ICANN75 | AGM – DNSSEC and Security Workshop (3 of 3)
Wednesday, September 21, 2022 – 16:30 to 17:30 KUL

KATHY SCHNITT: Thank you. Hello, and welcome to the DNSSEC and Security Workshop, our final session of the day, part three of three. My name is Kathy, and I'm joined by my colleague Danielle, and we are the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. If you'd like to ask questions during this session, please just type them in the Q&A pod or raise your hand in Zoom and we'll take questions during the time set by the moderator. You may access all available features for the session in the Zoom toolbar.

With that, I'm happy to turn the floor over to Kim Davies.

KIM DAVIES: Thank you. Hi everyone. I'm here to give you a bit of an update on all things DNSSEC when it comes to its own operations. Next slide please.

First thing I wanted to talk to you about is just our quarterly ceremonies. For those not familiar, in terms of managing the trust anchor for the DNS, the root zone KSK, the way that we conduct that work is that we hold transparent public key-signing

ceremonies, typically every three months. These are participated in by not only our personnel, but by community members who oversee the work, and where possible, external parties as well, to witness the work that's going on. Today they're now being conducted back that their regular three-monthly cadence. The reason why this is noteworthy is that for a couple of years they were not.

One of the mitigations for COVID-19 that we had in place was to minimize exposure, and to do that we took a few interventions. One was to reduce the frequency of the key ceremonies. We were doing them every nine months for a while. We also limited community participation. We basically sent a skeleton screw to the key-signing ceremonies. I think it was seven people. That was the absolute minimum we could have in person to exercise all the security controls. We mitigated that by ensuring that there was adequate public participation remotely, and we did it in such a way that our trusted community representatives were satisfied that no controls were being breached and that they had sufficient visibility into the process, that they could satisfy themselves that key ceremonies were being conducted appropriately and without compromise.

That too has resumed, so now we have our trusted community representatives in person. That's a great development. The one thing that we have not returned back to normal operations is

external witnesses and media. That's another secondary but important part of how we conduct the ceremonies. We want to build confidence in the system beyond having those trusted community representatives that are very familiar with the processes be satisfied. We also get value from having new people involved that otherwise are not familiar with them. We tried pre-COVID to allow— Any seats that we had free in the room were available to anyone that might want to observe from the general community, first-come first-served, and also media.

We've had a number of news outlets film in ceremonies. We've had documentaries made, we've had news reports and the like. We've had requests of that nature in that last year, but we've been declining them unfortunately, because we felt that having camera crews and so forth in the ceremony would be a risk. We continue to reassess that. We speak with ICANN's Security Operations Team as we plan each ceremony, and they make an assessment. Hopefully soon the risk will mitigate to a level where we can resume that public participation as well. Next slide please.

In terms of the trusted community representatives themselves, as a reminder, there are 21 TCRs, as we call them, divided into three groups of seven. Each group of seven performs a slightly different role. I think I gave a presentation to this group last year about Daniel Kaminsky, who passed away last year, and the efforts we took to retrieve his credential. Last I updated you we'd restored

it, but we were waiting for, again, our ability to resume in-person ceremonies to assign it to a new TCR. I can report to you now it's gone to Dave Lawrence as a Recovery Key Shareholder. That has been restored, but that's not all.

We started signing the root zone in 2010 and that's when the first class of TCRs were installed. Many of the TCRs have been serving ever since. There have been a few changes over the years, but many of the TCRs today still have been serving since 2010. A number of them have reached out to us and said, "Look, I've been doing this for a decade. Perhaps it's time to pass the torch on." We've been going through a process of identifying replacements. We're keen to not do it all at once, so we're staggering the changes over ceremonies where we can. Expect to see some changes to the composition of the TCRs in the coming years. I say years because, again, we stagger it over ceremonies every three months, but when you have 21 it takes some time.

