KOBE – DNSSEC Workshop (1 of 3)
Wednesday, March 13, 2019 – 09:00 to 10:15 JST
ICANN64 | Kobe, Japan

RUSS MUNDY: …long ways from where most of the meetings are but we'll be starting in here in about two to three minutes.

I think there's going to be plenty of room at the table, so please come on up to the table if you like.

JACQUES LATOUR: Good morning. We're ready to go. Welcome to the DNS Workshop in Kobe. So, we'll start with the presentation on that we usually do is deployment around the world for DNSSEC. How many here it's their first DNSSEC Workshop? I knew that. No? Him, that's his first time. Alright. So we got some new faces.

Okay. This is our Program Committee. How come the log bar shows up? Okay. It's weird … there's a little … oh, it's okay. It's alright.

This is our Program Committee. A little bit about the DNSSEC Workshop. We meet once a week and then we build the program for the next workshop and we do this year round. So, we do add some learn from the previous meeting and we try to make the next one better with relevant topics.

Today we have a lunch. I guess that's the second most important thing since it's the second slide. We have a lot of sponsor now that Steve is working on recruiting and getting funding for lunch in the DNSSEC gathering event. So, the sponsors provide the funding for our lunch. We also had a DNSSEC gathering event yesterday. It was hosted by JPRS and we had some good attendance for that event.

The DNSSEC Workshop is a joint initiative between SSAC (the Security and Stability Advisory Committee), and we're working with the ISOC (Internet Society) with the Deploy360 Program and they have a lot of information on DNSSEC deployment on their website.

The program today is – we have two major parts. We have our normal regional panel session where we get people in the region to talk about their DNSSEC deployment and initiatives. And then after that we have a break and then before lunch we have a panel on DNSSEC. So, DNSSEC, DNS over TLS, DNS over HTTPS session. So this should be really interesting to attend, and then hopefully we'll have time to do Q&A and then see where that stands.

We have a lunch at noon, 12:50 actually. You need to have this coupon to attend the lunch. No coupon, no lunch. But I think we have more than enough coupons here for today.

Then after lunch we have our special session which is KSK future discussion to figure out the rollover of the root key, if we should do that on the weekly or on a daily basis, so we'll have that discussion.

Deployment around the world. Counts. Counts. Counts. So, we're tracking the DNSSEC deployment. So if you look at this there's a six and the last couple of months, the trend went down before the KSK rollover but I think it's picking up now. People are turning back on their resolution. We're at a most 19%. So, this is good. Hopefully the trend is going to keep going up for DNS resolution. So, this is a test by APNIC where they measure around the world the ability for resolver to validate DNSSEC.

This is the stats of Asia on the deployment of DNSSEC. So, Micronesia is at 66% and then it goes all the way down to two. And their table shows the usage – the resolution using Google DNS which does DNSSEC validation versus ISPs doing it on their own. So, you can see the trends. So there's still a lot of work to do but it's coming along.

This is a new graph. It's hard to see but the first column is .com with 800,000 signed domains – is that the number? 876,000 for .com, followed by .nl with 640,000 and then there's .net with about 100,000. No, the second one is .sc., .net with 100,000. And then top ten is 4,000 with .arpa. So I think we have a lot of way to

do to get more domain signed. So, I think this is where we need to focus on.

UNIDENTIFIED MALE: [Andre] have some comment about [inaudible].

JACQUES LATOUR: And you don't chew up.

[ANDRE]: Yeah. I just want to say those numbers are wrong.

JACQUES LATOUR: So we'll show that.

[ANDRE]: I checked like three of them and all are wrong.

JACQUES LATOUR: Let's start to Dan York then.

[ANDRE]: And also if you look – no, no, these are all wrong.

JACQUES LATOUR: No, I agree. So we need to review this but take a note.

RUSS MUNDY: This is good. We want to hear input from folks and one set of collection statistics is just as wrong as right. We look in detail at it. This is the SecSpider result that's – yeah.

JACQUES LATOUR: So I'll fix this. Next session we'll have better stats. And then we build a map with the different status of the ccTLD with their deployment. So there's various stage in deployment, meaning someone can announce they want to sign their TLD, where it can be all the way to – we have a DS in the root but the registrar don't accept the information or they don't support CDS. And then the last stage before green is they're fully operational with DNSSEC for the second level domain.

So if we look at the map, we actually made good progress because five, six years ago there was a lot of red and a lot of empty. We have a couple of areas to focus on which is Africa and a little bit in Asia and Latin America. We have different initiative in this region to try to get more ccTLDs signed. The beauty is it's getting easier and easier to do this. The science behind it is more easily affordable and usable.

So, Africa, we had sudan.sd that is announcing they want to sign, so we'll track that progress over time. That was the only – since the last ICANN meeting, the only one that announced they were signing. That was the only change that we've noticed in the last three months.

