ICANN68 | Virtual Policy Forum – Tech Day
Monday, June 22, 2020 – 15:00 to 17:30 MYT

KIMBERLY CLARKSON: Welcome to today's first virtual Tech Day. As a reminder, this session is being recorded. If you would like to ask a question or comment please type those in the Q&A pod and you'll find that at the bottom of your screen. Alternatively, if time permits, you can verbally ask a question using the raised hand icon also found at the bottom of the screen. You will then be automatically placed in the speaker queue and we will take the questions in order that your hand was raised.

Your microphone will be muted until it's time to speak. At that time, we will announce your name and unmute your microphone. You will then be prompted to unmute your mic. We will not be monitoring the chat for questions and comments, so please use the Q&A pod.

Finally, this session, just like any other ICANN activity, is governed by the ICANN expected standard of behavior. And with that, I'd like to turn the floor over to Eberhardt. Thank you.

EBERHARD LISSE: Okay. Good morning, everybody, from freezing cold, maybe 7 degrees when I came to work, which is the reason for my lovely jersey that I'm wearing. It's also quite nice to do this from your office.

Short agenda today because it's on the one hand the policy forum where we only do the afternoon, usually, and because it's the first virtual Tech Day so we wanted to see how this goes.

At the moment, we are missing one presenter, which is Jannett Ibañez. We're trying to reach her, so we'll postpone her presentation if she doesn't come in on time.

Otherwise, Roy Arends will speak about his current proposal to allocate one or more or many of the 42 unused ISO codes to be used for nonfunctioning TLD names. He will go into much more detail on why and so on.

Then Jannett Ibañez will speak about the deployment of DNSSEC in .bo. Then I will speak about rolling .na. And we didn't just roll our key, we rolled a lot of other things at the same time, which made it a bit more complicated and therefore perhaps interesting.

Then we have, as always, the host presentation, then Davey Song will speak about the DNSSEC experience of Alibaba, which is going to be very interesting to hear from a huge organization what their experiences are.

Then Dmitry Kohmanyuk—who I'm also not seeing yet on the panelists—will speak about rolling their algorithm. That's always interesting to hear what happened.

And then Joe Abley will speak about the DNS plans for .org. The actual names of the presentations will be maybe a little bit longer or

different. I always try to fit them on one line so that it fits nicely on the agenda.

At the end, Jacques Latour will try to remain unasleep during the whole session because he was volunteered by me—and graciously agreed—to give the usual closing remarks, which include short presentation about what he felt was interesting.

So far, I must say we have 79 attendances, plus [12 panelists.] So that's a very good turnout. And without further ado—and six minutes early—I call on Roy Arends to start the proceedings off.

ROY ARENDS: Hi everyone. Thank you, Dr. Eberhard. I'm Roy Arends. I want to start with a short statement. This topic that I'm going to discuss with you is actually a private submission to the IETF and not an ICANN-endorsed proposal. I just happen to work here. So as everyone knows, any proposal made within the IETF is done on your own remit, not actually something to do with the organization. I [happen to have a collision] here. eventually, this policy is related to ICANN, of course, and is related to the IETF. But this is my individual submission, I'm not representing ICANN here. Thank you.

I want to talk about private names on the Internet. Next slide, please. So these are names that users and organizations can use in the privacy of their own network, and these are things similar to RFC1918 addresses, 192, 168, and 10.0/8, etc. So private use is pretty common in internet standards, as you can see here on the slide. So most of the

tech folks that are listening to this should recognize some of these, if not all of these. Next slide, please.

So these private use names are names that, when they leak, they won't collide with anything in public use, now or in the future and are recognized as only having meaning locally, independently of the global DNS. And while names shouldn't leak, they sometimes do, and that may lead to unexpected behavior if they get delegated in the root. And sometimes this is referred to as name collisions. Next slide, please.

So, who would use these? Anyone can use these. Organizations can use this internally or privately or independently. ISPs, device makers, software developers, technology companies, cloud providers, etc. If you use anything currently, it most likely will be squatting, but I'll get to that in a minute. Next slide, please.

So, what's the current advice? The current advice is to use a label under a registered name, something like [inaudible]. So in general this is good advice, but it doesn't work in all use cases. For instance, when you ship software or devices with example.com preconfigured, traffic that is meant to be private will end up at example.com, and that has privacy implications, and it also may cause a fair amount of traffic if a device or software becomes popular.

And then eventually, what might happen is that example.com may expire and the next user of example.com may have less noble intentions. Next slide, please.

And so the result is that .home, .lan, .corp, .dlink, .dlinkrouter, .internal, .gateway, etc. is now used everywhere, as you can see in this table. And this is what I see as squatting. So what you see on the screen right now is data from the identifier technology health indicators, ITHI, which is a project from ICANN. This data is available to everyone, but what you see here is the [top no such] domains that have been asked to IMRS, ICANN managed root servers, formally known as L-root, and it's quite significant. As you can see, .home is at the top, etc. And I can tell you that 2.5% of loads on the IMRS servers is a fantastic amount of traffic. You don't want to have this at one or two nameservers [locally.] Next slide, please.

So, the obvious solution—at least obvious to me—is to carve out a corner of the namespace for private use. Something that's short and without a semantic meaning, and [that's because] private or internal, home, local and corp, they do not mean the same thing. Those labels are too long, they're too semantic, and they're too English. Maybe we can use a two-letter ASCII domain. Next slide, please.

So I want to explore some of the guiding policies for two-letter ascii domains. RFC1591, that refers to some generic top-level domains, but I want to talk about the ISO 3166 for country codes. It says here literally the IANA is not in the business of deciding what is and what is not a country. Between you and I, neither is the ISO, but I digress.

So it goes on basically saying the selection of ISO 3166 list as a basis for country code top-level domain was made with the knowledge that ISO has a procedure for determining which entities should be and

should not be on that list. Now, this document is from 1994, and I translated it—at the time, and still am, but at the time when they chose this policy, the ISO 3166 was trusted to know what they're doing. So, what are these codes? Next slide, please.

These are 676. I've counted them, there really are 676 combinations of two letters. Some of these have been reserved, some have not been assigned, some of them are assigned. Next slide, please.

And I want to focus on the blue ones. Next slide, please. So these blue ones are what ISO refers to as the user assigned codes. They include AA and then QM through QZ, XA through XZ, and ZZ. Next slide, please.

So, what does the ISO 3166 say about this range? What it says is they can't be assigned or reserved by the ISO 3166 maintenance agency. Relevant part of the actual standard here, these codes are for the user of the standard to use as they see fit. And we'll get to a few examples in a minute. Next slide, please.

So, this range has been stable since 1974, and I think that's important. What happened in 1974, of course, the standard was created. So it hasn't been changed. These are still the same codes, and only ISO's technical committee 46 has the ability to reassign these from the user to the maintenance agency. So not the maintenance agency itself but the entire technical committee 46. Would they do that? I think if they'd do that, that's going to be a really bad idea, and I will show you [where they're used] in a minute and then you can see what a bad idea that would be. Next slide, please.

So the same is true for IANA. If the policy deviates from RFC1591, it would be an equally bad idea as well. After ICANN was born, Jon Postel's choice for aligning ccTLDs' assignments with ISO 3166 maintenance agency's assignment is a good idea. So not following that policy would be a very bad idea. It would open a can of worms, if you ask me. Next slide, please.

So, this user assigned range is used everywhere as intended, and I can give you a few examples and they're on the screen. But one I want to highlight here is the US dollar. The code for US dollar is USD, and the US is straight from ISO 3166. So is DK and DKK, the Danish krone, and MY and MYR, the Malaysian ringgit.

Now, gold is country agnostic, so it's designated as XAU in the standard. Silver is XAG. Bitcoin is XBT and XTS is used for testing. And this is ISO 4217. So the first two characters of this list are straight from the ISO 3166 user assigned list. Next slide, please.

Here are a few more. This is the ICAO, IATA and WIPO use these. The world intellectual property organization uses these for a long time already. Five of the user assigned code elements are used to identify regional agencies and patent offices, and they've allocated XX for unknown states, other entities or organizations. So as you can see here, it uses the user assign codes literally as intended. Next slide, please.

So here we have the United Nations, the World Bank, Interpol and CABforum. CABforum is an interesting one, it's the certificate authority and browser forum. That's a little bit closer to home. They have

certificates, of course, for domain names, and they actually reserve XX to signify a location not covered by ISO 3166. And again, that's a perfect use of the user assigned codes. Interpol is on here as well and Interpol sends out a transaction identifying itself as ZZ/ALL. Next slide, please.

So, here's Unicode. Unicode common locale data repository, CLDR version 36, uses all of these to identify things that are not in the ISO 3166 list. For instance, ZZ, the way that Interpol used before to distribute transactions, Unicode uses it in APIs or as replacement for invalid codes. Next slide, please.

So it gets a little bit more interesting. IETF uses these as well. For instance, in language tags. This information here on the screen, that's actually buried in every operating system shipped to billions of devices. It's there in the system you're currently using for Zoom, whether you like it or not. So you see what a terrible idea it is if the ISO would arbitrarily reassign these user assigned strings, something that they've never done since 1974. Next slide, please.

So it gets even closer to home. There's a relationship already with the domain name system. Internationalized domain names, they use XN— as a prefix. Have you ever wondered how this was chosen? I have, and what happened was in 2002-2003, the IASG used RFC2777, verifiable Nomcom random selection. You can forget that now, but it was interesting. Selected a dozen stocks and trading volumes on a future day. At the time, this was 11 February 2003, and they used 18 code elements from the 42 user assigned list. XN was eventually the winner,

and the reason for using this user assigned list was—and I quote—it removes the possibility that a code would duplicate a present or future ccTLD code. Next slide, please.

So in conclusion, these codes are used as intended already in various standards. They will never be ISO assigned, they will never be delegated as country codes, they have no semantic meaning, they are short, they are collision free now, and in the future.

Now, most other IANA registries have private user ranges. You have X headers, IP addresses, Q types, DNSSEC algorithm, etc. Even the ISO foresaw a need for private use already in 1974. So it's now time we fix this omission in the DNS namespace, in my humble opinion. Next slide, please.

Now, if this was done a long time ago, we might not have seen such a struggle with private use names or even special use names. It would have been obvious that any two-letter code, for instance starting with X, can be used for private use. I'm using it as well myself. Next slide, please.

