will be doing. Surfnet will be switching to ECDSA PT56 with a combined signing key scheme for all of the domains that we sign for our customers. We will migrate a new HSM. We will do a life algorithm roll over. And we don't operate to say huge number of domains, it's not only around 1200 domains. So, I guess we're a small operator in those terms.

But we will try to share our experiences. So, we're going to blog about our progress. We're going to share automation scripts and code, so that people can learn from this. We use open DNSSEC, so we're going to be sharing scripts that will help you do this with open DNSSEC.

If you are deploying open DNSSEC [inaudible] upcoming [inaudible] release, because that will actually support algorithm roll over in the software. So, if you want to change to a new algorithm, the software will help you do that, rather than you having to write nasty scripts to do it.

Next slide, please. I think that's… Yeah, so this is just for reference. The slides will be up if you want to read more about what I talked about, here are some links. And next slide, please. I think that's it. I want to thank the good people of SDIN again, for supporting open intel, which was sort of was used for the data that was used in this presentation.

And if you have any questions, feel free to ask.

DAN YORK: Yeah, I see a queue already forming. Let me just say first, thank you Roland for all of this work. That's great numbers and great information to see. So, thank you for doing this. I saw Paul, Jacques, I see Peter, others. Okay. Paul first.

PAUL: Thank you. So, one of the slides mentioned that EDDSA is faster, I'm assuming that is for signing that is significantly faster?

ROLAND: Both for signing as well as validation, it is significantly faster, and if you give me a minute, I can give you the numbers.

PAUL: Okay, that was my second question. You did a very good breakdown of why ECDSA was not quite as painful as some of us feared on the resolver side. Do you have performance numbers and CPU hits for EDDSA?

ROLAND: I do. And I'm loading the stats as we speak, hopefully this doesn't crash. Here we go. So, ED25519 in terms of validation speak, if you compare it to open SSL one dot L dot two, which has the patches, sort of the speed up patches from Oliver's people in it. It is, it requires 70% of the CPU time to validate.

So, it's about 30% faster. And ED448 is only two times slower than ECDSA P256. And if you compare it to P384, it's even better, right? [Inaudible] is almost four times faster than P384. And it gives you more security.

DAN YORK: All right. Shock.

UNKNOWN SPEAKER: That's a good presentation. I'm wondering if you have any stats on TLDs, I mean, the domains are signed, but no DS? Because for dot CA, I know we have a lot of signed domains.

ROLAND: I do have the stats. They're not in the presentation. [CROSSTALK]

DAN YORK: I've got Peter. Carson.

CARSON: Carson from [inaudible]. Roland, very good data, thank you. It's more a question for the room rather than Roland. Last time I did algorithm rollover, there was last year, with some bind and some older power DNS. I had to really get my hands dirty in doing that. How is the software support coming along with the DNSSEC limitations in the open source software?

Maybe some people here can shed a light on that, because currently it's very hard to do. It's not impossible, but it's hard. To do an algorithm rollover.

DAN YORK: Bert, Andre, who else do we have in here that could comment?

UNKNOWN SPEAKER: So, I was closest to the mixer, I go first. So, I'm going to make this, take this opportunity to preach a little bit.

UNKNOWN SPEAKER: You never do that.

UNKNOWN SPEAKER: No, this is going to be, this is really a problem we have. So, how does it go? We have the hosting industry, and they all use our software, that's the various people here in the room, right? And they come to us with questions indeed like this, can we…?

So, for example, in power DNS, we can do a key roll over by adding the new key with a command line, and then later running the command line that removes the old key. So, manually you can do it there, and it's I think, Roland called it, you need some nasty scripts to make that happen.

And we would love to make that better. It is on the roadmap. Do you know how many hosts have actually supported our power DNS development? It's about the same as the ECDSA deployment in dot gov. It is ziltch. We get, we left in this room, we love to talk about the operator community being slowed, and not being with it. They actually fund name server development.

No host name server development. So, even though they are making like serious integer Euros, integer dollars, per domain name per year, when you ask, could you please fund this development? It will make your life easier. They go like, nope. We never paid for anything in this company, and we're not about to start.

So, to run this off, I would love to automate the roll over stuff. It would not even be hard to do, but I'm faced with the prospect of implementing that stuff for people, that are not contributing codes, not contributing efforts, and not contributing money. So, I would love to make it easier, but to any of the hosts in the room that are hosting millions of domains, please ponder sometimes supporting software. Thank you.

