TIJANI BEN JEMAA: Good morning, good afternoon, and good evening everyone. Thank you for coming to this webinar. As you know, ICANN will change, or roll over the key of the root, of the DNSSEC. And we thought that it is an important event that requires to have some [light?] for the community of At-Large.

I will start by giving the floor to the staff for some housekeeping, and then I come back. Yeşim, please.

YEŞIM NAZLAR: Thanks so much Tijani. [Inaudible] of the housekeeping presentation, which is currently displayed on the Adobe Connect room. We will have a question and answer part during the webinar. If you have questions, we do encourage you to type in the question and answer pods, and staff will note your questions, and they will be answered by the presenter.

And you can [inaudible] of the bottom left part of the screen. We also have a pop quiz session, and we will have a very short pop quiz after the speakers' presentation, so please be ready to answer the questions posted in the poll pod.

This is all from me Tijani, back to you. Thank you very much.

TIJANI BEN JEMAA: Thank you very much Yeşim. And so I said that it is an important event, and perhaps the community of At-Large has some information about it, since it will effect a lot of us, a lot of end users. So for this purpose

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

today, we invited one important person for this issue with Russ Mundy, the Vice President of Research for the CTO office of ICANN, who will give us a presentation and answer our questions on the upcoming DNSSEC key signing roll over, which is planned already by ICANN.

The root key signing key is the most important cryptographic key in the DNSSEC. And as you know, the DNSSEC protects us from [inaudible] spoofed data, and protects us from attack such as being misdirected to a malicious website.

So, that's why we invited Russ to give us more information about that. Tell us who will be affected by it, and he will explain to us everything about the key signing key. Russ, please go ahead.

MATT LARSON: Hi. This is actually Matt Larson, I'm the Vice President of Research in ICANN's Office of the CTO. Hello everyone, and thank you very much for the invitation, and let me begin the presentation.

You've heard that we're about to change, ICANN is about to change the support [inaudible] parameter in DNSSEC. And for network operators, this might create a need for action. And so in this discussion I'm going to talk about very briefly, how DNSSEC works and then what is happening with the KSK role and when it's happening. And I will leave time for questions at the end.

So let me first talk about exactly how DNSSEC works to give some background. I think everybody is familiar with DNS, here is the brief example that someone could ask for, particular IP address for domain name, dub dot example dot com, and then what comes back is the address for that domain name, in this came, an IPv6 address. And DNSSEC simply adds a cryptographic signature to that, a digital signature over the data, over the response.

DNSSEC validation then, is the process of actually effecting that signature, to make sure that it validates, that is it's cryptographically valid and that signature vouches for the authenticity of that data. And in order to validate the signature, you need the public key. So the private key generated the signature, and a public key is necessary to validate the signature.

And the reason we have DNSSEC at all, is that the DNS protocol is somewhat gullible and easy to fool. If a resolver sends a DNS query, if you do not have DNSSEC, you basically have to trust the answer that you get back. You have no way to know that the answer you receive is really coming from who you ask the question in the first place.

And so this makes it possible to forge or spoof answers, and trick resolvers into believing incorrect information. We've gotten smarter over the years and figured out how to make resolvers that are somewhat paranoid, and they're not easy to spoof, but the fact remains that without DNSSEC, there really is no complete protection.

But with DNSSEC, we can now trust information in DNS more fully, because we have cryptographic proof that the data that you receive is the same data that the owner in the zone put in the zone, and that data has not been modified or tampered with, as it moves from an authoritative name server to the client. And not only does DNSSEC stop spoofing, but DNSSEC could serve as a base for future extensions of protocols, and future uses of DNS that would build them, a secure environment DNS.

So, for example, ways to secure email transfer, to put public keys in email and secure them with DNSSEC, and also to supplement X509 certificate operations, to put that information in DNS as well.

DNSSEC has three kinds of records that hold the cryptographic key data. Bear with me, this is somewhat complicated. I think if we had this all to do over again, we might not have designed it this way. But the way this works is every zone, every DNS zone that's signed, that's protected with DNSSEC, adds to what we call key pairs. The one is the key signing key, and the key signing key, that signs all of the other keys in the zone, and then those other keys can include a zone signing key.

And the zone signing key was what actually produces the signatures that are validated. Then we have what's called a delegation signer record, and this is a pointer to a key. As I said, this was supposed to make things simpler. The good news is the DNSSEC protects us, the bad news is it does add some operational complexity, but that is a topic for another presentation.

