PANAMA – DNSSEC Workshop (1 of 2)
Monday, June 25, 2018 – 09:00 to 10:15 EST
ICANN62 | Panama City, Panama

JACQUES LATOUR: Alright, good morning. Can you hear me okay? Okay, so welcome to the DNSSEC workshop at ICANN 62, here in Panama. We're live right, streaming? Yes, so welcome. So today the DNSSEC workshop is organized by the program committee that you see here. So, we meet on weekly basis to plan this meeting and to produce a quality session. The sponsors for today we have lunch, it's not in front here the space for lunch there is not for us so we won't accept there, it's near saloon 5, that's our place for the lunch, for the lunch you need to have your lunch voucher here and then it's sponsored by Afilias, by CIRA and SIDN, so thank you to all the sponsors. We're always looking for new sponsors, so if you have it's like a $1 000 something like that so if you can sponsor, work with ISOC with Dan York, and then if you're interested in sponsoring the lunch and the gathering event that we have at not policy meeting but Euro meetings the A and B or B and C or A and C, that's close.

So, the sponsoring goes to sponsor the lunch and the gathering events that we have. So, the workshop is a SSAC initiative, so me and Ross are on the SSAC and participate for this, and we also have a lot of help from ISOC from Dan York, the mailing list, the sponsoring the money part for this workshop is handled by the Internet Society, so do we have support for this? Like I said we are still looking for more sponsors.

So, the agenda for today, so it's this presentation for the first part as per usual from 9:15 to 9:45 we are going to have a panel discussion, focusing on original DNSSEC activities and also a focus on the post key signing, key rollover preparation, so the focus was -- what happens one second after the key rollover -- whose doing the preparation in case there will be collateral damage and the discussion is what are we going to do to address that, what should we look at, we still have time to prepare, but if you have any ideas on what we should so the one second after then please come forward to the mic and let us know and then we'll take that in note.

And then we have a presentation at 9:45. So, on the panel we have Angie, is she here? Angie, are you here? No, okay, then we have Fred from Brazil and Mauricio from Costa Rica, talk about the INEX's continuous improvement. At 9:45 Ondrej is going to talk about his algorithm rollover and then we have a break at 10:15 and then part two, the workshop is to look at -- so Ross is going to host a panel to talk about data collection analyses for the KSK rollover, and then we terminate as usual with how can you help and the quiz.

So, the deployment around the world this is Dan York's content, he is not here today, so I'm taking his place for this, and so we are trying to track the deployment of the DNSSEC around the world with measurement and stats so that is what we're going to present here. You can look at the Internet Society website for the state of the DNSSEC deployment 2016, so that's a pretty in-depth report on the deployment of the DNSSEC.

So, right now APNIC, they track stats on the DNSSEC validation around the world, we're running around 13% validation, we'll notice that there's a spike, not a spike but there is a downward or a leveling trend since April 2017, so some people there is a disabled validation that's something we need to address and look at and it's not going the right direction there but hopefully after the key rollover things should pick up.

In terms of the DNSSEC validation by region, so there is stats by all the different regional region, sub-region, and then there's which one does the DNSSEC validation, and also statistics on which region uses the Google DNS, the 8888, because the Google DNS does the DNSSEC validation so it adds to the number, so you can see which one are doing validation on their own and which region are doing validation using Google, so Micronesia is the region where there is more DNSSEC, and then it goes down to 2% for Eastern Asia, so we've got some work to do to raise awareness and grow, make more validation around the world but the statistics are live at APNIC and the link is below.

That's the standard slide that we have and we're running around 90% of the TLDs that are signed in the root, around 45 of these are the second level domains are signed, so we've got a lot of work to do at the second level domain to bring that to a higher number and around 13% of the users are validating so we got the TLDs signed, now we need to focus on more second level with more automation and the DNS software implementation and get more users to validate.

So, this is number of TLDs signed, so the number of domains signed inside the TLD, so number one is still [inaudible] with almost three million singed domains out of 5.8 million, and then followed by Brazil Fred with a million signed domain, we're talking about that, you're number two, two more million to go before you -- Dotcom is at almost a million, and then Dot [inaudible] is 800 000, and Canada is probably the last one with five or six hundred signed domains so I don't know what to do with that, I'm hopeful we'll bring at least 10 000 eventually.

