COPENHAGEN – Root Key Signing Key Rollover: Changing the Keys to the Domain Name System
Tuesday, March 14, 2017 - 17:00 to 18:15 CET
ICANN58 | Copenhagen, Denmark

MATT LARSON: Thank you, everyone, for coming to the session. We're going to get started shortly. We're just having last minute Adobe Connect issues because that's just what happens, so please bear with us.

Welcome, everyone. Looks like we're in business. Welcome to the session on the Root KSK Rollover. I'm Vice President of Research at ICANN. I'm in the office of the CTO and the office of the CTO is helping coordinate the Root KSK Rollover project along with various other folks in ICANN including IANA/PTI. And, we're going to give you an update today on the status of the project.

So, here's the agenda for the session. I'm going to give just a few slides to update everybody on where we are and then we have two panels, and I'll talk more about the panels when we get to them. But the idea is that I talk very little and we have the folks on the panel have time to talk, and time for questions from the floor as well.

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.

So, if you're here, you probably know what the root zone KSK is but just in case, it's this very important top most key that's in DNSSEC. And, the public portion of the KSK is configured in many, many places, anyone doing DNSSEC validation is configured as a trust anchor.

Since the root zone was first signed in 2010, we've had a single KSK and for purposes of this presentation to avoid confusion, we're going to call it KSK-2010. A new KSK is going to be used starting on October 11th, 2017. This is not the last time in this presentation you will see the date October 11th, 2017 nor will it be the last time you hear me say the date October 11th, 2017.

Because on October 11th, 2017, we will start signing the root zone keyset with KSK-2017, the new Key Signing Key. And so, that means work for anyone who's operating the DNSSEC validating resolver. It might be as little as reviewing our configurations to make sure that an automatic update happened or it might mean installing the new KSK manually.

Here's where we are in the project. Last October, we created the new key. I'm not going to have time to go into all the details about how ICANN manages the KSK but suffice it to say, it's securely stored in two places we call Key Management Facilities: one on the U.S. East Coast, one on the U.S. West Coast.

So, we created the key on the U.S. East Coast Facility in October and every quarter, we bring the KSK out, the current KSK, KSK-2010. We use it to sign ZSK. And so, there's regular quarterly cadence for the KSK where we have key ceremonies. And, we made the decision early on in this project because we're not in any hurry to roll the KSK we would do major events on this quarterly cadence when we have the key ceremonies. So that's why the key was created in October at the Q4 2016 Key Ceremony.

And then, in February at the Q1 2017 Key Ceremony on the West Coast, the key was imported into that facility. And at that point, we call it operationally ready because it's redundantly sort in two places and it's something we can depend on.

Basically, as of now, as of this phase of the project, out-of-band publication means we're telling people what the key is. It's not yet visible on DNS but shortly you'll see it.

Then on July 11th, that's when it will appear in DNS for the first time.

And then, on – let's see, when is the date? October 11th, 2017, that's the date of the actual rollover. And then, we will actually revoke the old KSK. And eventually, it will be destroyed, securely removed from the two Key Management Facilities.

So, that's the overall timetable of the project. So, where we are now is in the interval of course between the new keys created, we're telling people about it but it's before the rollover itself on October 11th, 2017.

I sense the joke might be getting old. That's part of telling a joke. You need to know when to move on.

So, here it is, this is big reveal. This is the most dramatic thing I can do in the presentation here. This is the public portion of KSK-2017. So, I say it half jokingly but indeed if you want to – if you need to configure the key manually, here it is and it appeared in this presentation, and you had me and ICANN employee telling you that I attest to the authenticity of this key. So it could be one of the pieces of information you could use, one of the factors you could use to decide that, well, this actually is the real public portion of KSK-2017.

So, sometimes you need to configure depending onto your validating software. You need to configure it as a DS record, so this is the corresponding DS record for KSK-2017.

Now, I want to talk just a little bit about how operators will get the new KSK. I realize we probably not have a lot of operators in this group but I want to talk about what happens because it's the most significant remaining portion of this project.

So, the good news about all this is that we are changing the KSK under good operational conditions. There's nothing wrong. We have no reason to suspect that there's any problems with the authenticity or the security of KSK-2010. And again, that's why we're taking our time doing things in orderly conservative fashion.

And, you can use the trust that people already have in KSK-2010 to distribute KSK-2017. This is a protocol called Automated Updates of DNSSEC Trust Anchors or just Automated Updates for short or RFC 5011 we call it for short because that's the document that defines the protocol.

As I'll describe here briefly, basically, if you trust the current key, you can use that to trust the next key. So under certain circumstances, if you have software that supports this, the KSK Rollover will be automatic from your perspective.

And the alternative is bootstrapping starting from not having trust in a key and that's when you would do things like trust the fact that the key appeared on the slide in this presentation and I said it was the legitimate key as a way to trust it.

So, the way this RFC 5011 Automated Updates protocol works is really very simple. If you trust the current key and you see the current key signing the new key, if you wait long enough to make sure that nobody is tricking you, and in this case, the wait is 30 days. It's called the add hold-down timer. If you wait long enough and have the old key vouching for the new key, the new trust is the new key and that's really all there is to it. The only, I guess, an issue with the protocol is that it does take a long, long time. You can't test it quickly and immediately if your infrastructure is doing the right thing because there's this 30-day hold-on timer. So, I'll talk a little bit more about that in a moment.

So, the timeline for this then is that the new key KSK-2017 you recall appears in DNS for the first time on July 11th. And, at that point, it will appear in the key set we call it at the root that holds both the KSKs and ZSKs. And so, at that point, it will be signed by KSK-2010 and that will start the 30-day add hold-down timer.

So, around August 11th, give or take a day, that's when anybody doing this Automated Updates protocol, their add hold-down timer should expire and they should now trust the new key. So, you can see that gives us plenty of time until October 11th.

