ABU DHABI – DNSSEC Workshop -- Part I
Wednesday, November 1, 2017 – 09:00 to 10:15 GST
ICANN60 | Abu Dhabi, United Arab Emirates

UNIDENTIFIED FEMALE: November 1, 2017. Hall A Section B, C, DNSSEC Workshop Part I, 9:00-10:15.

RUSS MUNDY: Good morning, everyone. And welcome to the DNSSEC Deployment Workshop. And I'm Russ Mundy with Parsons and Jacques Latour with the CA Registry are basically the hosts today. Are you not hearing? It's one of these. You have to eat the thing. Okay.

Okay. So we will be having our session today. I think there's some new faces. There's some faces we've seen before in the workshop. And we want to make this as much of an interactive activity as we can.

So everybody should have the program there in front of them. On the back of the program is your lunch ticket if you intend to stay and have lunch with us at noontime. And we have lunch courtesy of our sponsors. Our slide with the sponsors is – yeah, it will be coming up shortly.

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.

Here's our sponsors, okay. Afilias, CIRA, SIDN, .ca and dot – well Afilias registry. Anyway, nice set of sponsors and this is the important part. Let's give our sponsors a round of applause for lunch. There is a free lunch for the DNSSEC Workshop. Okay, and Dan York is often the one doing this but today well instead of being the Dan and Russ show, it's the Dan and Jacques show. I'm Russ. The guy not here is Dan. And so Jacques will be doing the presentation that Dan usually does at the beginning. And so with that, I'll turn it over to Jacques.

JACQUES LATOUR: [Let's] go to the agenda. Yeah. All right. All right. So for today, we're going to have the standard introduction around the world, and all the counter slide around DNSSEC. And then we're going to have a panel discussion on the DNSSEC activities with a focus on regional.

The second workshop is going to be around the current state of the KSK Rollover, and what's next, and what's happening. So we'll have a good discussion around that. And then we have the great DNSSEC/DNS Quiz. So a lot of people are here just for that. I know that for sure. And then after lunch, we have a couple of presentation on DNSSEC-related stuff. So should be a good date. Next slide.

All right. So let's go around the world. Next slide. I got the clicker. Yes.

So ISOC they wrote the state of DNSSEC Deployment 2016 report. If you search for that, you're going to find a pretty comprehensive report on the state of DNSSEC deployment and all the initiative up to 2016. So Dan and company did a pretty good job at putting all this together. So if you want to know anything about DNSSEC, this is a good place to start. It has a lot of reference to more link information to become more knowledgeable on DNSSEC.

Who here it's their first DNSSEC workshop? Okay, thanks. That's good to know. So that how fast I should go or not if you're all seeing all this before then I'll go slower.

So this is based on APNIC lab. It's a graph of DNSSEC validation worldwide. So over time, we've been tracking this. And when I saw the slide for the graph for the first time, I noticed there's a dip around July. I suspect that you might have some comments on that.

JEFF HOUSTON: The BSNL backbone had turned it on – it was about a year or so ago. And in India BSNL is very big. There's a lot of customers. In July, they turned it off. And that did a noticeable glitch in the figures because they turned it off. I've never approached them as to why. There are two possible reasons. One, they never knew that they turned it on in the first place, which happened in Yemen. So sometimes it just gets turned on by accident and it gets turned off when they realize.

The other possible explanation which is more depressing is that they looked at the incoming KSK roll and decided they weren't going to do it. And I have no idea which of those explanations is the case. If anyone here is from India and knows about the situation of BSNL, feel free to educate me. But that's as much as I know.

JACQUES LATOUR: Thank you. Anybody from India here?

UNIDENTIFIED MALE: Yeah, I'm from India but I don't have an update on that. So we don't know if [there is that aspect] with BSNL [inaudible] and all the things.

JACQUES LATOUR: So here's an action item for you guys. Send an e-mail out and we want to know which scenario it is. I don't know it was on or holy cow, I got to turn it off. All right. Other than that, it's pretty much steady growth, steady slow growth. That's where we're at.

So in the region, number one South Africa with 38% DNSSEC and then it goes all the way down to 2%. The good thing is the number on the reliance on Google public DNS is not that high. The regions are higher.

So that means you're running your own infrastructure and not totally relying on Google to do your DNS. So it's getting good. In terms of DNSSEC validation for Asia, we have Iraq at 57%. And 25% on Google. So that's pretty good. And then it goes all the way down to 0% in Kuwait so there's some work to be done either before or after the KSK rollover. We should think about turning validation on here. Be a good opportunity.

In terms of TLD deployment around the world, we're still at 90%, it's hard to read. 90% of all TLD and the root zone are signed. And about 4% of the second-level domain behind that are signed. And overall, 13% of users are validating. So these are key numbers to remember because you should remember them. So this is big based on Rick Lamb's research at DNSSEC Stat. So I suspect it's going to take a while to get the other 10% but it's a work in progress.