I'm using .zz as well. I've also now recently started using AA at home because my last name as Arends and m yes daughter is Amelie, hence the AA. But that aside—next slide, please—what I'm planning with this is to continue working on this on the DNS operations working group mailing list. The drafts that I'm discussing here, the draft Arends private use TLD, there's currently a call for adoption within the DNS operations working group. It has seen a lot of discussion already. The call for adoption closes this Wednesday, I think, or this week. Now, if

and only if the working group adopts the Internet draft, my plan is to engage with all the proper authorities in the space, the IASG, the IAB, IANA and ICANN communities to develop a path of least surprise.

Now, of course, that's already happening here, and the reason I'm doing this here is because I was asked to give this presentation by Dr. Eberhard Lisse, which of course, I'm happy to. But just so you know, it's not yet adopted as a working group document.

All right. Thank you. I hope I left a little bit of time for questions. If not, I give the mic back to you, Eberhard. Thank you.

EBERHARD LISSE: Okay. Thank you very much. Quite interesting presentation. I'm interested from the aspect of work we have been doing on the policy development group, removal of ccTLDs after the ISO code changes. So we have read the standards and we've looked at the details. It's quite interesting discussion going on on the appropriate mailing list of the IETF DNS op, which I'm also reading, where I sometimes am amused how serious techies who understand all this stuff technically on the bit level, how little they know about real world things and how things actually work sometimes in international organizations.

Unfortunately, nobody knows how absolute the promise of the ISO is not to move those 42 names off this unassigned list and maybe use them. It hasn't been done since '74 since it exists. It would make an exceptionally bad idea, and for my purposes and for my

understanding, it's good enough, but it's not 100%. So I don't know how it is with regards to writing of the standards.

We have Dmitry Kohmanyuk on his hand, so we can ask him to unmute and ask the question.

ROY ARENDS: Sorry, Ebehard, can I just respond to that? Thank you. The purpose of writing this draft was in first instance to basically point out that these strings exist and that the ISO intended for this purpose. It wasn't meant to actually allocate these for anything, just to point out that you can use these in private. And it's exactly for what you said. Even though the ISO—we're not going to reassign them, I think it's smart to have it at least documented that when they are used for private use, that it should be allocated somewhere for that reason. So if the ISO, which is an organization outside our control or reach, if they change their minds and do something we discussed, at least we're still on the safe side. So I agree with you. Thank you.

EBERHARD LISSE: Okay. Dmitry.

DMITRY KOHMANYUK: Okay. I do like the idea, but I would ask you this: just like .eu was at some point not a country and it's still not a country, or just like .uk is still not a country, just a special code, I know, but why don't we go and maybe ask one of those two-letters or maybe get a new one, like the

.pp for the private. I know .pp is probably used, I haven't checked. I think a better idea—just as this crossover XK shows, it can be a conflict of namespace at some point. So I do like the two-letter private, but I don't like the idea of borrowing one from those private list. Anyway, this is my two cents and maybe I should just join the IETF list and discuss it there. Thank you.

EBERHARD LISSE: I think the best thing is to discuss it on that mailing list, because that's the way the IETF works. Anybody who has got input to make. But the point to make, again, and the devil lies in the detail. .uk, .eu are from a different list. They are on what is called an exceptionally reserved list. These are exceptions mainly grandfathered. .uk is a grandfathered [one,] .eu is a special case. These are exceptions.

The idea here is to have something which is, as far as we know, cannot be conflict with the ccTLD to be used. We all see that we get nameserver requests, significant numbers for ccTLDs or others that shouldn't even reach us. So doing something that cannot reach a nameserver makes sense. I personally like the idea about .zz, but that's my personal feeling.

We have a question from Nigel Roberts. Can you please ask the question?

NIGEL ROBERTS: Thank you, Eberhard. You actually anticipated most of the comments I was going to make, but a little bit more—so when you said that there's

no guarantee, it's about what the ISO will do or won't do, the ISO has in the past done things which are classified in my book as a very bad thing, when they, within five years, reallocated a two-letter ISO 3166 code to a new country which had previously been used not only as a country code within the previous five years but as an active ccTLD. I'm referring to .CS. So unless or until you can get a formal statement from—I think you called it TC46—that these codes will never be used and will always be retained for private use, then I'm not convinced this is a good idea.

EBERHARD LISSE: Okay. Thank you very much. Anybody—Roy, do you want to answer this?

ROY ARENDS: Yes. It is for the ICANN community and the IETF community to protect its users. Yes, we can actually go and ask through one of our liaisons if that would be possible, to get such a statement. I don't think it's a useful use of our time to do that. I think a better use of our time to do that is to make sure that you can use private names or independent names on the Internet so you won't have things like name collisions eventually. You won't have people shooting themselves in the foot. Of course, just carving out a space on the Internet doesn't go without any best practice to make sure that you do it safely, securely, and in a stable way.

So I think a stable way is to have something—a string that is meaningless, as short as possible, so that's why I arrived at the two-letter codes. And I think if we—communal we, us in common—write something that basically says these strengths or some of these strengths are useful, then that's it. Then they are used for private use.

Now, if the ISO changes its mind and goes back on its 1974 statement, then basically says we're going to damage all of these other organizations by now using these users and strings for all these new countries that pop up, then at least the private use names here are fairly safe.

EBERHARD LISSE: Okay. Last question from Harald Alvestrand, I've unmuted you or you are unmuted. Please go ahead.

HARALD ALVESTRAND: So one thing is just allocating something for private use, but this will probably have the same problem as [net ten] is that every times organizations reorganize, you will have collisions in usage of those names. So you haven't solved all the problems just by declaring something private.

ROY ARENDS: You're absolutely right. In a sense, if organizations are going to shoot themselves in the foot, then maybe use a water gun on the least dominant foot. We have learned hopefully from the [ten-zero]

[inaudible] 192, 168, when you use things in private, and you go to buy another company or you're going to engage—take your device elsewhere, yes, you have collisions in the namespace, but these are collisions that are local, not global. It comes with private use and we've seen that. So you're right, there might be collisions, and this needs to be done in a best current practice in my humble opinion, that if you're going to use them, use them in the following way, take care of what might happen, etc. Good question. Thank you, Harold.

EBERHARD LISSE: I'm taking the very last question from David Conrad, because frankly, the question is very interesting. David.

DAVID CONRAD: This isn't a question really, it's sort of a response to Nigel. The example of CS is actually sort of instructive in the sense that when Czechoslovakia disappeared and they broke up CS and then reassigned it, it was an assignable code. The point—and Roy, correct me if I'm wrong—one of the points here with use of the private use codes, the user assigned codes that ISO 3166 has already designated as sort of assigned, is that you're not using or you would be using an assigned code. The functionality has already been defined for these two-letter codes, so it seems wildly unlikely that they would take a code that was assigned and is in use, because you can never know, they're user assigned so you will never know if they're in use or not, but you have to assume they are, and then assign them to another point, another purpose.

So it seems the analogy [inaudible] CS and the case that had occurred with CS doesn't seem like analogous to the situation we find with the proposal to use the user assigned codes.

EBERHARD LISSE: If this goes forward, it has to be one of the 42 ones that are currently not assignable. Taking one that is possible is mildly to very bad. Okay, thank you very much. I really appreciate this very interesting presentation. I will now call upon Jannet Ibañez, next presenter.

JANNET IBAÑEZ: Thank you. Good afternoon, and good morning. Before I begin, I would like to thank you, Kimberly and Eberhard for letting me be part of this tech day of ICANN 68, and all of you for joining this virtual session.

My name is Jannet Ibañez and I work in the ccTLD .bo until February of this year. I'm going to present the advance we have in the intent of deploy domain name system security extension, DNSSEC. And this is the agenda. Next slide, please.

First, I will present the entity who manages the .bo, then describe the plan we made to development for the final, the adjustments, and required to the plan, and some conclusions. Next slide, please.

The Agency for the Development of the Society of the Information in Bolivia is a governmental entity that depends on the vice presidency of the Plurinational State of Bolivia. ADSIB is a service provider of technologies of information and communication.

The first service which ADSIB [was doing] is the management and operation of .bo domain, Bolivia's country code top-level domain. It is the registry and registrar. We don't have registrars authorized yet.

The second service provided by ADSIB is digital certification. According to the law, it's the only public certification entity for digital signature that in Bolivia has legal probative validity equivalent to the handwritten signature. Next slide, please.

The other service are the administration of the state repository of free software that allows public entities and the general population to host their software projects. And finally, the service of sending notification through SMS, push and e-mail messages.

To May of this year, ADSIB has more than 13,800 domain names registered and active. 62% of the domains are third-level and 26 of second level.

ADSIB decided to deploy DNSSEC with the objective of decrease the vulnerability to attacks to the domain names .bo using internal resources. And besides this, [not to do it alone.] For this, it invited different entities, especially those that have digital services for the population, and in coordination with various entities, began the work. Next slide, please.

In the ISO page, we have maps that provide a view into global DNSSEC deployment. It breaks the deployment status of the country code top-level domains out into five categories, the status of the deployment.

The categories are experimental, announced, partial, ds in root, operational.

As you can see in this map, Bolivia has no—it hasn't state, and we hope this year it can change at least to announced. We're not the only ones, but it's a pending task and responsibility as a ccTLD. Next slide, please.

I imagine that most of our audience are familiar with what DNSSEC is. For which do not, I quote these two text that tell us that DNSSEC is a set of security extensions that strengthen DNS authentication through digital signatures. DNSSEC adds two important features to the DNS protocol, data origin, authentication, and data integrity protection. Next slide, please.

Here, we can see the initial plan deploying. An activity of high importance [is] defined to carry out the training of internal staff as well as the staff of the invited entities. The preparation of the environment and thee realization of exercise or trials were part of the plan. It was considered the reduction of policy statements and practices and procedures for last year.

At the end, we have an important task to evaluation and monitoring. This stage is also part of the training and must be considered. To make the plan, ADSIB was based on the experience of different ccTLDs, and also in its own staff, some of whom have more than ten years in the entity. It also was consult documents, webinars and other from technical events of LACTLD, ICANN, LACNIC, GFCE, IETF and ISOC, will

receive direct advice from some several friends too. At the end, we have a monitoring that is part of the training too. Next slide, please.

Now we can show the development. For the beginning of the training, a workshop was carried out in October of 2018, taking advantage of the visit of Stéphane Bortzmeyer of AFNIC to Bolivia. This workshop was designed especially for internal staff, but since ADSIB's plan is not large, other government entities were invited.

