HYDERABAD – DNSSEC Workshop - Part 1
Monday, November 07, 2016 – 09:00 to 10:30 IST
ICANN57 | Hyderabad, India

JULIE HEDLUND: Workshop, and I'll repeat this, but as you sit down, you should have a program, and on the opposite side of the program is a ticket. It's a ticket to lunch. Lunch will not be in this room, it will be at the Novotel at the La Cantina restaurant, and you will need a ticket for the lunch. So, if you plan to come back later for lunch or if you plan to go to lunch, you will need that ticket so please do hang on to the ticket.

Welcome to those coming in the room. We have plenty of seats up at the main table, and you're welcome to join, except for at the front of the table where we'll have the presenters. Please come on in and take a seat, and we'll start in just a few minutes. Thank you.

Welcome, everyone, to the DNSSEC workshop. My name is Julie Hedlund and I'm with ICANN staff. Normally, we would have Dan York from the Internet Society as our master of ceremonies. He unfortunately cannot be with us, so I will be a poor substitute today. Sorry about that.

At any rate, welcome, and we'll start right away on time in order to keep us all on time. We've got a lot to cover today, but I do want you all to pay attention to the back of your program. If you want lunch, there's a luncheon ticket there, and you will need that ticket in order to get into lunch. Lunch will be at La Cantina at the Novotel. It's just about a five to ten-minute walk away. That will be later on, but do hang on to that ticket. Now, without further ado, I'm going to turn things over to Wes Hardaker to kick us off. Thank you very much.

WES HARDAKER: Thanks very much, Julie. And welcome, everybody, to the DNSSEC workshop. We'll spend the first 15 minutes going over a little of how DNSSEC deployment has improved since the last ICANN meeting, especially the ccTLD deployment has been, and get to know a little bit more about all the numbers associated with those deployment stats. Go ahead, Julie.

First off, thank you very much to the Program Committee who is responsible for selecting the presentations that you'll see today. It's a wonderful set of presentations. I myself am conflicted today, so I'll be in and out all day, but I will be here any moment that I do not have a conflict. Thanks very much.

Next.

Thanks a huge amount to the lunch sponsors. They do a great job so that we can continue our conversations during lunch. So, thanks very much to Afilias, CIRA, Dyn, and SIDN. We always need more sponsors, so if you want to be a fifth sponsor for 2017, we'd really love it, so please contact Dan York at York.isi.org.

Next.

The DNSSEC implementers gathering, we had a great attendance last night and a lot of great conversations. Thanks very much to Afilias for hosting that last night, it was a wonderful gathering with some food and conversations. We thanked him last night, but thanks to Jim Galvin and the other Afilias folks that helped organize it.

Next.

The DNSSEC workshop and associated activities of ICANN are an ongoing organized activity of both the ICANN Security and Stability Advisory Committee – SSAC – and it also gets a lot of additional assistance from the Internet Society Deploy 360 program, so we thank both of those supporting organizations for making this day possible. It is always a day full absolutely fantastic information. Everybody you've seen on the previous slides are all responsible for making this day possible.

Okay, next.

You should have the agenda in front of you. It has little colored bars on it with green and blue. Make sure you keep it, as it is your lunch ticket as well. The green bars are indicative of sort of a beginning session. Easy to understand if you don't know a huge amount about DNSSEC. It's a great time to learn.

The blue bars are sort of more the intermediate level, and the gray are expert level. That doesn't mean you shouldn't come and it doesn't mean that you won't learn something, but it is a little helpful if you have a slightly more detailed background in DNSSEC as you go up in the class.

Next.

Let's go on to DNSSEC deployment around the world in terms of numbers and how things are going. First off, this is the use of DNSSEC validation around the world, and you can see that it has been going significantly and steadily up. If my eyes remember the screens when I was looking at it when I could read it, that top of the line on the right is a little over 15% if I remember correctly.

So, it's steadily increasing and validation is the key. We can get as much deployment on the signing side as we want, but it's sort of useless without the validation side, so this graph is a measurement of the validation side of things, and it's good to see it continually going up and up.

Next.

This is a list of various TLDs and when they had put their DNSSEC validation – various regions around the world that have DNSSEC validation in place, the percentage of that validation that makes use of Google's public DNS service, which also happens to do validation as well. We thank Google for their increased support to produce DNSSEC validation around the planet. It's been highly helpful that the instant that popped up, we got a huge uptick in validation.

There's interesting stats there, and we'll actually go on to the next slide, which points out a couple of interesting regional ones. Specifically, there's number of places where there's actually minimal use of the public DNS. A lot of ISPs actually decide whether they're going to use the public DNS resolvers or not and offer it to their clients, and then there are, of course, a lot of regions where users actually know about it and intentionally use Google's public DNS.

But these particular list of – it includes Nepal, Bangladesh and Afghanistan, India, the Maldives, Iran, Shri Lanka, Pakistan, and Bhutan – actually don't use a huge amount of public DNS, and it actually means that they are validating a large percentage of the validation actually comes from real world deployment there. So, it's specifically nice to call out that that region of the world as

promoting validation without necessarily relying on external infrastructure.

Next up, we have sort of the number of signed TLDs, and the root is the red bar on the left. The nice thing about the signed TLDs is that because of the New gTLD Program, all new gTLDs must be signed in order to get approved. It's a very high number, we're at like 90% of the root zone is actually contains TLDs which they themselves are signed.

Specifically, there are 1349 TLDs in the root that have signatures within their own zone data out of 1509. Approximately – the second level domains that are signed are actually running around 5-6%. Considering the number of second level domains, you have to realize that that's actually a very big number.

Over half a million zones and I think .com are signed, and that's a huge number of zones. However, of course, .com is composed of many, many, many more than that. And then, of course, there's the approximate number of users validating we talked about before, which his a third of the red bars. And then the trend of signed TLDs is the bar on the right, and you can see where the New gTLD Program started, as the new gTLDs were slowly introduced over time. A few would be introduced every week or so, and because every single one of them had to be signed, you

can see that the ramp goes up all of a sudden, right when that program started.

Okay, next.

This is a list of some of the important top-level domains. I'm going to skip this list, because I need to talk to the generator of it. It's actually slightly broken statistically. The number of signed second level domains within it is correct, but the total count is actually incorrect, which is why you will see things like – I'm really happy that Sweden has 838% of their zones signed. It's hard to have more than 100% of your zones signed, but Sweden accomplished it. It's actually a collection issue with Rick that we will have to work out, so we're on to the next slide.

Double signing, there you go. They're using multiple keys per zone. I'm trying to remember what this one was. I looked at it last night. Can you [inaudible]?