DAN YORK: You now know what Bert looks like. Come and talk to him. He will take money in any denominations.

[SPEAKER OFF MICROPHONE]

Patches are also very welcome. Contribute code, or fund code, whatever. Peter, you were right there.

PETER: Peter [inaudible]. I want to thank Roland for this excellent presentation, and the work that is behind that. I think I had one or two questions or remarks. First of all, of course there is this interesting split with one K and two K, and we also noticed that people only think, interesting people seem to think only in powers of two. I think when you mentioned the combined key, wouldn't it be natural that somebody having a two K, one K, key would continue with a one K combined key?

Because that's the strength of the super set, so to speak, anyway?

ROLAND: I wouldn't know why they would do that, but very few people actually use combined keys for RSA. I only saw any significant deployment of that in dot NL. And that was mostly people using 2448 bit RSA keys, fortunately.

UNKNOWN SPEAKER: Yes, I made this remark. I was wondering why when the registrar is running everything, it has everything in their hands, including the key rollover through the registration system, why they would split that. Maintaining RSA…

ROLAND: And then we told them to do that.

UNKNOWN SPEAKER: Sorry?

ROLAND: Because we told them in the RFC 4641 to have the key split, the split scheme, without really motivating why they should do this.

UNKNOWN SPEAKER: The updated version [CROSSTALK]…

ROLAND: 6781.

UNKNOWN SPEAKER: Did the right thing, so to speak. But staying with RSA, going to combined key, and then only thinking in powers of two, going to 248 signatures will probably have interesting effects on your outbound traffic, at least people should be aware of that. On the ECDSA side, yeah, I'd love to see vendor support for HSMs, for these new curves.

We had that exercise last year, and I guess we got a similar response, oh yeah, yeah, maybe it was will be on our to-do list, but what we heard from the vendors was that, this is of course, much, much more difficult then adding another curve of the ECDSA type, because they have to have all of the twisted adverse math in there, and so on and so forth.

And you may or may not lose your certification. Now here comes the compliance trap. If you are somehow required to use algorithms that have a certain certification stamp, because you're regulated or something, then you're screwed. You can't innovate. And that is bad, probably, here, regulators and legislators listen to this.

One property of EDDSA that you think, didn't mention but that it might be interesting for a fraction of the audience, is that they don't need random, and they produce reproducible signatures, which is interesting in redundancy scenarios. That's probably not important for Joe Random, but for bigger installations, including big registrars actually.

ROLAND: Yeah, it's also security issues. So, I didn't want to go into too much detail about that, because it is, you need to know quite a bit about how the crypt of ECC works, and that gives me a headache, so I wonder about other people in the room. But ECDSA does require… There are two implementations. You can either use a completely random input strain, so some [inaudible] ago into the [inaudible], that can be completely random, but there is also a RFC that gives you a deterministic way to generate that [inaudible] that goes into the signature.

So, you can actually do deterministic signatures with ECDSA, and actually if you're doing ECDSA, that's probably the safer way to do it, because if you somehow generate two signatures, and you use, and you reuse the same nodes, then your private key can be recovered. So, that a serious security issue with ECDSA.

DAN YORK: In the moment, you said non, you took us way down a deep rabbit hold of crypto. So, we flagged this on the schedule as an intermediate, but we've gone in the gray zones.

ROLAND: That's why I didn't mention it [CROSSTALK]…

DAN YORK: …we were like way down the crypto rat hole on some of this, which is awesome for some of us. But yeah, if anybody in here was, you know, if they didn't know they were at a geeky session, we showed them that. I've got Irwin, and Olivier, and anybody else in the queue? Okay, Irwin?

IRWIN: I was just going to confirm your suspicions about [inaudible]. There are a few new hosts that we brought onboard. The suspension about why the algorithm 13 has a 88%, so the new few new registrars who are hosting for others came onboard a few months, and they went straight to algorithm 13. And kudos to [inaudible], they've been, they brought us almost close to 1% by signing the domain name several years ago.

And yes, [inaudible] algorithm brought over, algorithm eight before.

DAN YORK: Pretty cool to see what one registrars can do in that regard, as far as making that kind of change. Speaking of one registrar who has made a change, Oliver?

OLIVER: Yeah, Roland, very nice. I wanted to pick on you a little bit.

ROLAND: Go on.