So, we're very -- it's 80%, no I'd say 95% of signed domain in less than 1% of the TLDs so there is a lot of work to still and DNSSEC here. So, one thing we do is we track the TLD DNSSEC implementation, this is where we need humans to help us because we track if they're testing the deployment of the DNSSEC so this is you telling us this country is doing DNSSEC testing and then we can put it orange.

And then, we track if it is announced if they're going to do DNSSEC, if its partial then it means that the zone is signed but the DS is not in the root, the DS is in the root. The last stage requires human intervention; it's if the TLD is actually accepting the DNSSEC registration to the registrar, so you need to tell us if it's light green or dark green on the picture, but dark green means it's fully operational.

So that's a picture of the world, one thing we should do probably next, I can, is to show from the first slides we have to show the momentum over the year, the trend because we made a lot of progress before five years, six years ago, it was pretty much yellow and blank, and we made a lot of progress. So, there's a couple of green DS in the root, there is 48 of them, so if those are known to be fully functional in accepting DS from the registrars, then we can turn those dark green, but you need to like I said you need to tell us about this. These stats are available on the ISOC website and the DNS 360 section and you can also subscribe to the mailing list and you'll get all the pictures on a monthly basis with a status so you can use this for your internal usage if you want.

Africa, so we need to work on that for sure, there's a lot of, it's not even experimental, they're not thinking about implementing the DNSSEC in a lot of the region but we may progress there, there's more and more TLDs getting signed so it's better than it was, because I think five, six years ago it was pretty much, there was one TLD with intention to sign so --

Asia Pacific's is making good progress, there's a lot of DS in the root, so we've seen the DS so you need to tell us if it's actually fully operational, so if you're here and you know you're light green and you should be dark just let us know.

So, that's a wrap, so there's Italy and the other one, there's eight that are DS in the root so I'm not sure which one but at least it's all green so there's no yellow.

Latin America made great progress in the last couple of years, so nine are DS in the root, so those are probably the Caribbean islands.

So, the last one that I did was [inaudible] and the [inaudible] in June.

And then North America, Greenland, we need to figure out if they're live or not so Erwin, that's your job.

So, there's some white lights, that I've raised and repeated twice, it could be useful for the quiz later on in the afternoon, at noon. So, if you want to receive those maps as I said go to the deploy 360/DNSSEC and maps, so that's nice to be connect, right future. Random text blocking.

Dan York is also tracking, well the DNSSEC deployment group is also tracking the DNSSEC history project so if you have and tidbit of history and information that you want to contribute that you know that's not already recorded in the history and you can go there look at it and your input would be appreciated for that.

And that is it for the introduction and now, you're going to hear a lot of me today so you better get used to it. Today we have the DNSSEC panel discussion on the DNSSEC activity in the region and post key signing, key rollover preparation, if that's not confusing enough.

Angie right, she's not here yet? Okay, so Fred, I guess you can start.

FREDERICO NEVES: Hello everyone, good morning, I'm Frederico Neves, I work for the Brazilian Registry, and I'll give you an update on our algorithm rollover that we have been planning since the beginning of this year, this our update slides that I gave during the Puerto Rico meeting

Just to give you a little bit of background, and context to understand the presentation, as Jacque said .BR is a silent zone we have been doing this for quite a while, we have roughly four million domain names, and one fourth of those are DNSSEC so, as we started early in the deployment, I mean we were not the sweets but we started providing services in 2007, we picked Eurasia 1 as the algorithm and for our large second zones we use Eurasia 1 NSEC 3.

So we are stuck with those, how can I say old algorithms, the root started in 2010 and already use Euraisa 256, so why we kept -- besides the fact that we did the key rollover for BR twice during this period we are still using the same algorithm, so those are the motivations for our algorithm all over, first one is actually be prepared to, if we eventually get to the need to do an emergency algorithm, we never know with those improvements in computing, so we are still using Eurasia 1, and as I said we're using [inaudible] we have the good property of the reduced the response sizes for the majority of the cases, with positive answers below 512 bytes, with minimal answers, because we started early we will not need any longer to use two different algorithms for the zones that we use in sector is proof of no existence, our current provisionary software is a little outdated so we have been rewriting it and that is basically that.