I guess a plea here is we're always looking for new candidates. I will say frankly we're looking for candidates that would not be in this room because one of the aspects of the way we try to select TCRs is to try and get a diversity of opinion and a diversity of perspective. There's definitely a role for DNSSEC experts, people that track this closely, but there's also a role for more general security experts, or others that can bring that alternative perspective, that aren't necessarily as familiar with what we do as

I'm sure everyone here that's following along is. It can be a challenge to raise awareness of this opportunity, and I'd encourage anyone here that might know of someone perhaps further afield that might be a good fit to apply. To be clear, I'm not dissuading anyone here to apply. Everyone is very welcome to apply as well, but when we go through our selection process what we're doing when we have a vacancy is we look at the complete set of seven, or six if there's a vacancy, and we look at the mix of skills, the mix of diversity, the mix of geographic locations. We try to identify based on all the statements of interest that we have who from this pool would best add diversity to the group, add new perspective and so forth. That's our approach to selecting new TCRs. Next slide please.

We started signing the root zone in 2010, as I mentioned. The first KSK rollover, replacing the root zone KSK, was in October 2018. There's a general commitment that after five years the KSK gets rolled. Whether after means at the five-year anniversary, or just sometime after I guess is in the eye of the beholder. Our rough target is every five years or so to periodically roll the KSK. We're coming up on five years soon. Last time we rolled it over, in 2018, obviously that was the first time, there was a lot of experience gained in that process. Part of it is originally it was scheduled for 2017 and there was a full year delay studying some telemetry and inputs that gave pause, but ultimately we were able to

successfully proceed. At the end of that project, we performed a public consultation process with our thoughts and gained feedback from the community on how to conduct future rollovers. I have the link on the slides. There was some really good feedback there for us to take into consideration, but I think the net takeaway from our experience and from the consultation is a general recognition that it went well and subsequent rollovers should be roughly modeled on the same approach we took in 2018.

That's where we're at. Our original plans called for, in 2020, for us to actually start the process again, knowing that it does take a couple of years to get everything going, to generate the key, to propagate the key, et cetera, et cetera, et cetera. Again, COVID struck. We felt that we could not reliably conduct operations when we couldn't have people come to the ceremonies, so we effectively paused that effort, at least for the foreseeable future, but now we're in a good place. We have a level of certainty where we think key ceremonies are almost back to normal, and so therefore it's prudent for us to resume that work. Indeed, that is what we're doing.

Our cryptographic team is looking at this. We'll be working with our partners at VeriSign who manage the root one ZSK and discussing our plans. My expectation is in the coming months we'll get a handle on this and start communicating more broadly.

Without committing, my expectation is sometime next year we'll probably be in a good place to have the generation event where the next KSK is generated, which is one of the first steps of a multi-step, multi-year process. Next slide please.

That leads us to algorithm rollover. This is a rollover of the key, but also to a new algorithm. We've committed to performing the necessary research into how to make this work reliably, effectively. The root zone, for those that are unaware, signed with RSA/SHA-256. There are a number of alternate algorithms to select from, notably elliptic-curve-based algorithms. It's never happened in production and certainly it introduces new considerations that wouldn't be in place if you were just rolling within the same algorithm. We believe the first step here is to study the issue, and to that end we're developing a project around that. To be very clear, this next KSK rollover I talked about on the previous slide would not be an algorithm rollover. We do not have any belief that this work would be conducted in such a timeframe that we could perform an algorithm rollover at the next rollover, but this work will happen in parallel.

Again, modeling it off something that seemed to work quite well, if we go back to, I don't know, I'm testing my memory, some years ago, 2015, something like that, ICANN convened a design team that came up with a set of criteria for KSK rollovers. We think we'll convene a team in much the same way, this time concerned with

algorithm rollovers. I'd expect that we will be soliciting volunteers in the coming months from the community, and we'd encourage anyone interested or who feels that they have relevant expertise to apply for that. We'd very much appreciate the support as we explore this issue and I'd expect that work would ultimately turn to test beds and the like. I expect that it's not just going to be community volunteers doing this work. We'll have contract support, and we have a number of people in OCTO, ICANN's Office of the CTO, to back us up on that project.

