ICANN73 | Virtual Community Forum – Middle East Space – DNSSEC Signing and Validation
Thursday, March 10, 2022 – 09:00 to 10:00 AST

TIJANI BEN JEMAA: Good morning, good afternoon, good evening to everyone. This is the Middle East Space session at ICANN 73, which will be about the DNS signing and validation. But let me welcome you all for attending this session. This is a sign of your commitment and [inaudible] to this work that we are doing together with Abdalmonem and [inaudible].

Today, we have the privilege to have four guests. Baher Esmat, ICANN Vice President for Middle Eastern and managing director for the Istanbul office. Maarten Botterman, ICANN Board Chair, Ihab Osman, the ICANN Board member from our region, and Adiel Akplogan who is ICANN vice chair for technical engagement. So you see that we are really well served.

I would like to thank all these guests because they are always supporting us, they are always here, they never decline our invitation. This is a sign of confidence and a sign of support. So thank you very much. We will start by an opening address done by Mr. Baher Esmat who is the Vice President for Middle East and managing director for the Istanbul office. Baher, please.

FAHD BATAYNEH: Tijani, please, there is a note that I need to read before you proceed please. So it's a note we have to read. So to mute your device notifications in advance of the session, please do the following. On

Windows devices, this is called focus assist. On Mac, Do Not Disturb. Both this can be found under the notification settings and a quick browser search will also provide step-by-step instruction.

Please keep your lines mute if you are not speaking. And if you need to speak, just raise your hand and we will unmute you. Thank you. Back to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Fahd, and perhaps if you send this note to the whole community, it will be good for the future. Thank you. So Baher, please.

BAHER ESMAT: Thank you, Tijani, and good morning, good afternoon, everyone. This is Baher Esmat for the record. Thank you for joining us today. Another Middle East Space is taking place. Always pleasure to see some familiar faces and old friends and also to see some new faces coming to our session.

Today's topic is one that is very relevant to our engagement in the Middle East region. As some of you know, our region engagement plan has been developed in alignment with the ICANN Org's strategic plan, which among its strategic objectives, has one specific objective on the strengthening of the security of the domain name system.

And as part of our regional engagement, there have been enormous efforts made in collaboration with stakeholders from across the region

and also from beyond to further improve the knowledge and understanding of DNSSEC and also to promote the technology and encourage more adoption across the region. And this has been—I mean the engagement has been taking various forms, from technical workshops to webinars to one-to-one engagement activities with relevant stakeholders. And also sometimes we get support from our technical engagement team at ICANN, who provide some sort of hands-on technical support to those who are ready to deploy the technology.

So over the past two years, we've conducted over 20 different engagement activities around this very topic. Just in the past couple of weeks, we organized a webinar on the topic, I was involved in a one-to-one sort of dedicated session with one of the largest ISPs in the region, on DNSSEC validation. So just to show how important this topic is for our engagement.

And yet, there is always more to be done. And the statistics that we have show that only 37% of ccTLDs in the region got their zones signed. And the vast majority of network operators in the region have yet to adopt or enable DNSSEC validation.

So this session is very timely, I think the timing couldn't be better. And as always, we look forward to collaboration with community members to drive our work further, and this topic is no exception. So thank you for picking this topic for today's session. And I would particularly want to thank Tijani and the Middle East space team for the tremendous work they have been doing from behind the scenes. So thank you again, and back to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Baher. And thank you for your continued support. I cannot forget to mention the support of Fahd Batayneh who is always helping us also to do this work. So thank you both.

Our guest now is the ICANN Board Chair, Mr. Maarten Botterman. Maarten is a friend, used to be my chair in the contact group at Internet & Jurisdiction, the contact group about the domain and jurisdiction. And he was always supporting our work, he never declined our invitation. And I'd like to thank him very much, because I know his agenda is very crowded. And it's making a lot of effort to be always with us. So thank you, Maarten, and the floor is yours.

MAARTEN BOTTERMAN: Thank you, Tijani. And that's not for no reason, because you'll invite me and that's always an offer we can't resist. But it's also good to be in the discussions and over time, what you see with the Middle East space is the focus on several areas and digging them out and go deeper and come back to ICANN with a view informed by the region and that's very much appreciated.