So, this is just a context because of the algorithm haul over that are to approach as one that is recommended on 6781 and we have been looking at this in the history of the many lists, some early algorithm haulovers that that first sign did I think 2012 or 13, they use what is documented as the conservative approach. There is [inaudible] the same thing, it's actually the double sign but on the conservative approach you first introduce signatures and just after the zone is fully propagated to caches you introduce the new keys. The liberal one is just straight forward double sign.

So, we decided to -- it's not working. -- we decided to test, because we .BR is a structure zone the majority of our delegations are on the second level so we decided to test the two algorithm approaches and then we did this last week so I was analyzing the data with our team in the last few days to get a conclusion so what would be the right algorithm to do, the Swiss did a algorithm roll over a few months ago, and they roll it from Eurasia 1 to Eurasia 56, and they did it using regular software we know that they use open DNSSEC, so open DNSSEC is the liberal mode, and they went just perfectly, SIDN labs did a paper on the rollover and it went pretty smoothly, we actually use their methodology to test and those rollover test that we just did , we use it six zones as I said because the majority of our delegations are on the second level so we emulate BR on a second level with two zones, ECDSAS for the conservative approach and ECDSAL.BR for the liberal one and for BR or these test zones we use split keys and for the second level ones we use a combatant key and we test it with both matters of proof of no existence.

Okay, so we picked a thousand Ripe Atlas probes and using as I said SIDN labs monitoring techniques and basically we saw no difference from each of the roll over methods so the amount of the clients seen is still a secure resolution from the beginning of the rollover up to the end they stayed basically constant and this is a way of measuring that the rollover is progressing the right way and so based on that analyses we have decided to follow the simpler and slightly faster liberal approach of algorithm haulover, this one as I said is the one that the current public choose to use, Ondrej will probably talk a little bit of his algorithms rollover later on today and they did a conservative way but we will push for the liberal one, okay so what people should expect from us, what are the visible changes in the next few weeks, so in the algorithm haul over will happen on August the 20th, because we will reduce the APEX and DS what we call infrastructure records on our zone they are currently two days and six hours for the APEX and DS we will reduce all of them to one hour and we will be able to complete the algorithm rollover in roughly one day, the BR will be kept we will sign it for a little bit longer as long as IANA accepts and publishes our DS and then we wait for two TDLs of the DS on the root, that is one day, so we will give some public announcements on many operational mailing lists on July 26 and if everything goes well on August 22nd we will be entered. So, that's it, it's all the updates that I have.

JACQUES LATOUR: Alright thank you Fred, any questions?

FREDERICO NEVES: And by the way, I am really grateful for the people that are helping and we will be paying attention to the rollover especially the large valuators around that gave us a little bit of assurance, if anything goes wrong there will be someone to help us somehow.

JACQUES LATOUR: Alright thanks Fred, so next one we have Mauricio from Costa Rica, talking about DNSSEC.CR continuous improvement.

MAURICIO OVIEDO: Okay so, good morning everybody, thank you very much for the opportunity as well of presenting and basically giving a update with what are we basically doing right now with the DNSSEC and basically the deal of this presentation is to go over a couple of things that we've been doing, some operational practices, really quick, then how are we doing the KSK rollovers, how are we working on capacity building, and also even though there are a lot of challenges we identified two of them and what actions are we taking with these challenges so that's basically what we are going to be talking about.

Alright, so regarding to the operational practices, how are we managing the DNSSEC, so we will be doing a couple of changes we have come up or using a model for a couple of years its quite stable, it's very stable, and then basically we wanted to share what we are doing with that.