OLIVER: So, you picked on my customers for being only in a pending state, but how big of a problem is this for the rest of the world? Yeah, because if you have looking at domains that are operated by non-registrars, it is a serious problem to get the keying material [inaudible].

ROLAND: I did not mean to pick on Cloud Flair. I was using Cloud Fair… So, if you interpret that as picking, my apologies. It was as an example, and actually, I appreciate that you wrote the RFC to get it fixed.

OLIVER: I'm trying, and we're also trying to deal with Jacques and Paul and myself and Matthew from right side, to get a protocol in the registry world that will actually will talk with the registrars also to get this information uploaded in a standardized way, so everybody does it the same way. But I also want to pick on Dan now.

That his wonderful maps that he published every Monday, maybe he can start showing the partial ratio in them.

DAN YORK: All I need is somebody who can invest some cycles of code, or maybe I need to talk to somebody about funding a developer to help with code. That's just code, right? That's all.

OLIVIER: It's just code.

DAN YORK: Actually on that note, seriously. The DNSSEC maps the code that creates that, that we took over, we internet side, took over from [inaudible], Steve Crocker's group, and Oliver you worked on that code, I know. And some of that that's there, and we are open to expanding it, and doing more with it. [Inaudible] things like that, it's just a question of cycles of time for somebody to work on that.

So, anyway. Other questions, comments, before we close the queue? Yes?

UNKNOWN SPEAKER: I have a question. [Inaudible] for the record. Actually, I don't know, and I would like to have an answer practical [inaudible] in this case. But if I sign my zone by using the most advanced ECDSA algorithm, and the resolver is just not capable of understanding that signature. It's just reverting back to giving to the client [inaudible], not authenticated. Is it this, the expected behavior? Or is breaking something in any way?

DAN YORK: Correct. The RFC state that if the validating resolver doesn't know the algorithm, it should send it unsigned, or send an unsigned response. [CROSSTALK]

ROLAND: The measurement… The people from APNIC, so George and Jeff have looked at this, and I think that they've found that this behavior is indeed what is implemented, there are no resolvers that break, because they don't understand the algorithm, they just give you an un-validated response.

DAN YORK: An exception to that came up on one of the mailing lists when, I think it was [inaudible], somebody had mentioned that they had to roll out where a version of whatever they were using on the CP, was configured the wrong way so that it was actually failing anything it didn't know. And so they were winding up with…

UNKNOWN SPEAKER: Two versions of DNS mask.

DAN YORK: That's what it was. The DNS that went out with basically, it did not implement it the way the RFC said, it basically just failed. It was, you know, gave back a fail if it didn't know the algorithm, and it didn't [inaudible], it said, oh it's signed, but I don't know how to deal with that so goodbye.

It was then fixed so that it is now not doing that. But for a period of time, there was the wrong behavior. On that point though, I do want to say, we are talking a lot about EDDSA, now that it's out as a RFC and other things. A quick question to some of the, I'm looking at you [inaudible] and others, as far as, where are you guys in making that available through unbound and others?

And I guess I'd ask Andre for the same thing and not in others?

UNKNOWN SPEAKER: Yeah, so [inaudible]. It's [inaudible] that RFC, so that it will be implemented soon. Of course, it's available in the libraries, the security libraries. We will adopt it soon, in the release, well, soon, yeah.

UNKNOWN SPEAKER: I think I had it in my slide in the morning. We're waiting for new DLS to support this, and as soon as it will, we'll implement it immediately, so we are ready for that.

DAN YORK: Going back to the point earlier, let's fund some development in open source projects on that. Anything else? Okay. With that, I want to thank Roland for all of the work around this. [Applause]

And now, if you thought we weren't already deep in geekdom, we are about to bring up Wes for our decent into the great DNSSEC quiz. Now, we should say a little logistical issue while Wes is coming up here. Julie, do you want to speak to us about lunch?

JULIE: Well yes. And also, please look for the answer sheets for the quiz. A white sheet of paper with a few lines on it that says quiz on top. If you don't have one at your seat, kind of root around, you probably have one near you. You could also use the back of a piece of paper. And Wes will give you the rest of the instructions on what ya'll need to do.

But we will break for lunch right after the quiz. We do have a set number for the lunch, and that's why we gave out tickets earlier. So, find your ticket, you'll need your ticket. They'll be ushers at the door, at the lunch room, and asking for tickets. There are still some tickets lying around on the seat, so you know, take a look around.

We have a few limited ones that we can give out, but do take a look first because there are quite a few around I think, still. So, anyway, that's it. And over to you Wes.