So top TLD in number of signed domains. So this is the TLDs with the most signed domains. Holy cow, that's small. So .nl with 48%

of the domains signed. So 2.8 million on 5.7 million domain, so that's good. Followed by Brazil at 23% with – so this is in total numbers of domains, so almost a million domains signed. And then it goes down. In .ca we have 500 so I think we have a little bit to go before we get in the million range. So new, Rick is not tracking the number of domain using specific DNSSEC crypto algorithm. So if you want to know more about that, then you can go to his website and look at more stats. So if you want to talk to Rick, he's right over there.

Now we're looking at TLD implementation around the region. So we have five different state and Dan actually tracks the state of each TLD based on whether they're experimenting internally with DNSSEC, whether they made a public commitment to deploy DNSSEC in their zone, where it's signed, but it's not in operation. So they got the technology to sign it. The DNS is in the root, meaning it's signed, there's a chain of trust but none of the registrars are accepting DS record yet. And then operational mean it's accepting full signed delegation to the registrar with the APP.

So most of this is done manually because it's not something we can poll over then it works so it's based on discussion. It's based on feedback from TLDs when they actually plan to do something, they let Dan York know so we can update our stats. That's how it works.

So based on this, Dan regenerates the maps of the world with the current state. Over the last five years, we made pretty good progress. I think that's something we should have, is show a year or two years ago and compare where we're at. But we're actually making good progress. Before there was a lot of yellow and red and it's getting much better. To note is there's 46 DS in root meaning getting the registrar, working with the registrars to accept DNSSEC keys seems to be a challenge with some TLDs so that's something we need to look at.

So in the African region, that shows the current state in the region based on the color. So Guinea-bissau .GW assigned in October and South Africa .ZA actually went operational so that's good. These are things to remember at the end. What? Need to remember. So in Asia, .SA went operational, great. We should give a round of applause. That's good. So pretty much same scenario. So 24 operational, 17 DS in the root.

Is there anybody here with a DS in the root? What's preventing you from going full operational? Anybody here from any of these TLD? No, yes? Or it's a matter or just a fact that we're not up to date on your operation? All right. I'll ask later when people are awake.

And then in Europe, we added Aland, that's for me is like island .AX in August. So missing is Italy, I'm not sure who these two other one are. Which one?

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Okay. So making progress. Like TLD, Argentina still somewhere to do. It's pretty much the same picture since the last while. So Bermuda got added in June. Still got some work to do around there. And Greenland is signed. No DS in the root. We actually met somebody from Greenland so that's good. We know they exist.

If you're interested, this kind of stuff you like, these maps all the jpeg images can be e-mailed – if you subscribe to that list, you can actually get that once a month, the full set of maps and all the changes. So if you do some research on DNSSEC, you can use that information. It's pretty much based on the updates that Dan does.

There's a DNSSEC history project ongoing. So you can go look at the current state. There's a URL for it. So Dan and company are working on that. You can look at where we're at, they need content, that's what they're asking for. If you have any tidbit of information that could be useful in the deployment of DNSSEC, you can go there, sign in, and contribute content to the history project. And that's it. Do you have any questions?

JULIE HEDLUND: We have a comment in the Adobe Connect room. This is from Abdalmonem Galila – and I apologize if I'm not pronouncing that correct. Actually two comments. So the first comment is with respect to the data [in] the maps is could you take IDN TLDs into consideration? And his second comment is "I think maps for ASCII and I think these maps for ASCII and IDN TLDs, so could we differentiate between ASCII and IDN DNSSEC signed TLDs on the map to be more clear?"

JACQUES LATOUR: I guess we can put a request in with Dan York and have him do the work. Okay so a lot of the work is manual and it depends on the community updating him on the state. So if he gets the information, I'm sure he could do it. So I volunteer Dan to do it. Yes, question?

UNIDENTIFIED MALE: My name is [inaudible]. I am from .ID registry. And I saw in that map from the Indonesia. They call the DS in root. What kind of the DS criteria?

JACQUES LATOUR: What's the criteria for DS in the root? That means you sign your zone with DNSSEC, and then you gave the IANA the DS record to put in the root zone, but if your registrant want to sign their domain, if your registrant signed their domains, they can't put their DS record in your zone because the registrar don't support it. So you didn't do the EPP to support DNSSEC or have the web interface or some system to do that.

UNIDENTIFIED MALE: I see, okay. Can you give some URL how to support this for our other another subdomain or another TLD?

JACQUES LATOUR: So in the registry? How to support?

UNIDENTIFIED MALE: Registry, yeah. We are a registry at .ID.

JACQUES LATOUR: Did you write your own registry or are you using a third party?