Asia, we got a little bit work to do. There's a couple DS in the root so we need to figure out – probably the challenge for us is to figure out when a registrar is actually accepting DS for those domains. Yeah. They need to tell Dan at ISOC or send an e-mail on the DNSSEC coordination mailing list to say they're accepting DS, so they're fully operational. And that's how we update this mailing list. There's no real way of knowing they're fully functional or not with this. But when there's no DS in the root, that's easy to see.

So, we have one last little green spot. So which one is this? Light green? Oh, there's two, yes. That's right. Croatia? Okay, so we have two more to work there to make it 100%.

UNIDENTIFIED MALE: The Scandinavian one is Oland, I think. That little Swedish-Finnish island. Say it again?

RUSS MUNDY: Mike, you're up. Please.

[MIKE]: Yeah, the little point island in between Sweden and Finland is called Aland, if I can properly pronounce it, .ax.

UNIDENTIFIED MALE: Dot ax?

[MIKE]: Yeah.

UNIDENTIFIED MALE: Yes. And I have one more addition. Slovak announced already the start of DNSSEC, so the last white spot now disappears. They should start it quickly, Slovakia the neighbor of Czech Republic.

JACQUES LATOUR: Oh, yeah. Sure. Those are not oceans, right? So, maybe we should have different colors there. There are – yeah. Okay. So, making progress.

Latin America is getting on its way. I think LACTLD has a low focus on getting more signed within the community and Fred is doing all the work on his own, so he's a good guy. Keep up the work.

I thought Greenland was full green. So, we got to figure out – but that was the last one in the North America.

You can download the map here and if you know or hear about another ccTLD in the region that is signed or making progress, e-mail Dan York or e-mail our DNSSEC coordination mailing list, and then we go there. ISOC is working on a DNSSEC history project. So you can go to that link and update the history as you see fit or have a look there to see what's in this project. And that's about it. Any questions?

RUSS MUNDY: This is Russ Mundy. Eric Osiakwan was here.

You want to say a comment in response to what [Andre] saw on the map?

UNIDENTIFIED MALE: Hey. Yes. I operate SecSpider and I'm certainly happy to have a contribution [it sounds right] now. It has to go out and discover them, so what's kind of reported is what has been tracking in for about 15 years or so. So, definitely interested in chatting if you have a corpus, we can put in there because it tracks all the way down to as low as you want in the hierarchy. It does stuff like tracks 12 LDs and stuff like that. So, it'd be cool to talk and show you – maybe get on base with you if that's cool.

UNIDENTIFIED MALE: Yeah, because there's a lot of [signed zones in cc].

RUSS MUNDY: Okay. Yoshiro, could you come join us at the front and we will now move into our regional panel. I think we have plenty of chairs. And as you can see we have four panelists from the region and we'll be – some have – do we have some slides? We may or may not, I'm not sure. Oh, okay. Wonderful. Thank you.

So, we'll just start and go in the order of the listing on the program here. Kenny Huang is from Taiwan and will do the first presentation.

KENNY HUANG: Okay. Good morning, everyone. My name is Kenny Huang, CEO of TWNIC. I'll just give a very simple brief introduction about our DNSSEC deployment in Taiwan. On the first page, it just introduce the [inaudible] trend from Google Trend for DNSSEC around the world. Okay. Next slide please. Okay.

That's introduction regarding to the Internet ecosystem governance structure. In terms of governance structure, it's more likely like the incentive model, whether we have sufficient incentive to promote certain technology.

For example, for governance structure we need to consider three components, three phases. The first component is market demand. The second component is network. Network stand for the upstream and downstream supplier. The architect – the hierarchy is same for the regulation model of governance model, whether you have sufficient regulation to promote certain technology.

So, here we take our DNSSEC as example. DNSSEC has tried to – sorry. DNSSEC from market point of view, there's very weak demand from – oh sorry, keep a distance. We saw a very weak demand for secure DNS resolution in terms of resolution. Their marketing is actually is quite weak from local – from Taiwan point of view. The network in DNS Working Group has been developed in ITF and Technical Committee pushed harder to adoption at ICANN and also pushed deployment around the region.

From hierarchy point of view, Taiwan government agency support deployment for DNSSEC and TWNIC also develops .tw signing process but TWNIC only registrar contract didn't require DNSSEC implementation, so next time we're trying to take some certain measure.

So, you can see there's some list from TWNIC registrar. With [inaudible] on top of the registrar level, meaning they have

deployed DNSSEC. So, we can see only six registrars among the 13 that have been providing DNSSEC service. So, we are trying to discuss with these registrars to see what's the problem, how to encourage them to deploy DNSSEC.

Here you can see a statistic for DNSSEC specific for the second level domain. You can see like the com.tw almost zero percent deploy DNSSEC. Most likely, edu.tw that belong to academic/education institution, they're around 10% of them deploy DNSSEC. So, we still a way to go to promote the DNSSEC in .tw.

