SAN JUAN – DNSSEC Workshop, Part 1
Wednesday, March 14, 2018 – 09:00 to 10:15 AST
ICANN61 | San Juan, Puerto Rico

JACQUES LATOUR: DNSSEC workshop. Today, we're streaming audio only. All the slides are available on the ICANN website for the DNSSEC workshop. There's an e-mail address there where we can respond to questions, so you need to send them via e-mail address. And that's the scoop of the day.

So welcome to the DNS workshop. The Program Committee is here. Like I said often, we meet on a weekly basis to plan the DNSSEC workshop, we try to have good and relevant content with people from around the world participating. And thank you to the Program [Committee].

So we have lunch today. It's sponsored by Afilias, CIRA and SIDN. So Jim, Christian, thank you. But you need to at least have one good response on the quiz to get the lunch ticket. No.

UNIDENTIFIED MALE: [The one this year or the one from the previous year?]

JACQUES LATOUR: The one from – actually it's the –

UNIDENTIFIED MALE: [inaudible] 2017.

JACQUES LATOUR: That’s right. So today’s quiz, you have to remember the question from that meeting and the answers in the right order. That’ll be the challenge for today. So we have a lunch sponsor. The ticket is behind – no. The ticket is on the table, so you need that to get your lunch.

So this is a joint effort with SSAC and ISOC with the Deploy 360 program, so we collaborate together on e-mail addresses, planning, and the collateral that is often generated from workshop here makes it into the Deploy 360 DNSSEC program. So Dan York is in charge of that, and it seems to be working pretty good so far.

Today’s agenda, it’s a full day, so we have a panel discussion on DNSSEC activities. So there’s Comcast, CIRA, Nic.PR, Nic.BR, so Fred and company so we’ll have about an hour there. And then in the afternoon, we’ve got a couple of presentations. KSK sentinel, CZ.NIC with the DNSSEC validation experience at the edge or at the CPE, CIRA on HSM and KSK rollover, and Joe on NTA, and a little bit of insight inside this.

After that, we have the great DNS quiz, and lunch, and then a couple of presentations in the afternoon on DANE. That should be interesting. There's a little bit of hands-on or more how to do it there, so that's going to be a good session. And then we'll have a panel discussion on the root KSK rollover.

So as tradition goes, we look around the world on DNSSEC deployment, so counts. Dan York tracks pretty much everything that's going on for DNSSEC. There's a detailed report available on the ISOC website with the deployment up to 2016, so that's the latest report we have there.

So stats around the world. The trend was upward until July this year when there was a glitch. It's India. I forget the name.

UNIDENTIFIED MALE: BNSL.

JACQUES LATOUR: BNSL turned off DNSSEC validation. So you can see the impact there. Hopefully they'll turn it back on after the rollover. So that shows the impact of one ISP on the global sphere.

UNIDENTIFIED MALE: There are a lot of Indians.

JACQUES LATOUR: There are a lot of users behind it, yes. That's unfortunate, but that's the way it is. In terms of stats by region, you can see that here. The top is 58% up to 2% on the low end. DNSSEC is not universally equal, so there are regions or ISPs that do it more than others. So we still have some work there to get the ISPs to validate.

On the other side, in the TLD deployment side, who signs their TLD? We're at 90% of signed TLDs in the root. I think that number is going to stick for a while. The last 10% takes 90% of the time, so we still have a little bit to go. We have 1544 signed TLDs, so it's good, we're making progress there.

That's a percentage of signed domains per TLD. It's hard to read. I can't read that. You can look at the slides. More stats from – the link is below there, DNSSEC stats. Some of these you should go and take a look for no other reason than you should look.

One thing that we built is global maps with colors on the map. These are the status for each of the colors. So you'll see here the global map for DNSSEC. I remember seven, eight years ago, these maps were a lot of empty, not a lot of green, and a lot of partial and experimental. Now it looks pretty good. There are a couple of regions we need to work on – we'll go through that – but this is getting to look pretty respectable. We still have a little bit of work.

So we need to do work here in Africa. There are a lot of CCs that have not announced that or not even in experimental stage for their ccTLD. It could be two things. If you intend to implement DNSSEC, you should notify Dan York or somebody in the Program Committee, and that way, we can update the map with at least an intent or a status that you want to do DNSSEC. That's coming along.

Asia Pacific is looking much better. We've still got a few that are missing, but we have good traction there. There's a little box with information there. Italy, finally, so the question – it's still colored as DS in the root, meaning it doesn't accept DNSSEC registration from the registrar. Is there somebody from Italy here? No? So we assume it's that color, DS in the root, so if anybody knows somebody from Italy, then if they do accept DS from registrar, then we should change the color to full green there.