I'll explain those records in a little more detail in an upcoming slide that makes it a little easier with the picture. So we here we show how you would validate a digital signature. We have the piece of DNS data at the top. So this would be a record with the IPv6 address of www dot example dot com. Then we have the digital signature that's part of DNSSEC created over that record, and in order to validate that digital signature then, we need the public key that created it. And once you have those pieces of information, you can validate, does the digital signature, does it validate? Is it legitimate? Does it mean that the data we have is authentic?

So, you can see you need the public key, the box in orange, in order to do the validation, but the issue here is, how do you trust that public key? You can get the public key from DNS, but how do you trust it? And that's where we get to where we are, why we're here today to talk about the root trust anchor.

The answer is that the DNSSEC requires what's called a chain of trust. In order to trust the public key on the lower left, the example dot com, you need to start from a key that you trust, and that's called a trust anchor. So let's look at the upper right of the slide. From the root zone, KSK, that is the trust anchor that everyone uses today.

And when I call it a trust anchor, it means that you can configure that in your DNSSEC validator, and you trust it implicitly. You basically are telling your validator, we absolutely trust this key no matter what. And then the DNSSEC validation process can start with that trusted key, and use that key to validate the root zone, ZSK, which can then validate what's called the DS record for dot com. And the DS record for dot com points to the dot com KSK.

And you can see, I won't read it all out, but you can follow the arrows and see that train of trust, of data and signatures. And by following that and building that chain of trust, you can eventually follow signatures and trust the example dot com ZSK. And then once you trust example dot ZSK, you can trust any data that was signed with that key, including, I'll go back a slide, including the record here in the upper left that has the IPv6 address for www dot example dot com.

So I know there is a lot of information here on these slides, but hopefully this helps illustrate the importance of the trust anchor, in that the root zone, KSK, is the starting point to validate any other piece of data in DNS. So it's very important that you have the right knowledge of what that root zone, KSK, is.

And many, many TLDs are signed so there is a lot of information in the root zone, and the point here is that this reinforces my point that the root zone, KSK, is an important starting point because so much of the DNS namespace is signed with DNSSEC.

So, as I said, the trust anchor is this key, within a key that an operator places great trust into for the purposes of verifying responses. And you might trust the trust anchor simply because you got it with the software that you installed. So someone else has put it in the software, and you trust it. Or perhaps you configure it yourself. You've gone out and done the research and found the trust anchor and configured it.

But one way or the other, the effect is the say, it's the key that you trust greatly. Now, I don't want to talk a lot about this. There are other trust anchors. You can put any other key, configure any additional keys as trust anchors in your validator, that tends to not be very common. The root zone trust anchor is by far the most important one, and that's the one we're focusing on today.

So let me talk a little bit about specifically how DNSSEC in the root zone works. The root zone administration is somewhat complicated in that there are multiple organizations that cooperate, that manage the root zone. ICANN is responsible for operating the root zone KSK, and then VeriSign is responsible for operating the root zone, VSK.

The VSK is used every day, every time a new root zone is generated, but it's signed with the VSK. The root zone KSK only needs to be used once per quarter, because once per calendar quarter, the DSK changes, and when it changes it needs to be signed again by the root KSK. So once per quarter, the KSK is used in what we call the key ceremony.

So these activities are operated separately, but they are coordinated. ICANN and VeriSign work closely together to manage DNSSEC in the root zone. The current root KSK was created back in 2010, when the root zone was signed for the first time. It's stored in what we call a hardware security module, which is a piece of tamper resistant hardware, and there are two different, what we call, key management facilities where ICANN stores the KSK.

They're very well protected with many levels of security and much process around access to facilities, and access to key material. That is a whole separate talk that we can talk about exactly how we operate the root zone KSK. But I'll leave it to say that the KSK is very well protected, and used very carefully.

So there are different ways to get the root zone KSK. Within this, you can whip a DNS query get the root zone KSK, but then that would be just as reliable as any other data in DNS. It would be unprotected. The whole point here is that the root zone, KSK, is the starting point. You can't use any other key in the DNSSEC to validate it, because it is the starting point. You can get the root zone KSK via that URL there.

It's hosted on the IANA dot org website. ICANN operates an X509 certificate authority, and that file with dash anchors, that XML file that maintains the root zone trust anchor, that is signed by a [inaudible] certificate that goes to the ICANN certificate authority.