Stéphane shared with us much of his experience about DNS and DNSSEC and showed us several available tools. For us, this workshop was very interesting, because we were able to ask about the care that must be taken, the tools used. We obtained firsthand knowledge of a person with a lot of experience. Next slide, please.

Last year, we began the hands-on workshops. Jose Machicado from ADSIB shared his knowledge about DNS fundamentals and BIND server administration. The sessions [inaudible] Two of the three could be held. The third session has to be postponed due to political problems that occurred after annulled elections and the establishment of a transitory government. This new government changed the executives of the entities that started process, and also some officials who participate in the workshops were also changed. But luckily, there were very few cases. Please next.

In this view, we can see the logos of the entities that assisted to the two workshops and also request their subdomains, test sobdomain, and were able to carry out the exercise. Here, we have an ISP, various

ministries, and some government agencies and companies. Please, next.

In this [inaudible] we can see the infrastructure that ADSIB has to operate the registry .bo and to provide a service which is complaint with the standard requirement. In the next page, we can see the structure with DNSSEC. The generation and protection of private keys will be carried out with SoftHSM. Only the generation of the KSK will be manual. The next stage of the process will be automatic, and constantly monitored. ADSIB uses BIND 9.14 that allows to automate some tasks.

Once .bo zone is signed, it will be sent to the IANA, and the ADSIB own zones will be divided into different—of their own servers. The signing system is placed on the internal side of the network, and it would receive data from the repository and deliver signed data to external authoritative servers. Next slide, please.

We are going to use two pairs of keys, the KSK signing key, key also called secure entry point used to sign the zone signing key, has its length of 2048 bits. The algorithm we are going to use is RSA/SHA256, and the time of change is going to be two years, and the method or scheme is going to be the pre-publish key.

To the zone signing key that we used to see in the zone data are set, it has a length of 1024. The algorithm used is RSA/SHA 256. They changed the time, will be three months, and the change scheme will be double signed. Next slide, please.

Here, we have the result of the DNSSEC analysis for the domain name we used to test DNSSEC .bo. Under this domain, all the entities also carried out their corresponding tests. After this stage, again, when conditions are favorable, ADSIB will establish the new date for the deployment. Next, please.

As you can see, there are some activities to complete in our first plan. We hope this year, ADSIB can complete those activities we show here in red. It will depend on the political scenario, on the evolution of the pandemic of COVID-19.

For the final, we are going to see some conclusions or facts we find. Next slide, please. For example, in the initial phase when we are measuring our forces and we decide deployment in our own, it serve to get more people involved. And I think it's not going the same if we decide to give to an enterprise or a company to implement the DNSSEC.

Another thing we saw is training and peer support help us to reduce deployment time. Then it's crucial to have the support of the executives so that the technical part can carry out the deployment, especially [if is necessary a budget] to get some technical requirements. Then the documentation of all processes is required to reduce risk, and the final roles and responsibilities can help that rollover keys be carried out properly. And one thing we realized is that the real work comes after the deployment.

Before I finish, I will thank for the work and all the effort of ICANN, LACTLD and the associations of other regions to reduce the gap that

some ccTLDs have in relation to the deployment of DNSSEC. Thank you.

EBERHARD LISSE: Thank you very much. Excellently with the time management, even. I don't see any hands, so that's fine. I propose we wait for questions until I've done mine because it ties a little bit in. I am going to share my screen now.

Okay, so I am going to talk about rolling the key. This little version number that you see here, 1.71, comes from the version control management. I like to have my things in such a thing, so whenever I make a chance, I up the number. This is very helpful, and we will see later why this is so.

The background is that we signed .na in 2009 when I was ill at home and I was board so I tried to figure it out, and I came to the conclusion that while DNSSEC is not difficult, it's not easy, and it can be expensive.

The way we did it, we had an inline signer with BIND on a hidden master. We SCP'd it to the public master. The question is always, why didn't you do a zone transfer? Because first of all, we were not sure about ourselves. Second of all, I like to have different versions on the nameserver that I can load in case there is a problem, we could always go back to the last functioning version.

In the meantime, our second levels, com.na and so on, were signed by packet clearinghouse. And we thought, eventually, because we

wanted to have this audited, we wanted to have an audited system that we can say we're fully compliant with whatever audits are being used so that the banks can start thinking about this, we wanted to do this in hardware side because we can't afford the hardware, you need three HSMs and for a small domain, a ccTLD with 4500 names, we couldn't afford three of those.

PCH does it in hardware, they're trusted, they're auditable. So we then approached them, [they] said go ahead, no problem, we'll sort this out for you.

We had an additional complication because DYN provided nameservers for us for many years very pleasantly and very nicely and free, they got bought by Oracle and after a year or two, Oracle got wise to us and sent us a very polite letter giving us one year of notice, which was perfectly in order, we very much appreciated this, and so eventually started the ball rolling.

Then ISC gave us an equally polite letter giving us a little bit less notice, about six or seven months, I don't remember, because they went out of the business of doing secondary nameservers as part of a consolidation process, I would think. No problem, we were very happy with the service for many years, and if they don't do it anymore, they gave us advance notice, no drama.

Our primary was in Redwood in their rack. It was our own hardware, it was running for 15 or 12 years or something, and then the power supply died, so it went on actual life support. They had to put it out of the rack, put it on a workbench and connect an external power supply

to it. And that's a situation that couldn't keep on, so we then decided to move on this.

In Montréal, we spoke with two of our new secondary nameserver providers, NetActuate and Gransy and they were very happy. This is how it looked. These images are done with Graphviz which is the underlying software that is used by DNSViz, which is what [we saw] images from Jannet as well, and we will see during the presentation.

We have green basically for hidden, red for removal, and blue for signing. So we have a hidden—our CoCCA tool software, that's the registration software, we sign, host swakop and send it to Merlin in Redwood, and from there, the secondary is ready.

We wanted to get from a system where—that, to a system where our registry software, CoCCA, on the swakop host, becomes the hidden master to the inbound. [This, signed in hardware,] it goes output from which the secondaries pull.

Again, point of departure. Now, what we did is we made an engineering plan. We tested this first out on lisse.na last year and noted two small problems which resulted in offline for my domain name for about an hour each, which was a good thing because we then had a proper plan.

We did this engineering plan as a presentation like this with running numbers, so turned out to be very helpful. You put it on Zoom, you said, "We are number so and so, we do this, next step is so and so," everybody is happy and we carry on.

So what we basically needed to do is to duplicate our SCP, our transfer, not only to Merlin but also to a new host called keetmans by modifying this provisioning script.

Then we told IronDNS and PCH, two of our secondaries, to pull off the new one. That necessitated thinking about a firewall. Then we sent in an RZM, root zone request, remove those hosts from the published zone and add these wo. And then when that happened, we stopped sending the zone to the old primary, and we were at this position. We were still signing inline, we were sending to Swakopmund, we were copying to keetmans, of which the two old and two new hosts that we have on our own control for temporary services, katima and sdc which stands for Santiago [and] Chile. That's where they're located. The other one is in Ireland. And so we had enough nameservers that if one fails, we have enough redundancy.

Then we [inaudible] the old key to the unsigned zones and pushed that to PCH so that we have got basically now this position. From swakop, we zone transferred to the PCH inbound and we copy to keetmans where they display [the signed] zone.

We now have the situation which is interesting that we have on swakop two different methods of transferring two different zones. It was for me too complicated to run two nameservers on two different ports, so I think the SCP and the AXFR method came in very handily because it required little modification and it was working and there was no risk of mixing things up.

Then PCH generated a key, they added their keys, and we have this situation. We told NetActuate and Gransy to pull off PCH and now we have got six secondaries, two of which were not in the zone. Okay, and here is these DNSViz images that everybody likes, that Stephane likes and that are visible under the training heading in the previous presentation where we can see that on keetmans, it uses the red zone signing key, and on PCH, it uses theirs, old and new.

Then we add the PCH's new DS record, wait for the requests. IANA is quick. It works very well, there is no question. The only time we had issues is when their returning mail wound up in the spam folder. So that is a lesson that we really learned: if you do a root zone request and you don't get a report back within an hour or two, look in your spam folders.

Now we have this situation. Two different keys in the root, and we are ready to roll. Different nameservers provide the same zone with different signings. We then changed the IronDNS, the old that were providing nameservers to us to pull off not keetmans anymore but to pull from PCH, and PCH internally changed now not to do it from us anymore but use the zone that they signed. And then we had our two old hosts, two temporary hosts, signing the same content but with a different key. No problem. Worked, no drama. None of our domain holders or registrars noticed. And then we tested this, waited for the caches to expire, and then we checked. The last one is katima, that's always using the old one. The right one is PCH, which used the old one, and is supposed to switch to the new one, and the middle one is IronDNS, they're already using the new one, green and red.

So if you switch to the next slide, we see that PCH switches while katima is still using the old one, the important ones, the Anycast servers, they are using the right one.

Here you can see in color the zone signing key that is being used. While the resolution is correct, the serial is correct, different zones—on these two red hosts, they were signed with our old keys, so they could just be removed from the delegation. We then sent a root zone request in to remove these two old hosts and these two ones waited and then we sent another root zone request in to remove the old DS record.

Now we are in this situation where none of our domain holders or our registrars even noticed. The difference in core management capabilities between some of our registrars and us is that they can't get an e-mail to work whereas we can do that.

And then some tidying up to do. Number 31 is an important issue, document this. What did we learn from this? You need to write a plan. This numbering that we have, turned out to be, this running numbers on a presentation type thing turned out very well. You can just make a Zoom, have people in different time zones available, we come to that, discuss on a Zoon, we accept so and so, works.

And then you must dumb a complicated situation down into a simple step that even a gynecologist can understand. Once you have simple steps, one step at a time, it becomes simple. Even I can do this. Nobody has to panic, nobody will notice, have enough people look at it.

Whenever we made a modification to the plan, we added this to the engineering plan and upped the revision control number on the first page and in the filename so everybody knows, when you circulate this, which version we're talking about.

Important, another thing is, take your time. Communicate. Details matter. One of our secondaries uses NSD and they expected the notification, the notify, to come with the TSIG. We usually don't do this, we usually only do the zone transfer with TSIG, but it took us a few days to figure this out because they only loaded the zone once a day roughly according to what the SOA record showed. So for us, no drama, we noticed, loading it once a day, there must be a problem with that. We communicated with them. At the time, [inaudible] from Granzy was traveling, so it took a day or two, but then we changed this and no drama.