Now as Baher said, DNSSEC is very important to us. It's explicitly mentioned in the strategic plan. And we work on many initiatives related to it. Security wasn't a driver when the DNS was designed in the early ‘80s. Attackers could compromise DNS messages and redirect them to another location on the Internet. And it's also only in the early ‘90s that the DNS technical community created this solution to the

problem of DNSSEC. It allows registrants to digitally sign information they put into the DNS to protect them by ensuring the DNS data has not been corrupted. And if it has been corrupted, it doesn't reach them.

So that brings two requirements. The first one is that the domain name registrants must ensure that DNSSEC data is signed. And secondly, that the network operators must enable DNSSEC validation on the resolvers that manage the DNS lookup for users.

If it does so, we know that on one end of the DNS query, you will find actually what you're looking for, and you're not redirected. So that is the big thing.

Now, today, there's about 1500 TLDs in the root zone. And of these, over 90% have trust anchors published as DS record in the DNS record in the root zone. In other words, they're fully signed and published. And the remaining about 8% are mostly ccTLDs and IDN ccTLDs that are not fully signed yet.

So the capacity building programs Baher talked about are explicitly there to help everybody to find its way there. Yet, the incentive needs to be there. And it is an extra effort. DNSSEC can't solve all forms of attacks against DNS. But it helps a lot. It'll only be realized after its widespread deployment.

So therefore, it's important to continue raising awareness. And particularly in this region, the awareness is right on this place. So I do encourage you to work with Baher together on setting why you want to do it, and then ICANN will help on how to do it.

One of the first examples of where I see this really made a difference was about five, six years ago, I'm in the Netherlands as you know, and SIDN, the ccTLD for .nl, started a campaign for DNSSEC where they gave an incentive, trainings to registrars, information to registrars, but also an incentive in the form of a discount for all those domains that were signed. Small discount, but together, it focuses the attention on it's really important and we need to do something about it. And we saw that that program that was specifically designed for the situation in the Netherlands, helped a lot and boosted. And today, .nl is one of the domains with the highest DNSSEC signatures.

So there's examples out there I also invite you to learn from and no doubt Baher and his team will be able to introduce those to you. And I really believe that if [inaudible] focus on this, you will see important uptake on this important element of a more secure Internet in the region. So thank you for the initiative. And I look forward to hear more about your plans later this session.

TIJANI BEN JEMAA: Thank you very much, Maarten, thank you for your support. And for the record, your support is not expressed by your presence today. It is also expressed by your response, continued response to our statements that we send to the Board. We always receive a response in which you are really encouraging us and you try to give your opinion about what we wrote in the statement. And this is very constructive. So thank you very much, you and Ihab, who is also a board director from the Middle East.

MAARTEN BOTTERMAN: [inaudible] that if I give a response, it's also a response carried by the Board, because we discuss it either on the list or even in session before we send it. So it's a heartfelt and full support.

TIJANI BEN JEMAA: It is what I am saying. Yeah. So, this is what I am saying. I am saying that Ihab who also is board director is one of the of those who are responding to our statements. So this is another form of opportunity for as well as all board members. So thank you very much, Maarten. I am really honored to have you always with us. Thank you.

Now we go to our friend, our brother, Ihab Osman who is the only ICANN Board member from the Middle East. Ihab has always supported us and I'd like to thank him very much and give him the floor so we have [inaudible].

IHAB OSMAN: Thank you, Tijani. Thank you, team. And it's always a pleasure to be here. I actually cannot wait to meet you in person. Hopefully as soon as COVID seems to finally be becoming part of just everyday life.

Thank you, Tijani for the invitation. I actually come to you today from probably the heart of the Middle East, from Riyadh, in Saudi Arabia, and DNSSEC signing and validation, as both Bayer and Maarten gave quite a bit of the numbers and its impact, the fact that only a third of the ccTLDs in our region are signed and validated is definitely an area that your efforts will help with to help close the gap and to make this hopefully all DNS records in the root zone are signed and validated.