So that's one way to trust the root zone, KSK. The other is to just trust the information that you get when you install DNSSEC validation operator. I mention that earlier.

So there is a plan to change the root zone KSK and that's why we're here today. And this is important because this is the first time we changed it. As I've said, we've been using the first root zone KSK that we created six years ago in 2010. And this plan will set precedent because of their many different parties that have the potential to be effected. Anyone who is doing DNSSEC validation, needs to get, needs to have this key changed.

Now, as I'll talk about, it's possible that they'll have processes in place that will cause the key to be changed, essentially automatically. But it is important that people are aware that the change is happening, particularly people who operate DNSSEC validation software, because they will have to ensure, even if the key does get changed automatically, they will still have to ensure that it is changed.

And it's impossible to know everyone who is doing DNSSEC validation. There is no rift anywhere because anyone can enable DNSSEC validation on their recursive name server. So one of the things that ICANN is attempting to do is get the word out with presentations like this one, to let the community know what's happening and to raise awareness.

People have asked, why are you changing the key in the first place? If it's not broken, why change it? And in fact, it's not broken. We still have full confidence in the root zone KSK. I don't believe that there is anything wrong with it, or that there is any weakness. But it is a good cryptographic practice, good cryptographic hygiene to change keys.

Secrets don't remain secret forever. This is very similar to how your IT department may force you to change your password every so often. We also want to have a plan in place. We want to change the key in normal circumstances. We definitely don't want to do this if there were ever a situation where there were a problem with the key, and we had to do a change more suddenly. We don't want that to be the first time we have to do it.

We want to change the key under normal operations, have a brand, and document it. And there is really no way to do this privately, because it effects doing DNSSEC validation on the internet. So I've mentioned how many people it effects. If someone does not get the message, and they don't update their software with the new key, then their software is going to believe that every response is invalid. It will appear as if an attacker is exchanging every response that they receive, because none of the signatures will validate, or rather, they won't be able to build the change of trust because they won't have a good starting point.

And that will cause every DNS resolution to fail. So let me talk more about the project itself. This is meaningful if you are someone who is performing DNSSEC validation. Jeff Houston, who is a researcher at APNIC, has done research and has published statistics that, about 15% of traffic, DNS traffic worldwide is doing validation.

And I should point out that DNSSEC signing is not affected by this. There are really two major parts to DNSSEC. There is the part, the signing portion when DNS information is published on authoritative servers, for DNSSEC it needs to be signed. And then when DNS information is looked up on the cursor servers, it needs to be validated.

And we're only talking about that second validation portion today. DNSSEC signing is unaffected by this, only validating DNS signed information is what is affected. So, if you are doing DNSSEC validation, it's time to revisit the configuration and the processes. And because we haven't done this before, it's new to everyone.

ICANN, to give a little background here, ICANN convened a panel of community experts and ICANN staff to come up with a plan to roll [inaudible] KSK, and they met and published a report in March of 2016. And then ICANN staff picked up the project and developed plans, and followed that recommendation almost completely. We made very few changes.

And in the interest of transparency, in late July, we published all of the plans at the URL you see on your slide. There are five different plans that were published. So we encourage everyone who is interested to look at the plans and there is much more detail there than you probably ever want to know about [inaudible] KSK.

And here is perhaps the most important side in the presentation, because the plans call for the actual roll of the root zone KSK. When the new KSK will be used and the old KSK will be retired. The plans call for that to happen on October 11th 2017. So I realize that's a long way off, it's almost a year away. But because of the importance of the project, and because so many people are affected, we are starting early to get the word out, and let people know what's happening.

I'm not going into a lot of detail on the actual plan and how it's going to happen, but we're also taking the process very slowly. We're not having any special key signing ceremonies where we use the KSK. Those ceremonies happen once a quarter, and we're doing everything we need to do within the cadence of those quarterly ceremonies, because there is no rush. There is no hurry to do this.

So we have decided to take the plan very cautiously and slowly. So, the plans don't call for changing for any of the settings related to cryptography. The key size is not changing, nor is the cryptographic algorithm. We are changing the key in such a way that the protocol calls automated updates the DNSSEC trust anchors will work.