So here just to prove it, we can put calendars on the slide is it's how that looks. You can see we have literally a full two months for people to confirm that they've got the new KSK if they're following the 5011 protocol.

To assist with this, ICANN released – it was just announced, David Conrad, the CTO announced during the opening ceremony yesterday that we have released the test bed to allow operators to test whether their validators can file this Automated Update protocol.

There have been other test beds that allow you to test this including one by my colleague, Rick Lamb, who's probably in the room. But the other test beds heretofore have required that you sort of speed up the RFC 5011 protocol that you artificially reduce your software's notion of what that add hold-down timer is. And we wanted to have a test bed that with all people to test it in real time.

We also didn't want people to have to test with the root zone because we can't legitimately sign a root zone to let people test that. So, the idea here behind this test bed is that we have a sequence of zones that are deep in DNS tree. You can see the zone name in italics there.

So, the current zone is actually – no, a bigger part and that's no longer the current zone but that's an example of one that big long zone name there in automated-ksk-test.research.icann.org, that is what you would configure as a trust anchor. So that's the zone from last week, the zone for this week, we have a new zone every week starting on Sunday. So, the current zone that's just starting the process is 2017-03-12.automated-ksk-test and so on.

So, every week, a new zone starts this process of a KSK roll, so it starts with a single KSK, another KSK is added, 30 days later, you should be able to validate with a new KSK because your resolver configuration should have properly updated, and then eventually, we revoke the original KSK.

So, the idea is that between now and Wellington next year, we're going to keep this operating. So, anytime you want to start, you can step on the 30-day treadmill as it were and you could even do this multiple times. You could have multiple zones going at once each separated by a week, so if there's something goes wrong, you have a chance to try again.

And the idea is that this would be safe for operators of production infrastructure to configure because it doesn't mess with the root zone. It's the zone that nobody is ever going to query anything but you could configure it, you could verify that indeed your infrastructure is doing 5011 properly. It does see the roll. It does write the roll, the new KSK disk. It survives a rebooter or restart of your validator software.

So, I don't have screenshot, I should have but I don't but go to that URL there and it's really straightforward in addition to the zones going through KSK rolls, what really drives the test bed is just a mailing list.

You'll get on the mailing list for that week's zone and it will send you instructions and updates. And it's not a mailing list you'll be on forever. We promise to automatically unsubscribe you at the end of that zone's KSK roll. So you get about eight messages with instructions and updates, and encouraging information and daily affirmations. No, not that. I made that last part up. So, that's the test bed.

Now, I realize that's – I need to stress that's for operators. And as I suspect, there aren't a lot of DNS operators in this room who need to test their infrastructure. So, a reasonable question at this point is, well, if I am not an operator and I'm also not a developer or a distributor of DNS software, I'm not somebody that needs to configure that new KSK. What do I do?

I guess the answer is there's not a whole lot you can do but you can at least be aware that this is happening on October 11th, 2017. See what I did there? I kind of did it. I kept the joke going just a little bit longer.

You could at least ask if you know a DNS operator or a software developer or distributor, anyone who would need to configure a package software with the new KSK, you could ask them do they know about it, are they doing DNSSEC validation, are they aware, are they ready? And then, you can direct them to the ICANN's website, which is here that has information about the status of the project, various documentation and we'll be constantly changing as we move through the project.

It's very important that we all get this right because we don't want David Conrad to go to jail or have anything bad happen.

All right, with that, enough of my talking and let's start with our panels. So, we have two panels as I've said. The first panel is the people you see up there and they each have short presentations.

Now, I'll go ahead and mention the second panel. The second panel consists of people who are Trusted Community Representatives. They actually have a role in the quarterly KSK ceremonies. And since a lot of those folks are here, we thought we would have a panel that would – I can't promise that I didn't drink out of that, so if you don't mind, [have at] it.

So, since we have so many TCRs here at the ICANN meeting, we thought we would have a panel so they could give their unique perspective on what it's like to be involved in the operation of the KSK.

All right, so with that, why don't we start with Joe Abley of Snake Hill Labs and he has a short presentation.

JOE ABLEY: Is this thing [inaudible] this? It is. This is how we do it? Oh, good.

So, seven years later, seven years ago, at about this time, we were a couple of months away from the first KSK going live in the DNS.

UNIDENTIFIED MALE: [Inaudible].

JOE ABLEY: What's happening? I think somebody has read my slides. I mean, that's what I'm about to say.

UNIDENTIFIED MALE: It's good to go.

JOE ABLEY: All right. I just gave these slides in about two minutes ago and you might think that I was taking the opportunity to actually speak my mind and say what I really think about the ICANN process seven years ago because it's time, and I am but it's not that interesting because it's all mainly good.

So, looking back over those seven years, when we designed these processes and I was a part of a team that focused mainly on the physical security, the Key Management Facilities, the alarm systems and the computing elements and networks. Not so much on the process that was really Rick Lamb's section. But we all work together as a team.

I think after seven years, we could look at this and say, even though we didn't have an awful lot to go on at the time, there wasn't an awful lot of public information about how you manage crypto secrets or run the CA. These things were largely done by commercial companies and kept everything very secret. In fact, we did a pretty good job.

I say, we, as a larger team with the smallest part of it came up with a process that is not only substantially the same today as it was seven years ago but it's also being flexible enough to be improved. We've had improvements suggested by people who watched the webcast from people who just visit the facilities during ceremonies, from TCRs who are involved in it, lots of tiny, tiny improvements that together make the whole thing stronger.

And, as well, we should probably mention that there's many improvements had been carried out by IANA staff, I can say IANA as a noun because I'm not employed by ICANN anymore, so I'm allowed to be free with my nouning.

And, for example, the original alarm system that was put in had some deficiencies. It works. There was no question that the security was maintained but it wasn't the best. It was difficult to manage. It was possible to replace that without compromising the security of the key without great fanfare, without flying people around the planet.