Important here is we're talking with different people in different time zones, most of whom do not speak English as the home language, so we must be clear that we understand what we're talking about and that our conceptions, we think about this, we think about that, are clear.

We also made sure that we had different contacts: one in Asia, one in Europe, one in east coast, and one in Costa Rica so that we have got enough people, whenever something serious happened, we don't have to wake somebody up in the middle of the night, we can get a hold of somebody over the phone immediately who is awake and in the office.

DNSViz is your friend. This is what I just referred to. Since the presentations are public, this is the link. If you click on it, you get to it. It's very cool. There's also a command line thing for it. It produces SVG, which is a sort of XML, so I can have my merry way with it to change the colors for demonstration purposes so I don't have to do this manually or to make file to do this.

Again, I want to thank DYN and also Oracle for providing a name service to us that was second to none for many years. When we were flooded once with attacks and our local nameserver was really aching, DYN couldn't even bother to isolate it by country, only by continent, because it didn't notice. So in the end, our services were done very well. The same to ISC, they provided also primary and Anycast service for many years, and I want to be very sure that everybody knows that they did a great job for us and we very appreciate this.

And then of course, our current nameservers, PCH, Gransy, NetActuate, and IronDNS, these are links, they are clickable, please find it free to click and use them. Any questions? I do not see any raised hands. Dmitry Khomanyuk.

DMITRY KOHMANYUK: Thanks. So, thanks for all this documentation. I was just curious, I know it's [too short,] but [inaudible] do you feel that PCH is like a critical point in your infrastructure that—I mean, we use PCH too, but [they fail and basically] it would be kind of difficult for you to regroup. Don't you think that's an issue maybe for the future?

EBERHARD LISSE: We thought about this very hard, very long. They have been so stable over the years that we would not anticipate a failure. And the worst that can happen is, since we have very few clients, okay, we unsign, we run it, we remove them, we run it. But then it's not just us who are affected. PCH provides this service for a number of ccTLDs. Before that happens, I doubt it ever will.

If somebody is willing to give us three HSMs on a sort of regular basis to replace them when they expire, we are more than welcome to do it ourselves. I'm quite sure [Stephan Bodsma] [really enjoyed talking to them, may be able to] help us out. So will the people from Gransy, and so will be [inaudible] and many others who [have offered.] We just can't afford the hardware.

I don't see any other hands, so let me just go to my agenda again. The next presentation—and we are one minute over time—would be the host presentation. You have the floor.

MASTURA MUKHTAR: Thank you, Dr. Eberhard. Good day to everyone. My name is Mastura from MYNIC, registry for .my. So it is an absolute pleasure to be part of the virtual Tech Day for today. Thank you again for ICANN for inviting .my to be part of your program.

So, Next slide, please. Okay, the agenda for today, I'm going to just brief overview about who are we, our history of DNSSEC deployment

for .my, our journey to adopt secure e-government services to DNSSEC for .gov.my domain name. Next slide, please.

Okay, who are we? This is an overview about MYNIC itself. We are an agency, and a ministry of communication and multimedia [inaudible] and we are the registry for .my domain name which country code for Malaysia, and [inaudible] part of national critical national information infrastructure, or CNII. We are also one of the key enablers for the digital economy ecosystem so that we can focus to develop and promote the usage of .my among Malaysians. So we encourage Malaysians to use the .my domain name, so this is to strive to empower all the businesses, industry, to be part of the digital economy through the development of the domain names, so we want our objective to grow our .my domain name. Next slide, please.

Okay, these are our core services. We're managing and administer for eight domain name categories. We have .my and we have another seven SLDs. So we are running as registry and registrar for .my. We deliver both services to our .my customers, including WHOIS, DNS resolution. Also value add services, .my domain dispute resolution, sensitive domain dispute resolution, and also we provided registrar services, we provide to our end users domain name registration and also direct customer service to our domain registrants and also our resellers. Next slide, please.

Okay, the history of DNSSEC deployment for .my. So just go through a general history of DNSSEC deployment for .my. We have started to research on DNSSEC deployment for .my in year 2009 where the

research itself conducted by our inhouse internal researcher. So we developed our own signer during the time based on the research conducted. So by end of 2009 we managed to have DNSSEC public trial. On 2010, we continued to conduct the seminar and awareness program to the public, especially to the sector which provides essential services such as government agencies and banks. Those are facing with critical services to the public.

2011, we deployed and signed DNSSEC for .my so DNSSEC registered in root, so we established chain of trust between root and .my. By Q2 2011, we ran full operation of DNSSEC system to receive the DS record for our TLD and also our SLDs domain category.

For November in 2012, we deployed DNSSEC for our IDN country code [inaudible], so DS record submitted to IANA somewhere in November, and from there, we managed to have a complete chain of trust from root to our [inaudible] zone. Next slide, please.

Okay, we would like to share our journey with our initiative to secure e-government services via DNSSEC deployment. Next slide, please. Last year, we grew an initiative to implement DNSSEC for .gov.my domain name. The main objective for this deployment and implementation to create a secure e-government services to support the national digital economy and increasing public trust. So the services that provided by the government to the public. That's why last year, we aggressively conduct a training to the government agencies. Next slide, please.

Okay, this is the five pillars. We are focusing on adopting DNSSEC for .gov.my domain name. The first one is policy and implementation, competency and capability of DNSSEC, domain registrant, resellers and partners. Basically, we don't have the registrar because we are the registrar and registrar. We have the authorized resellers and partners to carry out the domain name registration. And last but not least, monitoring and validation to secure our TLD and SLDs zone to ensure the chain of trust continues without any problem.

So we go to the first one. Next slide, please. We established collaboration with our stakeholders who is the policymaker for our country which is National Cybersecurity Agency—or NACSA—and the policymaker for all government IT services which is carried out by Malaysia Administrative Modernization and Management Planning Unit—MAMPU—in order to secure and also in order for us to drive the DNSSEC deployment for .gov.my domain name. Okay, so next slide, please.

While we are implementing the adoption last year, this is the challenges that we face for policy and implementation. Among the challenges that we face are clarity on responsibilities between the policymakers, NACSA and MAMPU, infrastructure and technology readiness to support DNSSEC especially for .gov.my domain name, lack of understanding on DNSSEC.

Okay, with this, how we overcame the challenges that we faced, we managed to get an approval to support our DNSSEC implementation for the gov domain name from both our stakeholders, NACSA and

MAMPU, and we received [inaudible] enforcement from the stakeholder in order to carry out this exercise.

And also, we [inaudible] refresh on the infrastructure and the technology to support DNSSEC. We conduct awareness program [inaudible] program to the DNS hosting provider appointed by the government to finish the government domain name, and also, during the training we provide testing environment to deploy DNSSEC in order to gain their confidence. So they have visualized from end to end how we can assist them to deploy the domain name and the DNS administrator and the government custodian. Next slide, please.

For pillar two, competency and capability, these are amongst the challenges that we faced. Administrative overhead concerns on DNSSEC key management, understand of the DNSSEC configurations, how they can configure the DNSSEC to ensure no disruptions on the domain name service, unclear SOP to manage the DNSSEC. So for instance, [once the administrator enabled it and signed the DNSSEC] under authoritative [inaudible] what they have to do next in order to establish the chain of trust.

So we overcame the challenges. Again, we provided technical hands-on workshop to upskill the DNS administrator to reduce the administrative and configuration issues and risks. We explained them why [inaudible] need to have the new signature, why [inaudible] need to be automatically generated instead of manual generate and how to set the interval signature in order to generate the new signature.

Also, we provide our processes and practices to help the administrator to manage DNSSEC. This is to overcome the unclear SOP to manage DNSSEC. We provided them step by step what they have to do next when they have sign and deploy DNSSEC on the authoritative nameserver. Next slide, please.

We also provide training. Domain registrant, another pillar that we focus on, so the challenges that we face, the domain registrant fear of domain name service disruption, DNSSEC implementation, they fear that if they deploy DNSSEC, they could have interruption on their domain name service, so no subject matter expert to consult related on the DNSSEC issues or queries, and low participation from government agency due ambiguity of direction.

So, how we overcame the challenges, yes, spotted from our stakeholders, the policymakers and also the MAMPU is the policymaker for government it services, the enforcement encourage for us to g et more participant onboard from the government agencies so we can brief them or we can train them on the importance of DNSSEC, we conduct awareness, and also again, technical workshop with end-to-end process using our best practice to deploy DNSSEC to prove it works.

[This is] also the most important just to get them assure and confidence they know how to implement and deploy DNSSEC without any issues and also without any risk. So to reduce human error on the DNSSEC record that the DNS administrator or technical contact required to publish to the registrar through the platform that we have

provided. So we implemented auto fetch DS record through our system. This is whereby the DNS administrator has to ensure the domain name already signed by that particular authoritative DNS server to avoid any error while the auto fetch generate or execute from our platform, meaning that when we auto fetch the DS from the authoritative server, we automatically fetch the algorithm, the key, and also the DS record. We also keep the fingerprint for that particular DS.

Okay, so this is one of the initiatives to encourage our .gov.my domain to roll out, to deploy the DNSSEC for the domain name under that particular domain registrant. Basically, we have now 1040, the total of domain name. Since we implemented last year, we do aggressive awareness and training, 500 .gov.my domain names are fully DNSSEC enabled without any errors. We keep continuing guide them, [serve them,] assist them for any related issues on DNSSEC. Next slide, please.

Pillar number four, we have reseller and partners, so basically, these are the challenges that we face. Briefly, we have about 60 resellers and partners, only these six partners support DNSSEC on their DNS hosting, on their authoritative DNS server. So among the challenges that we face are multi providers have technical skill gaps in DNSSEC, the deployment and administration.

Another challenge is half of the domain name hosted by the government appointed provider and the remaining balance by various provider. This is another [camp] we have to face whereby we have to

face with one [camp] which mainly managed for appointed by government [inaudible] government domain, then the remaining hosting provider, we have to [entertain] as well to get them participate for DNSSEC [administration.] And the last challenge is the high cost imposed by resellers to deploy DNSSEC.

Then how we overcame the challenges for our reseller and partners. Next slide, please. We do continue provide technical workshop to our resellers to close the gap about DNSSEC on how to deploy DNSSEC for the domain name under their administration.