So, what we do is basically during the DNS key ceremonies, we do full ceremonies, so we do have external witnesses and then we also roll the KSK once a year so the idea of doing this it's to lower the industry and operational load on the team so what we do is a single session where we generate all the information we need for the DNSSEC, all the material gets encrypted and then basically we generate the KSK one per year then we generate ZSK we sign the whole thing and then create bundles, so we have everything encrypted and then we use that material in the year to roll the ZSK around every two months, and then once a year when we do the ceremony we roll the KSK, so the way that we do that it's basically combining offline market for key generation with online cyber signing so to generate the keys we use this market in a totally offline system, it never touches the internet or the local network, so we generate the KSK, we generate the ZSK we sign them and then we only export what we really need to export so the KSK never reached the internet and it's kept securely and safe it also has a particularity which is quite useful but you can easily back up these market and the KSK so in case of a failure we do have a good backup so the KSK and easy to reach and recreate so this combination its important because especially with this market it's not a secret its very slow so you get around one signature per second so it won't work the way that we want it – updates, they always come in the best moment.

So, it's not fast as markets are not fast so we just need to do the signing for the ZSK with the KSK so we can manage that it's in a single ceremony but then for the date today in order to sign the zone what we do is to use cyber signing, so we just [inaudible] KSKs and then the public part of the KSK to a secure server and then from there we sign in sober so that much more faster and then with different traits the same moment basically you just need processor capacity, so in our case we sign in a couple seconds and everything is ready so that's the way that we're doing it right now, we think that it's a good model because it's a cost effective model so basically its markers are really cheap they're not expensive and then for the sober signing then you can use and service and different service in how you want to distribute it which is not something very expensive as well so, since the KSK never reaches the internet and its very secure and its highly replicable so within it's a good model we have been using for a couple years so far and it has been helping us a lot and having these ceremony once a year also lowers a lot of the administrative load, we are a small team so it's also important to consider that those rollovers to be automated also helps a lot. Okay, nope, can you please move to next slide, it was not Fred, so for the KSK rollovers as I mentioned we so it once a year so what do we do.

Next slide please, so basically we are using the double DS rollover, which is to find the section 4.1.2 from the RFC6781 so what we do is to prepublish the DS records in the root but it's interesting that for doing that we need a manual process current IANA system it requires both the DNS keys to be published at the same time on the root in order to approve it automatically, in our case we just publish the DS, or prepublish the DS, so that means that the automatic checks that IANA does they fail so even though its documented on the RFC that's not something that can be that fast right now so we just need to provide a proper justification and then they continue the process manually so this means that there's a time of not being automated, fully automated, that we need to account we need to know that it will take more time to do it this way we need those manual approvals and that means that we need to plan ahead of time and that is something we've learned, we've been doing this KSK rollover I think it's three years so far and it's been the same each year so now we can account that time, plan ahead and it works correctly so we haven't had any issues just that we need to do it with enough time to cope with that gap in the system.

Alright and then on the DNSSEC how have we been working with the community especially the local community, so -- did you did it or did I do it, alright so it works again, yeah so some key activities so basically we do a lot of capacity buildings, we do workshops, full size which for us is a one week long, we have received support from different organizations to do this, form ICANN, NSRC, and others, so we've been doing those workshops where we basically train the local community, government infrastructure, operators and so on, then we also participate in local regional events where we can also participate on the DNSSEC we regularly do talks at universities for advanced students, we want them to know that the DNSSEC and that they can use it and then we contain the chip from the very beginning before they even get to probably formal job. So, we do that a lot and it's been very interesting because that also generates a lot of questions and interest on them knowing that DNS is a key component that they need to have in mind and also to consider that for their careers. Then we also do technical assistance and training for different institutions within our community and then recently we started doing custom trainings for the ISP's. NIC Costa Rica is hosting right now the national internet exchange point. So that is good thing because we would merge that two groups, the ISP's with the DNS community, and it is quite easy to get them.

So, given that we have that community in house [inaudible], so we have been taken advantage of that, doing different talks and trainings and they really help. So for example, with the local ISP's, last year we did a training and as you can see we had a good a spike on the foundation with the local training and it presents to you to see the trend, especially if you see how it has been by the end of this year, so basically even though there are a lot of ISP's that are using Google DNS, we have been seeing a trend were they start deploying more and more local resolvers on their own, not only using Google, and that is something we really like, so we are working directly with them so they can not only validate through third party servers which we know they work perfectly correct, but those are [inaudible] intended we are to the connections that resolutions that are not necessary, so we are working with them in trainings, specialize trainings, basically to help them install their own resolvers and then to have DNS turn on since the very beginning. So, we have had good results with that.