JULIE HEDLUND: Yes. You should probably be sitting next to her.

WES HARDAKER: Oh, that's right, okay. This is a graph of the registrar breakdown and which registrars are responsible for signing that are helping sign the zones underneath their infrastructure. You can see that

there's actually a different percentage of each registrar kind of has. Some registrars have a little bit more underneath.

Some registrars actually sign by default for any client that registers beneath them, so they have a great big bandwidth out of that pie shape, and other ones use slightly less. But it's very important that if you're working with a registrar that doesn't support DNSSEC that you ask them. That's how we're going to get all of the registrars enabling that capability. Make use of the ones that do, of course, and please ask the ones that you think that aren't actually implementing DNSSEC themselves.

Alright, so we're going to dive into some maps now that are showing sort of the ccTLDs and their regions around the planet in terms of their status. There's four or five different colors that these maps all depict. One is if they're beginning to experiment with DNSSEC deployment, they get orange, and that usually means that they have a second zone that they're experimenting with but it's not their real zone, but they're planning on doing something.

If they have announced it but actually haven't started the program, they're in yellow. Partially signed means that their data is actually signed, but they haven't put their DS record in the root, which is the secure linking between the root and their zone. Maybe they have signed their zone, but without that link in place,

you actually won't be able to validate data from the root all the way down to their children.

And once the DS is in the root, then they get the light green color, and then finally when they're accepting signed delegations, in other words second level domains can actually register underneath them and they have a DS in the root and they have committed to it, then they get the dark green color. So that's what we're shooting for, we want everything to be that wonderful dark green color.

Next.

This is sort of the world view, and you can see that there's a huge amount of fully operationally committed DNSSEC ccTLDs, which is fantastic. It happens to do more with landmass being – the larger landmass countries happen to be doing DNSSEC, which is wonderful. We're going to dive down into each region next, so go ahead.

Here is Africa and the deployment of each country within Africa and their ccTLDs. You can see that there have been a number of dark greens as well as light greens, so there's work in progress going on there. Senegal was the last one in that region to deploy. This has happened since the last ICANN and it was in September just last month.

Next.

In the Asia Pacific and Australia region, you'll see that Singapore has been added since the last ICANN, also in September of last month, so they're now dark green as well.

Next.

Europe doing outstandingly well. We love seeing maps with that much solid green. This is absolutely fantastic. If you look at the map of Europe, almost every country in it is green. There's actually nothing new, because once you get fully green there's nothing new to add since the last ICANN, but they're getting really close.

So next.

South America also largely green. There's a few holes which haven't actually started yet, but there's a number that are pushing their way. Nothing new since the last ICANN, but still great progress in that region.

Next.

And then finally, North America. Which there's not a huge number of ccTLDs in North America, but the United States and Canada are both fully operational, and Greenland has their DS in

the root but they're not yet accepting second level domains as we talked about.

Next.

If you're interested in receiving those and following those maps – they're interesting to look at – you can go to that URL on the screen, which will take you to the maps. On a regular basis, they're updated, I think monthly. You can also send update requests to Dan York at york@isoc.org. If you think that any of these countries – if you are one of the responsible parties for a country and you want to disclose your plans or say that something has changed, if you think your color code is incorrect, he's the person to contact to get that corrected.

Next.

A quick couple of statistics about DANE, one of my favorite projects. DANE is the ability to tie cryptographic verification of certificate authority-based X 509 certificates or just even X 509 certificates that are self-signed into the DNSSEC tree. There is a number of great security properties that this helps with.

If you haven't heard about it before, there are some documents you can read, but Viktor Dukhovni is one of the primary pushers of the DANE technology, especially in SMTP servers where mail is

transferred. He keeps a record of every SMTP server and whether they had published TLSA records.

There are over 102,000 domains with TLSA records for SMTP. That is astronomical. We don't have a graph for this, unfortunately, but if you compare the graph of this to the graph of DNSSEC deployment, DNSSEC deployment kind of goes up slowly over time. This one looks almost exponential, it's just doing this gigantic curve and it's served by over 2200 MX host which is an absolutely fantastic number.

Speaking of DANE for SMTP, the NIST department in the U.S. Federal Government has actually just published a document called 1800-6, which is DNS-based e-mail security, and it talks about DNSSEC, DANE and S/MIME A and recommends the use of it.

So, we thank NIST very much for their increased encouragement of the deployment of DNSSEC and by adding DANE and S/MIME A into that recommendation block that they have published.

Next.

Finally, the IETF 97 is coming up in a week in Seoul, and every Saturday and Sunday before the IETFs, they always hold a hackathon. There are a lot of people who get together in a room and they work on whatever projects they want. There happen to

be a lot of people working on DNSSEC, DANE and DNS privacy at these hackathons. In fact, probably half the people in the room are coding related to that.

If you're interested in helping join some project and coding for a day sitting in a room with a whole bunch of other wonderfully smart people, there's things for everybody to do, so don't feel shy if you're going to Seoul and you're going to be there early enough to help. They would love anybody's help who can be there.

Next.

The DNSSEC history project is an ongoing project that collects and records the history of what's been going on with DNSSEC and its deployment. There is a URL for it if you want to go look at more details and even more information than what I've presented here today. It's a fantastic resource in terms of following and tracking how DNSSEC is getting deployed over time.

That is it from my point of view. Does anybody have questions about sort of the overview of where we are with DNSSEC deployment before we dive into the next panel that will be up shortly after I'm done? Any questions? Okay.

JULIE HEDLUND: Let's all thank Wes for a very helpful and informational presentation.

WES HARDAKER: You're more than welcome. I've got to disappear, but I will be back as soon as I can.

JULIE HEDLUND: And with that, I'll ask the panelists to take their seats here at the front table, and let me just explain what we have next here. As we usually do at the DNSSEC workshops, we have a panel discussion on DNSSEC deployment and activities in the region, and I'm pleased to say we have very good regional representation and very pleased that we're able to include Rajiv Kumar from the .in registry.

Thank you, Rajiv, for joining us. Always happy to have someone from our host country. You're here to tell us what's going on here in India, so that's very good. We also have with us Ryan Tan from CGNIC. We have Dang Duc Hanh from VNNIC and we have Yoshiro Yoneya from JPRS joining us.

What we'll do is we'll go in order as you see it on your program here with brief presentations from each of our panelists, and then we'll go into the questions and discussion. I'd ask unless you have a clarifying question to go ahead and hold your

questions for the panelists until we've had each of the presentations. Thank you very much, and I will turn first to Rajiv Kumar. Please.