UNIDENTIFIED MALE: Right now, we are using partial third party but we've looked at DNSSEC in the state of deployment, not fully operation with our own. Actually right now we use a third party registry.

JACQUES LATOUR: So you need to ask them to provide support for DNSSEC.

UNIDENTIFIED MALE: Yeah. We need to provide some –

JACQUES LATOUR: Then you need to work with your registrar to force them to support it.

UNIDENTIFIED MALE: Yeah, right now we ask the registrar to support the DNSSEC. But not all the registrar have fully support for the DNSSEC.

JACQUES LATOUR: So do you support the EPP with DNSSEC?

UNIDENTIFIED MALE: Yes, right.

JACQUES LATOUR: Then technically, you should be operational. If you're a registrar, don't support it, that's a different issue. If you support the DS or DNS keys to EPP then you should be green.

UNIDENTIFIED MALE: We have right now around 15 registrar but maybe partial, maybe seven to eight right now fully support for the DNSSEC. But the rest is not –

JACQUES LATOUR: So what's your TLD again?

UNIDENTIFIED MALE: .ID.

JACQUES LATOUR: ID?

UNIDENTIFIED MALE: Indonesia.

JACQUES LATOUR: Indonesia, okay. So you're green.

UNIDENTIFIED MALE: No, not green. I'm in the light green. Yeah. Thank you.

JACQUES LATOUR: So we should have a different color when all of your registrars support DNSSEC like a star, we put a star on there. See? I volunteered Dan to have stars. Great. Any other questions? This is an interactive session. The more you ask, the more we get out of this. Okay. Last chance. No? Thank you.

So now we have the workshop one so it's the panel discussion on DNSSEC activities. And the moderator is me. And then we have Raed Alfayez. And he's going to talk about implementing DNSSEC in Saudi domain names. Welcome.

RAED ALFAYEZ: Hello, everyone. My name is Raed Alfayez. So hopefully repeating it will not be annoying for most of you. I shrink the slide a little bit just to save some time. I'm from SaudiNIC. We have deployed DNSSEC recently in Saudi Arabia, both TLDs, .saudia and IDN. It was in 2016 and .SA, it was this year.

Okay, the Arabic font is not showing correctly. Sorry for that, I'm not sure why. But anyway let's have the language in English. Anyway, the letters are separated, I'm not sure why. It was not a problem but anyway maybe I'll send you an updated version. Thanks.

So we started handling DNSSEC in three phases. So our methodology was to spread in three phases. The first phase is the follow up phase. And we were monitoring the RFCs, the tools, and the softwares, and also waiting for them to be mature so that we can enter hopefully without any errors or any radical changes later in the future because you want to be smooth deployment for DNSSEC in Saudi Arabia. In 2015, we started the initial work.

So we started by doing a full study and we have many countries – we have done benchmark with many countries, leading countries in DNSSEC. We have read the RFCs and then we end up with having a deployment map so we know how we are going to handle this in details. And we execute the plan in the execution phase. The first one was in 2016 and the second one was this year, early this year, and we already completed it.

So our methodology was step by step. We don't jump or have big steps. We focus more on we learn about it, read so many reads and tests and we have established a test lab and whatever new terms we found in the DNSSEC RFCs, we try to read it and deploy and test it and play with it. And we have done the study. After the study, the study end up with having the deployment from DNSSEC in three stages. The first stage, gaining and building local expertise with in SaudiNIC and within our organizations SITC and our CERT and also within the telecom providers.

The second stage was building a prototype so we started signing .saudia at the IDN. It was a very small zone. We signed it and enabled our customers to sign the DNS codes and try to test it and make sure they grasp the information and they can then deploy it in a good way and a safe way in all of their domains and their customer domains. We built an internal mailing list, internal team, and we have so many people with it so anything we can to discuss, we just ask everyone to read about it and make decisions also what are the parameters for the DNSSEC, what are the parameters for the KSK and GSK and the technical stuff we have at this lab. And then we went to operational and open it for our customers to upload their DNS.

So we have done training. We believe training is a key success factor for DNSSEC. So we have done two training session. The first one was a three-day course. There was 25 participants from 11 government agencies along with ICT operators. The second one – this was in October 2015. The second one was in May this year. And we expanded a little bit and there were 41 participants from 29 government agencies and ICT operators and some banks also. And we hosted a one-day public event on May immediately after the training. And there were 120 participants from Saudi Arabia, most of them are either head of IT departments or head of security departments and ISPs and operations. It was open event for everyone interested in the

DNSSEC. And we have done all of these trainings with coordination with RIPE and MENOG and ICANN.

These are some images from the training session. The one to the right was the first one. The one to the left was the second one. This was the public event and we handled certificate for that trainers just to let them be proud of having DNSSEC knowledge. And so these are some of the deliverables. So we have the SaudiNIC DNSSEC practice statement and we were the first to build it in both Arabic and English languages. And it is compatible with the RFC 6841 and this is the it, the DNSSEC practice statement. And we have done also the DNSSEC setup.

