JOHANNESBURG – GAC Session on the KSK Rollover
Thursday, June 29, 2017 – 12:00 to 12:30 JNB
ICANN59 | Johannesburg, South Africa

CHAIR SCHNEIDER: So we have one more before the lunch break, which is about the KSK rollover. Important piece of information that ICANN wanted to share with us, and we have David Conrad here who will introduce himself in a few seconds and tell us why he's here.

UNKNOWN SPEAKER: (Off microphone).

CHAIR SCHNEIDER: Yeah, yeah, just take any seat, or you can also come here to the middle, David.

DAVID CONRAD: Hello, everyone, I'm David Conrad, ICANN CTO, and I'm here to talk to you about the key signing key rollover that we are in the process of undertaking right now. The key signing key is the key that we use in DNSSEC to sign something called the zone signing key. The zone signing key is then in turn used to actually sign the root zone. This is how DNSSEC is implemented. And in 2010, when we signed the root for the very first time, we told the community that after five years we would change the key, and that is known as rolling the key. And it's now 2017 and we're in the process of actually doing that change. So as soon as Adobe cooperates, I'll have a few slides to show you.

This talk is intended to be at a high level so you understand. We have provided a letter to regulators across I think 180 countries and CC'd the GAC representatives for those countries where appropriate. And in that letter we intended to just alert the regulators that the key roll is coming and that they should inquire within their network operators if they're prepared for that change.

So providing an overview. So the root zone DNSSEC key signing key is the topmost cryptographic key that's used to secure the data within the DNS. It's comprised of a public part and a private part. The private part is kept in what are known as key management facilities. There's two of them. One on the East Coast of the U.S. and the second on the West Coast of the U.S

They were established back in 2009 when we are under a contract to the U.S. Department of Commerce. Within these facilities there are -- is a -- a fairly high level of security. There's a secure room. Inside the secure room, there's a secure cage. Inside the secure cage, there is a safe. And inside the safe is what are known as hardware security modules. These are specialized devices that hold the cryptographic information. So the private key for the root zone is kept within this -- this HSM, inside the safe, inside the cage, inside the secure room, inside co-location facilities that have access control.

The public part of this private/public key pair is actually copied into every DNS resolver that does DNSSEC validation on the planet. We estimate they're on the order of probably 100 million resolvers on the planet, of which only a small percentage actually do DNSSEC validation. But we're still talking on the order of millions of resolvers that have this configuration information within them. The key roll is -- sorry, the key is used in DNSSEC to build a chain of trust from the root of the DNS down to the very -- the end node, the leaf of the tree that's actually being looked up, and it ensures that data that's been DNSSEC signed by the zone owner, it won't -- cannot be modified in flight to allow for things like man in the middle attacks and phishing and that sort of stuff. Next slide, please.

So why are we rolling the key? Well, common best security practice is that if you have a password you want to change it every now and then to prevent situations in which your password has been compromised without your knowledge and to ensure that the infrastructure necessary to change the password actually works in the event that you're forced to change the password for some unexplained reason.

The same is true with DNSSEC. You can think of the -- the key signing key as a password for DNSSEC and as a result, we need to make sure that the infrastructure that exists to change the key actually does work, if we were ever put in a position where we need to change the key. We would, you know, potentially need to change the key if there was some breakthrough technology that allows factorization of, you know, cryptographic information or we had an indication that the -- the key had been compromised in some -- in some way. The problem is that given the number of devices out there that we're going to have to update, we have to do this very carefully, very slowly. We -- and also we'd prefer not to break the Internet while we're doing this. The problem is that if we make a mistake during the key roll, it means that the resolvers, the machines, the servers that end users query to look up any name on the Internet, would sort of spontaneously stop working for any zone that's signed and since the root zone is signed, that sort of means that it would be a really bad day for anyone on the Internet. So we'd prefer not to do that. So we're taking a very careful and deliberate approach, with as much testing as we can do, to ensure that there's no significant risk in causing a problem with DNSSEC validation across the Internet. So it's actually basically a two-and-a-half-year process. Next slide, please.

There we go. And these are some of the significant dates that have occurred for the key roll, or will occur in the future. On the 19th of September, the size of the key was increased because we actually had to insert the new key into the DNS for its use in the subsequent what are called key ceremonies. The key ceremony is when we take -- we go into these secure facilities, take the private key and sign the zone signing key from VeriSign to use to sign the root zone. We do that every quarter. And that means that for all of these activities, it's basically clocked on these quarter key management -- key ceremonies that we do. So the last one in September -- or in September 27 -- 19 of September in 2017, the size of the DNSkey will get bigger, since we're adding a new key. In October 11 of this year, we will be using that key for the first time.