So, I think these are all signs that the process is a very good one. It's really robust. And at least if we imagine seven years on the Internet time, seven years is an enormous period of time, the fact that it still exist is substantially the same is a pretty good sign.

So, two sections for this – I only have four slides, so don't think this is going to be an enormous audio. But second I think worth mentioning is the people involved. So, first of all, obviously, the people from the community who for a long time volunteered their time and have no reimbursement for the travel that is changed more recently. But I don't think there's ever been a ceremony where there was a difficulty getting in the right number of people to show up in order to maintain the process. No corners had to be cut in any way about the number of people involved, the people who were selected turned out to be really good people, which means I think that the criteria by which they were selected to start with was pretty good. We have a good mix of part from some people.

And, it's all worked out remarkably well. And, as well as the TCRs, I think it's also important to mention that ICANN itself has had quite a bit of staff rollover in the last seven years. Most of the team – I would say most, probably most of the people who are involved in building this thing no longer work at ICANN. And yet, the processes are still maintained, the great accuracy and so obviously, this very, very good transition of process and procedure as people get hired. So, this is all the great big giant success story.

I guess leading up to the most important points, this is the second to the last slide worth saying that KSK-2010 has been well protected. I mean, the whole point of this system was to make sure that the private key for the KSK was kept in a secured way because if it becomes public, that kind of defeats the whole point of the whole thing.

It's been pulled out of the safe and used regularly. There's been the occasional hiccup in a ceremony, which has been dealt with professionally. And, I think this consistent chain of custody, unbroken chain of custody for the KSK from the day it was first created in Culpeper on July 4th or July 10th I think, July 10th, 2010, something like that until today. And, it will remain unbroken until the key is finally destroyed next year.

So this I think all these are old things leading up to the last slide, which is possibly the most important one, which is – that it's relevant. DNSSEC, whatever we think about the speed of growth and deployment is it continues to grow. People continue to use

DNSSEC. People continue to validate and it must go up. They maybe don't go up as rapidly as the number of the four addresses remaining go down but it's still going up.

And really, this is the ultimate thing, if the people didn't trust the KSK, then it wouldn't be relevant. And if it wasn't relevant, there'd be no point in any of this.

So, I think this is the biggest success from looking back to 2010 and seeing where we are today. We still have ceremonies. People still tune and they still watch them. That's still an ongoing interest in the trust to the system and the system continues to provide the security that it's supposed to provide.

So, I would say well done to ICANN, IANA and all the TCRs involved in the whole process.

MATT LARSON: Well, thank you, Joe. Why don't we wait until the end of this panel and then stop and pause for questions before the second panel.

So, with that, I guess Benno is next, please.

BENNO OVEREINDER: This is one of the – yeah, there we are. One of the players in the supply chain and one of the software providers in – the other software supplies have similar approaches and procedures, and things implemented in place. I can discuss this later also. It was done by other operators of software supplies.

So, how is the new trust anchor introduced in the supply chain? So, how did you get your updates – your software updates with the new key? And what, if you have run your resolver today and there's the key rollover?

Well, all right, I have something – anyway, this [criteria] it's been reformatted.

So, already gave something away, so I think I don't have to introduce these two pointers for the Unbound and I think for the other software providers. They implemented – well, actually, honestly, 5011 Matt just explained extensively. But also we, as a software provider, we have non-RFC 5011 Rollover. It's also specified in the SAC063 documents.

So, how do you run your network? So, if you don't run your resolver yet and has been a key rollover and you have the old key, how do you bootstrap your resolver and build trust?

And so, I can skip this one. The RFC 5011 has been explained, is being implemented by all the resolvers I know of. At least, open source and they also did the commercial. Not all the commercial

– no? Thank you. The one I know of but not all of them but the open source resolvers did do all implement 5011 resolver.

UNIDENTIFIED MALE: [Inaudible].

BENNO OVEREINDER: You can ask some questions or people can ask you some questions about. Good.

The non-RFC 5011 Rollover – so, what if 5011 fails or breaks in some way? And I'm now speaking for Unbound but the small procedures for all the resolvers. And we have something like Unbound-anchor.

But primarily, a software comes with an operating system and operating system suppliers, so they pack our software. They think of the RedHats, think of Debian being the source for – now, I'm completely blank, not [inaudible] but the [inaudible].

So, these packages, they take the sources, they take the new keys we distribute with the sources, the package – and distribute these binary packages to the distributions and they end up at your server. And also with automated operating always updates, so it's within new install office Automated Updates, you get with the software updates, also the new key material, the new trust anchor.

Even with your older system as old RedHat installations, we are discussing this also with our – well, with out context at the distributors – they will kind of deck boards, not probably the latest version but they will backport to trust anchors into the stable versions of their distributions.

We have implemented also another non-RFC 5011 Rollover in which we call it Unbound-anchor but they are similar. This is a program which test if the current anchor – if they can validate queries with the current trust anchor at your local resolver. If it does not, then… Let's see if I…. Right, yeah, that's exactly how it does.

So, Unbound-anchor, it test if the current trust anchor works. If not, it performs HTTPS fetch for root-anchors.xml and it's a well-known publicized websites by ICANN. IANA actually ran by ICANN. And it check the results within detached CMS signature. This signature is filled out until 2029, 2030, I don't know. Wait, 40 years ago, 40 years to go yet.

And, in this way, this CMS has been checked out of [bent], so we received a tamper-free envelope from ICANN with the CMS signature, so we did a visual check out of bent check. And this signature is also within our codes.

So, first, we check if the trust anchor works. If it doesn't, we fetch it from a well-known publicized public repository, we check if the trust anchor has been signed by ICANN. And if all checks are successful, we update the root trust anchor with Unbound-anchor.

So, this can be used if your site has been done for a period or you installed an old version with the incorrect trust anchor, Unbound-anchor will run your trust anchor, your resolver and you can go ahead. That's it. Questions later.