RAJIV KUMAR: Namaste. Good morning, friend, I am Rajiv Kumar, working as a system analyst with NIXI National Internet Exchange of India where I look after the .in registry. It is a great opportunity for me to share with you update about .in registry, DNSSEC implementation.

Next slide, please.

Today, I'm going to go [inaudible] detail brief history of .in registry implementation, registrar participation in implementation of DNSSEC, efforts of the registry to promote DNSSEC in the country and TLD, resource for registrar [inaudible] level for DNSSEC implementation.

Next slide, please.

.in registry had been an early adopter of DNSSEC. .in has signed in November 2010. After that we conducted DNSSEC Friend and Family program. In this program, we invite few registrars to come with and provide a testbed to play with their EPP client and give feedback.

In October 2011, DNSSEC introduced for testing environment of registrar. And after one month in November 2011, we started accepting DS records for .in DNSSEC update implementation.

Next slide, please.

In .in, there are 121 accredited registrars. Out of these, 34 are DNSSEC enabled, including the top ten registrars of the registry. We have 2.1 million plus domain names registered in .in registry. Out of that, 1173 are signed as of October, 2016.

Next, please.

In order to promote implementation of DNSSEC, we conduct a lot of workshop, awareness program. With the help of ICANN, APNIC, we can conduct our hands-on training, awareness and workshop. We can also provide every year five days of hands-on training with the help of [inaudible] South Asian Working Group Organization, and time to time, we conduct our awareness in [governmental organization] [inaudible].

Next, please.

Resource for registrar, EPP RTK add-on available for registry website. The link is available there. We update EPP client support DNSSEC commands and also DNS OT&E environmental level in registry.

Next, please. Thank you.

If you have any inquiry, don't be afraid to call me. Or there is an e-mail ID also. You can give me a mail. Thanks, namaste.

JULIE HEDLUND: Thank you very much, Rajiv. As I said, we'll go ahead and hold some questions until we had all of our panelists do their presentations. Next, I'd like to turn things over to Ryan Tan, please.

RYAN TAN: Thank you. I'm Ryan, I'm from the SGNIC. I'm the head of the technical operations there.

Next slide, please.

Just diving into the background, we started looking at DNSSEC pretty much the same time as everybody else. In 2009, we formed a formal working group to look at DNSSEC. The summary of the findings was it was very complicated and risky, especially for the DNS zone operators if something is not right and the whole zone may go away.

At that point in time – and there still is – there's no demand from end users or registrants. We also found that the software, the tools, the policies and the best practices are not that mature. By

any case, we went ahead with a DNSSEC testbed, and we found that actually, no registrar wanted to participate.

At this point, we decided we could go ahead with DNSSEC implementation, or we could not. Therefore, we discussed it and we found that if there's something that nobody wants and you start implementing it and something goes wrong, you are basically asking for trouble.

So, we decided, "No, this is probably not the right time to do it. "What we do is we will start to monitor, keep a wait and see attitude for it."

Next slide, please.

In 2015, after the root was signed, we found we had to look at it again. We found that it is slightly less complicated and risky for zone operators to do it, but then there was still no demand. I think at that point, we were looking at 0.5%, not like today. Today, it's about 5-10% already.

However, the good news was that the software, the tools, the policies and best practices were much better. So, we thought, "Okay, this is about the right time to do DNSSEC." That's the official reason. The unofficial reason is because of [inaudible] was on our backs, "Hey, when are you going to sign?"

Next slide, please.

Our implementation approach is pretty much what everyone else does: for the first part of the research, we wanted to be very certain that we are not running into the problems that the pioneer registries have faced – time issues, the [inaudible] signing, whatever, so we spent some time looking at what went wrong and what we could do to prevent it. We went to the development phase, do the software development, DNS practice statement, develop the key [ceremony] procedures, and then went on to rehearse the key [ceremony] procedures, conduct a key ceremony, and we actually had a pilot launch. Except this time, there were still no registrars who wished to participate in the pilot launch. While the pilot launch is running, we used the time to do emergency recovery drills, because that is the last time you can go anything, and then we finally went for the full deployment in September, so two months ago.

Next slide, please.

So, what's the current status? Out of our 18 registrars, there are only about five guys who are supporting DNSSEC DNS management. As of today, there are still zero domain names that are DNSSEC signed, but the good news is that the Singapore government has committed themselves. They said, "Oh, I'm going to sign the gov.sg zone by the first quarter of next year."

Last point is about the challenge that we're facing. Reality is we find it very difficult to convince the registrars and the DNS hosting providers to adopt DNSSEC. With that, thank you.

JULIE HEDLUND: Thank you very much, Ryan. Very helpful, and we'll go ahead and move along into Hanh Dang Duc from VNNIC. Please.

DANG DUC HANH: Hi, everyone. I am Hanh from VNNIC, [inaudible]. This is the third time I come here to the APNIC ICANN meeting, so it's my pleasure to be here to share with you about the current standard of DNSSEC deployment in [inaudible] domain name in Vietnam at the given time.

Next, please.

In Vietnam, VNNIC manage a national DNS system. We understand that security for DNS is very important thing, so we research about the net security quite early. In 2012, we have deemed to join some forum and conference about DNS, and write some document about DNS security.

After one year, in 2013, we also built DNSSEC as a test system, and we do some training for our men to prepare for [our project] about DNS and after that, in 2014, there are project, national

project about the DNS deployment for .vn domain name was approved by our Ministry of Information and Telecommunication, also called MIC, which are two phases from 2015 to 2017.

Next, please.

In the first phase, we call it preparation state with three main purposes. First is raising public awareness among our ISPs, reach out to Internet users about DNS security. We are also building policy and regulation regarding DNS security deployment. We have to prepare human and technical resources at the time.

The second step is the implementation step in [inaudible]. We are also implementing DNS security for the national DNS system and we have to connect our DNS security to DNS Roots and the international DNS system.

And for the last step we call in 2017, we have called accomplishment state, we have to upgrading our system, DNS system to support for DNS security, and we have to upgrade our domain name manage systems to support for our [inaudible] domain name with the DNSSEC support to our IP gateway. We are also providing Internet users in Vietnam with service and product with DNSSEC specification.

Next, please.

In Vietnam now, we have more than 10 ISPs and 15 registrars. For DNS, we also do with our [inaudible] our ISP and also apply DNSSEC for our system [inaudible].

Next, please.

For .vn implementing, we do not support secDNS:maxSigLife and we do not support for secDNS:keyData. We only support secDNS:dsData only for further investigation before upgrade to the national DNS, and we also only maximum of 6 DNS record per domain.

Next, please.