The kickoff for this project specifically, I think I'll get to it in a few slides, will be an event we're holding in November. I'd encourage anyone to attend that event, but certainly that's not essential. Much of the engagement consultation on this will be happening online at subsequent meetings. I'm sure when ICANN76 rolls around and we're having this workshop we'll have a lot more to talk about then. Next slide please.

I mentioned in passing, I think, that during the last ICANN meeting, in this workshop, that no one had asked for interest in CDS support in the root zone, but a few people stuck up their hand and said, "I'm interested. I'm interested." We took that as a minor signal that we should start thinking about it more. To be clear, it's something I thought about, we thought about five, 10 years ago, quite some time ago, and it just sat there as a nice to have, but with some confirmed actual interest from actual

customers that changes the dynamic just a little bit. I think for us and without going to far into the non-DNSSEC stuff that we do, and we did have a more detailed presentation about this earlier in the week, we are looking at the concept of proactive monitoring of delegations more broadly. It would just be monitoring for different signals about TLD health. This could be a component of that, so long as we're continually probing and monitoring TLDs, looking for the signals associated with that could be part of that work.

To be clear, the Root Zone Update Study, which was published last month, which was commissioned by a third-party researcher, had also recommended we institute this kind of health check concept. Not CDS specifically but monitoring of TLD delegations. As our thinking on this matures, I'm sure we'll engage more on this topic. Next slide please. That was backwards. There we go. I think this might be my last slide.

The specific event I was talking about, ICANN announced recently that it's holding its first ICANN DNS Symposium since COVID. This is a two-day technical event run by OCTO and we're hitching a ride on that. There will be a third day that will be focused on IANA topics, provisionally called the IANA Community Day. We're expecting to touch on two key topics. There might be others, but the two key ones are Tech Check Evolution, this is evolving the kinds of health checks we do on TLDs, and also the algorithm

rollover. Again, if you're there, and I'll note the timing has been deliberately selected and the location as well to be conveniently close to the next IETF meeting, so if you're going to IETF you'll have the weekend to transit from London to Brussels and then the IDS is the following week. Again, if you're not there that's fine, too. There'll be plenty of opportunity to be involved in these things in other ways.

I think that is it. Thoughts on any of this stuff are welcome at any time, including now. Other than that, thank you.

KATHY SCHNITT: Anyone have any questions? Warren, go ahead.

WARREN KUMARI: I'm a little surprised that I'm asking this, but if the key-roll stuff, the TCR ceremony was working fine every nine months, is there a reason for us to do it every three months? Should it instead be six months or nine months?

KIM DAVIES: It's a good question. I think inherent in doing them further spaced apart, it introduces new risks that there's more signed materials that is pre-generated, that it's a longer period of time for our facilities to be out of action. That was of particular concern for us because we alternate facility to facility. In normal operation we're

actually only exercising our equipment every six months, and if it was every nine months times two it would be every 18 months. Going 18 months between turning on equipment, greater risk that it won't turn on. I think those are just a couple of factors. I'm sure there are others. I think that's the key thing that reins it in, you want to exercise the process more often rather than less, and choosing a sweet spot between those two alternatives.

KATHY SCHNITT: Thank you, Kim. We actually have no further question.

KIM DAVIES: Thank you.

KATHY SCHNITT: With that, next up we have Adiel and KINDNS.

ADIEL AKPLOGAN: Thank you.

KATHY SCHNITT: I'll bring up the slides for you. One moment.

ADIEL AKPLOGAN: Yes, thanks. Thank you very much, Kathy. This is going to be the presentation on KINDNS, this new initiative that we have launched. You may have already seen this presentation either earlier this week or last time we presented it at the SSAC meeting. I will quickly go through this and answer the questions that you may have on this.

KINDNS is an initiative to promote DNS operational best practices. It's not specific to DNSSEC only, but DNSSEC is one of the practices that we are encouraging operators to implement when they are authoritative and validate when they are recursive or operators, for instance. This forum is appropriate to talk a little bit about this. Next slide please.