We have built lots of procedures on how to handle DNSSEC, how to do the key ceremony, how to install the keys, how to build a new safe if one of the sites have disaster – lots of procedures. And we have done this assessment for the DNSSEC so in case of some critical person handling some of the passwords or bins for the hardware security model or for the sign or what shall we do if one of the signer have a problem. What shall we do also? So we have a risk management table that'll show us exactly what to do. We have built a website and a tools and both website and tools have it in Arabic and English. And we went also fully operational.

These are the main deliverables. This is the [DBS] I told you about. This is the setup for our DNSSEC setup in the infrastructure. So as you can see, we have up to the right, there is the DNSSEC room where we do the key stuff, the key generation, key installation, lots of things and they are safe so we store the HSM along with the cards inside the safe after we generate it. No one enter or leave the room unless there is a specific procedure for that. And we have a backup room. We have two sites, Data Center 1 and Data Center 2 having the signer and the hidden master and the public servers.

So these are the set of procedures that we have developed. And we have launched the DNSSEC operational in .saudia as a prototype in 2016, June 2016. And we were the first DCC country to enable DNSSEC. And we invited as I told you the ISPs and the DSPs, Data Service Provider, to participate in DNSSEC. The official launch for both. .Saudia [inaudible] in Saudi and Arabic was in June this year. And we were the first in the region to open in the service for all of our customers. We have conducted a key generation ceremony. We signed the zones. And we published the DS [inaudible] to IANA. We update the registration system to start accepting DS for our customers. We have done awareness and promotion in the newspaper and in the Internet and in the mailing lists. We also built an Arabic website. It is www.DNSSEC.sa and it has the language Arabic and English.

This is from the ISOC DNSSEC deployment map. Shows that .SAs is green. Dark green. Thanks god for that. And this was the images from the key generation ceremony. These are the teams, all of them are executive in CITC. We have the auditor there also and we have the head of security department. We have the [CERT] with us. And we have some expert in DNSSEC.

This is the website. As you can see, this is the Arabic part of it. Because you have images, we have to write, to show to the people that DNSSEC is easy to grasp. So there are knowledge in their language because they will have difficult to read in English and their understanding. So if the user is not well aware of English, he can read it in Arabic. It will make it more easier for him or her.

This is the tools. This is the DS record verifier. So you put your DNS key and DS record and the tool will verify if they match or not. Or you can put your domain name and the tool will fetch the DNS key record from your zone file. And then it will help you to generate the equivalent DS record.

We have until end of September, we have more than 50,000 domain names. And we have 55 domain enabled DNSSEC until yesterday or day before. 33 domains was enabled and DNSSEC enabled in .sa and eight in .saudia, the IDN, and six in .com.sa, six in .net.sa, and one in org and one in gov. And we need to work more in .gov and in the banking sector, asking them to deploy the DNSSEC as soon as possible.

Again, we need to do more awareness and promotion. The numbers are very low but hopefully it will go increase in the future. We need to monitor any enhancement in the DNS protocol so we need to focus on the NSEC 3, 5, and new issues for automatic key updates and these things. They are important so we need to keep an eye. Also we need to keep an eye on our key rollover. So we have our KSK it's for one year and the ZSK is for six months, every six months they are changing. So we need to keep an eye on them.

So lessons learned, the things that I urge everyone to focus and especially for newcomers, they need to build local experience. And they need to have a test lab for testing – what happened? Yeah, okay. Yeah, [launch at this lab] to test the system, the application, the monitoring tools to test the parameters for the DNSSEC. And to monitor and test the tools for the zone file. Yeah, you need to develop monitoring and testing tools.

So you don't just build your zone file and publish it. You need to verify it before and monitor if the signatures are still valid or not valid. You may to put some important domains in focus so the zone file will not be published if there are problems in some of the domain names. You need to have automation. And especially in the key generation ceremony, don't abandon human because human make mistakes. You need to provide support tools, websites because user, they may get confused.

I think it doesn't change but this is the last of my slide. Yes, that's it. Thank you very much.

JACQUES LATOUR: Thank you, Raed. Any questions? I got one. Yes.

JOHN LEVINE: This is very important, thank you. What process do registrants use for uploading their DS keys to go with their domains?

RAED ALFAYEZ: Yeah. They can look into our registry and then upload their domain names.

JOHN LEVINE: Is there any API or is it all manual?

RAED ALFAYEZ: No, no. It's automatic. So there's a form. You fill the DS and there is a verification for it.

JOHN LEVINE: How can I ask this better? If I am a registrant with 20 names, do I have to enter each name individually in the web form?

RAED ALFAYEZ: Yes, yes.

JOHN LEVINE: Okay. All right. Thank you.