As Maarten said, this is not going to solve all the issues, but it will definitely help a lot and it will take us especially in today's world, with all the security risks, that comes with being online and all the issues around DNS abuse, any door that we can tighten to help increase the reliability, security and the overall effectiveness of our own DNS system will be very good step.

The Middle East Space is always picking areas and subjects that are important for the region. Your statements are always spot on and direct to the point. That's why I always support the statements that come from the Middle East Space and you will always get my support on the Board and anything that will help and support the security and stability of the unique identifier system. So, thank you again for the invite, Tijani, and the whole team. I look forward, as I said, to continually engaging with you and I look forward to meeting live in the near future. Inshallah. Thank you.

TIJANI BEN JEMAA: Thank you very much, Ihab. Thank you for your continued support. Yes, you always support us even offline, but this is a form of confidence again and we are really happy by these people.

Before I go to the subject matter expert, I would like to stress that this work was done thanks to the team, three persons, three co-chairs, myself, Abdalmonem Galila and [inaudible]. Three of us are working on this, are doing this work and especially this time it was Abdalmonem who did most of the work. So I would like to thank him very much because I am very busy with the NomCom. I am a member of the

NomCom. So he did the majority of the work and I would like to thank him very, very much.

Now going to the subject matter expert, Adiel Akplogan. He is a friend from long time, used to be the CEO of AFRINIC, and when he was there, we managed to have an MoU with him, because he wants to help the community. And today, since he joined ICANN, Adiel never, never refused or declined any invitation or any help we asked him. So, Adiel is very helpful. He's always here, is always present. And today he will be our subject matter expert. So Adiel, please, the floor is yours.

WAFA DAHMANI: Thank you, Tijani. Thank you, everybody. And also very happy to be here, as always, the region is dear to my head. And so I will never turn down any invitation to address the region.

So the topic of the event is DNSSEC, signing and validation. I will try to take you through a little bit what ICANN is doing, how things have evolved over the past few years, and what we expect as well from actors and the community in the region.

You may all know and Maarten has reinforced that as well a few minutes ago, ICANN has been engaged into secure operation of the DNS since the inception. It has been engaged in promoting DNSSEC as well from various manner through partnership with organizations like NSRC, through supporting NOGs and training activities all over the world since the beginning.

But since two years, this has taken a new turn, which I will call positive, where promoting and supporting DNSSEC and DNSSEC ecosystem security in general has become a little bit more prominent in ICANN strategy. That has led us to a little bit more resources for promoting, developing capacity and also supporting operators in the region, particularly Middle East region and Africa, in their journey to secure their DNS environment. And particularly, deploy DNSSEC.

As you know, since two years, we have dedicated staff now at regional level who are working day, night with operators to help them in the journey to deploy DNSSEC. So the way we are approaching this now is on I will say three different aspects. The first is signing the TLDs. Maarten just gave some statistics a few minutes ago at the TLD level, we have only have 8% that are not signed. And that's thanks to the contractual compliance that gTLD registries have to go by. Because there is no contract with ccTLD, generally, unfortunately, most of those 8% are made of ccTLDs.

To make the matter a little bit worse, is that the majority of those 8% are in our region, Middle East and Africa, unfortunately. So we try to focus on signing the zone as one aspect of our engagement and capacity building. But it's not only that, we try to put this in sequence whereby those who are advanced and already signed can go to the next level.

And what is the next level after you have signed your TLD? It's to be able to have a provisioning system so that your customer—that mean the registrant—can also sign their own second level domain and be able to

upload their DS record in your zone. So that is the second level for anyone who has signed. So we are approaching that aspect as well.

And the third aspect that also has not been also very actively pushed in the past is the validation. And we consider validation as the very low hanging fruit because validation doesn't request all the effort that you need, all the structure that you need when signing your zone. So we have that further validation as well as another aspect that we want to focus on.

So, now engagement, you will see those three aspects always in the way, we engage at the regional level, focusing on the maturity level of all the TLD we engage with.