In the process of DS creation in a national DNS when our system get request from the registrar, we do not create the DNS record as soon as reach out. We have to also compare the public key information between the secDNS:keyData with the DNS key we got in the hosting zone file, and if it match, we create, and if it do not match, we return the error key and inform to our registrar about this.

Next, please.

For 2015, we also implement DNSSEC security system. We also deployment our management software and the software for registration of domain names for supporting for DNS. We had to do training courses on DNSSEC for our ISP, registrars and IT

enterprise in Ha Noi and Ho Chi Minh city. And this year we're with the collaboration with APNIC and ICANN, we also host a free workshop on DNS for government and ISPs and CSPs. And we also have two week workshop with the registry .nz on August this year and now we also preparing for signing ceremony on December.

Next, please.

This is outcome now for our statement of DNS deployment. For DNS plan, for .vn domain name, we are done. To establish DNSSEC team and training skills, we are done. Infrastructure for DNSSEC with topology DC/DR, we are done. And building DNSSEC production for .vn zone, we are done. And building DNSSEC monitoring system, we are done. To building and preparing the DNSSEC document and DPS we are also done.

Next, please.

Now, we are in the process of prepare the key signing ceremony, and we have a plan to signing VN zone and update DS to root next month, in December of this year. And for the [inaudible] 2017, we open our OTE testing system for our registrar to connect and to test.

Next, please.

This is all about status of deployment DNSSEC in Vietnam. If you have some experience or some question to [inaudible], please e-mail me at the e-mail in the slide. Thank you.

JULIE HEDLUND: Thank you very much, Hanh. Very good. Now, we'll turn to our final presentation from Yoshiro Yoneya at JPRS.

YOSHIRO YONEYA: Hi, good morning, everybody. My name is Yoshiro Yoneya from JPRS. I'm working for the deployment of DNSSEC in Japan, and today, I introduce our activities regarding the explanation of root KSK rollover. I explain the findings from my experience.

Next, please.

The current status in Japan is the awareness for DNSSEC is not so low. Because, several times, we have DNS or DNSSEC-related events in Japan, and from the answer of the questionnaires they have a lot of awareness and they want to know DNSSEC much more. So, the awareness is not so low.

But the awareness or the interest for root KSK rollover is still low, so I think we – we means the DNS-related community – thinks we need more outreach activities in Japan, because the Internet users, especially DNS operators have to know what happens

correctly at the KSK rollover, because knowing after something bad things happened is too late. We are going to explain what will happen and what they have to prepare.

Our outreach activities in Japan for the root KSK rollover explanation is public fora or private fora. I explained KSK rollover last year in the Internet Week, which is the largest Internet conference in Japan, and I will also explain the KSK rollover this year. JPRS has a registrar day, and in that technical seminar, I explain the root KSK rollover also. I'm going to explain it again next year.

Previous slide, please.

So, the findings from my experience is the ICANN's root KSK rollover planning document – there are five of documents – are very helpful, but it is not enough, because these documents have no outreach template in the local regions.

Next, please.

What should be written in template document [I recognized] is the list of who will be affected. Of course, the full list of our operators should be maybe affected, but it is not only the parties who are affected.

A list of facts and how to prepare for each of them. Preparing RFC 1511 software is very important, but there are other things to

prepare. And what action to do around the important date? Important date is the date when the responses from root zone changes.

What actions they do allowing such important date? Also, the template should have the list of contact and the contact methods for when critical failure happens. This means both global and local authority over the information. Global means it is ICANN or IANA, and local means it's some governmental or registry, ccTLD, or very high, major ISPs. And the URLs which should be IP address, because when the root failure happens, the domain name cannot be resolved. And then some call number, etc.

Here, I explained about our presentation in Japan briefly. The presentation consists of my explanation of DNSSEC concept itself, especially the rollover of ZSK, KSK and TA, Trust Anchor. And I explained about what kind of root KSK rollover are there? So, two keys. ZSK and KSK both has its own rollover, and list of who will be affected by the root key rollover.

And through this presentation, I'd like to share and compliment 'lacking pieces' for this kind of outreach activity. Before I show you our local presentation, please note that these slides are written in Japanese. I put some annotations in English and I will explain key points if the time allows.

Next, please.

This is just start of the presentation. That says that key management at the DNSSEC and the preparation for root zone key rollover.

Next, please.

This is the agenda of the presentation. The content is as I said: DNS key, DNSSEC concept, key rollover, and impacts.

Next, please.

This section is DNSSEC explanation itself.

Next, please.

Perhaps you can understand what this figure says.

Next, please.

And this slide shows who the – relative to the DNSSEC operation.

Next, please.

And this is how DNSSEC works.

Next, please.

This explains about what is the KSK, ZSK – next, please – and what is the trust anchor.

Next, please.

This section says why ZSK and KSK are existing.

Next, please.

This section says what kind of KSK rollover exists in root zone.

Next, please.

There are three types of key rollover in each ZSK and KSK.

Next, please.

This slide shows what happens during the DNSSEC key rollover.

Next, please.

This section explains about the recent changes for the ZSK key size. These are very interesting because this ZSK change was very short notice, we are very surprised.

Next, please.

This says what happened.

Next, please.

We observed no impact from the ZSK rollover.

Next, please.

This graph is derived from root operators.

Next, please.

This section explains what kind of KSK rollover exists, what kind of things happen in the KSK rollover.

Next, please.

This slide shows the important date.

Next, please.

And how many, what kind of changes for the response happens in the important dates.

Next, please.

From this section, explains who will be affected and what is the measures.

Next, please.

Who will be affected is the full resolver operators and authoritative server operators, and the outsources.

Next, please.

This section explains who are the major full resolvers.

Next, please.

This section shows the resolver operators who are validating, DNSSEC validated.

Next, please.

This is who are not validating.

Next, please.

Both have to prepare for the KSK rollover, because this [inaudible] affect both validator and non-validator.

Next, please.

This slide shows what kind of points they should watch around the important dates. It just says that it's C, the root zone DNS key was validated.

Next, please.

When the operator finds the failure, then they should stop validating without other information. Just obey their observation.

Next, please.

If they want to start validation again, then they should see the external information from others.

Next, please.

This is for the authoritative servers. Authoritative servers are really not affected by the KSK rollover, but when the KSK rollover

failure happens, their domain names cannot be resolved, so that they should know what happens correctly.

Next, please.

They should know what kind of information they can get, and this is for the outsourcees.

Next, please.

Outsourcees do operation for the customers, so they should know what kind of things happen. And I put this blank for the cool down, because those slides are somewhat threatens the operations, but I will explain. Just a small preparation is a very big insurance.

Next, please. This is what I had.