MATT LARSON: Yeah, we'll wait just a moment. Thank you, Benno. And then, Yoneya-san.

YOSHIRO YONEYA: First of all, I apologize this write is written in Japanese but I don't explain all of this presentation but I explain why I made this presentation at the Japanese community.

So, the awareness of root KSK rollover in Japan is not high. It is still very low. So, too broad this event in Japanese community. Japan [inaudible] operators group, JANOG is one with the very good opportunity to explain.

I try to have a [inaudible] in JANOG several times but the awareness of DNS operation was too very low in Japanese network operators community. So, I failed to have [inaudible] several times and I changed the strategy how to explain KSK rollover in Japan.

So, first, I tried to explain what is a KSK rollover but it is not attractive to the network operators, so I changed to how its impact to your network operations. So, I use the title as an IP Fragment is Forthcoming. Are you ready?

So, this title shows that IP Fragment is Forthcoming. So, the next slide, please.

I explain that this presentation is to announce the important KSK rollover dates and what will happen, and new explanation about the DNSSEC itself.

UNIDENTIFIED MALE: [Inaudible]

YOSHIRO YONEYA: Next slide, please.

I made a very strong notification on that. DNS or the IP fragmentation of DNS response is forthcoming and it will cause the name resolution failure of all of the Internet. Because root zone name resolution will fail. And, this slide shows when the IP fragment happens, so the important date is differ from the KSK rollover process itself because they pre-publish of the key may cause the IP fragmentation because it's – the response rate will exceed 1,400 bytes. And, some of the network devices will see such large IP packets. So that it is very easy to understand the network operators what happens.

Yeah, next, please.

So, it's very easy way to check if you are network [inaudible] devices will see the large IP packet just show the two method. One is Verisign website and one is a DNS work site.

Next, please.

And [inaudible], yes. And, I just said if you find your network equipment fails, then ask to your vendors or upstream, upstream ISPs [also]. And, if you find something wrong, then prepare as soon as possible.

So, this is backup site for the useful information. And, at that time, I said that if something happen to the root zone, then we have to have some very quick communication between operators, so we have – we'd [direct] to have communication channel, which is not depend on the DNS. So, I direct the talk it – the communication channel in this [manner]. Thank you.

MATT LARSON: Thank you, Yoneya-san and thank you for reaching to the Japanese audience. Because that as I said at the beginning of the presentation, we're in the stage now of this project where the most important thing is reaching operators, so people know what's going on.

So, why don't I pause and ask if there are any questions about either the update that I gave or for any of the three speakers on the first panel?

UNIDENTIFIED MALE: Yeah, I got a question. I don't know if I should be up here. I'm a journalist. [Marcus] from Bloomberg [inaudible], Maybe I should be sat down there.

This is for Matt. Could there be any disruptions to Internet services during the rollover time? I know you've said that it should go off smoothly but is ICANN making any contingency plans? And secondly, are there any concerns about possible delays to the rollover date?

MATT LARSON: Thank you. Those are two good questions.

So, we believe that we are in good shape in terms of communicating, which is as I keep saying, the most important part. The good news is that a significant portion of DNSSEC validation occurring is coming from a few large operators.

So, as long as Google, Comcast in the U.S. and various other nationalized piece throughout the world, as long as they know about this and they make the change, that gets the vast majority of people who are doing DNSSEC validation.

So, it's still possible that there are other people who won't get the message but we're certainly doing everything we can to get the word out. We do have contingency plans if anything goes amiss with the rollover, we have the ability to back out any phase of the project up until a point where we actually revoke the old KSK, which is a revocation is irrevocable that you can undo that.

So, did I answer both your questions? All right. Thank you.

Any other questions?

UNIDENTIFIED MALE: We have one on the floor.

MATT LARSON: Okay.

[MARCO PISOLI]: [Marco Pisoli] for the record. I have a question but it is not really strictly related to the rollover but the decipher of the key. If I understand well, you're replacing a [inaudible] key with another [inaudible] key. So, so far, it's still out of scope but enabling elliptic curve rather, is it right?

MATT LARSON: Well, we want to approach one thing at a time, so we want to get through the KSK rollover but I know there are people who want to talk about that. There certainly would be advantages to switching to an elliptic curve based on the algorithm in terms of the size of the keys that would give us potentially more flexibility.

So, it's something for what it's worth and I personally am interested in doing. But I think it's the sort of thing that we need to do after October 11th and that's also something that ICANN needs to listen to the community on. I mean, that's not the kind of decision that we could make unilaterally.

[MARCO PISOLI]: Thank you. Because in your opinion because we are not talking about the plan but only an opinion [inaudible] time, do we have to wait at least one year, at least two years, at least three years for this?

MATT LARSON: I really would hesitate to give any kind of a date.

[MARCO PISOLI]: That's right.

MATT LARSON: But I will say that I think it's a conversation that we can start having. I don't think it's too soon to – well, it's maybe a little soon. I'd like to get through October 11th but I think soon after October 11th, I think that's a very reasonable conversation to start having.

UNIDENTIFIED MALE: [Inaudible].

[MARCO PISOLI]: Thank you very much.

JOE ABLEY: A few of us, ICANN convened a few people outside ICANN to [inaudible] on the kind of the design team to feed into the plans that became the polished plans that you've seen presented today. And one of the sets of test we did was with Geoff Houston's Internet-wide measurement framework that I'm sure you've seen in various places and various forms. He was able to test and find out that the deployment of ECDSA in validators was not high enough to be able to roll to elliptic curve key. In the timeframe we're talking about right here would cause more breakage simply because we have a long tail of software on the validator side that takes a long time to upgrade.

So really, I think the practical answer to when do you think we could switch to elliptic curve, if we want to be able to do it without disruption, it's an answer that depends on other people's choices when it comes to a grading software. It's not really anything that ICANN can control.