So the LAC region, there's a couple of missing, so we need to do some outreach there. So LACTLD I guess is working on that. Fred, it's all on you. North America, Greenland is almost full green, so we're making progress there. So this, just having that color changes the percentage a lot for North America, so – does this look better there?

UNIDENTIFIED MALE: Jacques, can you go back to the Central America one?

JACQUES LATOUR: Yes.

UNIDENTIFIED MALE: Just noticing Panama is all. Yes. I'm noticing that's where we're going next.

JACQUES LATOUR: Panama? Yes.

UNIDENTIFIED MALE: Yes.

JACQUES LATOUR: Yes, it's not – so maybe we should do a DNSSEC event on Saturday or something. Okay, North America. So the maps are available online at the Deploy 360. You can subscribe, actually, to get I think it's a bimonthly or monthly e-mail, and it sends all the JPEG and all the pictures, and everything you need to generate these slides. You can subscribe to that and they're online also.

Then the ISOC is working on a DNSSEC history project, so if you have a tidbit of history that you know of that's not in that site, you can update it. They're trying to track the entire history of DNSSEC. And that's it. Five minutes early. Any questions?

ABDALMONEM GALILA: Yes. Sorry. First time I am here. I'm Abdalmonem, ICANN coach from Egypt working for .Masr IDN ccTLD. My question is about what is the different between DS in root and operational? I think DS in root means the registrar can add DS records at the registry or that the registrar can offer DNSSEC facilities for the registrar.

JACQUES LATOUR: The lighter green is DS in the root meaning they're signed and there's a chain of trust with the root. The dark green is hard to measure, but this is when the registry accept DS from their registrant. So they can sign the child zone, yes.

ABDALMONEM GALILA: The registrar?

JACQUES LATOUR: The registrar.

ABDALMONEM GALILA: Yes. Okay.

JACQUES LATOUR: So they have EPP and they accept DS record or through the web.

ABDALMONEM GALILA: So Egypt should be in [dark green].

JACQUES LATOUR: Egypt?

ABDALMONEM GALILA: Yes. Should be in [dark then]?

JACQUES LATOUR: Okay.

ABDALMONEM GALILA: Also, another note that –

JACQUES LATOUR: Yes, so you're DS in the root.

ABDALMONEM GALILA: Yes. It should be operational as we accept DS records from our registrar. Another thing is that – thanks for taking my comment before in previous meeting about adding – I mean taking IDN ccTLD into account as is for IDN ccTLD of Egypt, but should we make just identification between IDN and ASCII? If I see this in [other view] will see that this is for .eg, not for IDN.

JACQUES LATOUR: Okay.

ABDALMONEM GALILA: But this is for IDN, not for .eg. Thank you.

JACQUES LATOUR: Good point. So I'll take a note of that.

UNIDENTIFIED MALE: Yes, and it's easiest if you can – especially for things like this – to send e-mail to either directly Dan York or to the DNSSEC Workshop Program Committee. We'd love to hear more details of this nature. Thank you.

UNIDENTIFIED MALE: Just a quick comment. I haven't signed any signed domains in Italy, so if they're delegating, they're hiding very well. My survey hasn't found a single signed domain in Italy.

JACQUES LATOUR: Okay.

UNIDENTIFIED MALE: So they're probably not delegating, or they're hiding the first few very well.

JACQUES LATOUR: It's a secret? Okay, thanks. Any other questions?

MATS DUFBERG: I wonder why the certificate of dnssecdeployment.org has expired.

UNIDENTIFIED MALE: In August 2017.

JACQUES LATOUR: Alright. Dan York, are you listening? So before you talk, you need to state your name, and when you go through the slide – I should have by the way mentioned which slide I'm on, because there are people who are following us audio only. So if you could just say which slide we're at then.

MATS DUFBERG: Okay. There's a link to the dnssecdeployment.org history that I was trying to reach, and the certificate has expired. And I am Mats Dufberg from IIS.

JACQUES LATOUR: Okay. Thank you. Somebody will look into it. Alright. Questions? So anybody from – we've got a minute left – Africa region that's planning to do DNSSEC who's in the room that could have an update why there's no activity there? Alright, thank you.

So the next session is the panel discussion for DNSSEC activities, and our first panelist is Joe Crowe from Comcast.

JOSEPH CROWE: Good morning. My name is Joe Crowe. As Jacques said, I'm from Comcast. I've been there as a senior engineer currently for around four years. Comcast has been doing DNSSEC since 2012. We have not only just done validation for all of our footprint, we also do DNSSEC signing for over 5000 zones.

We validate for over 20 million customers, so it is one of those things that DNSSEC gets brought up of, "Does it scale?" It does scale. There are operational issues that we've run into where if something fails via DNSSEC validation, we get calls and there is a cost association with that, and it is one of the bigger things that we have to deal with even though it might not be something that broke.