So, that's based on our operational feedback why and how we're going to deploy DNSSEC. At DNSSEC basically, they communicate like [man in the middle] attack less significantly but it doesn't guarantee the rest of the security issue we're concerned especially a malicious website, malicious domain. That's most of results we get encounter we got into DNSSEC security. And DNSSEC didn't provide much value added service to big operator, big service provider, that is why they're reluctant to deploy that kind of service. And operator, especially DNS operator, is reluctant to mess up the DNS setup because DNSSEC is too new to them. Although DNSSEC have been deployed for years but still from their operational experience, they prefer more conservative configuration, conservative software deployment. And if anything goes wrong with their DNS

configuration, you'll probably lose your entire Internet presence. Actually, based on our [measure], a lot of DNS configuration error in Taiwan so we also need to do a lot of work to mitigate that kind of situation.

So, what's our DNSSEC penetration strategy? Basically we were focused on three dimensions. The first area will be the contract enforcement. Basically, we've been proposed to the contract enforcement to enforce all the regular support DNSSEC but we see a very strong objection previously but we see it continue to dialogue with the registrar to see how possible to enforce based on contract enforcement.

Second category is we're doing from time to time is capacity building. We've been conduct a lot of DNSSEC training, DNS education training, operational training, hands-on training to the operator. So, we still continue to allocate resource for capacity building. The second category would be, we encourage the so-called DNSSEC hosting. For example, TWNIC also provide DNS hosting if the registrant – their registrar didn't provide hosting, we can happy to provide. In the current stage, we can happy to provide a DNS hosting for them.

Okay. That's my very simple presentation. Any questions? Thank you.

RUSS MUNDY: Okay. Thanks, Kenny. Bruce, do you want to do yours from there?

BRUCE TONKIN: Yeah. From where I am, yeah.

RUSS MUNDY: Bruce Tonkin from AUDA.

BRUCE TONKIN: Thank you, Russ. I'll just give an update I guess on the deployment of DNSSEC within Australia, within the .au zone. It's fairly minimal deployment. We've had DNSSEC available for some years but the take up is extremely low. There's about 1,400 domains that are signed. That's out of a total of about 3.2 million names. Because there's such a small number of names, 1,400 names, I've actually looked at them individually and got a little bit of a sense of the organizations that have signed.

In terms of some well known corporations in Australia, there's only three that have signed. One is a consulting company which is Accenture, one is a telco which is Vodafone, and one is a trucking company which is Scania. Really no banks, no government organizations have signed, so it's only a few that have signed. Other than those few corporates, there's a few

small businesses, a number of the registrars, a number of sort of hosting companies have signed their zones DNSSEC.

We've got quite a bit of concentration in the market between these three large registrars that between serve about 80% of the market. All three of them do offer DNSSEC but it's not something that is promoted to customers in any way, so if you're a small business and you know about DNSSEC, you can go to one of the larger registrars and they'll be able to sign your zone. And I think a lot of them do that through their customer service teams rather than through a convenient online interface. You certainly don't go through the checkout and say, "Tick the box and get something signed." So the process is complicated.

Apart from three corporates, some registrars and tech companies, the other major category of people that have signed websites are the adult pornography industry. So they seem to take security more seriously than the banks, it seems.

And so the question would be why has there been such limited take up? I had a discussion with one of the large telecommunications companies in Australia, and their perspective was that because there are so few DNS resolvers in the market that actually check the DNS signatures, they didn't want to turn on their resolver because they're one of the major telcos, because they are afraid that if customers couldn't get to

websites, those customers would blame the telco for something wrong with their service. When if I went through one of the other major competing telcos, they'll be able to get through to a particular website. And so they were worried that companies that don't maintain their DNS signatures properly that when this signature check hack happens, the customer gets blocked and they were afraid that that would reflect poorly on their service because most people don't understand why they're not able to reach a website and they'd just assume there's some problem with the telco. So, they were worried from a reputational point of view that they would stand out from their competitors essentially.

That's led me to be thinking that that probably in Australia we really need to focus on getting the major ISPs to collectively start turning on checking the DNSSEC signatures in the DNS resolution. And that then gives the incentive then for banks and other organizations to actually start signing their zones.

One of the initiatives that we have in Australia at the moment is we've got a project that we're sponsoring which is first you're going to develop a site to test for small business to put in their domain name, and typically we check out their website and check out what security features they have or don't have. One of those things we will check and notify the people is DNSSEC signatures.

But I'm also thinking we need some testing almost it's tempting to actually register variations of major corporate brands and then set them up on websites with false signatures and then when they use a lens on that saying, "You've landed on this page, which you shouldn't have, please contact your ISP and ask them why they haven't got DNSSEC in [inaudible] on their resolvers." Because right now there's now customer push either toward ISP to have any kind of any DNSSEC checking. So, we actually almost need some sites there that when you reach, we get a message saying, "There's no way you should've reached this site if you provide a head set up their infrastructure properly."