WES: All right. So, how many people were in Hyderabad and took the great DNSSEC quiz then? A few people. How many people got negative scores? Excellent. Next slide, please.

You'll be glad to know there are no negatives this time, so I guarantee everybody will end up with a positive score. And I don't even mean zero, I mean positive. So, a couple of quick rules. To be declared the winner, somebody next to you must have validated your answers. So, if you want to compete for the championship, make sure that you do hand off your answers at the end of us, to somebody else that will actually correct them for you.

Each correct answer will be worth one point. Multiple answers are sometimes correct, but if you choose any incorrect answer, then you will receive zero points for that question. So, if there is multiple choice, you're welcome to circle more than one, sometimes that's good for you, sometimes it's bad.

If you get any of them incorrect, then it will be a zero except when noted. There are two questions where that won't be true. And finally, I, Wes [inaudible], am always correct, even when I'm sick, like I am, but judgments are still final. Next slide.

So, first off, question zero, what chocolate treat is available in Denmark and is illegal to import into the United States? I'll give you a hint, it's either the Kinder Surprise, the Kinder Surprise, the Kinder Surprise, or the Kinder Surprise. So, this time we actually have a prize, if you win.

So, this extremely dangerous chocolate egg is illegal to take into the United States. It contains choking parts. If you have the highest score, you get it. If you tie with somebody else, you'll have to fight over you. I'll leave it to that. Please do not take it back to the United States, if that's where you came from.

Next slide, so note that all four of those are correct, so if you circle all four now, and you put A, B, C, and D, you'll get four points later. Isn't that nice? I'm so friendly. Next. That was question zero. Yeah, you'll have to write it above. I didn't coordinate with Julie about actually creating the slips, my bad.

And actually, it really was, I didn't want to go back and renumber all of the slides later. So, question one, which of the following ccTLDs became fully DNSSEC compliant in December 2016? Meaning they have a DS record. Yes, Peter?

PETER: Can I ask a question? One of them seems to be on the IETF special names use list, right?

WES: Pluto. You get a point actually. So, Hong Kong, South Africa, or Vietnam? HK, dot HK, dot CA, or dot VN. And of course, Pluto. Next, question number two. Did I hear wait? Are we okay? Good. Question number two. Where was the first key ceremony held for the creation of KSK root key?

It was either in A, California; B, Culpepper, Virginia; C, Paris, France; or D, Pluto in the Milky Way Galaxy. Just FYI, you can't hold a key ceremony in two places, so this may not be a good one to put multiple choices down on. But that's me being nice to you.

This will be a general theme. We're going to roll the KSK soon, so the next couple of questions are all related to rolling the KSK. Actually a number of these are. Hopefully, you've studied all about it, because if you wanted the slides from Matt and from other people, you'll do better on this quiz.

Next. Question three, when is the current KSK expected to be revoked? This was directly in Matt's slides, so hopefully you memorized all of his dates, because it's either in A, July 11th 2017; B, December 11th 2017; C, January 11 2018; or D, January 13th 2018. It's one of those dates. So, that's when the KSK that is currently in place, if everything goes smoothly and according to plan, it will be marked as revoked, that's the no turn back date, by the way.

All right, next question. Question four, what is the minimum length of time that ICANN must wait after publishing the DNS root's new KSK to expect all online RFC 5011 compliance validators to trust the new key? Note, I could have made that longer if I wanted to get it perfectly semantically correct, so you're going to have to live with my judgment.

But, this is based on a draft that actually I created, so you all would have had to read my draft to understand the answer. It's not yet my IETF document. So, it's either A, 30 days; B, 45 days; C, 61.5 days; or D, 365.25 days. That's how long ICANN must wait before believing that all of the RFC 5011 compliant validators have accepted it as a new trust anchor.

Next. We'll have to deal with that, won't we, Warren? And you were responsible for half the math, so it will be your fault, by the way. Question five. What properties match today's DNSSEC signed root zone? Is it A, [n sec] with a 1024 bit ZSK and RSA [inaudible] one? Or B, [n sec] with a 2048 bit ZSK and RSA [inaudible] 256? C, [n sec] three with a 1024 bit ZSK and RSA [inaudible] 256? D, [n sec] three with a 2048 bit ZSK and RSA [inaudible] one? Or E, TLS 3.1 and [inaudible] two with prop three?