With the new team that we have, we have also noticed—and I think thanks to the COVID situation as well—we have quickly noticed that what people want is confidence in handling their zone after signing it and understanding all the different components that come into a regular normal DNS management.

That led us to build online and virtual labs, which can allow people who go through our capacity building program to play directly with signing in an environment that is secure, safe, where they are not breaking anything, but they can build and work in a replicate of the DNS infrastructure in general.

That virtual infrastructure has been used very actively over the past two years to provide capacity building in Middle East. And our tea, Yazid and Paul Muchene who are the two team member covering the region have

worked very actively with Baher and Fahd to provide capacity building on finding DNSSEC signing for ccTLD, but sometime as well through ISPs that operate [inaudible].

On the validation side, we cast the net a little bit wider, talking mostly to ISPs, network operators, because they are the main resolver provider in most of our countries, trying to talk to them and let them understand that validation is not something very complicated.

Usually when you say DNSSEC, people just get afraid because cryptography, because all the complexity, but you can turn on validation very easily without having to get into the weeds of the of DNSSEC. And in today's operational environment, most of the DNS software have validation on by default, even, or just one line of command to turn on validation.

So we are also aggressively working with operators in the region to help them turn on validation. They worry generally is will this impact the resolution time, will this impact the performance of my resolver? But studies show today that the impact is almost inexistent in today's operational environments.

So those are the three component that we are pushing. And the Middle East is part of a region where we are very aggressively working with the operators.

For products that work, we have also start promoting those best practices by documenting them in a more comprehensive way. We have two initiatives that are going to that direction. The first one is KINDNS.

Of course, you have heard about that, which is a program to one, streamline DNS operation best practices among which DNSSEC of course, and promote them and convince operators to join that initiative as ambassador and as promoter of the best practices.

And one aspect of KINDNS is to develop guidelines. We have released over the past two years to guideline in the DNS arena and the last one, OCTO 29 focused specifically on DNSSEC. And why did we release that? Because through our engagements, we have noticed that the problem that most of the operators have is not the knowledge all the time, it is rather the confidence and also having a guideline that can tell them what to do exactly, at which step to do what and follow that guideline step by step. That is a help that we cannot provide, because we don't have resources to be with everybody, but we try to document what are the different steps if you are about to sign years old, how do you prepare, how do you do this step by step and check at each step if you are doing the right thing?

So, that guideline is meant to give an additional tool to TLD registry on their journey to sign the zone. And we are going to release more guideline in other aspects of the DNS security ecosystem, obviously, to help operators. So that is going to be a complement to KINDNS and KINDNS will be the umbrella of all our activities towards securing the DNS operation.

If I have a message for the region in terms of deploying or signing the zone, I will say that it is something that you can do. If you need help, don't be afraid to contact us, to contact our team, they will happily help

you through the process. You can use the guideline which we have published and assess yourself where you are in that guideline so that when the team comes in, they can know where to take it from there.

Second is just on validation. Ask your operators to turn on validation, because it doesn't make sense to sign zone when we are not checking the validation, we are not validating what is signed, right. So even if we don't sign our ccTLD, everybody should be able to validate what is already signed there. Because if you are not validating, not only we are not benefiting from domain name in the TLD we are using, but also when we are assessing any random domain which is already signed, we are not benefiting from it because our resolver is not validating.

So second thing, just ask your operators to just turn on validation. It doesn't take much for them to do. So those are the two thing and then we'll be happy to answer any question in that area if you have. So I will stop there for further. Thank you.

TIJANI BEN JEMAA: Thank you so much, Adiel, for this presentation. I agree with you that signing without validation doesn't have any [inaudible]. But if we don't validate, I think we are losing a lot. So thank you very much. Now will go to our community to present our work, and the first one will be Mr. Sami Mohamed Ali, who is from .BH, means the Bahrain ccTLD, and Sami will introduce the topic, the Bahrain ccTLD [inaudible] the statement and penholder. So Sami, please go ahead.

SAMI MOHAMMED: Hi, everyone, and thank you for the introduction. Adiel, it was a very good description and information you shared and it was a lot of knowledge that you provided us in the previous topic. I will try to keep it short and just go through the DNSSEC introduction regarding the topic.