JULIE HEDLUND: Very interesting, and that will tie in nicely with our root key rollover panel that we will have a little bit later today. At this point, I would like to turn things over to any questions. Do state your name for the transcription purposes before you speak. Let me turn things over to our audience and ask for some questions. Go ahead.

JACQUES LATOUR: Jacques Latour with .ca. For India and Vietnam, did you build EPP support for registrar like RFC5090? That's why numbered. Are they planning to implement using those interface?

RAJIV KUMAR: Heck not. But just the works open the hands-on training we are providing to the registrar and the hosting provided.

DANG DUC HANH: In Vietnam, we also deploy EPP for our domain management system for [necessary supporting]. We also have all the supporting. As I show in the slide, we will open data OTEs in 2017. Yes. Thank you.

JACQUES LATOUR: Then Singapore, you already have EPP. That's why I didn't ask you.

JULIE HEDLUND: For our panelist. If you aren't sitting at a microphone, there are still some empty spots up here at the table if you'd like to come up to ask your question.

UNIDENTIFIED MALE: [inaudible] from ISOC and [inaudible]. Special [salutation again]. We should have DNSSEC regular training sessions. It should reach to the [inaudible] ISOC is also active in educating on DNSSEC this thing through work order plan regularly. We have quarterly based training.

JULIE HEDLUND: Thank you very much for your efforts to raise awareness. It's very, very important. I want to emphasize too how pleased we are to have our panelists here to show how deployment is [there]. Any other questions for our panelists? I see. Yes, please. If you would step up to microphone.

[ABDUL MONEM]: I am [Abdul Monem] a second time Fellow. My question to my colleague from – this is another comment to [.gb]. Thank you very much for keeping your identity and your language in your presentation.

[DAN DUC HANH]: [inaudible], in that times, we invite approximately five to six registrar. But the only two or three registrar actively involved in that. This is a challenge to involve all of the registrar to take equal participation and give me feedback. It's the only challenge with this during the implementation of DNSSEC. [inaudible] we

are find more and more registrar to sign DNSSEC, there is no other challenges. Yes.

JULIE HEDLUND: Thank you very much. Any other questions? Yes, please.

[ABDUL MONEM]: Last question. For .im, I noticed that most of DDoS attack came from India and come to India. Could you comment on that?

RAJIV KUMAR: I will get back to you later. Thanks.

JULIE HEDLUND: Anything else? Any more questions? Then I would like to ask you all to please join – oh wait. No, we have more. Okay, please go ahead.

[MUBASHIR SARGANA]: Can I ask a question to you, guys? I'm [Mubashir] from Pakistan. If you guys know that .pk is not listed in the ICANN domains or ccTLDs. How can you guys help them and your intervention to bring them up and in this main stream and implement DNSSEC as well?

JULIE HEDLUND: Thank you very much for your question. We do have people at ICANN who can help do training and in DNSSEC deployments. In particular, Richard Lamb, Ric Lamb, is someone who I know goes to travels to various countries and gathers together folks for training sessions. It certainly that's something we could think of for Pakistan. But if you'd like to give us your card too and we could have further dialogue with you on this, that would be something we'd like to do. I thank you for your question.

WES HARDAKER: Are you from the registry?

MUBASHIR SARGANA: No.

WES HARDAKER: Okay.

YOSHIRO YONEYA: May I answer? There are several Internet regional meetings such as Hanoi or Apricot. There is a DNSSEC tutorial also. I think the local tutorial materials can be provided to that meeting. You can also ask at the meeting to give them, to ask them giving their local presentation. That will be very helpful because their language is very similar to your language.

JULIE HEDLUND: Thank you, Yoshiro. That's very helpful. Yes. Please go ahead, sir.

ABDUL-HAKEEM AJIJOLA: I wanted to know from Vietnam, what kind of timeframe, what was your time budget because I noticed a nice schedule but are we talking weeks, months, days, years? Then for the rest of the presenters, what were the budget components if you have some kind of ballpark in terms of what was in your perception the final budget?

DANG DUC HANH: I'm lost about the question but as I show in my slide, in the problem to deploy DNSSEC for .vn. We have two, three year. Three year, yes. But before three year, we have a team to do research and prepare of our [resource]. I think but now for the main timeframe, we have three. The first year, you do some prepare about raising the awareness of the IT and research to [change to] DNSSEC set. The second year is implementation about the DNSSEC in the DNSSEC system.

The last year, I mean for Vietnam until 2017, we also call it accomplishment that we have upgrade DNSSEC system signing in zone, VN zone and do some upgrade on management domain

system to support for that is a lesson from our [lesson]. Yes. Thank you.

RAJIV KUMAR: Budget park. [inaudible] there are no additional budget required for that implementation of the DNSSEC. But hosting provider and ISP will give you a better explanation. Maybe they want to update their hardware part. Maybe they will have some budget to upgrade hardware server and all the things. But there is still no need budget for implementation of DNSSEC. Only training and awareness program will have some budget. That's all.

YOSHIRO YONEYA: We're [forcing apart] the part of the cost went into the modifying the registry software for the support of DNS management. It depends on the country. For my country, it cost about, I think it's about 30 or 40,000. It's not a lot of money.

JULIE HEDLUND: I do have one question from the chat room. I think I have a couple that you just addressed, that the panel just addressed. But we also have a question from Robin to Rajiv Kumar. "What steps are you going to take for implementation of DNSSEC to the end users?"

RAJIV KUMAR: Our DNSSEC India had already implemented it. We are trying to implement an awareness. Our DNSSEC implementation, it depend on one little hosting provider and ISP. They still already there from 2010. The India [user] go to their DNS hosting provider, an ISP to facilitate them and their registrar. The [experience is no to little] but we can provide awareness workshops, hands-on training to [inaudible] as well.

JULIE HEDLUND: Thank you very much. I think we're now just right about out of time and ready to start, go to our next presentation. Please join me in thanking our panelists for a very interesting and helpful discussion.

Our next presenter then is Warren Kumari from Google. He's going to talk to us about aggressive use of NSEC/NSEC3.

WARREN KUMARI: That's better. Hi, everyone. I'm Warren Kumari. This is going to be a quick introduction to a draft in the IETF about aggressive use of NSEC.

You have something bouncing.

JULIE HEDLUND: No, just ignore it.

WARREN KUMARI: You can just ignore it? It'll go away? This is a quote. Microphone really loud.

This is a quote which apparently is apocryphal which is unfortunate because it would actually be nice if it were real. "Sometimes simply knowing that you don't know something is a really useful thing." You'll see why soon.

DNSSEC provides authentication for both positive and negative answers. If you look up www.example.com, you get back 19216811 but you also get a signature proving that that's valid.