For the government agency, we engage with single point of contact which appointed by government to deploy DNSSEC. We have close engage with this single point of contact to discuss way forward, to discuss the timeline and the strategy on how to deploy the DNSSEC for the particular domain name without any issues. Basically, we break the domain name into two group. For the domain name that managed by the hosting provider appointed by the government, we group into one critical domain and one less critical domain. So we work based on that priority of domain name group.

So by having the training and awareness, by the processes that we guide and provide to our resellers and partners, the resellers are now more confident and comfortable on DNSSEC working mechanism throughout the training, so they have now confidence because they have clear process, clear SOP on how to deploy and how to implement DNSSEC so that it's easy for them to roll out the DNSSEC for their customers' domain names. Next slide, please.

Last but not least pillar, monitoring and validation. Before that, I wish to thank DNSViz team, Verisign team for the facility to offer [inaudible] DNSSEC tool available on the net to public for benefit of using it. We do leverage on this DNSSEC tool to share with our partners, with the DNS hosting providers and also the domain registrant on how they can use the DNSViz tools and also the DNSSEC analyzer tools.

These are the challenges that we face for the monitoring and validation. They're not sure among our partners or domain registrant, they're unclear on how to validate DNSSEC the domain name that already DNSSEC signed.

So we guide them by using this tool to validate the sign zone to ensure their zone completely singed without any errors before they can submit the DS record to us. This is also due to lack of technical know-how to use the DNSSEC tool.

We overcame the challenges again. Yes, we conducted a series of trainings and awareness. Also, we provide them documentation to the DNS administrator on how to use the DNSSEC tools. There are a few scenarios. For instance, if the DNSSEC break, then how it looks like. So if the signature expire, how it looks like, and how they can monitor the entire chain of trust from root to the gov.my domain name.

In addition, we also perform to ensure the 0% break chain of trust, so zero tolerance, we perform the prechecks on zone file and full chain of trust such that before the signed zone published or propagated to the public DNS. So in the event if the system or script found any noncompliance for the particular zone, for instance the domain name,

the zone fail on zone shrinkage, the domain name not through the validation, so not able to sign, e-mail notification will be sent to us so we need to inspect and rectify the problems.

Among the prechecks that we carry out is 2FA, so we ensure that any changes of DNS most go through the 2FA. Another round of checking is domain validation. We ensure that the domain must go through 2FA. If not, we exclude that domain name to be published or propagated.

SOA check, make sure SOA check according to the policy that we set. Zone shrinkage also must follow through the policy that we set. If exceed that the percentage, we will conduct the investigation to identify the issues. And also, we conduct a test of full chain of trust before the signed zone for all categories to be published to be resolved by [inaudible].

So these are among our initiatives to the government domain name. It's not limited to government domain name. You also provide the services throughout all the domain name categories. Since the DNSSEC, we are open and the platform is ready to receive the DS from all categories domain that we offer to customers.

So actually, we continue to conduct the awareness briefing to the domain registrars in order to get more participation, to get more domain name to be DNSSEC enabled regardless of the domain name categories. Next slide, please.

That's all for my presentation, so any questions, I'm happy to help or to assist or to answer.

EBERHARD LISSE: There is one question from Dmitry.

DMITRY KOHMANYUK: Thanks [a lot for the presentation. I just have a question.] Do you feel like you're focused on any international partners, or it's mostly for the domestic communications, domestic partners, clients, registrars? I think you have a good strategy and I would actually be saying [inaudible] right now. Thanks.

MASTURA MUKHTAR: Okay. So as for now, our registrars and partners are only open to our local organization in order to be part of our resellers and partners. Yes, we have plan in the future to open up to the international registrars for .my.

EBERHARD LISSE: Interesting presentation. We also note [inaudible] .na that they will only [inaudible] and the more centralized it is, the easier direction is to give. Thank you very much, I quite appreciate this presentation.

MASTURA MUKHTAR: Yes. Thank you. With that, I end my presentation.

EBERHARD LISSE: Okay. Thank you. The next would be Davey Song who will talk to us about the DNSSEC experience from Alibaba, a very large operator.

LINJIAN (DAVEY) SONG: Thank you for all. I'm happy [inaudible] to be here to present the experience that [DNSSEC work] in Alibaba Cloud DNS team. First of all, I would like to mention that I may not be the perfect person to introduce this full experience. Before I applied to Alibaba DNS team, this work has already been done, almost done, so I just interviewed with my team, engineer team, and summarized my notes here. If you'd like to pose questions, I will try my best to answer it. And then you can send mail to me. [inaudible] come up with accurate answer to the questions.

Okay, I will provide there are three parts, who are we, DNSSEC in Alibaba Cloud, and then I'll give you some thoughts and takeaways from my point of view. Every slide, when I introduce Alibaba DNS, I first introduce where we are in the [inaudible] ecosystem. Alibaba's mission to make it easy to do business anywhere, to serve the sellers and the buyers in marketplace.

I won't go into details on each part, but I just want to mention that we are in the [inaudible] of the infrastructure. We are the foundation of Alibaba [digital] economy in Alibaba cloud.

There are two numbers of parts to Double 11 festival and we also break the record for the GMV, and we also reach a new record of transaction per second. We now have 544,000 transaction per second.

It's more than 1000 times as many as the first Double 11 in 2009, 11 years ago. I mention this because that requires the foundation of the economy to be stable, and that's the first goal of Alibaba Cloud.

We are in part of this team, as you know, some of you may know that Alibaba has [played different roles in this,] they have [registrar department and also sell the registry for TLD,] and we are cloud DNS team just provide authoritative server and for [inaudible] DNS. We also provide the operation for the cloud, the resolver part.

I need to emphasize that it's one thing to run DNS [inaudible] but it's a different thing to run DNS for large DNS companies like Alibaba. There are challenges to host DNS in huge size and scale. We saw more than 1 million users and we receive 700 million queries a day, RDNS recursive and also authoritative. So we serve 20 regions and millions of regions. That size put restrict requirement on [inaudible].

So fact background, I want to emphasize that it's very prudent to deploy new technologies, to consider HA and security issues. Most of the guys in our team are even reluctant to accept new functions if it is not [a masked, so that's the] background. Before we proceed in [inaudible].

Just a brief introduction of what we do. We do basic authoritative name resolution at our authoritative server. We provide private zone for the VPC in cloud, and we provide the health check and [failover] services and we also provide the [inaudible]. Now we are the largest DNS provider in Asia.

And I remember I presented this the last year when I gave a presentation in [OARC]and there's one update. Actually, there are two updates. One is the DNSSEC which is online this January for DNS data integrity, and then we also launched a [last man hour] public DOH and DOT in this April considering both data privacy and security.

So today, I focus on DNSSEC part. Firstly, I would like to [inaudible] some concerns and challenges on DNSSEC, especially for the large business. There are some issues on [inaudible] status and value adding to our customers.

[inaudible] department follow a long time on the status of the adoption globally. [inaudible] just today, I just checked the data. [DNSSEC,] now the penetration of the validating user were around 22% maybe, and we also, as far as I can tell, there are many people wondering why large Internet companies like Google, Facebook, Apple, Amazon is not [being singed today.]

This status presents some questions on people who are going to approach the DNSSEC. The issues we faced when we do DNSSEC. And we also identified that DNSSEC only provides authentication for data integrity, as I mentioned [inaudible] DNSSEC notify people that the data is compromised, but it cannot serve the solution. It's not a full solution against DNS hijack. That's one issue [aspect] on the DNSSEC.

Another aspect of the concerns related to how we proceed. If the large companies like Alibaba want to make a decision on DNSSEC deployment, we need to figure some issues first. First is that we need to [inaudible] DNSSEC signing at scale. Before we dive into it and work

on it, we lack experience and know-how in the beginning. And also, we need to decide how we integrate this infrastructure with the new functions so [inaudible] impact [inaudible]. And we also have concerns on the poor performance of DNSSEC signing for large, a lot of [inaudible]. it requires extra investment on the system if it is not [inaudible].

But finally, we already developed it, so that must be a trigger that we move into. So there are two reasons to deploy DNSSEC in Alibaba. The first one is from the business sense, customers asked for DNSSEC and our rivals start to deploy DNSSEC. So that's the very simple motivation from this sense.

From technical sense, I figure that DNSSEC provides a check for data integrity, it adds value to the domain and DNSSEC as an Internet authoritative directory, not only for the DNSSEC validation process or DNS function purpose but also for some offline purpose.

I will jump to the history of DNSSEC in Alibaba Cloud. Before 2017, the team just wondering and follow the discussion and read and study and follow the best practice for companies. There is a background that the awareness of DNSSEC and privacy and data integrity in China is not fully aware, so I just put that the penetration of the resolver is not as high as the resolver outside of China. So that's the background.

Just three years ago, we realized that DNSSEC feature is not optional, it's maybe a must for our services or customer may ask DNSSEC in near future. So we start [inaudible] setting up experiment and testbed and try different best practice and we also do gap analysis on Alibaba

DNS software. We have our own software. We cannot rely on any DNS [renders,] we just [do it from scratch] on our software.

And 2019, in January 2019, a notable time, date. I would like to mention that we—actually, it's not one customer but a bunch of customers start from 2019, I'm not sure what happened in that year, but [inaudible] important users ask for DNSSEC, especially for our paid version of DNS users.

So we start a serious task on the requirement analysis, we produced PRD and a schedule for DNSSEC deployment [inaudible]. The next two months, we kicked off the R&D process on DNSSEC function for the Alibaba DNS, and we also prepared product document for DNSSEC users. That's very important, [inaudible] technical function but also [inaudible] document [inaudible]. You need to receive the calls from customer, right? You need to prepare that.

January this year, full operation on Alibaba DNSSEC is online, and provide live signing for the paid version of service. And now we support the domain name including .com, .net, .cc, .tv, .name, .biz and .club. Not all the TLD, but we only enabled the DNSSEC on demand.

So when we analyze our customer, one thing surprised me, that now we have more than 1200 domains enable DNSSEC, but we expected that [inaudible] customer come from some company house at China cares about [inaudible] users also outside chine and ask the domain be signed. But we also noticed that the domestic customers are asking DNSSEC as well, which I just mentioned [inaudible] proposed to as example [inaudible] IKEA.cn is company outside China, and the

peopletech.com.cn is [inaudible] media very important media webpage that supports ask for DNSSEC. So that's a surprise, to say the least, [of the] domains.