So DNSSEC is a foundational requirement for securing data exchange around the Internet. DNSSEC needs to be widely deployed in order to make the Internet stable, secure, resilient DNS ecosystem. With the expansion of the Internet and its services, security became an important requirement. As a result a new technology was invented and it's called DNSSEC.

DNSSEC, basically the suite of extension that add security to the domain name system protocol by enabling DNS responses to be validated, specifically DNSSEC providers provides data integrity, origin of authority, authenticated denial of existence, reduces the risk of DNS spoofing attacks, secure communication.

And now talking about the signing and the validation. So the DNS zone can be secured with DNSSEC using a process called zone signing. And then signing and validation is part of it. So when we talk about there are two parts of DNSSEC, the zone administrator that generates a cryptographic signature on DNS records in a zone. Secondly, the DNS client needs to check if the cryptographic signature is expected for this record and that signature record that they received is authentic. If so, then they can conclude the DNS answer is indeed authentic.

So this was a brief intro to the DNSSEC. And I will leave it to my team, Layal and Mustafa, to give you a bit more description explanation. And sorry, just keeping the time in mind.

TIJANI BEN JEMAA: [inaudible] Layal Jabran and Mustafa Al-Rifaee will read the statement that we prepared for you.

LAYAL JABRAN: Thank you, Tijani, for the intro. Reading the statement on DNSSEC signing validation for the Middle East Space in the online virtual meeting for ICANN on Thursday 10th of March 2022.

We the Middle East community members participating in the Internet Corporation for Assigned Names and Numbers, Middle East Space, addressed the concerns of both the top level domains, DNS security extension signing, adoption and an enabling DNSSEC validation for the ME countries to contribute safeguarding the global and united Internet and came up with this statement.

DNS is critical to ensure service continuity, faulty or ineffective DNS services can negatively affect the perception of any organization from clients, partners or employees, impact your ecommerce applications resulting in lost revenue and ruin a brand image. 63% of organizations suffered app downtime as a direct result of a DNS attack last year.

Since the DNS is essential to the operation of the Internet, protecting the data provided by the DNS is critical. So to help making good

progress in DNSSEC signing and validations. I will leave the recommendations to my colleague, Mustafa Al-Rifaee to mention them.

MUSTAFA AL-RIFAEE: Hello, everybody. Thank you, Layal. I will start with the recommendation. From ICANN side, encourage ICANN community members to join and involve more with other groups, groups working on DNS and DNSSEC outside ICANN for knowledge exchange and experience sharing.

The second is address and promote the use of DNSSEC to secure the way information moves around the Internet, has an open discussion about the challenges faced and best practice with the countries and organizations that have implemented DNSSEC to be able to [inaudible] for implementation.

Conduct a study about the role of different stakeholder groups such as Internet end users, software providers, IDN ccTLD operators, technical and academic communities, governments, private sector, etc. to further promote DNSSEC.

Conduct sessions to identify the ROI, return of investment, and ROR, return of risk, about [inaudible] the DNSSEC deployment and resolving. Support in developing protocols that will allow the DNSSEC process to be automated in the future, training local initiatives, training trainers in DNSSEC validation and signing to help other stakeholders to implement it.

Increase the security awareness level about that dependency on DNS for the functioning of Internet and how costly is the exploitation that occurs if we don't have this protection. Spread the knowledge that DNSSEC not only protect end users or governments etc., but also could create opportunity for innovation and enable new technologies [inaudible] and facilities.

From the TLD view, TLD registry and registrar, ICANN encourage them to start enabling the entirety of DNSSEC data for registered domains in an automated and easy way. Promote the concept of authenticity and integrity after enabling DNSSEC. Identify which stakeholders need to secure their domain names and conduct awareness sessions, especially those who have the most popular online application, brands, service, etc. to increase their security awareness as a first step, then going to other domain holders.

Plan a training for registry and registrar administrators to be able to manage the signing key and their rollover plan. Network operators, ICANN encourage them to enable DNSSEC validation on the resolver that handle DNS lookups for subscribed users.