And that's sort of the most likely date where something odd could occur and where odd is that people who have not changed their key by 11th of October in the resolvers, they will be unable to validate. Any domain name lookup that they do will result in "host not found" or a 404 error, that sort of thing.

January 11th we actually take the old key and set a bit on it that says it's no longer to be used. On 22 March we actually pull the old key out of the root zone. And then in August of 2018, we actually destroy that old key just to be very sure everything is being kept secure.

Next slide.

Who's going to be impacted by this? Well, DNS software developers and distributors need to have the new key put into their software and their distributions. System integrators, people who take the software and deploy it need to make sure that they have the latest key within the systems that they're integrating. Network operators are typically the folks who run the resolvers. And they need to make sure that their systems can support this change of key.

The root server operators need to be aware, and we have been in close contact with them because they're the ones who are going to most likely see problems if the people don't change the key. What generally will happen is a resolver will try multiple times to get -- to resolve something if the DNSSEC validation fails. So they'll see an uptick in the amount of traffic.

Internet service providers are the folks who are almost likely -- almost certainly going to get the phone calls. If there's some sort of problem if the network operators do not update their -- the key, the ISPs are the ones that will start getting the calls.

And end users would be impacted if the network operator doesn't update the key because all of a sudden they won't be able to get to any site on the Internet.

Next slide, please.

So obviously we need to do a lot of preparation. We've been asking network operators to see if they've enabled DNSSEC validation. If they have, they need to make sure that they are able to update that key. Historically, resolvers were sort of started running, you never had to think about it again, and people would deploy it on read-only file systems which would be sort of a problem if you tried to change the key because you wouldn't be able to write to the disk.

Next slide.

So what do resolver operators need to do? They need to be aware whether the DNSSEC is enabled. They need to make sure that they understand how the trust is evaluated across their systems. They need to test and verify that their resolver is able to handle a change in the key, inspect the configuration files, make sure things are getting written to the right place. And if DNSSEC validation is enabled or planned within the network, then have a plan for participating in the key rollover. For example, watch behaviors on October 11th and know how things will likely fail. Typically a resolver that has not updated its key will start responding with servfail to -- indication of server failure, any time someone issues a query for a name that's been secured.

Next slide, please.

That's unfortunate. The little blue box there is actually an image of the letter that we sent out. But as I mentioned, we did send out a letter to regulators within the countries and GAC representatives basically suggesting that they talk with their network operators to make sure they're aware of the key rollover. Next slide.

And that's pretty much it. I'm happy to take any questions and happy to provide any information that I can to help you in discussing this with your network operators. Again, I'm David Conrad, david.conrad@icann.org. Thank you for the time to be able to present this.

CHAIR SCHNEIDER: Thank you, David. Well, I think my first question would be: Is there an analog telephone line number that you can offer in case of breakdown of the whole Internet where we can seek for help? And will that be operated 24/7?

The U.S. has a question or comment.

DAVID CONRAD: To answer that question, yes, the ICANN global support center does have knowledge about this and we have those numbers posted in various places.

UNITED STATES: Thank you, David. That was a very helpful presentation. This is an issue near and dear to my heart because I'm a nerd at heart, I believe. But we did receive the letter from Goran. Thank you very much. And I'll be honest with you, my initial reaction was we need to work with our ISPs. As a government, we typically rely on our resolutions -- our resolution with commercial ISPs.

But in terms of providing guidance for us, is there anything that we need to do as governments to make sure that our -- in addition to just making sure ISPs are doing what they need to do, is there anything that you recommend that we do internally to make sure that our operations continue? Thank you.

DAVID CONRAD: Yeah. Within any network, be it the government internal network or an ISP's network, there needs to be a resolver someplace. It might be external. For example, Google provides their public DNS service 8.8.8.8. And a lot of folks use that service.

All of those, you need to make sure that they are able to handle the key rollover.

Google is definitely able to handle the key rollover, so I'm told. I have no doubt -- I do not doubt that whatsoever.