Sorry. It's my first talk, and it's still early in the morning. So some of the operational issues that we've run into while implementing

DNSSEC across our footprint is making sure that all of our resolvers are up to date, making sure that everything as far as version numbers of our resolvers and vendor software has been in compliance with everything that we need to do with our automation.

Automation has been our biggest step forward in the past three or four years. We've gone through about two different types of automation tools. We ended up using SaltStack recently which does allow us to do one spot to automate multiple vendors on our authoritative side, on our resolver side and our DDNS/DHCP. So it's something that when you have hundreds and hundreds of servers across the footprint, it's something that you really want to get involved with because you don't want to go in there manually and try to change everything. Once you go in there manually trying to change everything, something is going to break and you don't want it to break.

We've recently started looking into doing EDNS0 in some of our locations, but again, at our scale, trying to implement that is – there is a CPU and a cost associated with our performance on some of our resolvers due to the fact of how many requests we get per day and per second. So we want to make sure that we are trying to do the right thing for CDN folks and that they get the correct responses for geolocation, but we also have to take into account what we need to do to ensure there's no performance hit for us and for our customers. That couple of milliseconds can compound at scale and can really just creep up out of nowhere.

We've also recently – as of 2015 – started utilizing DANE for our e-mail. It was an operational issue at first when we first started doing it because our authoritative servers at he time did not have TLSA records available for us to use as just a record. I had to find out how to use the type 52 RR set to put into our authoritative to make sure that the rest of the world could use those records.

After that was done, pushing that out wasn't really an issue. The mail team that I work with has been running that now since 2015. They finally went live with it. They started testing in 2014. The future of what we're going to do in our infrastructure, we're looking to utilize DANE more to anything that kind of needs to use TLS records or TLS at all. [inaudible]use it as an internal CA. This way, we can really self-sign for a lot of things that we do internally and not have to worry about using external CA, especially with the cost associated with that.

Some of you guys might know that if you're running over 5000 zones and internally you compound that by how many teams are putting in their own zones and FQDNs and they want to have their own TLS and certificates, it's really going to be a lot of money to try to say, "Yes, let's go over to Comodo" or "Let's go over and spend $100 per couple of years." It's really not what we're looking to do if we can do it internally and use DNSSEC to actually do our internal zones.

We are also looking into how we can operationally do our DS key rollovers. That is one of our bigger – again, as I said, over 5000 zones. That's a big task to take, especially where when you resign, you have to update your DS records. There's really no automatic way to do that, that's a manual process in a lot of the things that we need to do with our registrar.

It's one of those things that a couple of us on our team have really started looking into to make sure we can automate that to a point where we can safely roll over and update our DS and resign when we need to. We've run into issues where we have to move zones from one authoritative server to another authoritative server, and at that time, we need to resign. So we kind of need to make sure those operational things work for us.

Being a big company, we know that everybody runs into these issues, but like I said earlier, it's compounded by how much we need to do and how much we really need to make sure it works correctly without the hit of any hiccups. Because a hiccup of five to ten minutes could cost us a little bit of money. Any type of phone call that comes in for any DNSSEC issue really could get into tens of thousands of dollars per that five to ten minutes. and if it goes longer than that – it also depends on how many customers are calling.

Yesterday we actually ran into an issue where state.gov was failing DNSSEC, and we actually got an e-mail or a tweet from somebody saying, “Hey, you know, state.gov is failing DNSSEC.” Within 15-20 minutes, we were able to flush our DNS cache because they had actually updated something on their end. So there are little things where if somebody needs to reach out to our DNS team because of a DNSSEC issue, @comcastdns twitter handle is one of the fastest ways to reach us at the DNS team. You’re not going to get a comcast frontline person, you’re actually going to get to an engineer on our team. And we watch that 24/7 it seems like.

That’s pretty much all that I really have for our side of what we’re doing in Comcast as far as DNSSEC goes. If anybody has any questions, I’m open. Russ.

JACQUES LATOUR: Russ.

RUSS MUNDY: Thanks, Joe, and thank you very much for coming and joining us at this workshop. It’s been great to work with Comcast in the past, and we look forward to doing it in the future. One of the things that you mentioned in your discussion of what you were doing was the impact of EDNS0. And I'm sure that you all do some internal testing. We do have some published information about DNSSEC impact on authoritative servers, but we really – at least I don't recall that we have any publicly available information on validating resolvers, and especially to the impact of some of the specifics of whether EDNS0, which user, what the settings are, things of that nature.

And I know you can't answer that here, but I would ask that you take it back to your company and ask if it would be possible to look at providing some of the results of this testing to the DNSSEC community on an open basis. It would help others and it would provide a reference point that other people could look at and maybe build on or do other testing.

JOSEPH CROWE: I agree with you. I think that type of data would be great for DNSSEC community as a whole. I'll gladly take that to them and see what they think about that.