KINDNS, just to put it straight, is something like MANRS, but for the DNS. As you know, my team is heavily involved in capacity building and technical engagement with DNS operators around the world. Some of the feedback we generally get from people after our sessions is to have a brief, simple and straightforward guideline or referral point to go to, to know exactly what to do and build their design around. It makes sense, knowing how the DNS can be complex and how not everyone has an operation that has resources to follow everything that is going on all over. The idea was to build something simple that everybody can implement. I would say the 20 percent that allows to have 80 percent security in INS operations. Next slide please.

We named it KINDNS for knowledge sharing and instantiating norms for DNS and naming security. I was talking about MANRS. We tried to have something fancy as well that can play nicely with MANRS. Here we're talking about "KINDNS". Next slide.

The work that we tried to do was twofold. The first one was to actually scan and identify best practices around the DNS in general, try to categorize them per type of DNS component operated. Second is to be able to streamline those best practices into something shorter. We gave ourselves a goal to not have more than 10 practices per category of operators in general. Again, to be able to point people directly to those practices and go into them. The way we present those practices in the KINDNS framework is not very invasive to the way people operate. It's touched at the high level of what is expected. We do not tell people how to implement those practices in their different environments. If we stick to DNSSEC for instance, we say, "You have to sign your zone as a TLD operator, or even a second level domain owner, but how you do it is up to you." What we want is for people to say, "Yes, I think signing, having DNSSEC deploy is a good thing. I'm doing it for my domain name," or, "I'm planning to do it in my environment, and these are the things that I have in place to ensure that."

Those practices have been in first draft, shared with the community through the mailing list and the Wiki page that we

have maintained throughout that phase of putting the framework together. Got some feedback, adjusting as we go. The launch that happened last week is the launch of the portal that will group all those practices as we have defined them. As I said, it is the beginning of the journey, in fact, because now we have the practices. We can promote them, but also more actively, we can also engage the community around them to either refine them, evolve them as the DNS operation and practice also evolves globally. The call for action mainly for operators here is to assess themselves against those practices and see if they adhere to the practices and commit to join KINDNS as a supporter of the practices, of the fact that those practices indeed help secure DNS operations in general and support the global effort.

We have identified for DNS operations five categories, two for authoritative server operators, so TLD and critical zone operators, and second for the second level domain operators or owners in general. For the resolver category we have three. The first is for the closed, private resolver that we see generally in corporate environments. Then you have shared private, which are ISPs, all the DNS operators that are customer based, and then we have the public resolvers, that new category that is becoming more and more prevalent.

Another thing that we realized when identifying those practices is that we cannot talk only about DNS core operations if we don't

also highlight and drag operators' attention to the importance of having their core security. As an underlining category for all those five we have a category for hardening the core, which applies to all of the other categories. When we're enrolling people into KINDNS and we are getting operators to join KINDNS they are not really assessed on hardening the core particularly, but it is something that we raise their attention on. Next slide please.

The following slide will give a highlight on the different categories and the practices that were identified for each of them. If I take this example, it's for the authoritative and critical zones. You have seven practices here. The first is to have your zone signed, as I said, straightforward. Make sure that the transfers between your authoritative servers are limited. Control. You know who has access to transferring the zone. You have a mechanism in place to ensure the integrity of your zone file or your zone database. Your authoritative server and your recursive should not be running on the same infrastructure, to have a proper separation of function. You need to have at least to distinct nameservers to ensure a failsafe in case one server fails. When implementing those two, three or more servers you need to ensure that there is diversity in the ways they are operated and diversity in terms of networks. They shouldn't be on the same networks. Geographically they shouldn't be normally at the same geographical location, and if possible, you need to have software diversity. At least one or two

of those diversity practices should be taken into consideration when designing your authoritative servers in general and distributing them. Last, of course, monitoring your infrastructure in general to be able to react in a timely manner in case of an incident or anything.