MATT LARSON: All right, any other questions?

UNIDENTIFIED MALE: We do have another one on the floor?

MATT LARSON: Okay.

UNIDENTIFIED MALE: Begin.

NIGEL CASSIMIRE: Yes, Nigel Cassimire from the CTU. Does anyone else apart from network operators need to care about this?

MATT LARSON: Well, I'll go ahead and take a stab. I mean, certainly, operators have the most direct work to do. And to be clear, it's people who are operating software that has DNSSEC validation enabled, so not… That's by Geoff Houston's estimates, that's about 15% of the population that he surveys and the vast majority of that is Google public DNS.

So, it's only people who have enabled DNSSEC validation that have any action. As far as the rest of us, there's no direct action we can take is really what it boils down to.

UNIDENTIFIED MALE: [Inaudible].

UNIDENTIFIED MALE: Besides educating and outreaching, and spread the word, I think it's what we have been doing in forums for the last, I don't know, almost a year already.

[BENNO OVEREINDER]: Sorry. I want to add on that indeed, so thank you. So, for me, attending the [RIPE] meeting. There have been outreach at the [RIPE] meetings where many operators also attend this kind of meetings. And, it has been explained what is coming ahead and also in the next coming [RIPE] meetings, there will be more attention for the practical implications, what does it mean for your resolver, etc.

So, there's a lot of outreach to – well, regional operation communities and maybe also national [inaudible] and that kind of thing. That's important.

MATT LARSON: All right, why don't we move on to the second panel and I would hope we have time after that panel to take more questions if there are any?

So, as I said, the second panel consists of people who are Trusted Community Representatives or TCRs. Let me give a very, very brief explanation of what they do. Joe mentioned in his presentation but at the Quarterly Key Ceremonies, the way the system was designed requires like literally physically requires that members of the community, these TCRs be present in order to enable the cryptographic hardware that stores the KSK.

So, ICANN literally cannot perform a ceremony and use the KSK for signing unless a minimum number of the TCRs are present. And there are seven for the East Coast Facility and seven for the West Coast Facility. And so, we have a combination of East and West Coast folks here now.

So, first, could I ask everybody on the second panel, could we just go down the line starting with Dmitry? Could you please just give your name and affiliation, so people know who you are? And then, I know Ólafur has something he wants to say to begin the second panel.

DMITRY BURKOV: Just as a short – first of all, I want to support from very important point, which was expressed by Joe Abley because when we began all the story, its first question was about trust because for dozens of years, the DNS root zone exist on some simplified basic principles. First time at new [inaudible] and it was a key point key challenge.

And, for me, [inaudible] this is now a well-established ceremony. He's more trustable. He has the technology deployment. In fact, this still is the beginning because it's not so easy. It's [inaudible]. You'll try to estimate how many IETF standards were deployed worldwide during [close to] 20 years if we will find it.

And, it's a base for potential future use worldwide this technology on the – and the real obligations. Because now, I want to say from my opinion, my point of view, and don't expect any stress situation in the root KSK rollover. Maybe I don't know what's inside U.S. government. It was about strict validation requirements on such [inaudible] can be sensitive.

And, I want to say the best [words] about the people who are now inside ICANN but who did a lot during initial deployment and development of the DNSSEC is beginning from key documents and implemented on both side in this process. Thank you, guys.

JOÃO DAMAS: João Damas currently working for APNIC. I've been the CR since the beginning and continue to watch and participate in this process. Also, in following the rollover process itself, I think as part of carrying the word trust in the Internet interval means that you have to basically spend some time following things. And so far, everything seems to be done thoroughly and with thinking about what we think not only about the scenario where everything goes as it should but also the scenarios where things might happen.

First of all, I do have a lot of confidence in how this process will unfold. The trust that is put in this whole system is derived from being done in public really apart from the private key, which is obviously not shared but no one can actually look at it because it's designed to be so. The whole thing is done in public.

Actually, I wouldn't – as mentioned, ICANN can indeed access the keys without the TCRs because the process is not meant to block for instance access in an emergency if something were to happen where they needed the access to the key. They would be able to. What they would not be able to do is to access the key and detect it.

So, they would have to explain why this happened because we would be able to tell if an access outside the process took place, and that's where what creates stress that everything is happening clearly and [inaudible]. There is the [abbreviations], they are detected and can be then analyzed and reported.

I think that's it for now.

ÓLAFUR GUÐMUNDSSON: Hi, I'm Ólafur Guðmundsson. I'm from CloudFlare. I've been a TCR for three years. I was with [inaudible] before that. I've been working on DNSSEC for a long time and this is one step in the process of getting the protocols rolled out, getting trusted and getting out there. This is really important step. It's a little bit overdue and I want to talk a little bit about some of the operational things that might go wrong that… yeah.

And, it's very important because if we don't get the rollover key, then we are stuck with this one key forever. We have one chance to get the process right and this is it. And then, so far, everything we're doing has been on the conservative side and try to do it absolutely right.

So, Matt has mentioned the date here a few times, October 11th, but he has left out a very important detail. And when I asked him about it beforehand, he said he didn't know the answer. So, the question is, what time will the new key become available? Because when it becomes available on the first root server, that answer – that starts a clock – a window when things can start going wrong because a new key is in use.

Before that even happens, there are a few things that could theoretically go wrong. The only thing that could really go wrong is somebody takes in the new trust anchor and delete the old one. Based on the experiments people have been doing, that hasn't happened but human error might do that. So, that has to be checked for.

Once the clock hits and the new key is published, will everything go to haywire at that moment? No. The current root key has a two-day time to live and cache it. So, over the next 48 hours, the various validators will discover that they are not in compliance or working. And, that is the window where people will start seeing it. And if you're operating multiple validators, I can guarantee, they are not going to avail at the same time. One will go first, then the next one, then the third one and up to however many hundreds the large clusters have.