RUSS MUNDY: And I think it would be good for Comcast publicity too. Good for the company.

UNIDENTIFIED MALE: Russ, just a clarification question. When you were talking about EDNS0, you we're talking about specifically EDNS0 extension for subnet, yes

JOSEPH CROWE: When I talked about EDNS0, I'm talking about geolocation mainly for our resolvers.

UNIDENTIFIED MALE: Yes, what I just said. Yes.

JOSEPH CROWE: Yes, that's exactly it.

UNIDENTIFIED MALE: I curate DNSSEC interesting failures. I have a bunch in my history over the years. I see state.gov failing in 2016 and 2017, haven't seen any recently. If you could send me the technical details, that'd be great. Back in 2016, I saw RR sigs in there which weren't encrypted. It was just the raw data before the RSA signature. Somehow somebody managed to publish the pre-signature data into the zone. I don't know how you do that, but if that's what happened again, it'd be interesting.

JACQUES LATOUR: So did you go? Jeff and then Warren. You were late by like two milliseconds.

JIM: Jim. One of the popular myths out there about DNSSEC in the validating recursive resolver is that it takes time and it takes constant attention because of the negative trust anchor maintenance. What has been your experience inside Comcast, and what would you say to other large ISPs who are looking at this with trepidation going, "Oh my God, I don't think I can do it"?

JOSEPH CROWE: Enable DNSSEC. Operationally, for validating itself, it is very easy to turn on in every DNS resolving vendor out there right now, unless you're using something that's very obscure. But operationally, having the validation on, it's set it and forget it for us. We are no longer thinking about, "Oh, what's going to happen?" And as you mentioned, the NTAs and things like that, I'll be doing a talk a little bit later about that specific topic so I can get a little bit into that then.

JACQUES LATOUR: Warren?

WARREN KUMARI: I just want to say I feel bad because you all have the worst luck sometimes. Nasa.gov decided to have their exciting DNS booboo back during the SOPA stuff, and then state.gov decides to have an exciting DNSSEC thing right when our illustrious president decides to let go of the head of the state department. So yes, it would be good if people stopped breaking DNSSEC stuff when there's big news things happening. That would be awesome.

JOSEPH CROWE: And yes, we get the calls, unfortunately. Google doesn't get the calls. But yes, I agree with you. Especially when big things happen, HBO Now, when that goes live and DNSSEC breaks, we're the ones getting the blame.

JACQUES LATOUR: Alright. I had a question which – so you said you have over 5000 zones and you need to manage the keys. Have you looked at doing CDS or CDNS key automation? Is that in your plans?

JOSEPH CROWE: That's in our plans. We haven't really gotten that far into it because we have so many other projects on our plate. Anytime we try to look into something new and fun, something else gets brought up by management says, "Hey, do this."

JACQUES LATOUR: Alright. I guess the last observation I have is, so leveraging DANE to run your internals, yay. There are financial benefits for that. I think it'd be great eventually to have like a presentation around that topic to show that if you do this, you can actually save some money.

JOSEPH CROWE: I agree with you. The more we test it and actually start implementing something like that, I think having those conversations and showing how you can monetize it would be steps forward.

JACQUES LATOUR: Because if there's a financial return or savings, then there's value for managers to approve more work. So okay. Thank you.

JOSEPH CROWE: Thank you.

JACQUES LATOUR: Any other questions? Okay. Next is Jacques Latour from CIRA, me. DNSSEC activities in Canada and in .ca. So thanks to the APNIC [tool], we've been able to manage or monitor the trends in Canada, and like the global trends, there's a downward trend in Canada in DNSSEC validation. A couple of ISPs with the KSK rollover decided to turn it off. They're not the big ones, but smaller ones. So unfortunately, the trend is going the wrong way.

Hopefully after the KSK rollover we can go back and tell people to reactivate and turn on, and eventually – I few have information like that you can actually save money managing CAs with DNSSEC, then at least we need to generate some positive value there.

So within Canada with CIRA, we go, we present at various ISP summits and we talk about enabling DNSSEC, so even though we do quite some outreach with the ISPs, we still have a challenge to get it turned on.

So this is by telco in Canada, so I sorted somewhat by the largest telco that we have. And there's only one noteworthy ISP in Canada, TekSavvy, that actually does DNSSEC validation. They're also the kind of ISP that peer at all the Internet exchanges that we build in Canada, so they connect and share and talk. It's one of the more modern – I call – ISP that we have.

The rest are just not interested. So we have a lot of work to do with these guys to turn it on.

So activities within .ca. We have enough signed domains now to generate a graph, so it's a good sign. As of generating that graph early this month, we have 1256 signed delegation. Just to give you an example, in July 2017 timeframe, GoDaddy enabled the DNSSEC validation, the DNSSEC integration with CIRA. So before that, we've never had GoDaddy supporting DNSSEC with us, which is a shame, but now it's there. But the impact of that didn't really generate a lot of demand and traffic.