And then it's not something that just stops there, we know that it's a lot of work in progress, there is a lot of things to do and that also has a lot of challenges; two of them, is that even though we have been talking about DNSSEC and the .cr for a couple of years so far, since 2012, less than 1% of the .cr domains are signed. So that means we still have a lot of work to do. We have been approaching as we mentioned on the capacity buildings slide, different ways talking to people, doing workshops, trainings, local help for the local community but it is still going one by one, it takes a lot of time. So, what are we doing, or are the actions we taking going try to increase this number?

So, something that was recently deployed, and hopefully in a future presentation we can come out with some statistics and numbers, this is very recent this change was then a couple of weeks ago, so basically with the help of NIC.CZ we have implemented the automatic keyset management. And this is something we really think that's going to change the numbers that we have. So, CZ helped us a lot to get it up and running. We used FRED as our back-end system, so this also facilitate the work, So in their case they deployed, and we had their collaboration to turn it on the versions that we recently outbreaked to and it's now up and running, so it's excellent news for us, so we hope that this will change the numbers that we have, because going one-by-one or small groups, it hasn't provided the resources we want, so even though we will continue doing that, we want to move more on the automation side of people without knowing DNSSEC, to have the possibility to have it turn on.

So something we're doing for that, is basically to work the DNS hosting companies. We already started conversations with them and the idea is to work with the top 10 DNS hosting companies which have that .CR domains already there. So they can go ahead and automate the DNSSEC publishing and management of the keys. So that will move the operational side of DNSSEC to people who already know about the protocol, and it is not necessary for DN users to get to know it. So hopefully that will change.

And then the other thing that we have identified as a challenge, it is the KSK root rollover process, so basically what we have been doing is awareness activities, the name of the [inaudible], so we have been working with them, we also are part of the Costa Rica network operation group and we have done activities as well, and also local trainings and different tasks with some interested parties that are also concerned about the KSK rollover. So basically, that's what we have been doing, we have a email address that is quite easy to remember, DNSSES@nic.cr. Hopefully that will help in case something brokes and the moment of the rollover in either and ISP or end-user, so they reach us really quick, it's easy to remember, and hopefully that will also help. So that's it, so if you have any questions, I think I have a couple of minutes.

JACQUES LATOUR: Any Questions? Sure, Russ.

RUSS MUNDY: Thanks a lot, Mauricio. Back at ICANN 43, in Costa Rica, there was an announcement made that I think it was the largest bank in the country was signing. I was curious if there had been any further announcements, or work or progress in terms of especially the financial industry beyond that single bank at the time I think it was just the one bank but I was curious if there had been more progress there? Thank you.

MAURICIO OVIEDO: So thank you for the question and well basically that bank is still signing, so that is a good sign. But at right now what we are trying to do is basically working with the local government entity that covers the financial group so they can see the benefits if DNSSEC and also turn it on, or put it aside [inaudible] for the banks that use our domains, so we've been working with them, we have no news right now of the other banks doing it, however we're taking the approach of talking to whole group, and hopefully that will give good results.

JACQUES LATOUR: We can go to the --

LUIS ESPINOZA: Okay, yes, Luis Espinoza from Costa Rica; about the banks, I just want to add something interesting to the moss of the transactional URL's for banks are .com, not .fi.cr, that could be an issue to implement DNSSEC, because they will not be in the transactional work base. Yes, come in.

JACQUES LATOUR: Alright, well thank you for the panel and next up is Ondrej Filip.

ONDREJ FILIP: I am afraid that is the end of the presentation, can you roll it back. It was quick actually. That is true, there is not much to say. So good morning everybody, I am Ondrej Filip from .CZ from Czech Republic, and I prepared for you a presentation about algorithm rollover. I've done this presentation in corporation with [inaudible], who could not be here unfortunately, but I am sure he is watching remotely, so hi Jaramir, how are you doing?

So, before I start, let me introduce a little bit about the situation in .CZ, we have roughly 1.3 million domains and we have quite good penetration of the DNSSEC, about 50, more than 52% of those domain inside, so it is roughly 700 000 signed domains with DS record published. And I can also say so that more than 40% of those signed domains is signed by ECDSA algorithm. So, that means that the ECDSA algorithm is also widely deployed in Czech Republic and those signatures on signed domains also include major sides, even sides from Alexa top 20 in Czech Republic.