Something which people don't often realize is it also provides authentication of negative answers. If you look up login.example.com, if that name does not exist, you get back a response saying the name does not exist. You also get a signature that proves that. This is equally important because of the name login.example.com does not exist, it would be bad for an attacker to be able to make it look like it exists because users would naturally assume that this is really the login page and would enter their credentials.

Signing things with DNSSEC is a somewhat expensive operation in terms of CPU and resources. DNSSEC avoids doing on-the-fly

signatures because it has no way of knowing what a user might look up and need to make a negative answer for. It doesn't want to have to generate answers on-the-fly and sign them.

Instead, it's got this real clever trick which is called NSEC. That's short for the Next SECure record. The way it does this is it takes all of the names that do exist in the zone file and it sorts them alphabetically. Then it signs all of the gaps between those records. That's a little confusing to explain and understand so I'll show you an example.

A name which often gets looked up at the root which does not exist is .belkin. There is no tld.belkin but there's a bunch of home routers and stuff which keep looking this name up. It makes a good example.

So over here you can see… Does anyone have a laser pointer? Hang on one sec. Grab my laser pointer. Because lasers.

So yeah. There's an example looking up .belkin and you get back a response which is NXDOMAIN which means the name does not exist. You also get back this other NSEC record below which says that there is nothing that exists between .beer and .bentley. Then further down, there is this big signature group.

Because you know that you looked up .belkin and because belkin falls alphabetically between beer and bentley, you know for certain now that that name does not exists.

That's all good and interesting but why is it actually useful? Currently, when a resolver looks up a name and gets back an NSEC record, it only remembers that particular the fact that the name does not exist for that particular name it looked up.

This document allows recursive resolvers to use these NSEC records to synthesize negative answers. This means that if, in the previous example, there had also been a look up for .believe which does not exist. Instead of the recursive resolver having to go often talk to the root again and ask at a second time and then get back the same answer, it could just look and see, "I already know that there's nothing between .beer and .bentley" and immediately return the NXDOMAIN answer from that.

This improves privacy because it means that people's typo domain names don't keep having to go often be answered. It doesn't expose the fact that they're trying to look up these names.

Because the resolver can immediately answer from its cache, it decreases latency and increases performance. It also saves resources on both the recursive and the authoritative name-servers. Because the recursive server doesn't need to generate a

new query, it doesn't need to maintain state, it doesn't need to wait for the answer, the recursive server doesn't need as much resources. Also, the authoritative name-server doesn't keep on being asked questions that it doesn't need to answer. It's already answered this.

This also improves DDoS resilience, denial-of-service attacks. There is a well-known attack at the moment where attackers will ask their local recursive name-server or open recursive name-servers a bunch of made-up names. The recursive name-server keeps going along and asking the authoritative name-servers. Eventually, the authoritative name-servers get overwhelmed.

All around, a good thing but is it actually really useful? On May 12, 2016 which was a Friday afternoon because whenever anything goes boom, it's always on a Friday afternoon, Colin and Kaveh who work for RIPE who operates K-root poked me and said – I guess I should have mentioned I work for Google. Yes, poked me and said, "Google is sending K-root a whole bunch of queries and they look like this." It's a random string and then a dotted quad which is normally an IP address. "But for some reason, many of the octets are larger than 255 and what is this and why are you doing it? Please make it stop."

As you can see, the graph is growing really quickly. That's a graph of queries to K-root.

My eyes aren't that good. This isn't rendering properly.

Normally, they get around 4000 queries per second to K-root. They called me sort of over there where it was starting to grow. It was continuing to grow and ended up being around 10x the number of queries by the time we started looking at it more. "This wasn't actually causing K-root any issues but it was really annoying, please stop it."

Within Google, we started looking around. Initially, we thought this might be some sort of bug in our software and if it was, who touched it last and why? Then we thought, "Hey, maybe we're being used a DoS reflector. Maybe people are sending us queries in order to try and DoS something."

More concerningly, why does this look like organic growth and not a normal DoS attack? Normally a DoS attacks starts off really suddenly as a huge pile of queries and goes up in a straight line. It looked like it was growing and we didn't know when it was going to stop.

After some more looking around, we discovered it's not actually just Google public DNS that's doing this because Google public DNS is so popular. If you look at a graph of queries, it often shows up towards the top. It wasn't just Google public DNS that was sending these queries, it was everywhere.

That was a bit of relief. At least it's not entirely our fault. But what's causing this? Can we make it stop? Etc. A little bit more looking around and we discovered that there was a worm that was kind of like a virus that was suddenly circulating which infected a bunch of home routers and wireless access points by a company called Ubiquiti.

This was actually a fairly well-known vulnerability but there was a new worm that was busy exploiting it and this was circulating on the Internet as one of its liveliness tests to make sure they can reach the Internet. It would do a look up that looked like that, random string, that dotted quad.

Okay. Now, at least we know what's causing it. Can we do anything about it? Can we make it stop? Etc. The aggressive NSEC stuff. Google already had that built into its code, the aggressive NSEC features. They weren't enabled though. We've built the code and we hadn't turned it on. We're just giving it some time.

Over here on the far left, you can see queries from Google. Actually, sorry, this graph shows queries from Google to B-root. Under normal steady state, before the attack, Google was sending about 500 queries per second to B-root.

Over here, this huge spike that is on May 12 when the worm started happening. As you can see, we went from around 500

queries per second to around 2500 queries per second in a very short time.

As a response to the worm happening and ascending lots of queries to the root servers, we turned on aggressive NSEC at 100% at the top foremost affected locations. You can see that's where that graph goes down a whole bunch. Because it was a Friday, we don't like making production changes, we let it bake over the weekend. That's this big section.

Then on Monday or Tuesday or so, we turned on aggressive NSEC at all of the locations where we have Google public DNS but we only turned it on on half of the machines. We wanted to give it some time to bake, make sure that nobody saw any issues. We let it bake for about a week. Then over here, we turned on aggressive NSEC at 100% at all of the locations.

As you can see, before there was the attack, before we had aggressive NSEC enabled, it was around 500 queries per second to B-root. After the attack and after we turned on everywhere, it was more like 40 or 50 queries per second to B-root. Each root letter gets a different percentage of queries but it's a very similar scale change on all of them.

That was a bunch of background. What does the document actually say? It says if a resolver has records, NSEC or NSEC3 records which cover the question, it should just use it to

synthesize answers. It shouldn't bother sending the query to authoritative server.

It also says if there's a wild card which covers the question and the resolver has all of the information order to construct an answer, it should just do that. Basically, what this document is doing is it's relaxing some restrictions which were in RFC4035 which is one of the core DNSSEC RFCs.