And just very quickly to how to config DNSSEC, because they're having documents listed in the website, but I just want to mention that to the user, we only provide the DS record information and the key tag, algorithm, digest type, digest, and then DS record to domain registrar. We are not a registrar, so we provide the DNSSEC metadata to them and enable the DNSSEC.

We also provide and recommend users to use the dnsviz.net to check whether the DNSSEC is on or not so that people can be aware if the function is on or not, because not every user, customer can use [Thick.]

And one page to brief the technical overviews, as you know, we use the live signing, because we have the [execution of a lot of zones] require dynamically change the records according to where you query, and [inaudible] computation for all the [inaudible]. So live signing is a must for us. And t hen we also deploy the ECDSA, we use ECDSA P256 and SHA256. ECC has a smaller key and signature, it enables faster signing and has a better key strength, so it's stronger and the [NESC,] and a smaller size, because I have [studied] experience on the IPv6 permutation issues, so I do know that [feature] is very good, but I'm not aware—I think two years ago, one year ago, before I arrived [at] Alibaba, ECDSA is still in the situation that whether or not to deploy, but it's already workable in the production systems, so I'm very

pleased about the situation. [inaudible] more people who would like to deploy DNSSEC, you need to try ECC.

And we use NESC for negatives and we deploy global ZSK and KSK [for some parity.] We have our own Alibaba key management system for key management for the sake of the risk of compromised key.

We adopted key pre-publish for ZSK rollover to reduce the time of live signing, because that's the most resource consumption part, so we need to reduce the time.

So [inaudible] the best practice on DNSSEC [gave us some] input and we try and test on the signing part and deploying that, and until we reach the standard, it's ready for the production. So good examples are very key for—I mean, different example for different situations, because large company need the best practice for large companies and smaller size of the [inaudible] may have different best practice. So I think best practice for different level do have helpful for the DNSSEC deployment.

And there's one page I want to discuss a little bit about, the DOH and DOT. Many people have the opinion, some [inaudible] think that DOH will be a replacement of DNSSEC. In Alibaba DNS team, we deploy DOH, DOT and DNSSEC as well, and we compared the functionalities and we received different requirement from customer, and we think that they both [have some common] attacks like DNS hijack, but they are different scenarios. DOH are designed for privacy. I think all the tech people know that. But the DOH and DOT can be used to cover the

situation, cover the scenario that end users may impact by the hijack if DNSSEC is not enabled.

And we deployed DOH and DOT because we have the front end of server as the public DNS. We also have the backend server as authoritative. They can sync the data and propagate the changes swiftly. So that's the features that we provide as [a hybrid strategy] that we're doing that to enable the [inaudible] DNS resolution [inaudible] in control so that the DNSSEC actually [inaudible] but DNSSEC is also for other scenarios, other customers, so they both provide the application level of DNS and also the DNSSEC for the customers.

Okay, just a brief—we'd like to share some thoughts.

EBERHARD LISSE: Davey, can you come to a close? You're overrunning already by ten minutes.

LINJIAN (DAVEY) SONG: Okay. I'm sorry.

EBERHARD LISSE: No problem, I just wanted to mention it.

LINJIAN (DAVEY) SONG: Okay. I just have two slides. Okay, some thoughts are common in new technologies. I have a background of IPv6 transition, so I know the

story of IPv6, but a little different from IPv6 and DNSSEC, but share the common factors of successful deployment. One is the market demand and create more customer value. The second is to fit the evolution of the infrastructure technology. The system can be [scaled.] ANd also, to me, Internet governance policy enforcement.

And some experience and takeaway. I do think that good understanding of DNSSEC and your users' requirement helps. It will make the decision how your enterprise, how your company proceeds on DNSSEC.

The second one is that here are similarities between DOH and DOT and, as I mentioned the overlap scenarios for the DNS hijack, but different purpose and chosen by different customers, they add the customer values in different levels.

And I think follow and test the best practice of DNSSEC which fits your situation is very important, because there are different scales of network, different size of the system, so for different best practice, [inaudible].

And the last one experience and takeaway is that the full preparation of DNSSEC operation as a business, because you're not just using it alone, you provide services for millions, billions of users. So you need to consider the DNSSEC implementation in large scale, you need to consider the integration with your existing infrastructure, and you need full experiment and tests if you're not ready. And you need to consider the SLA and expected traffic load before you launch the

services, and also, you need to consider failover solution if anything wrong.

And for the business, help document and customer service for DNSSEC is also important. Okay, I think that's all for my slides, and thank you for your listening.

EBERHARD LISSE: Thank you very much. Very interesting presentation. A billion versus 4500 is quite the difference. Fascinating different way of doing things and what need to be done.

We are a little bit running out of time and I don't want to have the following presenters to be impacted. We can ask questions at the end anyway, and I'm giving the floor now to Dmitry Khomanyuk. Go ahead.

DMITRY KOHMANYUK: Thanks. Hello, everybody. I hope it's nice and warm and sunny in Kuala Lumpur, for those of you lucky to be there. I'm going to be talking about the history of DNSSEC implementation in Ukraine. The presentation has some extra things on it, so I'm going to just skip over the introduction.

Okay, so we have been signed from 2011, and we went to production in 2012. We had multiple zones delegated, similar to, say, South Africa, and so we had some adjustments done. So we moved registry to EPP and this was complete. We had started thinking of the optimization of DNSSEC. We had one of the first clients being Privat which is the

biggest private bank in Ukraine. They had tried to use DNSSEC [inaudible] some issues.

So we're thinking, what are the gateways to adoption? What are the things that we can do better? And in fact, the industry is kind of tepid and not enough response until 2019, the new government of Ukraine made a regulation, they mandated the use of DNSSEC to all government entities, namely those [inaudible].

And with that came a slew of requests and we started to think what can we do. We decided to rotate our keys and do the algorithm change. What happened after that, we had a test domain for DNSSEC [inaudible] and we did lots of experiments. So that's my first takeaway, never do things in production before trying it on some test environment. We have tested several algorithms and we came to the conclusion that he size of response and potential for [egress] attacks is one of the factors why you want to—algorithm rotation.

Back in 2012, there were no elliptic curve algorithms in wide deployment. I spoke to fine folks in Cloudfare and [inaudible] and of course folks in Verisign, [inaudible], and we had decided to rotate the algorithm instead of just doing a routine key rotation. So here is a brief timeline. We have created the new keys in October last year, then we started the parallel signing which magically increased the size of the zone. We basically adhered to the [inaudible] methodology so we had basically a weekly technical standby meeting, usually on Monday, and on Friday, we'd have internal taking stock meeting with my team

member Victor [inaudible] Thank you, Victor, so much for doing this with me. I would not ever do this without you.

So we had added a second DS record to IANA, and as you can see, took them three days, which actually is not that bad because considering that multiple checks and [open forums,] I'm very pleased with newest IANA streamlined performance and I know Kim Davies has been doing his work. Thank you, Kim, for that.

The ECDSA keys were not available initially when the DNSSEC, when the root zone management was added, but now it's all good. We had then basically inserted parallel KSK and we had parallel KSK, so we had made basically two signatures on each record [inaudible] and then we had rotated the ZSK. So just to put in perspective, we had the old pair, and the new pair which had a subpair, so we had five keys in the root [inaudible].

Well, that only lasted for about 24 hours. Next day, we submitted removal of the old DS record which, again, took three days for IANA. So that was basically two and a half weeks. And then four days later, after conforming to the timers and doubling all of the [inaudible] variables, we removed the old keys. After that, zone size dramatically shrunk. Shortly, in an experiment, we decided to enable full NSEC3. That means that we had signed cryptographically all delegations including those that have not been yet signed for the customers. I do believe that NSEC3 complete [inaudible] is a prudent solution for the 2020. I really wish for something like NSEC4 to be created which would allow for better performance, but those are IETF people [inaudible].

Then the next routine rotation of the ZSK came in December, then we had our new conference we done about domains. We have adopted the three year KSK rotation schedule, so that's entering date of the next rotation, give or take a month, which probably would be the same algorithm, just a key rotation. Next slide, please.

Now, I'm going to give you some graphs. As you will see, doubling the number of keys, of course, leads to—so the top left graph is about the UDP traffic. You can see the dramatic drop once the double keys were removed. I think these are Cyrillic, but you can get an idea. This is from our own anycast cluster.

The graph below shows the TCP traffic. Again, as you can see, the draft in TCP traffic is dramatic. What happens is that once you switch to elliptical curve algorithms—there's more than one now, but use one with shorter keys—the need for TCP transport decreases dramatically. I believe that it's the way that things should be with all of the DOT and other efforts notwithstanding. I still believe that UDP is similarly used for the DNS [inaudible] service for years on end. Next slide, please.

I'll show you some diagrams. Those who really want to zoom in on your session, maybe look later on the files posted. So the one on the left shows you the complete parallel setup where you have two gray boxes on the bottom which are two zone signing keys, key signing keys, and then subordinate to them are three zone signing keys.

Where, there's a fine detail here which I'm not going to discuss, but basically, strictly speaking, some of these [arrows] are wrong. That's a

limitation of the multiple algorithm visualization in DNSViz, but yet without DNSViz, I would not ever start to do this.

The middle picture is the one which already has the old key removed from the root zone. As you can see, only one arrow goes from the top box to the bottom. So that's the stage which you basically passed the switch. And the rightmost is the one that we have until now. This is a simple and sweet one.

These are dates, as you can see. Once again, it's 11/11, 11/14, 11/19. So the point is, you build the whole thing in two weeks if really [inaudible] but I would not recommend anybody doing this for the first time [inaudible] less than a month just in the technical switchover with all the communication [inaudible] and by the way, thank you, Eberhard, for your ideas of having multiple people in multiple time zones. I think it's an excellent idea. We did have a buddy in the west coast of the US, and so yeah, we had US West and Ukraine. So it was better than one. Next slide, please.

This is a bit older data, but Geoff Huston does excellent job of polling the DNSSEC and general DNS protocol deployment around the world. This data is applicable to the moment when switch was done. As you can see, the validation in Ukraine was 40%. There's three of these graphs. We're talking about the one in the middle. [inaudible]. Sorry, in the top.

So your mileage may vary. I do recommend APNIC lab resources to check that, say, for a national TLD or maybe your region, what's the state, but I think that we are now moving towards DNSSEC by default,

validation by default, and just like with IPv6, we can't ignore that any longer. Thank you. Next slide, please.