One of the trends I am seeing in Australia is that users that have more tech aware are starting to use public resolvers. So, the Google resolver is quite popular. Others are Cloudflare and Quad9. The government in Australia is interesting; it doesn't have a signed zone. It's the only second level zone that's not signed, so we have com.au, net.au, org.au all signed, the only one not signed is gov.au, but they are planning to progress with signing gov.au in the next month or so. So, that's positive progress. And the Australian government has just issued a tender for a DNS resolver service for use by government organizations, and they're looking to have their DNS resolver service take in feeds from [any phishing] feeds and things like

that to block government users from being able to go to sites that may have malware or other things, but I'm assuming that that those resolvers that they're looking at will also check the DNSSEC signatures. So, a bit of progress in government but pretty slow.

Generally, in summary, we don't have many domain names signed. One of the causes is lack of use of resolvers in Australia at least in the major Internet service providers and telcos that check DNSSEC, and that's where I'm going to sort of focus some effort in trying to collectively get them to actually use appropriate resolvers in their networks. And then I think we can do push to get domain name signed.

RUSS MUNDY: Okay. Thank you, Bruce. Do we have questions for Bruce? Yes, Paul.

PAUL: On your comment about telcos and reputation and their concern about turning on – I suspect this is really more of a concern about support calls and that cost than it is, and my response to that the numbers about two years old for Comcast. I can get you with the Comcast Team to get you today's numbers. But at the time that we were doing a half a trillion queries a day,

we were getting about two dozen DNSSEC-related issues a month. So, the support cost was such that their Comcast management was purportedly happy to have us take what was effectively – it's $25 a call was the metric we use. If someone picked up the phone and said, "Hi, Comcast," we just spent $25. And so I think it's safe to say that the cost or support cost to an ISP for someone else blowing up their own zone has gone down pretty dramatically.

BRUCE TONKIN: Has gone down, did you say?

PAUL: Yeah. If you get to the point of half a trillion queries per day generates two dozen incidents a month, that's a pretty good percentage.

BRUCE TONKIN: Yeah, that's right. Some data on that would be helpful. Yeah. So, I was just telling you what I was told rather than trying to argue with them. But absolutely, yeah.

PAUL: I'll get you with the Comcast team.

BRUCE TONKIN: And you are right, it's too far I think, its customer service cost in comparison with what the competitors are doing. Yeah.

RUSS MUNDY: One other point I should have made earlier is we are in a room that does have translators, so I ask everyone to speak somewhat slowly so that the translators have a good hope of keeping up with us. And also we should always remember to say our name before we speak, and so in view of that, I'm Russ Mundy and I have a question for Bruce.

Since the statistics we showed earlier about the adoption generated those work come from APNIC and it's Geoff Huston's work along with others but primarily Geoff, and that's included looking at the use of the public resolvers that are [due] in DNSSSEC. Have you had any interactions with Geoff or anyone else in the organization to see if there are possible information sets from that work that they do that could help convince some of your ISPs particularly if the ISPs are not getting the data and the traffic flow that they might want to get because they are not doing DNSSEC if they're going to Google or 999 for validation?

BRUCE TONKIN: Yeah. Well, I don't know – so, you're trying to make a pitch saying you would get more traffic on your network if they were using your resolver, is that what you're saying?

31:41

RUSS MUNDY: The people who are using Google or other public resolvers are usually not doing it because of DNSSEC but it can provide a good measure and comparison because very often – I shouldn't say very often. I know the reason people operate these public services, so they get data and material to deal with and ISPs can also acquire information from the data that comes to them from the traffic [inaudible].

BRUCE TONKIN: From the traffic information. Yes. So, data mining the DNS traffic. Yeah. Yeah, that's possible. Yeah, look, I think Geoff is certainly being consulted on this project that we're looking at for a new website to help small businesses test their domain names. It's actually based on the concept in the Netherlands. They've got a website called internet.nl. It works globally. You can type in any domain name and it runs a series of checks. And so we're working with Geoff. Part of the debate is how much do we bias the effect that a site has DNSSEC in terms of the score they get. So, we're going to score and you get a score out of 100, let's say. So if you don't have DNSSEC, is that worth 1 point, 10

points? So, we're having a debate internally in Australia about how to score. But yeah, I think if we can get a combination of data peps and Comcast peps from Geoff's reports, and being able to give decision makers in the technical areas of ISPs just the data and the facts, so I think that would be helpful. Yes.

RUSS MUNDY: Warren.

WARREN KUMARI: Warren Kumari, Google. Just a correction to something that Russ said. At least one of the large DNS open public DNS providers definitely does not do this to get information. We've got a very clear statement on our 8.8.8 privacy thing saying we don't use this data for anything blah, blah, blah. The obvious question then is why do we provide the service? And it's simply because a lot of ISPs resolvers either make up answers or are just really slow and so the reason Google runs this is a faster Internet means more people use the Internet, which means more people click on ads, which means Google gets money. So it's not completely selfless but it's a service which we run so that people get fast answers.

RUSS MUNDY: Okay. Thanks, Warren.

WARREN KUMARI: I'm [contractually] obligated to say that or my lawyers shout at me.