So, basically that was a good prove that if somebody has DNS resolver that has issues with this algorithms, then such a user couldn't access top sites in the Czech Republic, including also all websites NIC CZ so the probability that there is someone like that is pretty low. So, that is why when we are considering making a KSK rollover, we are thinking about this issue. The reason for KSK rollover is that we our last rollover was 5 years ago, so that's according rules time for a changing key singing key, and since we knew that ECDSA is widely deployed, we decided that the new keys will be based on elliptic curve cryptography algorithm.

We set a date for such a rollover. We did a planning and we hope that this transition will be done in five working days, so we decided on June 4th, which is Monday and hopefully finish the end of the working week, so before June 8th 2018, so quite recently. We are quite experienced with that change, although of course changing to ECDSA isn't really common but we did two KSK rollovers in the past.

First was done in 2010, when we rolled, we changed algorithm from RSA NSEC to NSEC3, then we did a second KSK rollover, it wasn't algorithm change over, it was in 2013, the main reason was again time, that those old keys were old, but we also split the roles, the KSK is now managed by a different part of CZ NIC, it's SIR.CZ the national cyber security team which is part of NIC CZ, but has you know has different administrative coverage and management coverage, so it's kind of independent on the administrative team whose managing zone signing keys so because we did this management change, we also changed the keys of course, and now we decided to change from NSEC3 to ECSDA so, basically that's our third KSK rollover a, second algorithm rollover and first deployment of ECDSA at TLD level.

So before we started we did some public announcement of course, were my speech was like "check your DNS resolver", it was mainly targeted to professionals, ISP's, so we send it to local exchange point community, and to other technical working groups, but the message wasn't very strong because the part of it was that if www.nic.cz works for you, then your server is probably fine, because then it means it can handle the fact that this domain is signed by ECDSA algorithm. We also did some training, some internal but also one external and that was rollover of ENUM domain, you know we also manage ENUM domain for Czech Republic, which is 0.2.4.e164.arpa so, we actually did this, you know they danger that something will break is little bit lower, this ENUM is not really heavily used these days, so it was a good training domain for it.

But it's operated in the same system and the mechanisms is like the the TLD domain of course. Base on those training in the preparation to change it should be decided to make two changes, normally we publish zone every 30 minutes and we decided to increase that period to 60 minutes, probably not a big deal for all users, but we wanted to sure that we will be able to create a domain in such a period, and also, we knew that some of the messages will be bigger that 1232 bytes, which is default by our DNS servers so the increased in the message size to 1300.

And this is the situation before we started, so our DNSKEY response message size was 907 bytes, the zone files size was 875 megabytes, and the time it took us to create a zone, sign it, verify it, do all the sanity checks of course, it's not just the singing or generation, but all the mechanism that creates a new zone, took us 15 minutes and if you can see the details in the presentation I am sure it is not visible on the big screen, you can see the screenshots from DNS [inaudible] which algorithms they used.

This was day one Monday morning, it's 10 o'clock, or local time, 8 o'clock UTC. So, we added ECDSA signature so the zone was double singed this that moment, the DNSKEY response size increased to 1103 bytes, and the zone files size increase to 1.2 Gigabyte roughly. The zone publication time increased to 21 minutes so you know we are getting closer to the previous limits of zone publication periods, so you know that shows that the prolongation of the period was really important and the keys are not added yet you know, they are just the signature, so we have now signatures and there is no key who is pointing to them, so they shouldn't be used. We did this change and the plan was to wait roughly 24 hours, and actually that's exactly what we did, we added new keys, I think it was 26 hours later, there is a mistake it the time it was not 12 UTC, but 10 UTC, I apologize.

So 10 am UTC we added ECDSA keys that of course increased the DNSKEY response size to 1263 bytes and that was the reason we increased the UDP message size, and I really do not the remember from the top my head what was the zone file size but, it increased probably slightly because the keys were added, but the zone publication time increased by 29 minutes, of course, the reason for the timing increases because once the keys are added the DNS signal does some other additional checks and that is why the time increased, otherwise you know there is of course no need for time increase if you just want to record.