I think just a quick overview on the document where we added wild card support, we expanded the implementation section a bit, we mentioned the fact that Google and Unbound implement it and the document has completed working group last call in the IETF. Just need to finish going through the process. Then it should be published. I think that's the end of my slides. Questions? Hopefully lots.

[ABDUL MONEM]: Could you elaborate more about DoS reflector?

WARREN KUMARI: The DoS reflector? Sure. Where is a good example for that? I try to think way to start answering this from. A DoS reflector is something which people using a DoS attack use to hide their address. With a DNS DoS reflector, an attacker will use a bunch of

bots or a bunch of spoofed addresses. He will ask a recursive resolver to go on off and ask the authoritative server a question.

He will spoof a query to recursive resolver or he will query on recursive resolver. Can you please look up [inaudible] for me? The recursive server will then go and ask the authoritative server. If he does this enough times, the authoritative server will get overloaded. A DoS reflector is something which an attacker uses to serve reflector's query somewhere else. I'm not sure if that answers your… Okay.

JULIE HEDLUND: Jacques.

JACQUES LATOUR: That's interesting because I never actually spend a time to read about this. Now, I get it. Good stuff. Can you go back to your graph where you implemented the –

WARREN KUMARI: That one?

JACQUES LATOUR: Yeah, this is where because you turned on the aggressive NSEC for 50% of your site and yet it'll drop in traffic. Then when you

implement everywhere, you have a massive drop, it's not linear. Which was it?

WARREN KUMARI: Yeah. You mean the fact that that isn't half of that. Well, over there, it's about half. I guess that that wasn't exactly we turn it on at 50% of all locations. We turned it on some there. We turned it on a bit more there. We turn a bit more. Instead of just being an arrow, that should be I guess a slightly shaded area but no. We turned it on and then it took some time to roll off to other places.

Yeah, the reason that the final steady state is much lower than the before steady state is all of the space over here. If you just drew a line from there all the way across, all the additional space is just junk queries that had been hitting the root which no longer need to hit it.

[PAUL VARTERS]: Just a quick question. Does this work with NSEC3 and opt-in because then you're giving a denial over a whole lot of domains the do actually exist?

WARREN KUMARI: This works for NSEC3 but not for NSEC3 with opt-out. If you do NSEC3 with opt-out, then- I think you meant opt-out not opt-in.

Yes. If you do just normal NSEC3 without opt-out, then it works okay. If you do it with NSEC3 with opt-out, then it just doesn't enable for that.

[PAUL VARTERS]: It doesn't work for .com? That's a shame.

WARREN KUMARI: If .com were to turn off opt-out on NSEC3, then it would work okay. But that would require things were being signed. Yes. For a rough scale thing, currently, the root – and I'm keep using the root as an example because it's an easy example and because I have statistics – currently, the root gets around 60% of all queries depending where it look 60% or a little bit higher resulting it in an NXDOMAIN answer, a no such domain. Once this is turned on, it should be substantially less than 1% of queries get NXDOMAIN depending on cache time, etc.

ROBERT MARTIN-LEGENE: Robert Martin-Legene from PCH. Which resolver software do you use in the Google public DNS?

WARREN KUMARI: I don't actually think I can answer that but it's not one of the… I think I can. It's our own staff. It's our own customer staff. I believe that that's public. It is now.

ROBERT MARTIN-LEGENE: That was my next question because is that a software you're going to publish since you're so open source about everything?

WARREN KUMARI: I have no idea. I would suspect not because it's very custom, relies on a lot of internal services. It wouldn't really be useful by anyone else but I honestly have no idea. I think that that's the longer version of no comment.

JULIE HEDLUND: I'll just note, I do have a question in the chat. I'm just going to switch back and forth between the room and the chat. Going to the chat now, Geoff H. asked and he says, "Cloudflares dynamic synthetic NSEC response defeats this approach. How prevalent is Cloudflares limited NSEC response type? Do you know?"

WARREN KUMARI: I have no idea but yes, he's correct. The way Cloudflare does NSEC or does negative answers is it generates an NSEC record on-the-fly. It only says that the name that you asked for and then

the name plus one character off from that does not exist. This is a implementation thing which Cloudflare did because they answer for a lot of different users and it was easier for them.

Cloudflare is large enough that they probably don't worry about the DoS attack potential of this. It's not something that they use or need. But who knows, in the future they might change that or something. Yes. For the specific case of Cloudflare and people doing NSEC3 with opt-out, this doesn't help them at all and doesn't help the resolver either.

JULIE HEDLUND: Go ahead, [John].

[JOHN ODEEN]: I have two unrelated questions. One is can you compare and contrast just the RFC7706? That's the one you wrote about marrying the root zone. The other is that I'm glad you put the wild card synthesis back in since that was my idea. I was wondering do you actually have much experience with does it make any difference?

WARREN KUMARI: RFC7706 which, yes, it's called something about decreasing access chime to the root by running one on loopback or

something like that does something kind of similar to this but it does it only for the root zone. For people who are not familiar with it, basically, what that says is if you run a recursive server, you can just slave a copy of the root on your local recursive server. Then if you get a query, you can send that to yourself basically.

There's probably a whole separate presentation on that. That accomplishes some of the same things. It means you don't have to send queries to the root servers. But it only applies for the root that supplies everywhere for all people who are doing NSEC or NSEC3 without opt-out. The new kind of similar things, this is much broader scale.

What was the other thing? How this works with wild cards? We don't really know. Getting statistics is hard. It depends hugely upon what the query looks like, etc. There's a good source of queries that get NSEC record so it's an easy thing to see and that's the root. For wild card specifically, there is no zone that I know that gets queried that often for it so it's hard to figure it out. Or at least, those zones that have I easy access to look up.

JULIE HEDLUND: Thank you. Go ahead, sir.

[RASHIV]: Hi my name is [Rashiv]. I'm representing the government of India. My question is that while cache server is returning the cache resolver is returning, sorry, rather the resolver is returning a cache entry for NSEC, there's the possibility that the root zone server is getting a better simultaneously. You might get a false [inaudible] in that case. Do you have some sort of a TTL which expires regularly?

WARREN KUMARI: Yes. This is sort of my additional notes thing. Yes, this isn't just for the root zone. It's for any zone. But what you're asking is if you currently synthesizing records and the zone changes, what happens then. Yes, there is a TT on the record. The NSEC record you currently get back anyway. We're just saying just use the NSEC record and the NSEC record has a TTL.

The NSEC record you currently get back anyway. We're just saying just use the NSEC record and the NSEC record has a TTL. You will only use this while the NSEC record exists.

[RASHIV]: What is that like? What is a usual TTL you said for a cache resolver?