This protocol is defined in our RFC 5011, and this is the automatic mechanism I mentioned earlier for updating a trust anchor. Very briefly, the way this works is, when you publish a new trust anchor, you have the old trust anchor sign the new trust anchor, and a DNSSEC validator will see that the trust anchor that it trusts is signing a new trust anchor that it hasn't seen before, and after 30 days of observing that, the validator decides that the new trust anchor is legitimate, and it then trusts the new trust anchor.

So this is one piece of good news for this project, which is that any DNSSEC validator that also follows this protocol, the automated update protocol, that validator should automatically update the new trust anchor. After we publish the new trust anchor in DNS, that trust anchor will be signed by the current trust anchor, and the validator will, after 30 days, realize that the new trust anchor is also legitimate, and it will configure that as well.

So we're hoping that for many people, they won't have to take any action because the new trust anchor will be updated automatically. And as I mentioned, we're fitting this process into the normal maintenance events, the normal [inaudible] key ceremonies. And then the plans also include a lot of testing and monitoring to make sure that we're requesting the process ahead of time, that as we make the change, we're monitoring to understand the impact.

One possible area of concern deals with response size. There is one particular response from the root zone, and that's the response when you ask from all of the DNS keys in the root zone, or I should say, all of the keys for the root zone itself. That response grows to a size of 1425 bytes at one point during the project. And that is a historical maximum, this particular response. In fact, no response from the root zone has ever been that large.

And some experimentation, especially with v6, suggests that there might be a concern. Now, this is the case where the standards and experiments suggest one thing, but actual operational practice, evidence from other people who are doing DNSSEC in other zones, suggests that there is not going to be a problem.

But in the interests of being very conservative, we're pointing out this issue, and we're watching this very carefully. The issue surrounds fragmentation. With IPv6 the minimum size, I beg your pardon, the maximum size that IPv6 software is supposed to support, but the maximum packet size, what they call a MTU, is 1280 bytes. So it is possible for someone [inaudible], they won't be able to receive a response that's 1425 bytes from the root zone.

And in that case, that packet is going to have to be broken up into fragments. And there is a possibility that the fragments won't reach the recipient and therefore the entire response won't get there. There is an URL, you can read here, to look into this in more detail, if you're interested.

I personally am not concerned, I'm not very concerned about this issue. There are other DNS zones that are using DNSSEC that are using, that have already generated responses as large, or larger, than the response sizes we're going to get in the root zone. And those don't foresee no operational problems whatsoever. So as I said, this is a case where we do not we will cause fragments to happen for, particularly for IPv6 users.

We do know that in some cases, people filter fragments and fragments don't reach their destination, and we do know that that is theoretically possible to cause problems. On the other hand, we have operational evidence that suggests that that doesn't happen in any widespread way to cause problems.

Here are some of those states. You can see when the size increase to these larger sizes. And again, I'm highlighting the important date of October 11, 2017, when the actual roll over happens. That's the date where if you don't have the new key configured as a trust anchor, DNS resolution will stop working.

So as an operator, it's important to know, how have you trusted the root in KSK and how have you configured it? As an operator, how do you update the trust anchors in your software? Are they updated by hand? Are they updated by some configuration software? Do you rely on a trust anchor that was embedded perhaps in software that was provided by the author of the software, or perhaps the organization that packaged the software?

For example, an operating system distribution, are you monitoring DNSSEC validation [inaudible], would you even notice? So that's important to know. If you're doing validation and you have a trust anchor configured, it's important to know how you're going to update it. As I've said, it is possible that you're using the automated update protocol, and the update will happen automatically.

I'm not going to talk about [inaudible] trust anchor management. One of the things we're doing is working with DNS software and tool developers and distributors, because we do recognize that many of those organizations embed the root zone trust anchor in their software. So for example, organizations that write DNS software, they will either put, sometimes they put the root trust anchor actually in the software code itself, or they include it in sample configuration files, and then people who package that DNS software, such as operating system distributions, like Linux distributions, like the Red Hat, those organizations, when they package the software, they might also put [inaudible] the root zone trust anchor.

So we're working with those organizations to let them know that the trust anchor is changing, so that they'll update their software, and then as people upgrade their software, they'll get the new key. So that certainly is one path for people to get the new key, is simply by updating their software. We do have test beds that are available for people who are developing code.

These are test beds that allow them to make sure that their software can file the automated updates protocol. ICANN is also in the process of developing a testbed where operators themselves, that will allow operators to determine if the software that they're actually deployed and running, if it correctly follows the automated trust anchor update protocol.