But this happens, so it was Tuesday let say morning, or it was roughly noon actually in the local time. We wait a few hours and then we submitted DS record change to IANA, we expected that and we knew from experience that this can be done roughly in a day or maybe a little bit longer, and actually the expectation was correct, IANA made like in 28 or something like that, it was a little bit more than a day, so perfectly on time what we expected, it was great, it worked like we expected, so the DS record was swapped in the zone , on Wednesday night, it was 10 o'clock pm local time, the DNSKEY response of course hasn't change because there we no change in the zone, zone file size hasn't change as well and zone publication time, also hasn't changed, the only change you can see between those two slides, and I will show you, is in the screenshot of DNS [inaudible]. You can see that the number of algorithms change there so, I am sure you can't see it on the big screen, but I suggest you to download the file if you want to see the details.

So, the algorithms change and since that time you know we are answering or clients started to crave using the new key signing key and zone signing key of course. So, we waited till the Friday morning at 9 o'clock local time, we removed the RSA keys, so that it means the response size to DNSKEY crave decreased dramatically of course, the zone file size hasn't changed much, and also the zone publication time hasn't changed much, but it was the one before last step to the algorithm rollover, which was done a few hours later.

So in the last, it was one o'clock pm on Friday, we removed the RSA signatures so then the DNS Key message response size decrease dramatically to less than 400 bytes, the zone file size decreased dramatically to 700 megabytes, and also the zone publication time to 22 minutes. So, and that was done, it was Friday afternoon, and we after the work, isn't it great you can have a nice weekend.

We did some clean up, we were to take zone publication time to 30 minutes and also the max UDP message size to the previous value, so that was 1232 bytes.

So, I was a bit quicker than I expected, so this change, we now know that this change can be done in 5 days, we didn't face any issues at all, except one report, one guy reported that his OpenWRT with Unbound 1.4.5 stopped working or stopped resolving DNS actually, we didn't pay much attention to that because it was 8 years old software, so we suggested him to upgrade it. He was quite a knowledgeable guy who knew what was happening, so that was the only report so far, we got, it's not so bad, given the fact that the software affected 10 million people.

So, we changed to ECDSA seems to be working there are no other issues, reports, nothing else, good thing is the zone file size decreased quite significantly I would say. The response size also decreased, we saved some network bandwidth, of course the only things that increased is zone generation time, because you know calculating signature with ECDSA needs some a little bit more computation power than the RSA signatures, that's not a big deal for us, we can again make a zone in 30 minutes, or I think it's pretty quick and the service is quite okay. So the service level hasn't changed with the ECDSA for the end users. And that's all, thank you very much.

RUSS MUNDY: Do we have any questions for Ondrej? This is a very impressive series of events we walk through here, and I think it's helpful for everybody in DNSSEC to that somebody has stepped out and said we're going to do this first. Any comments or questions from folks?

Ah, here come someone to the mic, I think it's Duane.

DUANE WESSELS: Hi Ondrej. Duane Wessels from Versign. The longer time to produce a zone, is it really because it's takes longer to produce a signature? I thought ECDSA was better in that regard?

ONDREJ FILIP: Our experience has that it takes more time actually to make signatures, that is the experience. And that we learn in the training phase, so we knew it was going to happen and that we knew it was not significant for all zone sides. We are using the

DNSSEC signer from [inaudible], so maybe that's the case of the tools, or maybe that's a case of the library, so I am not sure --

DUANE WESSELS: Okay, thank you.

RUSS MUNDY: We have another one on the way [inaudible] quick question to Ondrej after -- go ahead.

LUIS ESPINOZA: Hello Ondrej, quick question, you did measured the time decoding the algorithm in the client's side? Okay, I mean the resolution of the clients, maybe could be speed up because of the lower side of the package, but the algorithm should be processed to the client's side, or at least in the resolver? Then, did you measure some benefit there?

RUSS MUNDY: So would you say name and affiliation also please, so we can have it for the remote people, can hear who you are?

LUIS ESPINOZA: Luis Espinoza.