Thanks. These are some individuals that helped us in this work. They know who they are, this is more for the local crowd. Next slide, please. And I would also note, thank you, well [inaudible] very nice support from the government, the e.gov.ua is the E government agency which was their efforts were paramount to really forge us ahead in implementation of our DNSSEC operation. These are all of the second-level domains that were [inaudible] the operator and my employer is now running. So we have multiple domains. Some of them are not yet signed. Next one, please.

These are my short takeaways which I can expand to, but the first one is set small goals. Don't try to take on the world and change everything at once. Always try your own dog food, meaning that start validation in your office or corporate network, anywhere you work. And fix things that would fail. Okay, sometimes it's really bad idea to fail, but fail in the test environments. And then, ask industry experts, then become one. I would not put myself in expert shoes, but if anybody here in the ccNSO community wants to do something similar, please ask me by e-mail at dk@hostmaster.ua or dk@cctld.ua and of course, I wish we were all there in Kuala Lumpur, but I guess maybe next year. And as this says, don't panic.

I would also like to emphasize the importance of having monitoring and graphing, keeping those statistics and those numbers continuously collected before you start any transition as well as after

you've done it is crucial part of the job. Don't ever skimp on that. Also, it's a good idea to have third parties, [let's say, PCH.] By the way, they're great. Thank you, [Bill] and all the folks. And we use the 9.9.9.9 resolver as well.

Having third parties that would help you to monitor you is important. Don't forget about subscribing to TLD ops mailing list run by IANA. And I would check the Q&A, I guess, but I believe that's it. Yeah, these are our contacts. You can use the first e-mail as well, it would reach me as well as other folks in our team. So, any questions, please? I don't know how we handle that. And I'm aware of a bit of the time constraints. So let me check the Q&A window. I don't see any there.

EBERHARD LISSE: Okay. Thank you very much. Interesting presentation. I fully agree with what basically all presenters have said so far: DNSViz is important. With a little bit of skill and boredom, you can actually hack the SVG so that it produces images in color when you want to make a point.

The other thing that is very important is something that I have always found since 1991 since I've started doing this, there's always somebody on the other end of the line that you can ask. And usually, what happens is if somebody helps you, you pay it forward and that's the way this works. There is no real need to always go commercial if you have got time and energy to read the manuals. And if you [use sound] engineering practices, databases, keeping the data, reviewing the data, monitoring the data, are very helpful.

I don’t see any hands, so the next and final presenter is Joe Abley. Thank you very much, Dmitry.

DMITRY KOHMANYUK: My pleasure.

EBERHARD LISSE: Our final presenter will be Joe Abley who will talk to us about .org, but from a DNSSEC or DNS perspective.

JOE ABLEY: Thank you, Eberhard. I will not dally too much with these slides. So, .org. I'm Joe Abley, I work for Public Interest Registry—PIR—and we run .org and a few other, smaller TLDs.

This is where we are with DNSSEC, this is our abridged history. Back in June 2009, working with Afilias who are our backend registry provider and had been since 2002 or so, we signed the Org zone and we signed it with the best choice of parameters that existed at the time according to all the advice we could give. It wasn’t me. When I say we, as in the organization.

It was signed with the algorithm seven, RSASHA1 with NSEC3, which was the recommendation at the time. Then October 2009, RFC5702 was published which standardized algorithm eight, RSASHA256. June 2010, we were live, and we accepted DS records from children, from registrants via our registrars. A month after that, July 2010, the root

zone was signed and the root zone at that stage used algorithm eight, RSASHA256, and the root zone used NSEC.

So one of the considerations for choosing the parameters for the root zone was that RFC5702 had only recently been published, and one of the reasons for choosing Algorithm eight in July 2010 was to encourage update amongst validators, amongst the deployed software on the Internet that otherwise might take some time to implement Algorithm eight.

By putting it in the root zone, anybody who wanted to use the root zone trust anchor, which was at the time more or less everybody, that meant that everybody had to support algorithm eight. So that process accelerated the time or the process by which 5702 was implemented.

So the end of this timeline here, we have .org signed, algorithm seven, we have the root signed, algorithm eight, and we have substantial deployment of algorithm eight support in validators across the Internet. And that's 2010, ten years ago. Next slide, please.

So then we had a decade during which the parameters in .org were not modified. They still worked perfectly well, our backend provider has excellent uptime, we continue to try and work with other parties to get DNSSEC deployment. And also importantly for this, what happened during this ten-year period, is PIR grew to an organization of somewhere between 30 and 40 people today. And importantly for me, it also gained a technology department. So instead of being solely dependent on the excellent people at Afilias for technical decisions, suddenly we now have people at PIR, in which I include myself, who

know something about this stuff and we can make decisions for ourselves as well as allowing Afilias to make recommendations for us. Which takes us to 2020. Next slide, please.

At the beginning of this year, some of you may have heard a presentation given by Suzanne Woolf, my colleague in the technology department at PIR, at OARC 32 in San Francisco, and she announced that we're ready to do some changes and review these parameters that have not been changed for ten years in the .org zone.

She made a presentation and we had quite a lot of good feedback. We had researchers, other TLD operators, some of which are no doubt here who have experience doing these kinds of things, gave us their advice about what parameters perhaps were due for a refresh, and then in March, just as this momentum was starting to build, we closed our offices. Afilias closed their offices. Kind of everybody closed their offices and we suddenly have a global pandemic to deal with. Next slide, please.

So the kinds of things we were looking at doing this year, back when we made the presentation in the OARC meeting in San Francisco, I've summarized them here under three headings. I'm not going to go through every line.

The first one is really housekeeping. We had a very large DNSKEY RRSet, which was a combination of factors. We had some previous KSK rolls that have been completed somewhat but not completely, and the signers were still leaving old DNSKEY records in the root zone. We had some particular parameters around ZSK rolls which caused

prepublication of ZSKs that perhaps weren't useful. We had signatures by the ZSK over the [inaudible]. We had various opportunities to try and improve—by which I mean reduce—the size of the DNSKEY response. And we know that this is a concern, although we don't think it was a concern that caused everybody any actual problems, we still want to do the right thing and try and reduce the possibility of inconvenience for other people.

Then we had the fact that .org is signed with algorithm seven, as I mentioned before. Now, the reason algorithm seven is now an issue is it incorporates the hash algorithm SHA1. Without going through all the titles, this is an enormous amount of academic research that emerged in the last ten years finding new and interesting vulnerabilities, collision opportunities, weaknesses, really, in SHA1. And I think it's reasonable to say that there is an advantage to not depend on SHA1.

So we were interested in changing our algorithm to stakeholder that doesn't use SHA1. And then the last ambition we had was that Org is signed using NSEC3. And to be honest, as a technologist, I've never really liked NSEC3. I understand why it was important at the time that it was written. I don't like the fact that NSEC3 is described in 50 pages of dense RFC when NSEC is described in about a paragraph. I think it's operationally complicated, I think the number of people in the world who truly understand the nuances of NSEC3 are relatively low. I also don't think these days it does necessarily a very good job at protecting the zone walk problem, protecting the contents of the zone from people who want to [inaudible] and these days, people can get

contents of the zone anyway, particularly for gTLDs. So these are all areas that we wanted to address. Next slide, please.

The first part, we could just do that housekeeping. That's easy. That's fine. The second part, ORG is signed using algorithm seven. We could look at an algorithm roll to a new algorithm. The obvious targets we thought are algorithm eight. That's what's used in the root zone, and algorithm 13, which uses ECDSA, which results in much smaller signatures, and we think algorithm 13 is a good choice too. And lots of our early responders who offered us advice also confirmed that they thought algorithm 13 was a good target.

So we started doing some lab testing with Afilias. They actually did the testing, we were interested in asking for it to try and find out which of these things was plausible.

And then we had the last thing, which is changing from NSEC3 to NSEC for these various good reasons. That of course comes with some cost, because the nice thing about NSEC3 that we do make use of is the ability to have large opt out sections in the zone that don't require any signatures because those sections of the zone don't have any DS records, nothing to sign.

If we did NSEC, we would need an NSEC for every owner name and we would need signatures over those NSECs which means even without a ZSK roll, we're looking at an extra 20 million resource records in the zone. And there's no reason to think [that would be]a problem. We would love to have the problem of a zone even having 20 million domains in it. However, it does mean that there's a difference in scale

in terms of distributing a zone and serving it. There's a memory footprint we have to think about. There are practical considerations for this.

So we started looking at that and trying to work out what are these tradeoffs, what are the costs, and what are the operational considerations for which we could imagine doing these changes. Next slide, please.

Next question was, who should we work with to do this? So at PIR, we have the benefit of being a nonprofit, community-focused public benefit corporation. We want to work with other people. we don't want to do this quietly behind the curtain. This is not a proprietary system. We want whatever we do that's interesting to other people to be open and transparent.

So we wanted to be able to talk to other people about it. So there are some practical things here. We want to talk to validator operators and make sure that they're aware of our change, that we don't cause anybody any panic if something changes in the way that the validator works. We think there might be some research opportunities, and the roll from algorithm seven or eight to 13 has been well studied in some other TLDs. Perhaps the roll from NSEC3 to NSEC is not. Perhaps that's actually more interesting and we can encourage some people to work with us and get some academic research out of this and publish something that will inform the rest of the community.

So we started talking to people at DNS OARC about what we're doing, as one of the sort of preeminent forums for collaboration,

communication around the DNS and technical subjects. They offered to host a mailing list and we even started talking about how we might do data collection, host webinars to get people more information.

And then we ran into a couple of headaches. The first one is the signers that have been used for .org, since the zone was first signed, do an excellent job with the algorithms we've got, they're very stable, excellently maintained, patched regularly, high performance. However, they only recently acquired support for ECDSA, and it exists right now in the kind of codebase that we would run on those signers as an early sort of technology, proof of concept. It's not been optimized, in particular for large zones. And the performance impact of using algorithm 13 on those existing signers right now is significant. So that turns out to be something that's very difficult to contemplate doing.

There is another signing platform, because as in most engineering, you make sure you have a backup plan. There's another signing platform that's under development, and alongside these—the platform that we're using in .org. However, it is under development, and it's not quite ready for production, so that would add additional time to the timeline and will effectively push out the point at which we can stop using SHA1.

Linked to that, there's now no travel. People are not going to the office in Toronto, Afilias' office, not going to the office in Reston, Virginia, our office. We're not really going to datacenters. If we had to get people together to do new procedures for managing keys for HSMs, for a new

signer, that's difficult, because we don't want to put that many people in the same room. Borders are closed between the US and Canada, between the US and other places and between Canada and other places. So this doesn't seem practical either.