As you can see, these are very high level, simple practices. Nothing very complex if you run DNS. We're calling those operators to look at those and implement them. Next slide.

Same thing here. We have seven, with probably less emphasis on the diversity, for instance, because in most cases second level operators don't have full control of how their DNS is housed, but the other feedback we have gotten as well is that this can be used as well for people who are hosting their second level domains to have a more meaningful discussion on technical best practices with their hosting company so that they know what exactly they are providing them and if that matches a certain level of security. Next.

Next, we have the same thing for the closed, private resolver operators. Of course, we want them to have validation turned on. We want them to have ACLs or any means of filtering to be in place to restrict who may have access to their resolution service. This is specifically when you have a close, private resolver you need to have that in place. We have added, and that is also some feedback

on the mailing list, some consideration for privacy. We have added the need to have QNAME minimization when especially you have a closed, private resolver. That's a very real event in that case. It may not be very important when you are running fully open, but for this one specifically it's something that we have there. You need to have your authoritative and recursive supported again here. It's valid in this case as well. At least two distinct servers as resolvers. You can have more than that. Separating the authoritative server— I think there's a glitch there. This is about the authoritative server, but what's it's about, it's again about the diversification of where your different resolvers are located, and of course, monitoring, again. Next slide.

For the shared private resolver, we have the same set of recommendations or suggestions for them as well. Let's get the next slide.

This is for private resolver operators, for instance, and again, for the privacy consideration you see that DOH and DOT is listed here as something that with a public resolver operator must have or should look into when providing service to their customers. Again, this is linked to privacy considerations here. Next slide.

For the core hardening we have a set of practices here that are our usual security basics when you are running services. Filtering what reaches your network, implementing [inaudible] aids, so

implementing or adopting MANRS practice as well. Again, the complementary effect of this with MANRS shown here. The configuration of your DNS services must be locked down. You need to have a proper tap on them. Basically, classic, basic security practices when you are running a system, what is here. Of course, you can do much more than this, but at least these are important as a complementary element to the core DNS best practices. Next slide.

We have launched the website last week on kindns.org. It has all these practices, plus the rationale behind each of them, why they are important. It has guidelines of how to implement those practices, using examples of some of the DNS operations software, but it also has a self-assessment survey with operators can use to see where they stand against KINDNS practices in general. The survey is self-explanatory. At the end you have a result that gives you approximately a score, but it also allows you to download the report. The report, where it is interesting is where you don't have the full score in the self-assessment it gives you guidelines on how to improve those practices. In the report you have your score, but you also have guidelines on where your scores are low. It's a way of also helping operators or encouraging them to look at what they should do to improve their practice. Next slide please.

As I mentioned, the goal here is to get more operators to work within this KINDNS framework. We are going to launch an enrollment form in the coming days. Right now, we are doing it manually. The difference between the self-assessment and the enrollment is that in the enrollment form the operator will be required to provide a little bit more information about how they're implementing the practice, but also, if they are not implementing a practice that doesn't mean they are not qualified. All those practices try to mitigate specific risks of running the DNS. If an operator is not implementing something specifically, he has the possibility of saying, "Yes, I'm not doing this, but I understand the risk, and this is how we are mitigating the risk." In the enrollment form the operator may have the opportunity to explain that. That doesn't mean he's disqualified to join KINDNS, but he knows what he is doing, and he has something in place to mitigate the risk. We want to engage and bring as many operators onboard to this to support, and also to show that these are practices that can be easily implemented and critical for the overall security of the internet in general. Next slide please.

That's it. Sharing some early, I will say, observations that we have been able to collect in the week since we have launched the self-assessment, so far we have had around 250, up to today, people who took the self-assessment, which is encouraging for us. Some

of the data that we have collected also show what we know already about how the DNS landscape looks. The self-assessment was taken mostly by people who have a second level domain. They represent 61 percent of people who took the survey. Something, also, that we know from those who took the survey, only 51 percent of them have DNSSEC activated for SLD operators. For the TLD we have a higher level of DNSSEC [inaudible]. We also see that the majority of people who took the survey are people who are running private recursive resolvers, for instance. The vast majority are from that category, followed by public resolvers.