So that is the end of my presentation. These are some URLs to find more information. There is quite a lot of information on the ICANN webpages, in the bottom bullet. And there is also a mailing list you can join if you're interested. And with that, I will be happy to take any questions.

TIJANI BEN JEMAA: Thank you very much for this presentation, for the [inaudible]. I think it was a little bit complicated and a little bit technical. We need to understand what will happen because most people [inaudible] if they don't [inaudible] update this.

So, are there any questions?

MATT LARSON: I do see one question in the chat room, which is asking about the size of the KSK, the actual key size. So, I'll say that that's not changing. The key is a RSK key, and the current trust anchor is 2,048 bytes and the next trust anchor will also be in 48 bytes.

TIJANI BEN JEMAA: Any other questions?

Of course, anyone who is not [inaudible]…

HEIDI ULLRICH: Hi, Tijani, this is Heidi.

TIJANI BEN JEMAA: Heidi, please.

HEIDI ULLRICH: Yes, we have Olivier with his hand raised. But also Tijani, could you speak much louder. We can… It's very difficult to hear you. Thank you.

TIJANI BEN JEMAA: Okay. Thank you very much. Olivier, please go ahead.

OLIVIER CRÉPIN-LEBLOND: Thank you very much Tijani. Olivier Crépin-Leblond speaking. Thanks very much for this information and this presentation. It's pretty interesting to see some of the hidden work that takes place for the DNS to continue working, and be a safer or more stable than it ever was.

Just quickly, on this key signing roll over and so on. Are there any…? Is there any chance that this might not work, or there might be a bug, or somewhere along the way, and what would the repercussions be if such a thing happens?

MATT LARSON: Okay, thanks a good question. Thank you. We are taking several precautions. One thing that we're doing is, having a provisions in place to back out or reverse any changes. At these quarterly key ceremonies, we create the signatures necessary for the following quarter. And so as a result, we're sort of always working in advance.

And what we're doing during the roll over process, is actually creating multiple versions. So if necessary, we can immediately go back from the current key to the prior key. We, of course, hope to not need to do that, but we do have the provision in place, that if something happens, we could. So then the question is, well what could go wrong? And really, the thing that we would be concerned about is, if someone doesn't get the message, and they don't update their validators for the trust anchor, then as I've said, DNS resolution will fail.

But the good news here is that this is a very easy thing to fix. All they need to do is update the trust anchor. So it might, that certainly might be a painful experience, for example, an ISP to have customers calling and wondering why DNS resolution has broken, but the fix is very easy once the diagnosed it, they need to update the key and that's very easily done.

And you can imagine a situation where, you know, what if they had to say, get your software, or wait for a vendor or something? But that's not the case at all. If you're already doing DNSSEC validation today, you will be in a position to update to the new trust anchor. So, the good news is then that the fix is very easy if someone does miss the new and doesn't update their trust anchor.

That would be what we would be most concerned with, is if people who are not using the automatic update protocol, and therefore, for whatever reason, don't hear about the update, the KSK roll over, and don't update their trust anchor.

Even more good news about this project is that a lot of the DNSSEC validation is coming from very large ISPs and providers, you know, for example, Google public DNS, which carries a very large number of, a percentage of the DNS traffic, they do DNSSEC validation, but on the other hand, we know that they are well aware of this change.

So I'm not at all concerned about Google public DNS. Comcast, a large cable provider and ISP in the US, they do DNSSEC validation for their customers, but I also know that they're well aware of this. So our belief and our hope is that the larger organizations who have taken the time to actually enable DNSSEC validation, are also active members of the community and watching, and will know in plenty of time what's happening and will update their configuration accordingly.

It would be smaller operators, or even individuals who have configured their own recursive server, those would be the people who might not get the news, and might be affected. And while I certainly don't want anyone to be affected, I would think it would be certainly better if they were individually affected as opposed to a large ISP that would affect many, many of their customers.

TIJANI BEN JEMAA: Thank you very much. Any other questions? Of course, everyone knows that we may not change those keys. The internet will not be in failure, and we will still be in security, but as you know, any password that we have, if we use it for a very long time, it would be known, and we will not be secure anymore.

So we are using now this set of keys for six years, and people think that it is not time to change them, to be more secure. Any other question? Olivier, is a new hand?