Next. Question six. Which of the following ccTLDs have DS records in the root as of, well, yesterday? A, dot AC, dot BE, dot CF, and dot DK, Denmark. B, dot AD, dot BW, dot CN, and dot DK, Denmark. Have to give them props, so they're going to be in every answer. C, dot AE, dot BG, dot CC, and our host, Denmark.

D, dot AF, dot BH, dot CR, dot DK. Everybody has memorized the root zone, right?

If you have, then you would know that dot www dot xx dot yy and dot zz don't actually exist in the root zone, but you're welcome to put down E if you want. Next. Go back.

By the way, no computers, no looking up stuff. That's cheating. Okay. Five, four, three, two, one. No going back. Okay, next. Question seven. This is where you get lots of points if you happen to know the DNS protocol really well.

Write down any DNS or EDNS header flags registered with IANA. Write both their two letter abbreviation and their registered expansion names. So, the example up there is the do bit, which stands for DNSSEC okay.

You might want to write that one down, because that is one of the answers. So, that's question seven. And there is only one more question, I'm going to go on, but you can fill-in that one as you think about it. We'll give you a few minutes in a second, but go ahead and go on to the next question.

Question eight. [Laughter] What are the five digit key IDs of the root zone's active keys today? So, there is both the KSK and the ZSK, active today. If you happen to know their key IDs, like everybody knows, right? Then you can write that down.

It's worth guessing a five digit number, note that that could start with a zero.

UNKNOWN SPEAKER: Of the two active ZSKs for like the roll over…

WES: There is only one active ZSK at the moment.

UNKNOWN SPEAKER: Okay. Can I trick into this?

WES: It doesn't matter, because it would be the one on the [inaudible]. The one that's signing, you know. All right. So, why don't we go back to question seven, so people can consider that? But that was the last question. So, I'll give you a few minutes to think about it.

I would have had to stay up that much later to write a nine and a 10, and I was sick last night trying to do these, so I'm sure they're all letter perfect.

UNKNOWN SPEAKER: I'll just note that that was just a boiler plate answer form. So, it wasn't anticipating that there was going to be a nine or a 10.

WES: There was a zero, though.

No, no, so we went back to question seven, just so you can read it again to make sure you thought about it. So no, there is not two question sevens. The final question was number eight.

Two letter.

So, no, thank you Paul. So, for both this one and the key ID one, so both the last two, you are welcome to guess, and put down… If you get something wrong on these, you won't invalidate the rest of your answers. So, if you get three of these wrong, and you write down AQ for [inaudible], that's okay. You can write that down, you won't get penalized for it.

By the way, that's not a bit.

All right. Anybody still writing? Yes, Paul is still writing. Roy is still writing. All right, we'll give them a minute.

Yeah, there was actually one acronym expansion that surprised me, because it took me a little bit to find the two letters in the two words.

Okay, time is running out, Roy, write faster.

Paul has stopped too. All right. So, I think we are done. Julie, can we go on? So, remember that to be eligible for this prize, you must pass your sheet to somebody else to score it. So, please swap with somebody else, preferably somebody that's not your significant other, because we don't want that Kinder egg being cheated by, you know, a spouse.

I will ask, at the end of this, when somebody you know, gets that final score, who corrected your sheet for you.

All right. Let's go on to the answers. Julie, go ahead. So, question zero, if you did guess Kinder Surprise, you could have up to four points. Congratulations, I hope you wrote them all down like I told you should. Next question.

Which of the following ccTLDs became fully DNSSEC compliant in December of 2016? All three of the top ones. I hope you didn't write down Pluto, because that would invalidate and give you a zero for the whole question.

What?

Yeah, the slides earlier, or at least the copy I got, said December.

Well, it's okay. Remember, I'm correct, so I don't care what really happened. I'm giving credit for all three, because the slides I read in my sickness, you know, early this morning, finishing up these slides said December.

All right.

UNKNOWN SPEAKER: …wrong. It was… Oh, you're right, actually, it was 16 December, it was added to the zone.

WES: I told you, I'm always right. Did you not read the first slide?

UNKNOWN SPEAKER: Added to the zone is not enough. When did the…

UNKNOWN SPEAKER: Guys, guys, this is between us and lunch, so let's just proceed.

WES: I like doing this before lunch, people are less picky. Okay, next. Where was the first key ceremony held for the root key? It was in Culpepper, Virginia. [Inaudible] was the second one. Question three. When is the current KSK expected to be marked as revoked? January 11th in 2018.