ONDREJ FILIP: I'm sorry, Luis, nice to see you after a while. I didn't catch your questions. Can you please repeat that?

LUIS ESPINOZA: Okay, the question is, when you changed the algorithm for a solution, then you measure the time that the server need to sign the song, right, but did you measure the time for the resolver to process the DNS with the new algorithm?

ONDREJ FILIP: Well we can't measure the time of all clients of course, but when we measure time for all resolvers, not resolver in laboratory, there wasn't any significant difference, so shouldn't be a problem. The message processing in quicker of course because the message size is small, so it should decrease, but I don't have any scientific evidence to proof for that actually.

LUIS ESPINOZA: Okay, thanks.

RUSS MUNDY: One question for Ondrej.

JACQUES LATOUR: I had a question.

RUSS MUNDY: Oh. Go ahead, Jacques.

JACQUES LATOUR: So I had a question for Fred. Did you see the same behavior with your zone timing?

UNKNOWN SPEAKER: [Inaudible] China, first time to be here. Your presentation is very helpful, but I'm not very clear what is the difference between algorithm rollover and normal KSK rollover. Is there anything special if I want to update the algorithm to ECDSA is there anything special we need to pay most attention?

ONDREJ FILIP: Yes, the process is a little bit longer and the double signage in the zone, so there is a different process when you want to change the algorithm and when you just want to change the keys actually, so it takes a little bit more time.

UNKNOWN SPEAKER: Takes more time, but the whole process is similar to a normal KSK rollover.

ONDREJ FILIP: The double signature part is longer, but you need to have double signature for a while so that it makes it more complex and longer.

UNKNOWN SPEAKER: Okay, thank you.

FREDERICO NEVES: Frederico Neves from .BR. First of all, thank you, Ondrej for [inaudible] IANA earlier because IANA was not ready for receiving those kind of keys in the past, so it will be easier the other one in the future. And in our case, actually and trying to elaborate on the Lewis questions, actually, it is lower for validators because the validations ECDSA is much slower than RSA, but as far as we know this is not an issue at all. Regarding our signature time, we use a complete different library, our new signor that we are developing is written in goal, and we are using our largely parallel signor for the ZSK, and we can fully generate our zone in less than 3 minutes, and not any issue at all, and actually we are lowering our publication frequency from actually hazing it, from every 30 minutes, to every 5 minutes.

ONDREJ FILIP: Thank you for that. Using [inaudible] tools which creates a little bit internal fight because not all the developers believe we should use their tools, on the other hand the administrators of the zone are very conservative so there is a little bit internal tension and this time we decided to stay in the current tools, but probably in the future we might migrate to some modern tools to sign the zone, but thank you for the fact that we can make it in less than three minutes because I believe four million domain rights so that says to us we can make it in less than a minute, but the publications, the whole time the whole like 29 minutes it’s not just the zone creation and RSA signaturation, there is a lot of sanity checks and it’s quite heavy process before we publish a zone of course, so it is not just the signing part of it.

FREDERICO NEVES: I totally understand we have some checks as well. And there is the fact of the propagation of the zone to all the alternatives to getting sync and we have been playing with double signage zone as well, just to make sure we can make it, because as you guys, the zone is especially the KSK is completely pre-signed in ceremonies so we have to take into account all these possibilities of taking a little bit more time than expected to propagate. Thank you very much again.

JACQUES LATOUR: Alright, so I am thinking this is a good opportunity to probably for someone one to create some sort of a playbook for ccTLD into follow step by step, here is what you need to do, based on different technology, these are all the steps. I am not seeing any volunteers, but that is something that will be useful for all of us to migrate to this, because if it makes us own files smaller, makes everything faster, then it is good for all of us. I think Erwin raises his hand saying I'm volunteering? No? Any questions?

ERWIN: I am, no I am not volunteering, and actually I think we, this is the work the ITF, we definitely need a 6781 update, because that document is a little bit dated, and some of the recommendations are actually not any longer valid, yes.

JACQUES LATOUR: Alright, thank you, so this is, now we have a break from 10:15-10:30 --

RUSS MUNDY: Enjoy your coffee break, we plan on starting right at 10:30.

[END OF TRANSCRIPTION]