So, the errors will start showing up. There will be indicators. Hopefully, operators will notice it because they are watching and have time to react. There are a number of things they can do to fix it. On October 14th, we can start partying because it will have worked, hopefully.

So, the best thing that can come out of this process here today is all of you who don't speak English as a native language and if you're from countries where people don't speak English, is you'll tell your community about it. Like Yoshiro there in Japan, do it to your communities. Make sure information that this is happening is available in your community, in your languages. Write blogs. Get articles published. Tweet about it. Whatever it takes, go to conferences, spread the word. I'm sure the English language community is fully covered. I can talk to the Icelandic one but you can talk to yours.

So, spread the word and nothing is going to go wrong. We can talk about what is going to happen. It could be somewhere between a total fiasco unlikely or a [inaudible]. Because of the preparation, I'm very confident it's going to be very close to a [inaudible].

There will be minor incidents here or there. For example, if I answer the prior question what can go wrong, well, if you happen to be one of these [inaudible] who run on your own Recursor at home, that is validating, it may not get updated and your spouse may yell at you. That is not a big deal for the rest of the world. For your marriage, maybe. Thank you.

MATT LARSON: Could I just jump in and address the question that Ólafur said he asked me a moment ago, which is what time on October 11th? And my answer was, well, that's not completely an ICANN/IANA decision. Without going into yet more details, people may be familiar with unique arrangement that is used to maintain the root zone. It's a partnership between ICANN, IANA and Verisign. Verisign is really the root zone maintainer, so they hold the ZSK and they generate the root zone on a twice daily basis.

So, I'm going to put him on the spot but Duane Wessels is here in the room from Verisign. And, could I ask Duane what we had Verisign given any thought to timing?

DUANE WESSELS: Yeah, thanks, Matt. I believe that we have discussed this at some point in our planning meetings between Verisign and ICANN. And, as everyone can imagine, this will be a very exciting day for everybody and we'll be paying very close attention. So, the zone file that gets published that day will get a lot of attention, a lot of manual inspection and I expect that there will be some kind of call or something with parties from ICANN and Verisign. And, really, the timing is sort of up to you or up to us. We can decide the time. We can delay the normal publication schedule and decide the time at which the zone gets pushed out to be determined.

Thanks. Yeah. So, I think the answer is we will figure out an appropriate time and let the community know so that it's not only October 11th but we can offer a very specific time on October 11th.

YOSHIRO YONEYA: Can I jump in? So, not only October 11 but the September 19th is also the very important date because the DNS [inaudible] size increases, so it may cause the IP fragment. So, I [direct] to know the exact time also.

MATT LARSON: That's a good observation. I didn't know that we had so little time, didn't talk about packet size issues. I noticed you talked about them. My Japanese is not real good but I could tell what the slide was about. And, Yoneya-san is absolutely right. For the first time in the history of the root zone, we will have four 2048-bit keys in the key set. The Zone Signing Key will be undergoing a roll and of course, the Key Signing Key will be as well, so there'll be two ZSKs and two KSKs. And that first happens on September 19th, and so that will be a historical maximum size for the key set at that point.

There is a possibility that that will be passed a threshold size-wise that some people aren't able to hear the response. And so, it's possible there'll be fragmentation. It's possible that there'll be issues. So, that's a day that's on the project team's radar as something to be aware of. We're almost certainly going to do special data collection that day and we're watching carefully.

And so, I would say the request to give a specific time for zone publication for that zone where that first happens, I think that's a very reasonable request and I'll go out and [inaudible] speak for the project team. I think that's something we can do with Verisign's cooperation of course.

UNIDENTIFIED MALE: May I?

MATT LARSON: Yeah.

UNIDENTIFIED MALE: So, just to add one more [meat] to this whole thing. I mean, ICANN is certainly engaging in [inaudible] that is to be expected from an organization in a process like this. But there's also a limit to what any given organization can do.

So, with that part covered, if you are an operator of a DNS resolver and you have decided in the past or someone else decided for you that you should activate validation, you actually also created a new responsibility for you if you are providing this as a service to your customers or to some other population. And as part of the responsibility, it is your duty to verify that these things are going to continue to work. So, it's not only an obligation on ICANN to voice things in a high voice but also you as a resolver operator have an obligation to be able to listen to these things.

This other thing that was mentioned by Yoneya-san just now is a little bit different because it doesn't involve either ICANN or the resolver operator. It's got to do with the network between. And so, you could – ICANN can [inaudible] as it wants, the operator be listening and be prepared, and still thinks it might fail because of whoever is providing you with Internet access.

So, what's the resolver operator to do in this situation? Basically, the test beds are out there. Test these things early. Don't wait for the last minute because there are factors that are not – don't depend only on you, so that's probably something that we haven't voiced so much but is clearly – there's a need to communicate it because none of the parties that we are talking about actually are the ones involved in creating these potential issues.

FREDERICO NEVES: Hi. My name is Frederico Neves. I work for the Brazilian registry and I have been doing this DNSSEC thing for a while as a lot of people here as well.

We started signing the BR zone before the root was signed. And then, when the root was signed, then we were rolling our key. We had this same experience trying to reach out especially the local community regarding this change of key and the removal of those [inaudible] root zone that time in their resolvers and we have quite of them already doing validation in the country.

So, we have been trying to do this for operators meeting in the country and in our language. And, the fact is that the way the processes have been conducted by the ICANN and by the community I think is definitely it will be as Olafur said. I know [op] situation in the October 11th, 2017.

And then, from the perspective of someone that is a trusted community since the beginning, it's a lot of time as you all said, it's quite time – it's not quite a little bit of time – it's a lot of time. It's not quite sometime. You have to travel. You spend at least three days in each ceremony and to get there, if you don't live in the U.S.