OLIVIER CRÉPIN-LEBLOND: Yes Tijani, thank you. I do have another question on this. And it's… Yeah, thanks for this. So, effectively, yes. There are of course these big organizations that will deal with this, and you'll also have smaller organizations that might be challenged on this. Is there any plan to have some easy, how to type of presentations or manuals to show a step by step way of something that might need to be done?

Or some kind of, how do you call this? Not a frequently asked questions document, but a bit of a thing of saying, well if you have this symptom of a problem, then check the following things, like a checklist or something, that might be able to help those operators that are not 100% clued up about this.

I am aware that DNSSEC in general is not fully understood by a number of people that are running domains. They're implementing it, but it really goes kind of on the fringe of their knowledge as such. So I wondered if there was such a plan for this, that's all. Just to help out with this, because this, of course, is quite a significant change, ultimately.

MATT LARSON: Yes, that's another very good question, and yes there is. One of the things we're going to prepare are resources that describe how the trust anchor is configured in various popular recursive name servers, and that's where DNSSEC validation is almost always performed, is in the recursive name server.

And there are only a handful of recursive name servers in use. So the actual problem space, if you will, is not at large, and one of the things we want to do is publish resources so that people can understand how they can change the trust anchor, or even better, how they can turn on the automatic update protocol to make sure that they will automatically get the trust anchor changed.

OLIVIER CRÉPIN-LEBLOND: I have another question. It's Olivier. May I?

TIJANI BEN JEMAA: Yes, go ahead.

OLIVIER CRÉPIN-LEBLOND: Thank you Tijani. So, the next question is, how does all of this affect those top level domains in zones that are not signed?

MATT LARSON: Well, it still affects that in that because the root zone is signed, you know, every response from the root zone does include DNS signatures. So it really does affect everyone.

TIJANI BEN JEMAA: Thank you very much. Yeşim, you have your hand up.

YEŞIM NAZLAR: Thank you very much Tijani. There is a question from Afifa on the Q&A pod. Let me read it out. Hi, I am Afifa from Bangladesh. I don't think

ISPs are well aware of this change. What is planned to propagate the news to remote areas? Thank you very much.

MATT LARSON: Sure, well one of the things we're doing is travelling literally all over the world with versions of this presentation. We're trying to reach the operator communities all over the world. So, for example, a colleague will be presenting at AfriNIC in [inaudible] in a few weeks. He presented in APNIC in Asia just recently.

And it's our intent to reach out to operators all over the world. I anticipate that my colleagues in the operation space will be quite tired of me and my ICANN colleagues by the time this happens, because they will have seen us over and over again telling them that the root KSK is going to change.

TIJANI BEN JAMMA: Thank you, Matt. Thank you very much. Are there any other questions?

If there is not, perhaps I will give the floor to Yeşim for a pop quiz.

YEŞIM NAZLAR: Thank you very much Tijani. Yeşim speaking. We have only one question for the pop quiz session. Let me read it out for you. When is the actual date of the root key signing roll over event?

October 11, 2017, January 1, 2017, July 11, 2017, or October 11, 2018. Please cast your votes now.

And the correct answer, Matt, is?

MATT LARSON: October 11, 2017.

YEŞIM NAZLAR: Thanks so much. That was the end of the pop quiz session. Tijani, over to you.

TIJANI BEN JEMAA: Thank you very much Yeşim. Any other questions to Matt?

HEIDI ULLRICH: Hi Tijani, I believe we have a question in the chat from Glenn.

TIJANI BEN JEMAA: Go ahead please. Can you please read it?

HEIDI ULLRICH: Yes, I will read it as soon as Glenn permits me. It says, "We have seen uneven updates by operators on the IPv6 issue. Will the operators act more diligently on this issue?" Thank you.

MATT LARSON: Well, I certainly hope so. And as I've said, we're going to make every effort that the people hear about this. I would say one difference between IPv6 deployment and this is that inaction with IPv6 deployment doesn't necessarily cause an immediate issue for users. Whereas inaction when the KSK roll occurs, is going to cause outages for users.

There will definitely be an immediate impact on the day of the roll over. So, to a certain extent, this will be self-correcting, in that anyone who has enabled DNSSEC validation and doesn't roll the key, or does not have the key automatically roll for them, they are going to very quickly know that something is wrong, and they will need to take action to fix it.

But again, as I've said, the corrective action is very easy.