RUSS MUNDY: Yeah. I should've not made it such a blanket statement but a number of them do do it for the data collection. Barry.

BARRY: And another very minor correction to something Russ said. They're interpreters, not translators. That's a very different thing. And in this meeting we only have two language choices besides English, it's French and Spanish. So, unfortunately, you can't use Japanese.

RUSS MUNDY: Okay. Any more questions or comments for on Bruce's presentation? Thank you, Bruce. Okay. Next we have, David Morrison from internetNZ.

DAVID MORRISON: Good morning, everyone. Great. Next slide please.

I'm just going to give you a brief more non-technical overview of the DNSSEC adoption in New Zealand. We've got a full DNSSEC

practice statement on our registry website if anyone's interested in the technical details of how we run it. Just a quick plot at history. We deployed DNSSEC back in 2012 and figuratively in terms of our normal operations, it's mature. It's core to our key operations now and the architecture aligns very closely with our disaster recovery and business continuity plan, so it's very much part of what we do rather than an addition to what we do.

Since 2012 we've had really low registrar adoption. So, we have 88 authorized registrars and 2 of the 88 only offer signing and 7 offer support for DS records. So, in terms of engagement with our registrar community, we have quite a lot of works still to do. Probably similar as to what Bruce was saying with the AU environment.

Let's jump to the next slide.

Current state. One of our success here is for DNSSEC is our .gov.nz zone signed and it's 41% of the 1,000 .gov.nz domain names have been signed. So it's pretty good adoption. The government in New Zealand deployed – we now have 10 different new registrars and DNSSEC was part of the requirements of the platform. That was a number of years ago and I think they're in the process of moving to a new platform now. So DNSSEC's baked into the key requirements.

Out of 714,000 domain names, we only have 1,649 that were signed, so really low adoption there. From secure, just over 1,100 names.

Checking on the most popular names using DNS traffic to determine popularity, we've only got 195 of the top 10,000 websites in New Zealand signed. Again, we have quite a lot of work to do.

Chatting with some of our Technical Team, we are seeing use of DANE and SMTP for opportunistic encryption. From a validating perspective, I think we're doing okay. We've got a few large ISPs that have turned on validation and so we're covering a little over 60% of New Zealand is behind validating service. So that's some good progress.

Where to from here? For us, it's really going to be about education. I think less about education of the end user. I'm leveling more around the ecosystem, network operators, and registrars. I'm very much against the perceptions of complexity. In recent years, more tools are coming on board to help automate DNSSEC processes, so we're looking to educate folks, that it's not as complex and hard as they might think. Also looking to check all the economics of change. Other big changes are in HTTP so IPv6 PDP as sort of relatively slow adoption and then building over time. So we need to tackle that.

Finally, registrar adoptions, we're probably not going to – I don't envisage that we would enforce registrars to take on DNSSEC or to at least offer. But looking at ways in which we might be able to incentivize our own courage and to provide greater services too and security to the consumers or the customers.

` That's really brief snapshot for New Zealand. Thank you. Any questions?

RUSS MUNDY: Okay, do we have … Yes, John?

JOHN: I'm going to ask the question I always ask, which is if your DNS is not hosted at your registrar, what's the process for getting the DNS Record into the zone?

DAVID MORRISON: That's a technical question that I'm probably not equipped to answer.

JOHN: Okay.

DAVID MORRISON: I can get an answer for you and come back to you.

RUSS MUNDY: More questions for David. I have one if there aren't others. I noticed the Hide option in the Validation. You said that was primarily from getting the larger ISPs to turn on validation.

Have you seen, since the validation was turned on, any change in number of sign zones? In other words, by having more validation present, does that have any observable effect and how many of the zones are signed?

DAVID MORRISON: Given the low uptake and the numbers now that you're not really crediting significant spikes or change.

RUSS MUNDY: Is there an education program that you all are looking at organizing and pushing to try to get this, especially since you have so many validators in place perhaps with your partners there in Australia, in terms of the education type of thing just to get more people interested.

DAVID MORRISON: We've got a program we're going to start reviewing. Our security [inaudible] ccTLC operator. We're going to be doing that with our registrar community over the coming year. So DNSSEC will

also be part of looking at lifting I guess in improving security landscape in New Zealand. Whatever we're doing in that security space would also encompass DNSSEC. Also, we're looking at how we can improve our engagement with registrars with this specific attention.

RUSS MUNDY: Any other questions for David? Okay. Thank you, David.

Next we have from one of our host activities for this meeting, Yoshiro with JPRS perspective on DNSSEC activities.

YOSHIRO YONEYA: Good morning. This is Yoshiro Yonira from JPRS. I also DNS host .jp board member. DNS host .jp is a DNS community acting in Japan. I introduce the DNSSEC deployment status and our outreach activity. You got into the root KSK rollover today. Next slide.