There's no universities. Universities are thrown into disarray. People who've been teaching in classrooms for years are suddenly not able to teach in classrooms anymore. Courses are going online and with varying degrees of success. Suddenly, it's not as simple to talk to associate professors and say, "Do you have students that could help us with this stuff or are they interested?" Because those associate professors are far too busy just keeping the university afloat.

And at the same time as all of this, suddenly everybody's working from home and apart from everyone else, using the Internet even more than they used it before, and this is a terrible time to do anything that is new or not widely tested. It's suddenly turned into critical, critical infrastructure. Next slide, please.

So that was March. And then you may have heard in April, there were various issues relating to PIR that were in front of the ICANN board, which you may imagine had other impacts on us in terms of our planning. So this was April. Next slide, please.

At the end of April, there was a resolution to those questions, and now we are planning as our own again, and now we can readdress what we're doing. So this is May. Next slide, please.

Which leads us to June, which is where we are now. So, half a year has now passed with our various calamities, global and local, and we're now asking ourselves the question, what can we do? What can we do this year? Because we still want to be able to do this stuff for all the good reasons that we wanted to do it back in February.

First one, we can do the housekeeping. We can look at the key pre-publication strategy, we can look at the signature lifetimes, the signer that we're using has a configurable internal during which it will not just do incremental signature refresh but will resign the entire zone. Perhaps we can reconfigure that. There are ZSK rollover policies we can look at. There are TTLs we can look at. We can review all the policies around this for the entire zone, and we can look at what we need to do to make changes when those changes are useful.

We can also do some performance testing and imagine a roll to algorithm eight. We think algorithm 13, for the reasons I mentioned, is going to be difficult this year, but maybe algorithm eight is a reasonable target that's perhaps easier to support. And the perhaps algorithm eight gets us away from SHA1 and achieves something tangible this year that we wanted to achieve.

So, towards that, we could test that algorithm seven to eight rollover using the current signer platform. We could do it in private, we could also do it in public perhaps. We could do a dry run in some smaller TLDs. PIR also runs some smaller TLDs like .ngo, .ong and some IDN TLDs. These are relatively small, very small compared to .org, and just because they're small doesn't mean they're not important, but it

certainly means that if we had to do communication, the scale of that communication is much lower. Next slide, please.

So, having worked out what we can do, the next stage is to try and work out what we should do. And our approach to this is to talk to other people and to see what they would like to see, see what we can do that would be of use to somebody else. And to that end, we have this mailing list where the link is on the screen. if you've ever been to DNS OARC or subscribed to a DNS OARC mailing list, it should be very familiar. The mailing list is called .org algorithm roll, and we invite anybody who has an interest in this either because they run their own TLD and they are interested in the thought process, or because they run a validator, or really they have any interest whatsoever, please join the list. We have really not yet started the conversations on there. The archives will confirm that. But we're about to. So if you were to subscribe now, you can be part of that from day one.

The next thing we could do is a feasibility study for a roll to algorithm eight. We can not necessarily say for sure that we can roll this year until we worked out whether it's feasible. Perhaps actually doing the feasibility study and discussing it in public and publishing the resulting document would be useful for other TLDs who are also looking at these kinds of transitions.

And in particular, I think it's always nice to have a situation where you take a disaster recovery scenario such as everybody has to work from home, and then you have to live it. so in a way, we have an interesting opportunity right now which is to actually make decisions and build a

study and consider the feasibility of doing these kinds of changes in a big TLD when we actually do have a global incident underway which actually puts real constraints operationally on what we could do.

And having said all that, if we can, we would still love to complete the roll. We're not trying to reduce our achievement this year to just writing a document, we want to write a document and execute based on that document. So we'd still love to do that in 2020, but of course, if we decide that it's more prudent to wait until 2021, then we'll do that. Next slide, please.

So where are we right now? So we have presented a version of this document with some changes. We've been updating it as we go. The DNS working group at RIPE at the end of May 2020, the DNS OARC meeting that was not long ago, Suzanne did that one, and then today, here at Tech Day, which I'm presenting because I'm in a better time zone today than Suzanne is to do it.

And so this is probably the last presentation we will give like this. We don't want this to be recycled forever. But we've had a good amount of feedback so far, and I think this is a useful different audience, so I would love to hear from ccTLD operators for example who would welcome the kind of guidance that we could work through in this process at PIR and perhaps using their own TLDs.

We have also done some preparatory work at Afilias. Again, when I say we, I mean Afilias, they actually did the work. And it looks very much like rolling from seven to eight is entirely feasible. Using the existing

signer platform, no one required to travel anywhere. That's being tested and we're pretty convinced that that's fine.

We've also done—Afilias have started a production roll. They're so confident in their testing that they've taken one of their small TLDs—not one of ours but one of the TLDs that Afilias manages—which uses the same signer platform, same code, and they are using that to complete a roll from seven to eight. And in fact, the TLD they're using, we have the obligatory DNSViz on the next slide, not quite yet though, is .black, and I think the snapshot I have is from Friday and I've just had a quick look today and the old DNS key algorithm seven DS key I think is being withdrawn or close to being withdrawn, or is not being used to sign, anyway. So we're getting there, which is good news.

We have about 40 people subscribed to this mailing list, and I see we just got another couple based on me mentioning on the screen. These are mainly technical audiences, but again, everybody is welcome, and I think we would like a good cross section of people who have different perspectives and hopes of what they could get out of this, because really, this is not just about PIR and .org, this is also about everybody else and what we can do to support the community. Next slide, please, for the obligatory DNSViz.

This one has not been expertly updated in the XML, but you can see here in the .black zone which is the test—well, it's in production, but it's a small, lightly used TLD that Afilias operates. You can see the algorithm seven DNS key, ZSK there, being replaced by an algorithm eight. This is the snapshot from Friday where they're both still being

used for signing. And again, if you have a look right now, you'll see that the algorithm seven ZSK is no longer being used for signing and in fact the entire path of trust now down to everything else in the .black domain is all algorithm eight.

That's it. Any questions?

EBERHARD LISSE: There is one hand from the attendants. I will open this. There is one raised hand. Mohammad, you have the floor.

MOHAMMAD ALMOUSAWI: My question is that a while ago, we had a DNSSEC workshop, and our host was forcing the port 53 to resolve from their own resolver. And their resolver didn't support DNSSEC. So even if we put in our DNS resolver to use DNSSEC to enforce using a DNSSEC resolver, but if the host is enforcing another resolver which doesn't support DNSSEC, the signed zones, we couldn't see the failed DNSSEC thing. So, how can we protect the user from hackers that hijack the port 53 redirect?

JOE ABLEY: Okay, so that is not a question about .org, but I think it's a good question. So your question really is, in this scenario where the upstream network is forcing all queries to an off-path resolver and that resolver doesn't support DNSSEC, how do you protect the end users? And the way that DNSSEC protects those end users is it

interprets that scenario as an attack, and if the end user is actually validating responses, they will not validate.

So if you sign your zones, if you sign your TLD, if you sign your second-level domains if you have them, and if you encourage your registrants to sign their zones, then what it means is their customers, their end users who are going to their webpages or trying to send mail or trying to do something else that looks up their names in the DNS from such an environment that you described, those things will not resolve because they will be interpreted as being broken.

So that is exactly what DNSSEC is designed to do. Now, two things you can do in that scenario as an end user: you can say, okay, well, I guess I'll just turn DNSSEC off, which is equivalent to clicking “okay” when your browser gives you a certificate error. Or you can say, “Okay, I'll connect through a different network.” And I think the pragmatic choice then is up o the end user, but the end user is at least aware that DNS path is not as it’s supposed to be, and the answers they're getting are in some sense insecure.

EBERHARD LISSE: Thank you very much. I will give the floor to Jacques for the usual closing. My take home of this presentation, no matter what the scale was, you need to have an engineering plan, you need to consult widely before you write it, while you write it and after you’ve written it. You need to test it on a smaller subdomain level, and DNSViz is your friend. Interesting to see that this happens no matter what the size of the domain is.

All right, Jacques.

JACQUES LATOUR: Okay, so I'll do these quickly, those are the closing remarks for this session. I'll just go through each presentation and give a quick overview.

Roy presented on .zz. It seems like a reasonable approach and solution to have a TLD for private traffic and private use. But there's a lot of discussion ongoing on the IETF mailing list with this.

Jannet gave a good presentation on DNSSEC for Bolivia. I believe she's trying to literally put Bolivia on the DNSSEC map. It's the last dot in South America, I think, that needs to be populated. So good luck in getting there. Key message is if you have any questions, there's a lot of people in the community to help you get .bo signed.

Eberhard did a good presentation. it's very important to note it was version 1.71 that you presented, so that goes on the record. And I think if it works for you, it's a good approach to move your signing with PCH. As far as I know, they would have a more robust infrastructure than the one you had. So I think it's a more resilient infrastructure for you, and a good job on doing the migration.

There was a presentation from the host, .my from Mastura. It was all about the plan to adopt and implement DNSSEC in the e-government services. Davey did a good presentation on the deployment of DNSSEC at Alibaba. The scope of the infrastructure is pretty impressive, it's

very large. There's certainly a lot of issues to address when you're doing DNSSEC at a scale like this.

There was one statement Davey made that I really liked, is DNSSEC provides the I in CIA, so for security, confidentiality, integrity, availability, DNSSEC is the I. So that's something I'm going to use forward.

Dmitry did a presentation on the timelines for doing an algorithm change with .ua in Ukraine. So that was a good presentation.

And finally, Joe talked about good presentation on getting DNSSEC rejigged, to look at how DNSSEC is done and building a plan, collecting feedback and building a go forward plan to have a next generation of DNSSEC with .org.

So those are the highlights for today.

EBERHARD LISSE: Thank you very much. We checked this, at the maximum time, we had 116 attendants, which I found is quite nice. As you can see on the screen, it's the agenda. everything in blue is a link, so if you wanted to e-mail the presenter, just click the link, it goes to their current e-mail addresses. And I have neglected to specifically thank James Mitchell from PCH for working with us on this. Even though the time zone was quite different, it was very helpful and I forgot to mention this during my presentation.

So now we can stop the recording. Thank you very much, everybody, and have a nice day or a nice evening or a nice morning wherever you are.

[END OF TRANSCRIPTION]