Internet users, registrant, start enabling DNSSEC for their domains, spread the knowledge to their organization about what is the DNSSEC and why DNSSEC is critical for the security of the DNS.

Finally, we want to thank all those who are working hard to push the DNSSEC signing and validation project forward. We hope that these recommendations will be taken into account to make significant progress. Thank you.

TIJANI BEN JEMAA: Thank you very much, Layal and Mustafa, thank you for reading this statement. Now, we will give you a best practice. Mr. Imran Qazi who is the CEO of Gemnet enterprise solutions from Pakistan will tell us about enabling DNSSEC validation experience that they did on their network. And they did that exactly after they attended the webinar a few days ago. So Mr. Imran, please go ahead.

IMRAN QAZI: Yeah, sure. Thank you very much, Mr. TIjani. I would like to thank [inaudible] and ICANN for inviting me to this session. In today's world after COVID-19, Internet has been essential, and need of everyone. People around the world are very much dependent on it. We as an ISP are responsible for our user security and privacy. Hacking and [cyberattacks] are very common nowadays.

In today's stats, 26% with DNSSEC validation, and Pakistan is about 26% validations. Before enabling DNSSEC in our network, we were about at 4% validation. I would like to thank ICANN and Mr. Yazid especially and his team who helped me enable this DNSSEC security in our resolvers and currently, today's stats are showing our resolvers are at 97% today.

Certain [inaudible] and webinars are very important for operators around the world to gain the knowledge and improve our network security. Thank you very much.

TIJANI BEN JEMAA: Thank you so much. Thank you for speaking [inaudible]. So this is a best practice, an example of people who managed to sign their network and this is very, very good example.

Now, we will go to the discussion of the statement and I give the floor to madame Wafa Dahmani who [inaudible]

ABDALMONEM GALILA: We lost you, Tijani.

TIJANI BEN JEMAA: Sorry. I said now we will go to the discussion of the statement. And I'll give the floor to Madame Wafa Dahmani to moderate this discussion. Go ahead please.

WAFA DAHMANI: Yes, thank you, Mr. Tijani, for giving me the floor. I would like to start by thanking, of course, the pen holders of this statement and also thank the ICANN Board members who joined us and staff also joined us and gave us very relevant contribution.

So now we are going to the part of the discussion of the statement, will be any modification in this statement. I will start to see in the chat box. I don't see any question or comment, neither in the chat.

Perhaps I can start my comment. and hope that I can see panelists—

TIJANI BEN JEMAA: Wafa, Maarten is asking for the floor.

WAFA DAHMANI: Yes, yes. I just saw the hand of Maarten and Abdalmonem. So yes. Go ahead, Maarten.

MAARTEN BOTTERMAN: Thank you for the statement, I think it's right on the point. It doesn't only express the need to implement DNSSEC, which it does very well, but also that there's opportunities with that. And so I'm not speaking, not as Board chair but from my own experience. I can say that when we talked about IoT and IoT security, we see that even there, there may be opportunities because really secure the connection between two endpoints with DNSSEC. So just highlighting one of the opportunities for business models and other things. I really appreciate to see that you recognize that as well.

WAFA DAHMANI: Thank you, Maarten. Abdalmonem, go ahead.

ABDALMONEM GALILA: Thank you. Just a small note, a small two cents about the statement. The first cent about ROR and ROI, return of investment and the return of risk. So let me talk about the point of view of ISP. What is the return for me in order to enable DNSSEC resolve? I am stable now. I am fine for that.

So for return of investment, is there any document or guideline that explains the two matters from the point of view of ISPs to encourage them to deploy DNSSEC and have an investment and away from the risk from such disturbing the function of the DNS? That is first cent for me.

The second cent for me is about—let me try to [inaudible]. Ah, sorry, I already said my two cents inside one cent. Yes. That's all for me. Thank you.

WAFA DAHMANI: So Abdalmonem, if I might repeat what you are asking for. So you were asking if there were any documents about return of risk for ISPs that have deployed DNSSEC? That's it?