But for other ISPs, other network operations, particularly enterprise-level network operations, it's good to just -- just ask to see if they're aware that the key is going to change. And if they are -- well, they should first check to see if DNSSEC is enabled and encourage DNSSEC to be enabled, if possible. But then if it is enabled, then check to see if they are aware the key is going to change. And if they aren't, suggest that they participate in the key rollover efforts that ICANN has been publicizing.

What we're doing here mirrors what we've been doing in many venues, basically just trying to make -- increase the awareness that this is occurring but obviously we're not going to be able to touch everybody. So we actually would ask that, you know, governments undertake some effort to make network operators aware that the key roll is going to be occurring.

CHAIR SCHNEIDER: Iran.

IRAN: Thank you very much for the presentation. Do you have any feedback channel to ensure that the action that you have indicated, duly implemented before anything going to break down? Not everybody is so familiar and so quick following the actions. So just a question of feedback that, yes, we have received your letter, we are implementing. Perhaps any potential difficulty indicate? Or you don't have that system of feedback? Thank you.

DAVID CONRAD: We generally, in all cases that we've been, you know, speaking, we've encouraged people to contact us, have any questions that they might have or any concerns they might wish to express.

We don't have any explicit mechanism to sort of require people to provide the feedback. But we are working particularly with various network operations groups, various TLD organizations, that sort of thing, to provide a venue in which, you know, communication channels can be established to allow such feedback to be provided to us.

CHAIR SCHNEIDER: Thank you. I have Egypt, Norway, and the U.K. Netherlands, sorry.

EGYPT: Thank you, Thomas. And thanks, David, for the presentation. I have a question on Slide 5. But meanwhile, if I understand correctly, there's some tool to check that you're ready for -- I think this is useful to know.

DAVID CONRAD: Yes. We have created a testbed that will allow resolver operators to participate in a realtime test of the KSK rollover. The testbed unfortunately, it isn't in this slide deck. It was more oriented to the more technical slide deck, but I can provide that information to GAC members to provide to their network operators within their countries.

EGYPT: Yeah, thank you. I think this is very useful.

And my question is on Slide 5, please.

Just to make sure, does this impact resolvers in specific? Because I don't see here ccTLD -- I mean, TLD registries, operators. So is it resolvers in specific? Thank you.

DAVID CONRAD: Right. So the folks who are impacted here are on the sort of the side of the DNS that actually fetches information from the TLD operators. The TLDs, ccTLDs, gTLDs will not be impacted by the key rollover. They don't have to do anything. There's no functionality that they provide that's impacted here other, of course, than their internal systems and the resolvers that they operate within their internal systems.

CHAIR SCHNEIDER: Thank you.

Netherlands.

NETHERLANDS: Yes, thank you, David, for your explanation. Just double-checking a couple of things. I think governments don't have a formal responsibility in this. But you're using them merely as an outreach to contact ISPs. But there's no, let's say, governmental responsibility?

DAVID CONRAD: Exactly. We're looking for any communication channel we can touch, yes.

NETHERLANDS: Secondly, there was a list of DNS resolvers, recursive resolvers, which do DNSSEC validation in each letter. In our case, it's just about seven or eight, I think. Of course, these have also been directly contacted, I presume, and these are the ones who really do have to do a change, a real change in their systems. Other all impacted stakeholders do have the effect of but do they really have to change their systems? Thank you.

DAVID CONRAD: So the way -- the actual operation of how the key change will occur, there's actually an automated mode, if you're running up to date -- if a resolver operator is running up-to-date software and have enabled automated updates, then they actually don't have to do anything. It would probably be prudent to participate in the testbed to ensure that nothing odd will happen when actually the key rollover does occur. But ultimately there's an automation built into modern resolvers that will handle this key rollover automatically.

If they're not running old -- sorry, not running new software or they have not turned on the automated rollover, then they do have to change a configuration data point. It's the actual -- the public key associated with the KSK, it would need to be copied into a configuration file. So that's the case in which resolver operators will have to take some action.

CHAIR SCHNEIDER: Thank you. U.K. briefly.

UNITED KINGDOM: Yes, thank you. Thank you, David, for coming to brief us on this today.

I haven't actually talked to the U.K. members of the ISPs' constituency here, the ISPCP. Basically, they are all the connectivity stuff, so I will check. But I presume you would look to them to do a very critical outreach, to ISPs worldwide. And are you confident that that is going on? It would be very useful to have that reassurance.

And actually I haven't seen the letter so I have to check that out as well. I don't know where it might have ended up.