First, I explain about the status of the DNSSEC deployment in Japan. For the validator side, some major ISPs providing DNSSEC validator to the users. Some of them provide full service but some of them provide opt-in, partial service, because many ISPs are still very worried about the DNSSEC failure. If people suffer from the DNSSEC failure then support operators have to have low [inaudible] from the end users but the support

operators don't know the root cause of the failure. So they're afraid of the cost of the operation is getting higher. But recently many ISPs are going to search on [inaudible] data.

The signing side, we have very few signed zones in Japan. So this table shows that some organizations – very important organizations – who have signed. For example, governmental organization is about 800 but only 15 signed. So you can see the statistics on the website dnsops.jp provide.

Many of DNS operators expect the driving force of DNSSEC deployment. TOKYO 2020 Games is a big driving force because the cyber security has a very high priority. Do you know DNSSEC is one of the very important building blocks to provide cyber security integrations.

We also have G20 Osaka this May and we also have Rugby World Cup this September. So these kind of big events requires very high cyber security so that DNSSEC will be used to secure their website.

Service improvement in registries, registrars, and DNS providers are also going on. For example, Elliptic Curve Cryptography for the DS Record will be provided from the registry. I hope this is within this year.

Some automated DNSSEC or key management support from the DNS providers will also provide it in the summer. So there is no official announcement at this moment but I know many operators and they say they will do it. So I am very positive this will happen in the very near future.

Next I explain about outreach activities regarding to root KSK rollover. In Japan, DNS ops started raising awareness of the KSK rollover since 2015. So very early. We started very early. We made a lot of presentation at Internet conferences and NOG meetings. JANOG is one of the biggest NOG meetings in Japan. Also DNS hosts community meeting. At that time we use a very strong term like “IP fragment” will be coming or “Internet-wide outage” will be coming. We have to attract people to know this very big event. Also, we provide the document in Japanese, the local language.

Technical community provides a lot of documents in English but very few in Japanese. Some or many of operators do not read English so the translation work is also important. Also, Japanese government [inaudible] is Ministry of Internal Affairs and Communications pushes the DNSSEC and KSK rollover preparation to many governmental organizations so that this also has a very big impact to our areas in Japan.

Due to the raising awareness, many of Japanese DNS operators did very good production test for running DNS software. Some of them found very critical RFC 5011 related bugs in the very famous commercial products and very famous free software, and that the result is [rating] on the [inaudible] document of the ICANN.

Also I made a very small but wide range of survey in Japanese community. You can still see and answer the survey. The summary of the survey says that almost one-third of answers said they started to provide to provide DNSSEC [inaudible] data. Most of them prepared for 5011. Also they prepared for the failure of KSK rollover. So Japanese operators are very serious about the rollover and they prepared very well.

The lessons learned regarding KSK rollover. As I said, ISPs are very seriously prepared for KSK rollover. Documents how to test RFC 5011 with running software was not enough so they have to prepare their own testing environment. There's very few knowledge sharing, so I think this kind of document and knowledge testing is very important for the future. I think monitoring channel such as Twitter or [inaudible] graph possibly useful because the going events, they have to know what happened on the going event.

Finally, I'd like to say bilateral communication between operators are very important because their comment are very, very practical and realistic about the operation. So knowing their knowledge and sharing with others are very important to prepare this kind of event and for the success for DNSSEC deployment.

RUSS MUNDY: Thank you, Yoshiro. Do we have questions for Yoshiro? Go ahead, John.

JOHN: Did you start to look at implementing CDNSKEY automation?

YOSHIRO YONEYA: Dot jp is not there. But I heard some ISPs preparing to provide [CDNSKEY] as their managed [inaudible].

RUSS MUNDY: I have a question for you, Yoshiro. With the large amount of preparation that your ISPs were doing for the KSK roll and I don't know if there has been any sharing of that information in any manner, whether it's written down or test plans that were done, distributed around. But that is something I think certainly would be very well received and input for presentation for future

DNSSEC workshop because I think that's a very important aspect and if there was material or information or someone who wanted to share that, that would be of great interest.

The other comment I have was, especially with that amount of preparation and then looking at the relatively limited number of signed zones, the high visibility of things coming up – I think if I remember the numbers correctly, there is 800-some government agencies that explored but only 15 zones signed or something like that – do you anticipate an improvement in the number of signed zones especially now that the KSK roll is done prior to these events particularly by government activities in preparation?

YOSHIRO YONEYA: For the first comment, many Japanese operators are very shy and they do not want to explain their experience in the public. So if we can provide anonymity, I think they can explain their experience. But I hope Japanese to English translator would be mandated.

For the second question, as I said, Olympic Games or such kind of international event will be the driving force of DNSSEC signed zone in the governmental organizations. Because the information to the tourist or journalist is very important to live in Japan, and the confidentiality of the information is also very

important because if the information is fabricated on the fake side, people have to know or have to be protected from that kind of fake information. So I hope many governmental organizations and some news sites should have DNSSEC signed with strong server certificate.