ABDALMONEM GALILA: Yes, actually, any guidelines related to ROI and ROR for ISPs from the technical point of view? This is the first. The second, I remember the second cent for me, this question for an Adiel about do you think that DNSSEC enabling for domain name could have a cost for registrant, or it should be for free for registrant? What is the best practice or experience or around this? Thank you.

WAFA DAHMANI: Okay, thank you, Abdalmonem. Before going to [inaudible], I will give the floor to Adiel. you can, I think, answer the two question.

ADIEL AKPLOGAN: Yeah, thank you. I'm not sure I catch the first question. But if I understand well, it is about the return on investments for enabling DNSSEC for an ISP. And the second is how to pass that cost on to on registrant, if here is a best practice in there.

I tend to explain this to ISP this way. DNS running in most of the case, including activating DNSSEC, in most of the ISP, they see it as a cost and not a line of revenue, right? It is a cost that you don't usually charge your customer separately, but it is a cost that allow you to provide your service, right?

If you are a registry and you are managing a TLD, you have a responsibility to make sure that that TLD is run securely and in a stable way, but also protected from misuse. And that's where DNSSEC comes in.

And it comes in as an economical advantage because it's a reputational, what it adds, the value it adds to you as a registry is your reputation. You don't want your TLDs to be labeled as poorly managed and responsible of a global failure of the DNS, right. The DNS is a distributed database, distributed service. Failure of one part of it impact everyone.

So the most important, I will say, value here is reputational. And if you're an economist you will start going from the reputational and dealing down to how your reputation impacts your bottom line.

So I'd probably like to suggest that the return on investment is not the return on investment directly as a service that you sell to your customer because nobody charge DNS resolution to their customer.

Now, if you are talking about a registrar to registrant, there are different models. There are registrars who charge a fee for their registrant to sign their zone. But today, there are more and more registrars that are providing simple, straightforward platform that automate everything and add that to their registration fee. That mean you can register your domain name and just tick a box and say yeah, I want to sign my zone. And the registrar through their online platform, do all the magic behind the scene, sign your zone, add it to the parents zone, and voila, it just done.

That's why when I was talking before, I put the emphasis on those three critical element there. You sign your zone, that is fine, but how do you allow your child to be able to sign theirs as well? There is a process there and you have to make sure that you optimize the way that happens. So it make it easy for more people as registrant to sign.

So that investment, you need to find a way of course to [redirect that to your] your registrant through the service that you are providing them. As I say, there are different models. Some charge you for doing that, some just bundle that into your registration fee, it is part of it, it is there. You do it or you don't do it, you are paying for it. Right? That is an incentive as well. If you know that you do it or you don't do it, you have been charged for it and it just takes a click for you to sign your zone, why not do it?

So, that aspect is also very important. I don't know if I cover those two questions, but I think it is for—and we are talking here about signing the zone. I'm not talking about the validation. So validations are very simple. So we are talking about the zone signing part of the process.

WAFA DAHMANI: Thank you, Adiel. Yes, I agree with you that in case of failure, the cost will be another investment that will be more and more important than the investment of signing the zone. So I see Abdalmonem is satisfied with your response. Ulrich Wisser, you have the floor.

ULRICH WISSER: Yes, hello. My name is Ulrich Wisser. I work for the Swedish Internet registry. And we have actually been the first TLD in the world to be DNSSEC signed. So safely to say that we are a big proponent of DNSSEC. And I'm really happy to see this session today. It's really something that we have dreamed of in the past.

I just wanted to chime in. There was a lot of talk about the benefits of DNSSEC and a lot of technical stuff. But what I really want to emphasize is that this is making the Internet more secure place for everybody. And if you really don't—on the border of doing this or not doing this, I want you to think about your children and your parents. And would you rather see them go to an insecure side or to a secure site? And if it's a secure site, which I hope it is, I would say that you and we all are the experts in this matter. And we have to make it happen. Nobody else is there to do it. It's our purpose to make this Internet a safer place for

domain names. And with that, if you have any questions about DNSSEC in the past, or what we have done as .se registry, we are happy to answer questions. And good luck in implementing DNSSEC.