TIJANI BEN JEMAA: Thank you again Matt. Any other questions from the floor? From the attendees? Yes Olivier, please.

OLIVIER CRÉPIN-LEBLOND: Thanks very much Tijani. Olivier Crépin-Leblond speaking. I've got another question. I'm curious why the key size needs to grow. I'm not sure whether Matt explained the need, the actual need for this. I mean obviously growing it might introduce further problems then if one just rolled over with the same size key, wouldn't it?

MATT LARSON: Indeed, the key size is not changing. It's a 2048 byte key today, and it will be a 2048 byte key when we roll out. You might have heard, what's potentially confusing, is there was another recent change that VeriSign made of the zone signing key for the root zone, was originally 1024 bytes, and just recently, in September, VeriSign increased that to a 2048 byte key.

And indeed, that did cause generally larger responses from the root zone, and that was something that VeriSign and ICANN monitored very carefully, and as far as we can tell, we've seen no ill effects from that. So as of now, the root zone KSK and VSK are both 2048 bytes keys and they will be going forward.

OLIVIER CRÉPIN-LEBLOND: Okay. So it's Olivier speaking. So, but you mention here that the root zone DNS key, which is the other key, will increase to 1414 bytes for 20 days, and before that, it was 1039, and you're looking at January 2018 where it would increase to 12455 for 20 days.

MATT LARSON: Oh, I see. It is. So that's the consequence. And unfortunately, I have a great slide that's not in this presentation that would make that easier to explain. But if that particular slide, that's referring to the size of the response when one queries a root server for the DNS keys in the root zone. And at any point in time, there could be one or two ZSKs or one or two KSKs, depending on the particular moment in time.

Because when the ZSK rolls, for a brief time, there are two ZSKs in the root zone. And likewise when the KSK is going to roll, for a brief time, there will be two KSKs in the root zone. So, the normal state is one ZSK and one KSK, but there will be a time during this process, where there are two ZSKs and two KSKs. And at that point, that is when the size will be, the size of the response, will be that 1425 bytes, but that's unrelated to the cryptographic strength of the key itself, which is 1148 bytes.

OLIVIER CRÉPIN-LEBLOND: Okay. That then makes sense. Thank you. It's Olivier speaking. So, has that been tested already on sort of an internal network or something with different scenarios? Or is this pretty much the first time this ever happened?

MATT LARSON: No, it's not the first time, and it has been tested. I mean, you know, under normal operations, this is something that any properly configured operating network should be able to handle the name server responding, will potentially produce fragments, fragments travel over the network, and they're reassembled by the receiving system.

The primary concern would be, are there systems that would drop those fragments, or would the sending name server send a packet that's too large, but that would be dropped somewhere in the middle because it was too large? And that's something that's impossible to test, because that's just depends on various configurations and operational practices. But, you know, the good news here, as I mentioned, is that as a consequence of VeriSign's recent change increasing the cryptographic strength, and therefore the size, of the zone signing key, that led to a small size increase in the DNS key response size from the root.

And that produced no ill effects. And there are other TLDs that are signing DNSSEC with DNSSEC in such a way that they consistently produce larger than 1425, and these, I'll just go ahead and say, one of these are dot org, so dot org under its normal operational path, are certainly fine, there is no issue with that.

Their DNS key response size is even larger, and that's a very popular TLD that we see no reports of anyone claiming that they can't resolve things in dot org because of response size issues. So we do have, I personally have a high level of confidence that any issues are going to be corner case issues, and certainly not widespread.

OLIVIER CRÉPIN-LEBLOND: Thanks…

TIJANI BEN JEMAA: Thanks very much Matt. Yes, Olivier, you have another question? No? Okay. [CROSSTALK] Thank you very much Olivier, and thank you. We have to thank our speaker, Matt Larson, Vice President of Research for the CTO Office at ICANN, for this great presentation.

Again, it is a little bit complicated. It is a little bit technical, but we need to understand that when the exchange will happen, there will be all people using the DNSSEC [inaudible] more or less. So there is an update to be done on their software, etc. So this presentation was needed for the At-Large, for the end users, thank you very much again.

And I hope we will have other briefings later when the KSK key roll over will happen step by step, and I really would like to thank again, Matt, for this presentation. I also would lik1e to thank our technical staff, our staff, ICANN staff, and I thank you all for being here.

Thank you very much and this webinar is adjourned.

[END OF TRANSCRIPTION]