JACQUES LATOUR: That was my question. Any other questions? Russ?

RUSS MUNDY: There we go. Thank you. Raed, thank you for that excellent presentation. You guys have done a lot of good work there. And I know this is the DNSSEC emphasis but I was curious if you had similar risk management procedures and looked at the flow of the actual zone content for when registrants provide the information of their DNS records, their A records and so forth to you. Do you have a comparable set of processes, procedures, and emphasis on the content of the zone itself? Because that is actually what DNSSEC is doing is preserving and protecting and verifying the content of the zone. So I'm curious if you've looked at the same set of activities for zone content.

RAED ALFAYEZ: First of all, if someone want to upload his DS, our system will check and verify that the DS matched the DNS key. Currently, this is the only check that we do and we will give him a warning if he want to ignore it then he will have the – we will show a warning message. This will maybe have your zone bogus and maybe people will not be reaching your domain name. But maybe in the future, we can have some tools that look to the zone files, and see are there signatures are valid or not valid. But currently, we haven't done anything. But it's in the plan hopefully. I hope I answered your questions.

RUSS MUNDY: Pretty much but we do need to move on. I want to ask a little bit more later. Julie?

JULIE HEDLUND: So we have a question in the chat and we also have a comment as well. The question, passed it. So the question is from Zainab Al Farsi. What are the main challenges that you faced?

RAED ALFAYEZ: Actually, the main challenges building a team that is specialist in the DNSSEC. And this was the main obstacle for us because the tool was there. Everything was ready but we need to go and read the RFCs, understand the behind the scene of it. The things that you need if you want to build it, you need to have a team that can understand and grasp the different times, the different parameters for the DNSSEC because they are related to each other.

And we spend maybe four months just to know that if you increase the TTL, then the key signature have relation with that and this parameter has a relation with the third one. So it's a little bit easier for us if someone had built actually like a relation between the DNSSEC parameters like a formula. If you put the TLZ 3, then this will need to be doubled the TTL land. That one will be troubled or something like that. So if there is a parameter formula, it will be better. We have it now documented and we plan to do something that will help others but we haven't done. Plus local expertise, building local expertise was the main challenge for us.

JULIE HEDLUND: And we have one comment. The comment is from Abdalmonem Galila. Thanks a lot, Raed for keeping the Arab identity to use Arabic language at your presentation. And you do a good awareness plan using your own local language.

JACQUES LATOUR: All right. Thank you. So next is Kadir Erdogan from Turkey. And you're going to talk about DNSSEC activities in Turkey.

KADIR ERDOGAN: Good morning. I am waiting for the slides. Yeah. There is something wrong with it but anyway yeah, okay. This is Kadir Erdogan from .tr ccTLD. I am the technical manager. Not working? Okay. I am from Turkey and I will give you a short presentation about DNSSEC activities in Turkey. As you see, very colorful country. You should visit it if you haven't done yet. Sorry? Okay.

Turkey might one of the most DNS aware countries in the world. Is there anybody who doesn't know 8.8.8.8? Yeah, if you can see, you can find this configuration from a [inaudible] apartment in Turkey. This photo is taken a few years ago while the government was looking social media by DNS filtering. Everybody in the country learned how to configure their DNSes. I know this is a DNSSEC presentation. But in Turkey, there is no DNSSEC validating ISPs right now. So Google DNSes are important. So by filtering DNS government [inaudible], people knows Google DNSes.

JACQUES LATOUR: Google validates?

KADIR ERDOGAN: Yeah. A short history of nic.tr, the ccTLD. In 1991, first Internet connection established from the University of Middle East Technical University. In 1995, monetizing.tr. 1998, we have established DNS Working Group. It is the early multistakeholder governance model actually. We have all the parties deciding how .tr should be regulated. In 2003, we have established a web application, fully automated applications, payments, document processing, etc.

In 2006, we have implemented IDN. We have six letters, which are not in ASCII. It was easy for us. It is not like Arabic language. In 2008, we have implemented a registry/registrar system. It is not EPP. It is [so based] APA. And in 2010, a Bylaw published by the government, we have a conflict between the ministry, Ministry of Transportation and Communication. We are negotiating, we are still negotiating.

About DNSSEC in Turkey, nobody knows it actually. Nobody cares about it. And it will be a cliché but we are not nobody. We are working hard. We are active people working. Current status, .tr not signed yet unfortunately. None of the big operators validate. And it is not just one of the big operators. None of the operators, I think. And because of that, we don't have a KSK rollover problem in Turkey. Maybe I should return it in – yeah. And decision makers are not aware about DNSSEC.

There are some good things. We are keen on signing as a ccTLD. Technical community talks about it. We are getting a few requests from domain owners to sign their domain names. It is good. And we are organizing some trainings and workshops in the country. What we did until now, the first training happened on 2014. We have hosted the training. And with the help of ICANN and NSRC, we have organized the training. It was a national one. All the technical team of .tr were trainees. Rick Lamb from ICANN and Phil Regnauld from NSRC were trainers.