WAFA DAHMANI: Thank you, Ulrich, for your hand to help. So we have only two minutes left. So I will give the floor for Mustafa. Please be short, and then we'll go to the question of Chokri Ben Romdhane.

MUSTAFA AL-RIFAEE: Thank you. I just have a question to ICANN, if that was [inaudible] question. Because I'm talking as a ccTLD administrator, for example, the most thing is the DNSSEC maintenance. Key roll over, for example, required or I lost my key, and I need to upload the new DS records or new DNS key to IANA, for example, it can take many hours. So maybe I will lose or my end user will lose their access to their domains. So my question is, does IANA or the root server support managing DS record from the [inaudible] DNS key? Does that support? This is just my question.

WAFA DAHMANI: A technical question. Who can handle it from ICANN?

ADIEL AKPLOGAN: If I understand well, you're asking if IANA do automatically check the key and can update it instead of you doing it manually. But quite frankly, I cannot answer that question from the technical perspective.

But I'm sure that there are a process even if it is not the automated one that will allow you and prevents you to suffer from the cuts that you are mentioning or for of course, if you want to roll your key, you have to prepare and make sure that during a period validation, taking consideration your two keys and stuff like that.

There are processes that allow you to do that transition manually as well. But from the automated side, I will check with our friend from IANA to validate that they can do that from that perspective. I will be sure that there is a process for that.

WAFA DAHMANI: Okay. Thank you Adiel. I will read the question of Chokri now, since we are short of time. “I can hardly see the role of end users in the DNSSEC validation process. The statement considers registrants as end users, which not always the case. It's possible to clarify this issue.” I agree with you that the registrant does not have any role in the validation process. They are the demander. So the penholder of the statement, would you be able to clarify this?

ABDALMONEM GALILA: Actually, registrant is may be an end user, may be an organization that owns a domain name or registrant owned a domain name. So, what will we do the validation is the DNS provider itself or the registrant who add my domains and who will help the organization to add—who will offer the service of DNSSEC for their clients, whatever the client, organization or an end user.

For example, here in Egypt, I own a domain, for example, for [inaudible], I will go to the registrar and if the registrar enable DNSSEC or provided DNS service, I will check the box I need DNSSEC security for my domain name, they will create the keys offline away from the registrant or organization that owns the domain name, and all the process will be done behind

TIJANI BEN JEMAA: May I jump in please?

WAFA DAHMANI: Yes.

TIJANI BEN JEMAA: We are four minutes out of the time. So I ask you to be really very brief because there is no possibility to extend this meeting. I was

WAFA DAHMANI: Yes. I was to end with [inaudible]. please, you raised your hand. you will no longer want to speak, [inaudible]? So I can see no other hand.

ADIEL AKPLOGAN: I just want to add something just to clarify the question there. I think that is a common mistake, the registrant and validation. I think the registrant have a role to play in DNSSEC signing, the zone signing, but anyone that use an ISP and use a resolver, any user of the Internet are concerned with turning on validation. So those two aspect needs to be

clarified. Registrant, they deal with the zone file, right? Because they put their domain name in there. So it has to be signed. So it is different from we all that use resolver that need ISP to turn resolution on.

WAFA DAHMANI: Thank you, Adiel, for this clarification. We have to close now. Thank you all for your contribution. And the floor is yours, Mr, Tijani—I will give the floor, the closing remarks, to Abdalmonem.

ABDALMONEM GALILA: Yeah, thank you. As we have no time, I would like to thank Maarten, thank Ihab, thank the penholder and [inaudible] did the statement and thank all the participants. It is really appreciated that you help us and attend the meeting. And if you have any comments before submitting the final statement to the ICANN Board or agree for that, you are welcome to submit your ideas. Yes, thank you. The floor is yours, Dr. Tijani, now. Thank you.

TIJANI BEN JEMAA: Thank you very much. I am obliged to close this this meeting now. Thank you very much for all persons who attended, to Ihab, to Adiel and to all of you. Thank you very much, Layal, Mustafa, Sami, everyone who participated in this.

[END OF TRANSCRIPTION]