So the best thing that CIRA is working on right now is to do CDS automation the way CZNIC is doing it, by scanning the entire .ca zone file and automating the adds and delete of DS with CDS and CDNSKEY record. There's a lot of CDS available in the .ca zone file, so there's something there we can do to make this work.

So slow adoption. Also, the other thing we have is very few registrars today support DNSSEC in .ca. So GoDaddy turned it on, but the registrars are simply not interested in doing DNSSEC with their registrants. So transferring keys that they don't control or don't manage or don't really have any interest to them, any support phone call they get from a registrar. That proves that there is a need for CDS and CDNSKEY automation.

A couple of years ago, two years ago, we started working on the automation for CDS at CIRA. The challenge is we never got it into production due to a lack of resource or priority associated to that. Even internally, we're trying to get – we're having challenges getting this prioritized. So we're building a lot of good stuff with our D-Zone firewall and new registry platform that we're building, but getting the specific pieces is still lacking. So I think by six months from now, we should have that in production. So it's disappointing because I'm pushing this, but internally, we're not making it happen. So I wish I had better news, but it's sad. But it's life.

The Internet draft DNS operator to RR, so that's the API to accept requests from DNS operators to add and delete DS records. I think we're going to review that entire draft, the protocol, to make it less API and more automated on scanning the entire zone. If we build an API for DNS operator to do something, it cause them to do something when they can just publish stuff in their zone without any update or any coding to do so. I think scanning a large zone is the best way to go, but for large – but there is a need for some operator to support this, so we'll refine it and make it more based on reality.

And that's all I have. That's pretty much – not much happening in Canada and .ca. Any questions?

UNIDENTIFIED MALE: Jacques?

JACQUES LATOUR: Yes.

UNIDENTIFIED MALE: As one of your registrants – and actually one of your registrants through one of the few registrars who will do it, I have some signed domains, but I also have some signed domains where I have the usual problem that I am the DNS manager but I'm not the – you know, so when can I use CDS, please?

JACQUES LATOUR: Actually, you're like 10% of all of this. Yes. Another, yes.

VIKTOR DUKHOVNI. Hi. I have a quick comment.

JACQUES LATOUR: Can you state your name before, please?

VIKTOR DUKHOVNI. Yes, I did.

JACQUES LATOUR: Oh, sorry.

VIKTOR DUKHOVNI. I found 24 domains in .ca that actually do DANE, so there are some people who are out of those 1200 are actually doing something useful with it. I noticed that CIRA labs is one of them, so it looks like you guys are testing it. Great. And that's all for now.

JACQUES LATOUR: Alright. Thank you. Russ?

RUSS MUNDY: Jacques, do you have any plans to get more registrars in Canada engaged in DNSSEC? Or have they continued to be pouting recalcitrant, "It costs me money and I get nothing from it" in the corner?

JACQUES LATOUR: The discussion we have with our registrars today is to work with them to do something like PowerDNS, and then enable the CDS and the CDNSKEY. But them interfacing with us to exchange information is not going to happen. But they're all very interested in enabling DNSSEC, turning on DANE, publishing

CDS, and then we take care of bootstrapping and working with them. But the EPP part, transferring DS record, not happening.

RUSS MUNDY: So the cooperation in terms of supporting DNSSEC is good as long as there's no substantial financial or operational impact. They'll put the records in, but they don't want to spend the money to incorporate all of the capabilities in their systems. And yes.

JACQUES LATOUR: So we did a workshop on DNSSEC way back, and transferring DNSSEC information is not part of the registration of domain. It's not part of that, so registrars don't care about DNSSEC because it's not part of their registration information per se. I think it's more operational data in the backend that gets automatically updated. Any other question? Christian?

CHRISTIAN HASSELMAN: Do you also talk to these ISPs that you showed on the list?

JACQUES LATOUR: Yes. So I do go to the ISP – like Canadian telco and ISP summit across the country, and I present those stats, and I got the name and shame on DNSSEC, and they don't care.

CHRISTIAN HASSELMAN: Okay.

JACQUES LATOUR: Except the IPv6 stats are much better. So if this was IPv6 workshop, we have good stats for Canada. But DNSSEC, still got some work to do.

CHRISTIAN HASSELMAN: Okay. Thanks.

JACQUES LATOUR: Other questions? Okay, so next is Carlos Acosta from NICPR and Jim Galvin, their .pr DNSSEC history.

CARLOS ACOSTA: Hello. So a short history of how DNSSEC came to be in .pr. Well, at first, the registry was a research lab involved with various projects that range from everything from watermarking to public cryptography and various other projects, and, well, since it got its starts as a computer science center, obviously dealing with all these encryption topics, DNSSEC always seemed like an area of interest for them.