RUSS MUNDY: I guess only one very last question with respect to this. Have you seen any uptake in DNSSEC that relates to DANE, particularly DANE with respect to the e-mail opportunistic encryption? Have you seen any indications that that's helpful or just nothing is particularly visible to you?

YOSHIRO YONEYA: I don't see any DANE deployed in Japan.

RUSS MUNDY: Okay. Well, thank you very much, Yoshiro. I'd like to also one more time thank all four of our panelists for their presentations. Very, very useful and interesting to get firsthand information on what's going on, and hopefully what we've heard today will help each other make progress here. I think we are just a few minutes ahead of our planned schedule so that means we might even be able to have Bruce complete in about the timeframe for the real

coffee break. So, Bruce, do you want to go ahead with your presentation now on the transition?

BRUCE TONKIN: Sure. Oh, good. They're up there. Thank you. First, I'm responding to a question we had earlier about what happens if a small business is trying to put in a DNSSEC entry and their registrar doesn't support that. At least in the Australian environment, our general response would be transfer the registrar that does. We have a competitive market. We have multiple registrars. They have different levels of service. There are registrars that support DNSSEC and we would just recommend that they take advantage of the opportunity to transfer their names to a service provider that meets their needs. Just a general response to that.

Just some background, I work for the .au Administrator. We outsource the registry backend for the second level domain names of .au. So the Australian environment we have registration with their names like com.au, .net.au, .org.au, .gov.au, .edu.au, and several others. In rough terms, it sort of maps the original set of domain names that came out of the U.S. market with .com, .net., .mil, .gov, .edu, etc.

We operate the top-level nameservers for .au and we outsource first the registry operating of the registrations but also outsource the DNS operation for the second level names.

Last year, we transitioned to 3.2 million names from operator to the other. We had a target of doing that in the 1st of July. Things that complicate our transition. One is it's the biggest transition ever. It's 3.2 million names, but also complex in that it had multiple levels. So not only do we have registration at the third level, we have registration at the fourth level and fifth level as well that is managed through the registry. For example, we have schools within the state of New South Wales and an education domain. So the transition of both the domain names as well as DNSSEC record is at multiple levels at once. In fact, five levels of transition.

So the registry was cut over on 1 July. The approach we tried to take because of the scale and complexity, we tried to get as much done in the months preceding the 1 July so that their cut over was a minimal number of things that needed to be done. And the cut-off weekend we allowed essentially 48 hours to do the cut over and we completed it in another 24 hours, mostly because all the steps had already been done.

With respect to DNSSEC records and DNS nameservers, we started operating the new nameservers from the new operator

in parallel with the previous operator's nameservers. We also started to introduce as many of the DNSSEC records as we could with the different layers so that at least they could be caged and essentially propagate through constellation of DNS servers around.

And also so that we could do a lot of the testing well in advance so that we were essentially testing live in production and that we could see that before we did any cut over, you could actually read the records and that they were properly configured, etc. before we actually did the cut over.

Just taking through those steps and I think … I'm conscious that much of the people in this room I'm preaching to DNSSEC experts but I thought it's just useful to have it documented if you like the approach that we took.

So the first step – one of the things we do is we rollover our keys I guess at a higher frequency than perhaps ICANN does. We have a key signing key that we rollover every year. We've been operating for multiple years so we've done multiple key signing or KSK rollovers in the last few years. We rollover our zone signing keys every quarter. So every 90 days essentially we rollover the zone signing key. One of the things we needed to do consciously is to say, "Let's not try and do a key rollover in the

middle of doing a transition." So our first step is don't rollover the keys.

The next step was we generated new keys throughout the levels, bearing in mind that we didn't transition the KSK for the top level because that'll continue to run the .au for the top level, but we transitioned them all in the levels below, so signing com.au, .net.au, and so on. For each of the levels, we generated new Key Signing Key (KSK), Zone Signing Key, and they have a relevant DS record.

We sent these keys to the current registry operator and they published these keys in the zone. So, understanding the hierarchy. [UADA] would publish DS record, and then the current operator would then publish the DNS key record at the next level for .com.au, and then so on for the levels below. They were then published on 5 June, so nearly a month before the transition day, which is 1 July. We had published the DS records all the way down through the hierarchy with the exception of .gov.au, which we were originally going to sign on transition day but our government asked us not to, so we did not sign .gov.au in that process.

Then in a little bit more detail here. The new operator was set up nameservers in parallel with the existing operator. Then the new operator began to publish the zones that were signed by the

previous operator on 25 June. Prior to that date, they were actually receiving copies of the zone and if you queried the nameservers directly, you'd see the zone there so it was live, but if the SOA records weren't published, the public wouldn't reach those nameservers prior to that date. But on 25 June, we then put the nameserver records public and the new operator was then serving the zones.

Then we reduced the TTLs on the various DS records there as well as the SOA and other records to 300 seconds. We did that on 26 June. So about a week out, the new nameservers were publishing the current zones. The zones were signed by the previous operator and we then reduced all the TTLs on all the records to allow us to make changes relatively quickly.