We have organized another DNSSEC training on 2006, March at Istanbul. It was an international one. We have organized it with RIPE at MENOG 16. Again, Rick Lamb from ICANN and myself from nic.tr was the trainers. Another training was at 2006 again. It was a national one. Those trainings are five days very technical, very complex trainings. It is not easy to organize them. It is not easy to find people to train because DNSSEC is – actually DNS is a narrow subject. And DNSSEC is narrow of the narrow. So it is not easy to find right people.

We have organized another workshop at 2017 at Turkey DNS forum. It was a third one actually. And it was a half day workshop. These are pictures from them. Yeah. That's Rick teaching us.

Who we educated. Until now, we have educated 50 plus technical people, who are mostly responsible for DNS at their organizations. 20 of them were from government ministries, regulators, army; 10 of them from universities, 10 from registrars, and 10 from network operators. Again, as I said, it is really difficult to identify them. But we have a good committee right now. Sorry.

We have to organize more trainings because we taught experts DNSSEC is a grenade. You don't know when will it explode. So we need more experts. We need workshops. And we need gossips. I said gossips because we have to make big boss to be a friend of DNSSEC. If you talk technically, they don't know about it. They don't understand about it. So I think gossip is the right word.

What is next? Sign it. Anyway, thank you. By the way that is my voice. That's all.

JACQUES LATOUR: Thank you. That's pretty good. That's the first time we got one of those. Any questions for Kadir? Yes, Christian?

CHRISTIAN: I'm with .nl with the registry for the Netherlands. Where do you think that DNSSEC is supposed to start in Turkey with the ISPs in terms of validating or with the registry in terms of signing?

KADIR ERDOGAN: Actually, it's just not with us with the ccTLD. We should sign it first. Then the ISPs I guess.

CHRISTIAN: Because we follow the same model in the Netherlands. So initially when we started to sign, there was nothing either on the validation side and we just – I mean you got to break the tie somewhere and we started at the registry side.

KADIR ERDOGAN: Yeah.

JACQUES LATOUR: Questions? Jeff.

JEFF HOUSTON: I noticed over the last year and a half, the use of Google's public DNS has actually dropped from around 23% of users in Turkey to around about 7%. Is this because they've stopped Google or the ISP's putting in DNS interceptors?

KADIR ERDOGAN: I don’t know the right answer to that. But I can say my guesses. I think government is intercepting things, I don’t know exact stage.

JEFF HOUSTON: Does this prompt an interest in forms of encryption and tunneling DNS privacy that kind of prevent that degree of first mile interception? Is there interest in that technology to get around this problem of forced interception?

KADIR ERDOGAN: I don’t know what changed.

JACQUES LATOUR: Questions? All right, thank you. So next one is Rajiv Kumar from NIXI. So the .in registry DNSSEC update.

RAJIV KUMAR: Good morning all. Hello? Good morning. I am Rajiv Kumar from nixi.in registry. System analyst in [inaudible] registry. It is a good opportunity give me – hello? It would be a good opportunity to update .in registry updates, DNSSEC update. And the agenda is the .in registry DNSSEC and registrar participation, registry’s efforts, resources for registrars, DNSSEC validations, and the current status.

.in registry is an early adopter of the DNSSEC. .in zone was signed in 2010. We conduct DNSSEC Friends and Family Program. In this program, we can allow top ISP and registrar to test their environment, play with environment. And if there is any bug, then come at me and we will do all the things.

After one year in 2011, DNSSEC were introduced in testing environment. So where we start DNS testing environment for the registrar. Then tested registrar test their environment and allowed the registrant to sign DS record. After one month in 2011 November, we are accepting DNS record.

The registrar participation, we have 121 accredited registrars all over the world. Out of these 39 are DNSSEC enabled including the top 10 registrars of the .in registries in developed DNSSEC. They provide DNS services to their registrant. We are 2 million domain name registered [inaudible]. Out of that, 1287 were signed as of September. It is less than 1%. But we are trying [my] best to do better.

We report that we conduct session of registrar to encourage them to promote DNSSEC. We are conduct every year one face-to-face meeting with registrar [inaudible] and give a presentation. As well as we are organize hands-on training, workshop, awareness program for technical community like ISP [government] India and registrar with the help of ICAN, APNIC. During every year, we conduct a SANOG. It's the South Asia Network Organization Group where we organize a DNS hands-on training for five days.

The resources of [registrar] level on our website, the EPP RTK add-ons available on registry website. Update EPP client to support DNSSEC command. DNSSEC OT&E environment is also available in our website.