Question four. What's the minimum length of time ICANN must wait after publishing the DNS root key to make sure that all validators have picked it up? It is 61.5 days, the math is up there. Warren, read it.

UNKNOWN SPEAKER: No, that's validators that are actually online. If your validator is turned off, it's an infinite amount of time…

WES: That's why it says online in the question, Warren. Right there. Third sentence, second…

UNKNOWN SPEAKER: Can Warren please distribute his lunch ticket?

UNKNOWN SPEAKER: Wes is right.

WES: Next question.

UNKNOWN SPEAKER: Wes is not.

WES: Question five. What properties match today's DNSSEC signed root zone? It is B, we use [n sec] in a 2048 bit ZSK, which is new as of not that long ago. And RSA [inaudible] 256. Next question. Which of the following ccTLDs have DS record in the DNS root? It is the top line, AB, BW, CN, and DK.

You can see all of the ones marked in red with a slash through them that do not.

There is one for CN. Show me. I did it last night. Did they revoke it?

UNKNOWN SPEAKER: Hey, [inaudible] says December 2015.

WES: I'd like to note that Warren's screen just showed me that it did exist. So.

Warren, what did slide number two say?

It said I'm always right.

I don't know. You're using a bad resolver. Next question, please.

UNKNOWN SPEAKER: Lunch, Warren, lunch. Focus.

WES: Write down any DNS and [inaudible] flags registered with IANA. They are, so you don't need the bit numbers for those of you grading other people's, but you do need to know that it's AA, authoritative answer. I accept misspellings because I'm horrible at spelling. TC, truncated response.

If you put truncated anything else, it doesn't count, even though response doesn't happen to have the C in it. It has to say truncated response and TC. RD, recursion desired. RA, recursion available. AD, authentic data. Not authenticated data, authentic data. CD, checking disabled.

And of course, the one I gave you free, I hope you wrote it down, the do bit, for DNS okay, DNSSEC okay, excuse me.

UNKNOWN SPEAKER: You missed one over there. The QR bit.

WES: You ought to tell IANA, because I pulled this off their webpage.

UNKNOWN SPEAKER: No, the bit is in there.

WES: Don't tell me, tell IANA. I thought that there was more too, but I copied… That's literally straight off their webpage.

UNKNOWN SPEAKER: IANA has been notified. [Laughter]

WES: Next question. The current key IDs… Wait.

Can you go back one?

UNKNOWN SPEAKER: Lunch, guys, lunch.

UNKNOWN SPEAKER: [Inaudible], it's not the same text as you wrote…

WES: That's true. I will accept both answers if you don't put the word answer in the [inaudible] that is fine, because I gave it to you for free. Next question. Finally, question eight, the five digit key IDs that's 19 zero three six, for the KSK, and 64045 for the ZSK. Anybody actually get either of those?

UNKNOWN SPEAKER: You said we could put down multiples, right? So, I put 123 dot, dot, dot 63535.

WES: That is one answer, which is incorrect. Congratulations.

UNKNOWN SPEAKER: No regular expressions. Lunch, lunch. Stay focused here, okay?

WES: Okay. That is it. I think next slide, there is nothing on it though. All right. So, pass your scored sheets back to your associate. Count up all of the correct number of points that you got, and we'll start, did anybody get less than five? Because if you did, you really weren't following instructions. But that's okay, that's okay.

Did you have a question? No, okay. So, who had more than eight. Anybody have more than eight? A number of people had more than eight. Excellent. Who had more than nine? So. All right. So all of these people had at least 10 points, excellent. Who had 11 or more?

Narrowing it down to this half of the board, this is the expert panel over here, apparently. How about 12 or more? 13? The Kinder Egg, let me go get it.

This is me making them exercise before lunch. 14 points. All right, well I leave it to Paul and Warren in order to figure out how to split. Please be aware that there are choking hazards in here, that's why it's banned in the United States. So, be careful. And thank you everybody and have fun at lunch.

UNKNOWN SPEAKER: Thank you, Wes. [Applause]

So, lunch is in room C one dot one, the back of your ticket shows a map. You also can just walk straight back down that blue rug and turn right, when you get down to there. It's there. If you don't have a ticket and you want to join us, we should have a few more floating around, come find me and I can help you with that.

And we will reconvene here at 13:45 is the plan, right? Yes, 13:45. So, come back in about 40 minutes.

[END OF TRANSCRIPTION]