So around the year 2000, a couple of local government sites were redirected at the ISP level, which is something that .br determined was something that would have been avoidable if DNSSEC had been implemented. And a little bit after that, Sweden became the first ccTLD to offer DNSSEC. So we just saw like it was a right way to go.

So around the year 2006, exactly in July, we started signing the zones but it wasn't until August of that same year that we actually served those records on the public servers. And here's the list of all the zones that were deployed using DNSSEC. A considerable list, considering. And after that, we made a little webpage to just inform the people and all interested parties of what was going on with DNSSEC, what is it exactly, etc. And during that time, we also encouraged the government to sign the government domains using DNSSEC to prevent the same attack that happened a couple of years earlier.

A couple of years ago, we started an incentive program, and under that incentive program, we started signing those clients using DNSSEC as well. Here's a little graph of, as of December last year, how many signed zones we had and how many are unsigned. So we had a little over 1% as of December of last year. Here is in greater detail what that 1% entails. 91% was signed by us, and 9% was signed by the registrants.

Here's a little oversight of the details of how we managed to sign the zones using DNSSEC. We used a Windows 2003 server machine. Underneath that are the comments that we used in VBScript to perform the DNSSEC signing. And we verified that everything was functioning properly using OARC's DNSSEC resolvers at the stated IPs and using DNSViz which is a great tool. And that's pretty much it, that's a quick oversight. Any questions? Alright, if there are no questions, I'll let Jim take over.

JIM GALVIN: Thanks very much, Carlos, and I'm Jim Galvin from Afilias. I'm going to skip right up to Slide #4 here. Afilias just transitioned .pr to our services in January of this year, and this seemed like a good opportunity to spend a little time talking about the process of transitioning TLDs.

I know that we talk a lot about key rollovers, but I think that it was a good experience for us, it was a pleasure to join with .pr in this experience as one of the early adopters of DNSSEC. So I just thought we would spend a little bit of time talking about this whole process of doing this.

Moving on to Slide #7, Afilias, like .pr, we've been involved in DNSSEC for a long time. We weren't first as far as all this is concerned, but we did get started with DNSSEC in 2008 and began signing TLDs in 2009. So we've been doing this for a long time, and along the way, we have actually transitioned quite a number of TLDs. Sadly, some out, but we like when we transition TLDs in.

So moving on to slide number nine, I think what's interesting is there's a lot of attention being given to the root KSK rollover, and obviously because it has a fairly substantial amount of risk. And although we do do key rollovers and DNSSEC does these fairly ordinary, and there's a fair amount of technology that does that, what's interesting at the TLD level is like the root, it's a very high-risk proposition. The consequences, the effects of doing this wrong can be quite dramatic.

At the TLD level, you could lose an entire TLD and have it go invalid. And I know that we all appreciate that, those of us who are into the technology and we see what's going on, but you know, wanted to take some time to sort of walk through that whole process a little bit and see where some of the sticking points are as we get into this.

So moving on to Slide 11, I think what's interesting here is there are some administrative steps that are outside of one's control. As a service provider, one of the things that you run into is there are actually two other parties that you have to deal with. It's easy to say that, "Yes, I have to talk to the other service provider" wherever the DNS is currently being hosted, but at the

TLD level, you also have an interaction that has to happen with IANA, because you have to arrange to get the new DS records to put into the root.

And so there's just this extra administrative process and extra thing which is not under your control, and of course, IANA has its own validation steps that it conducts in order to make sure that this is the right thing that has to happen. So there's an interaction that needs to go on and documented and keep track of.

The next thing that happens of course is when you're ready to initiate all of these things, there are still additional interactions with IANA as you complete the transition. We're used to the idea when you're just rolling your own key in your own zone to add and remove the new key records or moving your name servers, you just add and remove the NS records back and forth, but when you have the coordination that you have to do with this extra party, the real issue here is the timeline that happens.

It's a fairly straightforward process if you're just doing your own zone in your own environment because the time that all of this takes is generally bound by some multiple of your TTLs and how you manage that. But you have – in our case when we do these kinds of rollovers with TLDs, this process actually moves into taking weeks to conduct and get done properly, just to make sure that all of the administrative steps are done.

For our purposes, we also do double checks. Every time that we do something., you have to check to make sure that it was done right before you move on to the next step, that all the keys are present. So it's fairly burdensome from an administrative point of view process in order to make all of this happen.

So moving on to Slide #14, just thought I would take a minute to talk about some of the more interesting challenges that we ran into. We did hear.pr talk about how they were running a lot of this stuff on Windows machines, even now and today. We have run into those things and really run into some seriously old technology and old, small processes from a lot of people and a lot of smaller TLDs especially.