As for the validation part, we can get the individual researchers the status of India. And give me a status of the 447 name server, open resolver. Out of the 34 name servers are validate DNSSEC only. 144 name server are aware of DNSSEC but not validate yet. 299 name server do not support DNSSEC. This is the status of validation in India, validation part. And we are also support the IDN domain name in DNSSEC signing. And [inaudible] signed and it is good for us to IDN start signing the joint domain name. Thank you. If any question?

JACQUES LATOUR: Thank you. Any questions? Russ?

RUSS MUNDY: Thanks for the presentation. And I'm curious if we could go back to the validation slide, I think it was the one just before this. How you identified the numbers of validating resolvers?

RAJIV KUMAR: Actually, there is in university, and Amrita University they conduct and evaluate the Indian community and maybe there is a tool that provide me the status of the DNS validated parts and all that.

JACQUES LATOUR: So do you think there's more open resolver in India than that?

RAJIV KUMAR: Yeah.

JACQUES LATOUR: Way more?

RAJIV KUMAR: Maybe. This is subject. I will check with Amrita University and get back to you because they provide me the status of that.

JACQUES LATOUR: Thank you. Any other questions? Three, two one. Okay, thank you.

RAJIV KUMAR: Thank you.

RUSS MUNDY: I think there was a question online.

JACQUES LATOUR: Sorry.

JULIE HEDLUND: There will be a question in the chat although it's not ready yet. But I just wanted to also note that Abdalmonem Galila is not able to be here but has recorded his presentation, speaking through his presentation on an audio clip. So we'll go ahead and start his presentation with the audio clip, and so he won't be here. Virtually, he will show up later for the Q&A, he just has a conflict right now.

RAJIV KUMAR: One second because I don't understand the question.

ABDALMONEM GALILA: …Deputy Manager of .masr ccTLD. Also I am ICANN Fellow and Task Force on Arabic Internationalized Domain Names member. [inaudible] means in Arabic [inaudible]. My presentation will be about the challenges we had during the deployment of DNSSEC. Actually I will say the challenges before and after the deployment, and I will talk a little bit about DNSSEC automation script. We used to sign or resign .masr [inaudible]. Next slide.

We deployed DNSSEC for .masr ccTLD in 2015. Before the deployment of DNSSEC by six months, we didn't have an idea about DNSSEC. At least we should know what is DNSSEC and how DNSSEC works. We heard the word DNSSEC at Africa Internet Summit 2014 in Djibouti. From there, we started thinking about the word DNSSEC. And wanted to know some information about DNSSEC and we got that through attending DNSSEC workshops. We had two environments for that mass registry system.

The first environment is the production one. And the second one, we used it for testing, which is completely identical to the production one with registry database, 3 DNS server WHOIS. We still want to have a certain information about how DNSSEC works so we had to build fake root server and the resolver with DNSSEC validation enabled at our testing environment. We did that and we did have the information required to start the deployment of DNSSEC at our production environment.

At our testing environment, we signed the zone of the .masr and all were working well. But our version of registry software was all the version regardless to adding of DS recalled feature for .masr child domains through registry interface. By the way, we use CoCCA registry software. So we upgraded the registry system and it was working well. One of our testing DNS servers time was delayed by 10 plus minutes. So we must make our system timely synchronized so we build a time server and make all our server as client to the server.

We wanted to secure the communication between the master and the slave DNS server so we used TSEC Transaction Signature to handle this issue at our testing environment. And we tried to be familiar a lot with DNSSEC troubleshooting before we went to a line with DNSSEC. After testing succeeded, we wanted to replicate what we did in the testing environment to our production environment. And we took less than 15 minutes to reconfigure the production environment to have DNSSEC and this TSEC deployed.

Most of the problems with DNSSEC are related to firewalls. So please make sure to involve your security and networking administrators so that they can make the required changes before taking DNSSEC into production. There are two types of firewall problems are most common. The first one involves the TCP, the Transmission Control Protocol. There is a misconception among firewall vendors and security administrators that you delete user data ground protocol – sorry, DNS queries use UDP and that zone transfer use TCP. Unfortunately, this assumption is not entirely true. DNS queries first try UDP but revert to TCP. If no response is received from the initial UDP query. Or if the response leaks important information because it is truncated, the possibility of something in the past looking and the response to the initial query is much higher with DNSSEC because of the increased size of the responses. So for DNSSEC to work correctly, it is mandatory that you open your firewall. It is mandatory that you open your firewall for both TCP and UDP over port 53.

The second problem is related to IP buffer reassembly size. The old source of DNSSEC standard realized that a potential problem might exist with TCP queries. TCP bots higher burden on the DNS servers. TCP is much more expensive to process than UDP. To avoid too much TCP traffic, the [inaudible] the EDNS(0) extension mandatory for DNSSEC. EDNS(0) is one of the extension mechanism for DNS. A standard that among other things allow a client to signal that it is capable of receiving DNS replies over UDP that are larger than the previous limit of 512 bytes.