What is interesting here is that from those who are running public recursing resolvers, the majority of them actually have validation activated, which is something good. They have proper control over access to their server. This is specifically for private recursive resolver operators, and so on. We have this backend dashboard as well, which gives us insight as well on what people are saying, and this kind of insight can also help us tailor our engagement and know exactly where the weakest links are and where we can focus our capacity building program more effectively. Next slide please.

That's it. We really encourage the community not only to join KINDNS, but also to keep informed about its evolution. The mailing list is still active and open. We are not going to continue

to maintain the Wiki page, though, because most of the things are moved onto the website, but the mailing list will continue to be the conduit through which we will continue to engage the community in general. For any other direct information, you can reach the team at info@kindns.org and we'll be happy to engage on it.

That's it. Thank you very much.

KATHY SCHNITT: Anyone have any questions? Lars, go ahead.

WERNER STAUB: Is it welcome if on some of our webpages where domains can be looked up, such as what used to be the WHOIS lookup on registrars or others, if we link this tool from a given domain, or is this not welcome?

ADIEL AKPLOGAN: Sure. You mean for people to self-assess themselves using kindns.org and look at the practice?

WERNER STAUB: Essentially, yes. It would be promoting it, because in the context of a specific domain we would suggest, "Go here," but as it would be a public page it wouldn't guarantee that the people going

there would be the actual owners of the domain. It would be just whoever saw it.

ADIEL AKPLOGAN: Yes, sure. We haven't limited any users of this, and actually our goal is to publicize this as much as possible, those practices as much as possible, working with anyone who wants to contribute. That is helping to spread the word. Yes, sure.

KATHY SCHNITT: Liman?

LARS JOHAN-LIMAN: Thank you, Adiel. Now I've got a better picture of this thing. I have two concerns, though. I went to the webpage and downloaded the guidelines for, in my case infrastructure zones, and it seems that there's a conflation between different roles here. We have the role of generating the DNS data, the zone file, and we have the role of operating the server that provides the DNS service to the internet. There's a mixture of these in these recommendations. For instance, DNSSEC must be enabled. Fine, that's the zone administrator's role. Zone transfer must be limited. That's the operator's role. You can't really have the same entity fulfill all the recommendations in the set, which makes it impossible for me, for instance, as a root nameserver, to say I support this, because

there are things that are out of my control, that I cannot vouch for.

ADIEL AKPLOGAN: Yes. We have had that internal discussion about some of those things, but we think that if you are the owner of a name, for instance, if you are not even doing it, you have a certain level of control of who is doing it for you.

LARS JOHAN-LIMAN: That is probably true for many zones, but not for all. My second concern is, is there more documentation than the downloadable thing? There are lots of recommendations in there, but there is precious little explanation as to why they should be put in place. For instance, it says some transfers must be limited. Why is that? That's actually an honest question?

ADIEL AKPLOGAN: If you look at the website, when the practice is there, if you click on the plus button, you will see the rationale. The rationale is there. It is not a lengthy rationale, but there is a rationale on each practice. If you go into the implementation guide there is even more information there, but we got that feedback as well, that not everybody is [inaudible], so maybe we should go a little bit

deeper, adding illustrations and helping people. We will try, but right now if you click on the plus button, you will see the rationale.

LARS JOHAN-LIMAN: I understand. Thank you very much.

ADIEL AKPLOGAN: Actually, even, we have a report which is published on the Wiki that explains how we got to those practices and the rationale as well, more detail on the rationale.

LARS JOHAN-LIMAN: Very good. Thank you.

KATHY SCHNITT: We have no further questions. Adiel, thank you. With that we actually conclude the DNSSEC and Security Workshop for ICANN75. Thank you all for joining. You may stop the recording.

UNIDENTIFIED FEMALE: Recording stopped.

UNIDENTIFIED MALE: Thank you.

**[END OF TRANSCRIPTION]**