WARREN KUMARI: The NSEC record comes from the authoritative server. That's whatever the authoritative server operator has set. You think of this TTL is being similar to negative cache time TTL. It's the same sort of thing. If you already had looked up the name, the specific name which got added and was in your cache, you still wouldn't be able to resolve it for a while because it would be that actual record was cached. This just caches the range.

I think I worded that really bad. I need a white bad board to point at. Yes. The NSEC record that comes from the authoritative server has a TTL. You can only use it for as long as the TTL is valid.

[WARREN BARRY]: [Warren Barry] from .ca. Regarding this graph, I notice that the time has dropped off immediately when you implemented it the first four locations. Any insight as to why is that a saturation issue?

WARREN KUMARI: Sorry. You're asking why they dropped down so quickly?

[WARREN BARRY]: No, specifically, the time that's a green line.

WARREN KUMARI: That one or?

[WARREN BARRY]: No, no. The green line right at the bottom and follow it back to the first spike. There's an immediate drop off on the first four site implementation.

WARREN KUMARI: I need to go see what the green line says.

[WARREN BARRY]: It's time out. At least my aging eyes tell me.

WARREN KUMARI: Yes. I'm not entirely sure that the time out's line actually is exact accurate. But I think that what we think that that is, is yes, that's places where we were sending queries and B's wasn't quite able to keep up with answering. Basically, B was becoming somewhat overloaded at that point and so latency increased.

ROBERT MARTIN-LEGENE: I have one question. The TTL you get from the NSEC is not usually what the zone operator means with the minimum TTL which is a conflicting thing. People are not really aware of the TTL being interpreted that way.

WARREN KUMARI: Yeah. I thought I had more information on that. Yeah. Potentially, some operators might want to change the TTL in the NSEC record. We did have somewhat of a discussion on the fact that there are two different sets of record lifetimes there and they might not be expecting it.

I'm guessing at some point, signing software might start using things like the normal negative cache time and using that for NSEC. Yes. I think the view that people had was the NSEC TTL was kind of the authoritative for that particular engine. Yes, it's a little weird but yes, there has been a discussion that were probably possibly-

JULIE HEDLUND: Jim?

JIM GALVIN: Right up until Robert asked this question, I was just taking this in and figured, "This is pretty cool stuff" and then suddenly it dawned on me. Some registries care that you can buy a domain name and it's propagated and available immediately. I think there's some effect here against that. It makes me wonder if this becomes too popular and too many people do it, if they're going

to move in the direction of what Cloudflare did for authoritative service. Any thoughts about that?

WARREN KUMARI: When somebody buys a domain name, it's not really available immediately everywhere. If the name that's got bought is something that somebody had been looking up already or if it was something, in fact this often seems to happen, specifically for the person buying the domain name, they first go look it up in their web browser to see if it exists. It doesn't and then they go off and buy it. Then it still doesn't. That's because they just looked up the name that had been cached.

Yes. That might make that happen a bit more. But if the TTLs are not that long and many of the NSEC record ones aren't, it's not that long before it shows up. Yes, there's whole lot of hand waving there. More people might start doing the Cloudflare white lies thing.

JIM GALVIN: But if your TTL default is… you might want to manage your NSEC defaults differently from everything else. For us, it's a couple hours I think or is it a day. I actually forget now some of them and what it is. I guess it varies by registry for what we're doing. So it's kind of interesting. You could make this ugly for a while.

WARREN KUMARI: It does somewhat change the operational meaning of NSEC TTL.

JIM GALVIN: I'm sorry, I didn't say in advance. I'm Jim Galvin from Afilias.

JULIE HEDLUND: I did say Jim but I didn't. Thank you. Any other questions for Warren? Yes. Please go ahead, John.

[JOHN ODEEN]: [Apropos] of Jim's thing, I've been typing away. I'm just looking in the TLD zones I am looking at. The TTL on the SOA is typically five minutes. The TTL on the RRSIGs is typically a day. Yes. If you haven't mentioned in the draft, this would make a difference, it's worth doing so. I still think, over all, the benefit is significant. I think you would have to be fairly unlucky to do a specific series of queries that would hide a newly registered name from someone who cared it for a significant amount of time.

In this environment, I know there are people who are convinced that it will ruin their business plan so it's worth thinking about.

WARREN KUMARI: Yes. At one point, I'm not sure if there is still text. At one point, there was some text. The draft has moved a bunch. We should check to make sure it's still there. There had been some discussion nonetheless. I'm not sure whether text ended up –

JULIE HEDLUND: Go ahead, sir.

MOHIT BATRA: Hi. This is Mohit from NIXI, National Internet Exchange of India. Okay. I'm not sure whether this is the correct place to ask this question but I think it's related. My question is what is the arrangement between IETF and RSSAC (the Root Server System Advisory Committee)? Who decides if DNS protocol needs to be changed in some way that is a new feature or modification? Okay. That's it.

WARREN KUMARI: I think there are a couple of different questions there. The RSSAC is made up of two representatives from each of the root server letters. This isn't really DNSSEC stuff, but just background.

Two representatives from each letters. Most of the letters also have people who – and they [serve] many [inaudible] policy. The letters also have operational people and most of the letters

possibly all as far as I can think also have people who show up at the IETF meetings. But those are more operational stuff.

The IETF defines the protocols and things about how the DNS works and people who happen to work at root letters who participate obviously contribute but in the IETF, everyone contributes as an individual. There is a lot of back and forth stuff on that.

I don't know if that actually answered your question. There isn't a formal relationship between the IETF and RSSAC other than possibly the Internet Architecture Board and ICANN talk together. I suspect I didn't actually answer anything you saw there is a lot of words there.

JULIE HEDLUND: Well, thank you for that. I'll check one last question. We're running out of time. Please go ahead.

[AIRA KNOLL]: [Aira Knoll] from Nigeria. I wanted to know if NSEC is coming as a patch to DNS or is an alternative to DNSSEC. I don't know.

WARREN KUMARI: Actually, NSEC is one of a core pot of DNSSEC. It was in the original set of RFCs when they were published. It's an integral

part of DNSSEC. What it is it's simply the DNSSEC record that says the name that you looked up does not exist. It's built there.

JULIE HEDLUND: Thank you very much. I want to have you all join me in thanking Warren for a very, very interesting presentation.

Now, I'll note that we do have a break. There is coffee out and about. If you go outside, this is a general break. There should be coffee in various areas.

We will start precisely back at the top of the hour at 11:00 to make sure that we continue to be on time. Please do return in time for the next, part two of the DNSSEC workshop. Thank you.

[END OF TRANSCRIPTION]