One of the advantages, I guess, that we have in being a large service provider is we have all of this stuff automated, as many of the folks here do this. So one of the big surprises for us in all of this is the setup that has to happen. You really do have to do a look at what the current provider is doing, you have to find some way to integrate with them and get zone data from them, and also how you're going to manage the steps of changing the keys.

Another thing that we often run into is different policies. I know that we focus a lot on the technical side of these things, but it is obviously a much more best practice position always to have two name servers, but it can be a little surprising to find out that there are actually ccTLDs that have only had one name server object in their systems. And that's kind of an issue for us, it requires us to go through and we have to fix that along the way and we have to get them to upgrade and to fix their other registrations in the systems.

So it's not just about the TLD, it's also about the data that we're getting on the registry side and all the second-level domains and ensuring that all of those policies are up to date, and additional work. And these kinds of things can slow down the transition process and slow down moving things over. You get an effect from the registration data too.

The other problem that we've had is finding inconsistencies in the data. And even for us, when we have issues and we have problems, sometimes we've had issues which were present in a zone or as part of the transition which we didn't even notice, and so even we had to update our processes in order to not have problems in the future.

I think that the message from us here in doing this is it really is a high-overhead work to roll over a TLD and do the KSK roll. It's not just the technical pieces of it which we frequently talk about, it's all of the extra activities on top of it. You do have – we have a very careful checklist that we follow when we do this, and even so, problems can happen, new things pop up that you hadn't seen before, and you have to address those as you go along.

So I think that we are moving in this environment to a much better understanding of DNSSEC. I love listening to – we track a lot the penetration of DNSSEC in the community At-Large, but I think that these kinds of issues are important to recognize. It's still not as easy and as trivial as we would all like it to be as we move into this space. And that's it from me.

JACQUES LATOUR: Thank you, Jim. Any questions? Jaromir.

JAROMIR TALIR: Jaromir Talir, CZNIC. I see that you are using algorithm five for DNSSEC. Are you thinking about changing algorithm of DNSSEC?

JIM GALVIN: We don't have any immediate plans to change, but yes, it's obviously on our radar and something we're paying attention to. We haven't gone down the path of deciding that we want to do an algorithm roll just yet.

JIM GALVIN: And what is algorithm five? Any questions? No? Alright, thank you, Carlos, Jim. So next up is Frederico Neves, Fred, with .br DNSSEC algorithm rollover.

FREDERICO NEVES: Yes. We are using RSASHA1 as well. Good morning. My name is Frederico Neves. I work at the NIC.BR, the .br registry. Okay. Slideshow. So a little bit of history of the .br registry, DNSSEC. Basically, we started in 2007 using RSASHA1 and 1k KSK.

In 2009, with the advent of [opt-in transversed as] nsec3/opt-out, we have the ability to sign large zones, so we did it and we signed all of the .br zones at that time. We have roughly 75 zones at that time. Today, we have roughly 90 zones with a lot of additions of geographic names of second-level domain names for cities in Brazil during the last year.

2010, a little bit prior to the root signing, we did our first KSK roll, and we updated our DPS and the key size to 1280 bits and introduced a complete new ceremony schema with HSMs and complete DR setup. And this is what we have been using since then. We managed to hit the root with DS in June that year, and in 2015 following our DPS, we rolled our KSK again. At the time, we increased the key size again to 1536 bits.

Currently, we have roughly 3.9 [million] delegations in .br. The majority of them are in second-level zone .com.br, and we have roughly one million signed delegations.

Going now directly to the point of the presentation regarding our motivations to do algorithm rollover, the biggest one of the motivations is basically be prepared to an eventual algorithm rollover and prepare the software for that.

We have our own signer, so the current software doesn't have the ability to roll algorithms. So we prefer to use these – how can I say – peace times to exercise this and be completely prepared.

We decided to go ECDSAP256. Thankfully for our colleagues here on my left side, they already had the challenge to ping IANA to support that algorithm, and so IANA is now ready and we will not have any issues trying to roll to this algorithm in the future. And there is a side benefit for us that's because some of our large zones we use NSEC3, the proof of nonexistence of names and records and types, we no longer need to have a special separated key because of the history of the protocol, the algorithm roll that we had to use to introduce NSEC3.

Our current provisioning system is a little bit – it's aging a little. It was written in 2004. By that time, we didn't have all that good DNS library, so we had to write our own that we have been maintaining since, and we would like to get rid of this. And that's another advantage of changing this piece of software.

Slide 4 now. The algorithm rollover approach. As I said, we have our own signer. We had to decide how to do the algorithm all over. And so we started to research what we have, the recommendations, and 6781 recommends that we do the rollover what they call the conservative way. But all the open source signers that we could get our hands on basically bind with the managed keys modes. And the OpenDNSSEC does another approach – let's call it the liberal approach – but we were pretty inclined to go the conservative way.