Some firewalls are not aware of the fact that EDNS(0) standard allows for larger packets and the easier block EDNS packet using

EDNS(0) or block any DNS packet larger than the 512 bytes regardless of EDNS(0) signaling. Other firewalls allow for the larger packets by default whereas a few vendors require the firewall to be manually configured to do so. It is defined in the bus that does packet is make sure that the application layer must be aware of EDNS(0) standard to be able to make the correct decision about whether to forward the packet or not. It is not enough to test that you follow your firewall allows large incoming DNS replies by sending DNS queries to the Internet.

You must also test that an external source can receive larger DNS replies that your DNS server is sending. One way of doing so is to use open DNSSEC aware resolvers. So you have to test and configure your firewall to allow for use of EDNS(0) and for DNS packets larger than 512 bytes over UDP. Finally, we ask .masr administrative contact to submit the DS record to ICANN to check and add the code inside the root zone.

Next slide. After the deployment of DNSSEC, we showed know how to keep our system online all the time without signature expiration. So we did a script for resigning the zone after new zone generated from the registry system with the capability to look any errors for the administrator. DNSSEC also introduces new operational tasks such as rolling keys, resigning the zone. Such tasks must be format at regular intervals. We didn't do any rollover for the keys until now. But we will do during this year.

Again, we should be [inaudible] your firewall for DNSSEC. Most problem with DNSSEC are related to firewalls, take care. So you have to make sure to involve again your security and the networking administrator. Our mission now is to spread the word DNSSEC to our four local registrars. Next slide.

Also we noticed that one of our DNS doesn't respond to CB queries. The [MQ] most commonly found in the core of the internet is around 1500 byte. And even that limit is routinely exceeded by DNSSEC signed responses and may network elements limited to this size of [MQ] that mimic this signed response to be dropped. So to avoid that, we signed the zone with only ZSK. Most of our ISP resolvers don't have DNSSEC validation enabled until the moment. Also it is only one line of the configuration. Next slide. Next slide.

Most of our registrars are ISPs. They think that it is difficult to sign their domains and not [inaudible] it to do that. Also they have another thought that their system is stable so why do they have to change the current system. Next slide.

Other thoughts like more time required to resolve the domain names. Also the security gain will be better. Domains with invalid signatures will be blocked. They have attacks but they can mitigate it. The registrants don't have an idea on DNSSEC. And registrar interface doesn't have the ability to send DS records to the registry system through ABB. Not enough staff to monitor and troubleshoot DNSSEC. Next slide.

Now I want to show you the structure of the .masr signing and resigning automation script. This script was originally done by CoCCA to only handle newly generated zone files and was edited by the .masr team to handle DNSSEC signing as well. Next slide.

The structure of the script started with some variables initialization like the director of generated zone files from registry, the director of generated –

JACQUES LATOUR: That's it. Thank you. Any questions? All right. We're just on time for the break. So we'll see you in 15 minutes.

JULIE HEDLUND: I know that Abdalmonem was going to try to come for Q&A but I don't know if he's here, if he's made it. And here he is. So if we do have any questions –

ABDALMONEM GALILA: Our script started with some script initialization like the director of newly generated zone files. And the director with the signed zone will be in. And then apply some checks for the newly generated zone files to see if this zone is generated in order to apply some DNSSEC first or not. Then after that, we unzip the registries automated generated zone file. And it is generated at the file from the registry.

So if you have many zones you want to generate it, you want to DNSSEC sign it using our script, it is acceptable. Just look for zones. And then we sign the zones and after that, we use rndc reload. Maybe you wanted to restart your buying software. But I don't recommend that if you have many number of domain names like other registries but you only have around 800 domain names, IDN domain names. Next slide.

This screenshot of our automation script, the first one will be the initialization of variables. Second one will checking if the zone file, if you change it or not from the previous one. After that, unzip the zone file, after that I will look for the zones if I have multiple zones to DNSSEC sign it. After that, I use rndc reload. And that's all from me. Thank you.

JACQUES LATOUR: Thanks. Any questions?

UNIDENTIFIED MALE: Thank you Abdalmonem for this two halves of the presentation. One is remotely and one was physically. I have a question. Do you accept staff accepting DS records for your customers? And have you done any tools to validate their DNS or not?

ABDALMONEM GALILA: From day one, we accept DS records from our registrars. But until now our problem that our registrar not aware enough about DNSSEC. And same as our client, our registry not registrar. So accept only DS record from our registrar. We only have around eight domain name, DNSSEC signed only.

UNIDENTIFIED MALE: Thank you.

JACQUES LATOUR: Any other questions? All right. So now we're officially on break. Back in 15 minutes. Or no, 10:30.

[END OF TRANSCRIPTION]