And so, there is a lot of effort put by the community to make sure that these keys are really used in the correct way and we do actually have an audit trail of the use of the key. And as others said here in the panel, we are really confident that we have been doing a really good job in taking care of this key. And, definitely, this process and the care that we are taking for this rollover will finish in the correct way and in a good way.

ALAIN AINA: My name is Alain Aina. I'm one of the three TCR from the African region acting as crypto officer because there is a different group inside the TCR acting in different role.

So, yes, I've been lucky to be part of the process since the beginning and I'm lucky to be selected to serve as the crypto officer. And as João presented and Joe said, the system is well-designed and I think we have all rights to trust the system, trust the people, trust the infrastructures and I think we shall also trust in – for the key rollover process. For sure, as Frederico said, for sure, it will go smoothly. But we can also trust them to manage the new KSK for maybe the next five years. We don't know yet. But hopefully for [inaudible].

But I think for this KSK rollover, one thing we also need to look at is, for sure, as many people said here, things may go wrong in terms of updating the trust anchor and people may go manual update. And this bring the issue of how do you fetch, how do you authenticate and then, you said it, how do you authenticate the key. Because for sure, around that date, Matt, your date, the 11th [inaudible], we will see many KSK flying here and there. This is the key. This is the key. Take this [inaudible].

We need to make sure people know where to get the right key from, how to authenticate, etc. So, I think this is something I want to focus on in my region from now to at least June or July. Thank you.

MATT LARSON: All right, thank you, Alain. Thank you to the whole second panel. And so now, why don't I open it up again for further questions about anything we've talked about or addressed to any of the panels? Are there any other questions? I see one. The mic is coming around to you.

UNIDENTIFIED MALE: [Inaudible] Sorry for not speaking in French because we said English was covered, Japanese had some, so I was – but next time, I will go in French here and then who go in Portuguese?

ALAN BARRETT: Hi, I'm Alan Barrett. I'm from AFRINIC. I would like to tell our members that they need to be ready for this but I'm not sure exactly what to tell them. I've seen lots of details about what's going to happen in the center. What's the IANA going to do? What are the root zone maintainers going to do? But I have seen very little about what the end users have to do.

I think I'm looking for something like if you're running such and such software, then make sure it's at least this version. If you're running such and such other software, then make sure you download this little add-on file. If you're worried about your cell phone, then don't worry because it's all automated. Something like that directed to end users. Is there anything?

UNIDENTIFIED MALE: If we are to give advice to your mother, what she needs to do to prepare for this momentous event, nothing. If it was for your kids, we'll have hacked up your network with validating resolver. You should tell them, "Is this going to work?" That's the question.

So, for the end users, there's nothing they can do. It is the core. It seems they have their act together. We have to get the middle to pay attention and do the right thing. How to talk to them? I don't know.

Benno, for example, as a software vendor could put up explicit instructions on their sites that could come out with security releases that say that they switch to the new key and there are all kinds of things like what would be useful.

I can write blogs.

ALAN BARRETT: Yeah, right. So, I guess I'd like to see some kind of a table or a list showing that the software, which we know is in common use and the versions of that software that we know should support this, so that I can tell my members, "If you're running an ISP or you're running a network at the university, make sure you're running the software that supports it."

UNIDENTIFIED MALE: Yeah. So, I think I'm not good at the numbers but I think RFC 5011, so with the first thing, what should you advice you need to do? Make sure that the resolver is running up and ready, so 5011 can take place.

But I'm really bad at numbers but I think RFC 5011 is already implemented for many versions [inaudible]. So, with most table for OS distributions in [inaudible] or Linux, it's all fine. For Windows, well, we don't know about the packet size of Windows software for bind for that sake. We distribute for convenience a 64 and a 32-bit locally but that's the exception.

Yeah, run a recent OS distribution, keep your resolvers running. And indeed, it's good for us that the software community developer, maybe make very explicit which versions from which versions on RFC 5011 was implemented.

And, I know from my colleague software developers that all the past month in February, they did release new – well, source packet size of course with the new key, the KSK-2017 included and it's up to the OS distributors to pick up that one also.

UNIDENTIFIED MALE: Yeah.

UNIDENTIFIED MALE: And so, very last comment, I did talk with one of the software distributors and they are very aware of their role in this, and they will make sure that before 20 – sorry, what was the date here on that?

UNIDENTIFIED MALE: I believe it was October 11th, 2017.

UNIDENTIFIED MALE: Yeah, before October 11th, the distributions will be updated with new key.

UNIDENTIFIED MALE: So, I think what I'm getting from this is search the documentation for your software to see whether the number 5011 appears. And if it does, then you're fine.

MATT LARSON: Well, you have the – hopefully, high potential to be fine but that's one of the reasons that we created the test bed that I mentioned so that you have a way to actually test, "Am I going to be fine? Will the 5011 support work as expected?" We're not worried about bug and Unbound, not doing 5011. We're more worried about somebody got the permissions wrong and so maybe 5011 work but it couldn't write the trust anchor back to disk, so it worked within Unbound, restarts when they reboot and then it doesn't work. So, that's the whole idea behind the test bed that you have a way to actually test.

And if I could make one more comment, one of the things that I've realized this week is you saw only a small fraction of the presentation material we have that this phase is aimed at operators. So, we have a whole bunch of more detailed information in Slideware to tell operators, "Here's the context. Here's what you need to do." Talk about various implementations and things.

And, what I've realized is that we need that in [prose] form on a webpage and a blog post, so that when you ask that question, I can say, "Well, maybe not for end users but for operators. Here's the link for operators to know. In prose form, here's what you need to know, here's what you need to do." And I've realized that that's something we need to produce.

JOE ALBEY: I have a little comment.

MATT LARSON: Thanks, Joe, yeah.

JOE ALBEY: I can make an admission in the year 2000, I was working at a phone company and – in New Zealand actually. [Inaudible] the first big phone companies to cross Y2K, and so Y2K was a big thing at that time.