But I think I also heard you say it will be valuable for us to sort of double-check with our global network -- government network providers. For me it's a cabinet office in London. What are you doing on the 11th of October? Are you looking forward to that day? I mean, if there's something that might go wrong because of failure for people to undertake the necessary switchover, if that's the right word, will there be any comeback on us as governments safeguarding how everything resolves? Or how would you deal with a significant failure at that point at 11th of October? Yeah, sorry.

DAVID CONRAD: So yes, we have been in contact with the ISPCP and have encouraged them to contact their members and other bodies that we've been dealing -- you know, going to network operation group meetings quite extensively.

The -- with regards to the "should the bad thing happen," we are -- we've set up a very elaborate observation system to watch traffic to the root servers that would be sort of the first indication that sort of bad things are happening, and we do have fallback plans that would be implemented, should there -- we detect, you know, some sort of significant event that indicated that the rollover had failed.

We are fairly certain that -- it's unlikely that governments would probably get the wrath of the end users and network operators. I anticipate that that would actually be targeted at ICANN or, more specifically, myself, and that's one of the reasons I've been very engaged in trying to get the information across that it's really important that people do update their key.

CHAIR SCHNEIDER: Sorry. Please don't leave the room. There is an important announcement that I'm going to make in one minute, so let me just give the floor to the gentleman in the back. I think if I'm -- you're Nigeria, is that right?

NIGERIA: Nigeria, yes.

CHAIR SCHNEIDER: Thank you. And please don't leave the room. That is the last intervention that we'll take and then we have to have a hard stop. More or less hard stop. Nigeria, please go ahead.

NIGERIA: Thanks for the presentation on the DNSSEC rollover.

My question is that for those network service providers that has not enabled DNSSEC, what happens to them after the rollover? That have not originally enabled DNSSEC on their network. Thank you.

DAVID CONRAD: Yeah. They will see no change. If they have not enabled DNSSEC, the key rollover will have no impact. If at some point in the future they decide to enable DNSSEC, they'll need to make sure that they have the most recent key. If they don't, then their validations will fail and it will -- they'll be confused. So they just need to make sure that they have the most recent key or the most recent distribution of software, which will actually most likely fetch the most recent key automatically.

CHAIR SCHNEIDER: We have to stop here because -- there are several that want to make just a short and then we know what this gets -- because we have something important to tell you. That as you know, this is our last lunch in this meeting, or lunchtime, and that means it's the last lunchtime for Olof in his function as --

What is your function, actually? ICANN staff supporting the GAC and making good jokes at any time of the day or night on phone calls and whatever, like support is necessary.

So actually, Julia, who is probably again hiding as usual somewhere, she's actually been going out to bring this organized -- helped us organizing a small present for Olof.

[Laughter]

You will see -- we'll check with the technical people on how to get this home. This is just -- I think there's a card in there, and this is the present. It's not too heavy so it should actually work, so we just basically wanted to again and finally and really and with all our joy say thank you to you, Olof.

And there's some glasses in the back hiding, so this is a little bit of drinks and a little bit of snacks to celebrate the last moments with Olof in this capacity. Thank you very much, Olof.

[Applause]

OLOF NORDLING: Thank you ever so much. I always wanted an anvil --

[Laughter]

-- as a convenient hand luggage.

Oh, it's been great. Thank you so much. And, well, I hope to stay in touch, even though I'll go into retirement and so on.

So -- and I will still be around until the end of July, so -- well, you won't get rid of me entirely just yet, but thank you so much.

CHAIR SCHNEIDER: So okay. We can all go to the back --

BRAZIL: Thomas, may I just ask you?

CHAIR SCHNEIDER: Yes.

BRAZIL: In regard to after lunch, we are going to meet here and then we have this geo name, but what do we intend? Because I think we also need at some point to come together to discuss the communique or it will not be necessary? What will happen in that regard? Because yesterday we talked about meeting sometime at 3:00 or having some interaction.

CHAIR SCHNEIDER: We will -- we will see the text bits that we get -- or have gotten already. Tom has the overview on this. We will look at this during lunchtime at some point in time and then after -- the idea is to, at 3:00, have things ready and then maybe spend five minutes or so, hopefully, on finalizing this. But thank you for reminding us.

So don't runaway. Work is not yet over. Thank you.

But first, it's not work, it's celebrating Olof. Thank you.

[Break]