The current operator then stops serving the zones from their nameservers on 26 June. So at this point, the new operator was doing all the public DNS nameservers but the previous operator was still creating the zone. It was getting updated every day with new domain name records and the previous operator was signing the zones using their key signing infrastructure.

Then 30 June, we then essentially shut out the registrars so that they couldn't make any changes to the registration records. So from that point onwards, the zone was essentially frozen. No changes to the zone.

The new operator then began to generate the zone and then sign the zone using their keys. So we still have the DS, DNSKEY records from the previous operator. It was still public in the zone but we were signing using the new operator's key signing infrastructure. This is on a Saturday, 30 June. And then we began on 1 July cut-over and then the new operator was publishing zones that was signed using their keys. After that happened, we then removed the previous operators – DS and DNSKEY records from the zone then increased the TTLs back up to 900 seconds. That's basically the series of steps.

Another more recent change we've been doing. I mentioned the frequency that we rolled the keys. So .au, the zone signing key is rolled every year. That should say Key Signing Key out there. The KSK is 2,048 bits and the ZSK is at 1,280 bits. We had a request from our government to essentially increase the level of encryption that we were doing for the Zone Signing Key, whether the key link essentially. So that's a change that we are now are currently deployed which is to shift the Zone Signing Key to 2,048 bits, which is fairly strong given that we roll that every quarter. But I'm not sure what other … interesting to hear what other people are doing in terms of their Zone Signing Key lengths. It obviously increased the size of the packet size but we've taken that decision, recommendation of some of the security recommendations from the Australian government.

So that's all I have, Russ. Hopefully gets you on time for coffee.

RUSS MUNDY: Excellent, Bruce. Thank you very much. I'm sure there are some questions. I see Paul.

PAUL: What algorithm are you currently using for these keys?

BRUCE TONKIN: The same algorithm is at the root level. We've actually just upgraded the hardware signing modules, and I do support elliptic curve algorithm, so we're able to move to that. Part of the initiative is not changing too many things at once. The thing we've changed at the moment is the key length so let that settle. But we are looking to potentially move to elliptic curve algorithm as well.

PAUL: Got it. And algorithm key rollover – another exciting exercise, so good luck.

BRUCE TONKIN: I think probably the general approach we take is we don't really want to be on the bleeding edge. This is a big zone and critical

infrastructure within Australia, so we tend to let some others have a go first on smaller zones and then we progressively pick those up.

[KATHY SCHNITT]: We have a remote participation question. “Greeting all. This is Zeinab Mohamed from Sudan, ICANN55 at NextGen. Question to Bruce, David, and Yoshiro. Is there any kind of collaboration with universities or academic institutions to help you in raising awareness towards encourage more small business and users to sign their domains?”

YOSHIRO YONEYA: Frankly, we do compromise to the public. The university or small business are also target or the audience. But we didn’t do special tutorial or session to the academic or small business because it is to narrow the scope. This was limited so such kind of activity is not done before. If the DNSSEC deployed much more wide range then that kind of grassroot activities will be getting more important. But at this moment we didn’t.

DAVID MORRISON: Similar answer. In New Zealand, we don’t have any direct education programs around DNSSEC in the university space. We do have some really good networks in the network operator

groups and hence do work to educate and that had impact on organizations turning on validation. I think it could be something we'll explore but again, similar to the other answer, our resources are fairly limited so we're working at it where we can get [best to fit] in the coming year.

BRUCE TONKIN: Yeah, similar. There's not much direct involvement in the universities and discussions on DNSSEC. Having looked at the list of domain names signed, there is one university that has a signed domain name as at least one indicator. That's Bond University in the North of Australia. No other university has a signed zone but it is available within edu.au for those that wish to use it. I think it's fair to say that involvement with university tends to be more from the legal department. They're fascinated with their policy. They're a little bit like the ICANN environment here but we tend to have more lawyers involved than we do technical people.

RUSS MUNDY: One comment that I have in response to that question is there are more and more universities developing and promoting themselves cyber security fields of study, and it's a possibility that there can be some useful teaming. I know some parts of the company I work with work with local universities on the set of

things and I know I have seen in various course layouts DNSSEC development, DNSSEC instruction. So, you might be able to actually get some free support from the students through mentorship and so forth. It's just some possibility.

BRUCE TONKIN: I should say that we do have a board member from the university on our board. His name is Nigel [Fair] from the University of New South Wales. We'd like to put his hand up. So we do have some involvement with universities.

DAVID MORRISON: We do have contact with universities. Several are doing research and [inaudible] and we have a grounds program where we fund research. I could see a future where perhaps we could encourage research into areas around DNSSEC adoption. That's my takeaway for today. Watch the space.

RUSS MUNDY: Okay. Was that the only online question, Kathy? Okay. Any other questions from Bruce in the last presentation? Okay. I would say we hit it almost exactly as coffee break time, folks. At 30 past the hour we will begin again. Thank you very much, Bruce.

[END OF TRANSCRIPTION]