We had recently – oh, this information is not on this slide. Sorry. Anyway, in the last week during the OARC meeting, we got to know a little bit more information regarding this, and we know that the piece of software that did this conservative approach is already seven years old, so it's a long time ago. And even five years ago, we had the clarification on 6840 regarding this confusing 4035 language that it's basically applied to the signer side, not to the validators.

Anyway, this is a small controversy, and we had a very successful algorithm rollover from another colleague from .se, and they use OpenDNSSEC and it went completely smoothly. Next slide. No, sorry. Yes. But anyway, we will test both approaches, and I will show this a little bit further.

So what we will be doing in the next few months is to, as Jim said, roll the TLD. It's no fun job, there is a lot of procedures and steps to go through to make sure that everything works smoothly. And so basically, what we will be doing is in mid-May, we will upgrade our HSMs, and we will be commissioning a third site in a far location from the two current sites that we have in Sao Paolo.

Our HSMs are bought in 2010. They are still working well, but we will substitute two of them and we will make upgrades to support the new algorithm. Even in May, we will do a regular ceremony algorithm rollover. That ceremony took over the period from August 2018 to January 2019.

Regarding the ceremony test rollovers, we will do one ceremony test rollover and we will exercise the two methods. There is a small glitch on this slide. It's Slide 6 now for the ones that are remote regarding the new algorithm. It's P256SHA256.

So we will do with six zones. With three of those zones, we will do conservative method, and with the other three zones, we will do the liberal ones. The reasoning for those three zones is because in the .br zones, we have a schema with split keys, and with the child zones, we have a combined key. So it's a single key. And we have one that use NSEC3 proof and the other ones use NSEC. The majority of them use NSEC. So we exercise all of those situations. And we expect to have the beginning of those rollovers on June the 19th.

Rollover monitoring, we will be following the .se successful rollover. SIDN Labs published a detailed report of the monitoring of the rollover, and we plan to use their methodology to monitor the tests and the actual rollover. I really recommend people to take a look at this report.

The rollover ceremony that we will do in July 23rd and 24th in our two sites, basically, we will upgrade all of the singing software and hardware, and we will prepare for the export of keys because when we do have new keys generation in the ceremonies, we have a lot of steps to export those keys to importing all the for production HSMs.

And besides that, we will change a little bit the way we do serials. We are moving to Julian serial format so we have the ability to have more increments in a single day because we are increasing the frequency of publication of the zone form every 30 minutes to every five minutes.

And just to finish up, the last slide, the visible changes that people can observe in the next few months are the test rollovers starting to happen on June the 19th to June the 22nd. And mostly, the algorithm rollover, if everything goes smoothly, we plan to do it on August the 20th. And if everything goes as planned, we plan to end it on August 27 if that happens on the first window of pre-signed keys because there is the interaction of IANA. So that’s what I had to present. Does anyone have any questions? We still have some time.

VIKTOR DUKHOVNI: Hi. Congratulations on having lots of DNSSEC adoption. There is a small pocket of residual problems in some of the domains [you] delegate. If you can help me get in touch with them, that’d be great. Mostly jus.br that have been having problems ongoing for years.

FREDERICO NEVES: Sorry, I couldn’t understand, Victor, what you said.

VIKTOR DUKHOVNI: There’s a small number of domains you delegate whose own DNSSEC management is a little bit less than perfect. If you can help me get in touch with them.

FREDERICO NEVES: Sure.

VIKTOR DUKHOVNI: That'd be great.

JACQUES LATOUR: Any other questions? So I'm going to – I've got one. So .cz was trying to migrate to the ECDSA protocol, but that was not supported by IANA or something like that. Are you trying to do the same thing, or is it supported now?

FREDERICO NEVES: As I said, it's supported now.

JACQUES LATOUR: It is?

FREDERICO NEVES: Yes, it is.

JACQUES LATOUR: Okay, I missed that. Alright. Three, two, one, questions? Okay.

UNIDENTIFIED MALE: [inaudible]

JACQUES LATOUR: Oh.

UNIDENTIFIED FEMALE: Hello. Can I speak in French, or do I need to speak in English?

As far as the application that you used, do you have any documents regarding the tests that you carried out? I wanted to know how the tests that you carried out could be communicated to the community, especially for a French-speaking Caribbean, for a Guadalupe, because I come from Guadalupe.

JACQUES LATOUR: So the documentation of the tests you're going to do, and if you're going to share that with I guess the LACTLD community.

FREDERICO NEVES: Sure. We expect to at least publish our report in late June, early July, and at least we will put that in a blog post.

JACQUES LATOUR: Translation achieved. Perfect. Thanks. Any other question? So we're good for break. So we get an extra five minutes for the break. We come back here at 10:30 for Part 2 of the workshop. Thank you.

[END OF TRANSCRIPTION]