And, what made project managers at the phone company very happy was to have Y2K compliance statements from the vendors. They were very simple. They were the simple format. You could basically enumerate this is all the software we've gotten. Do we have a statement from each one of them? Is it compliant or does it need to be upgraded? Do we need to schedule some work?

And that made a very simple process for making sure that you're going to be prepared for this thing. I think when they have – Alan is saying, is you could make that yourself but it would be awfully convenient if there were some – given that we don't have that bigger diversity in the kind of DNS software that's in use on the Internet, it would be awfully convenient if someone like ICANN could produce a matrix like that, which we could just point people at and say, "If I'm running [Mind] and it's version 4-point something, then that's bad. You need to do something. If it's version 9.11 or higher, then you're fine." Then that would be much more straightforward than saying, "Read these dense cryptic documents."

YOSHIRO YONEYA: So, I have one advice to the end users. If the end users uses a very old home routers, many home routers running DNS [inaudible] what DNS resolvers inside, so it will cause [alert]. So, if users using a very old home router, they should replace the new one.

UNIDENTIFIED MALE: Next.

[ALLAN]: Hi, [Allan] here from Internal Registrations. Just a little bit of history – a historical question, the new 2017 key is going to be trusted or we expect to trust because it's signed by the 2010 key. How did everybody come to trust that key in the first place?

MATT LARSON: Well, you can search various places and – like for example, you can find on the blog from my podcast, it sounds like I'm pitching my podcast but I'm not. I won't say the name. That was sort of the most permanent place on the Internet that I had. So, PDP signed a statement that said – I was in the room when this key was created with this cryptographic cache and I attest that it's right.

Now, I'm one guy that some people know but the idea is you could build at the stations like that. You could find them and know that people you trusted said, "Yes, this is the key." I literally had a t-shirt that had the key on it. It's probably time to roll the key because my t-shirt has literally worn out and I've thrown it away. I'm looking forward to a KSK-2017 t-shirt. But you could literally find t-shirts, the RIPE NCC if I recall they made t-shirts.

So, on the one hand, it sounds kind of funny, "Oh, yeah, t-shirt." But literally, if somebody went to the trouble and a RIPE NCC person handed you a t-shirt that says RIPE NCC on it, chances are pretty good that that's the right key. So, it was a combination of informal and more formal communications like that.

But you point out bootstrapping trust is a difficult thing and it collides with the real world right there. Things in the real world have to happen in order to bootstrap trust. It's not something that can be done necessarily completely from the – or electronically.

Do anybody else have any questions?

UNIDENTIFIED MALE: Yeah, let me add. For historical reasons on both ceremonies in 2010 and 2011, we made another station of the process. We signed the public part of the key. We have a paper with the signature of everybody that was there and we have pictures of that as well. And, that's part of the bootstrapping of the trust. If you trust the people that was there.

UNIDENTIFIED MALE: Yeah, and this is software developer [inaudible] resolver, so you actually distribute your software with the root key. And so, we didn't [read] Matt's t-shirt. But we got out of bent, a paper, a letter with the root key signed with the CMS [inaudible], so tamper-free.

So, we had out of bent communication with ICANN that this was the root key that was advertized and published by ICANN. So, just to double-check.

BENNO OVEREINDER: I think I could take one comment.

JOE ABLEY: One comment, Benno raises an important point that I probably should have said first in my reply, which is that many, many people get the key from their upstream vendor whoever that is.

They install Unbound, they install Bind and it comes with the key. So, for many people, they're basically relying on the trust that they've placed in however they obtain their software or get their operating system update.

So, I gave sort of the security nerd DNSSEC nerd answer but the practical answer for many people is they got it from whoever they get their DNS software from, and they got it automatically and maybe didn't even realize they got at that way.

UNIDENTIFIED MALE: Sorry, yeah, I realized that the questions will be more fair to call them practical. But just supposed I've got that 2010 key, I'm not happy with it, I know someone went to the conference have got the key. Post in two years time, I'm building a brand new resolver from scratch, where's the reference for the new key if I haven't got the old key, if I haven't got the signature of the new key from the old one anymore?

JOE ABLEY: So, there is actually a document that describes how you bootstrap a validator with no previous trusted items at all. This is actually what was originally implemented unbound-anchor. So, there's a series of levels of trust. Some of them are somewhat weak, for example, the TLS certificates that you use for downloading the XML from the ICANN webpage that provides you some sort of channel security, it doesn't provide you with any confidence in the integrity of the data itself.

The data itself is signed in multiple ways, will this in PDP signatures, this – it was originally envisaged that significant vendors would build a relationship and a process with ICANN. So, for instance, Microsoft would come, inspect the processes in some sort of way that preserve the chain of custody and then actually use a signing key to record that trust at which ICANN would also publish. So, for example, a Microsoft device retrieving the key would have a part of trust similar to the way that the code is signed that it's built from. So, the trust in the key is equivalent to the trust in the browser itself.

So, I don't know – I think the extent to which this has been implemented varies widely between different things. Unbound actually was an early implementer of this thing. Other vendors have decided to kind of hardcode the key in recognizing that doesn't change very often and hoping that they can hardcode future keys in [inaudible] 5011 or something in the future.

So, there's a variety of methods but it's not just the case that you need to know somebody who went there. They're asked some cryptographic methods, too. It's fair to say they could be more widely exercised I guess.

MATT LARSON: Yeah, ultimately, you have to trust somebody. It's just a question of what's the starting point of the trust that leads you to trust in the key? I personally would trust my blog posting.

All right, well, we're one minute past the time. The session goes until 6:15, right?

UNIDENTIFIED FEMALE: Yeah.

MATT LARSON: Yes, okay. So, I'd like to thank everybody for coming. I especially like to thank the panelists and thank you for your time at one of the last sessions of the day. And I know I've stretched the joke but October 11th, 2017 is the date you need to know. Thank you.

[END OF TRANSCRIPTION]