HYDERABAD – DNSSEC Workshop - Part 3
Monday, November 07, 2016 – 13:45 to 15:00 IST
ICANN57 | Hyderabad, India

KUMAR ASHUTOSH: You can choose three options. One is customize the zone signing parameter which means you select your own parameters. The second is you sign the zone with existing zone. So you have already have a template and use that template. The third is use default settings. This is – the third one is for test the people who are new to this or people who rely –

They don't want those complicated settings. They just want that standard default which has been achieved upon by operational practices. Use them, rely on Microsoft 2. Sign them with that.

I choose Customize because if I click this, this will be in one step. It will sign. You don't need to do anything. But here, I will just walk you through what happens next. The first thing is selecting the key signing keys. Now, all of you are aware, for those who are novices – very less in this room, so I'll just tell you – what it means is key signing keys, the key which is used to sign the keys.

I have already signed it, so it just preserves that data. I will add a new signing key here. You see, it gives a lot of information there or what all you can do. I can choose Cryptographic algorithm,

which algorithm I can choose. There are a set of algorithms used from ECDSA like elliptic curve, and [RSA] one. There are a set of algorithms that you can choose. These are all standards like IANA defines.

You can set the key lengths. If you are using RSA, you can set the key length as well. You can use any third-party storage provider which is CNG-compliant – which is Cryptographic New Generation compliant, third party group. But most of the KSM or HSMs or key storage providers are already compliant to that. Or you can rely on Microsoft. Microsoft provides you an inbox. I don't have any HSM connected, so I am using the Microsoft Software Key Provider.

Then there is this DNSKEY that is generated. What is the time? It will sign something. Right? What's the signature validity period? Then we also do automatic rollover. You can select to do automatic rollover and specify what all details are required. You just do an OKAY. Done. One is created. You cannot create more. I will just use one for this moment. Right?

Similarly, you go and pick a ZSK which is Zone Signing Key. I had added already one. I will remove that and I'll add one more. All these same things, Cryptographic algorithm. You can choose anything, you can combine them. It doesn't matter. ZSKs are

used to sign the zones. Why ZSKs? These [refresh] very frequently. The KSKs have to remain there. Right?

There are two keys. Just remember these two, ZSK and KSK. That's enough. Then there is a key length you specify. There will be a same storage provider that will use. You can use different storage provider for the signing. It doesn't matter. There is flexibility on that. DNSKEY signature validity period. DS signature validity period.

Now, DSE is delegation signer. Right? If you have some delegations inside, then you sign them. You say that, "Okay, I will generate a DS required for this NS record and I'll give it to the parent." Then the zone record validity, then the key rollover stuff. All this, I do. I'll, again, move to NSEC. This is the third part. Once you do KSK, ZSK, then you go to that Denial of Existence. You can select NSEC3, you can use NSEC.

Then you have Trust Anchors. You select those Trust Anchors. I'll just explain what Trust Anchor is. You select some small Signing and Polling Parameters. Then you have DNS security extensions. This is the summary of what we did. I do this, and zone has been successfully signed. This is done. If I refresh this, go here and I do F5, I have all the signatures generated – all the records generated, whatever it is.

Now, how do I verify this? I just export this stuff. I go to the DNS server. I will just bring it down, get my stuff here. This is a partial. This is just a command which – I'm just exporting the public key to a common location. I exported it. I go to Resolver. This is what I have exported is the secure entry point or the trust anchor for that zone which says that, okay, if I have that validation logic with me, I have that trust anchor with me, the Resolver can say, then I can validate using that. We don't have a root or anything.

What I'm saying is I have a signature here and I have a validated sign there. Sorry. I'm just importing that validator here. Just I do this one command, this is done. I go to the DNS client. I'm sorry. Yes. I go to the DNS client, pray to the demo gods that it works. This command here, it's not visible, but this has resolved DNS names, www.contoso.com minus server, resolver, DNSSEC. Okay. It's very similar to the Dig, or nslookup, that people might use. This is partial version for automation purposes. I hope this works. It works. Perfect.

I go to server. What I do is, I un-sign the zone. This is one step un-sign. You can go here and un-sign as well. Just go here. Right click, un-sign the zone. That's done. You go here, Resolver. You clean up. Yes. Done. I just clear up the cache here in Resolver. I go to the Client. I clear the cache and I run this. This will fail. That means my resolver validated and say that, "Okay, you have

unsigned the zone. I cannot trustfully give it to you." This is very basic demo of DNSSEC. I think my time is over, I've been told.

JACQUES LATOUR: That's right. Your time is over.

KUMAR ASHUTOSH: Yes. I took exactly 12 minutes to do this.

JACQUES LATOUR: All right. Thank you. Any questions?

KUMAR ASHUTOSH: Yes, please.

UNIDENTIFIED MALE: I have two question. The first question is can this server generate DSK or KSK?

KUMAR ASHUTOSH: Yes. This is all inbox. These three machines you see are hosted [inaudible]. They're all there in a single, small-

UNIDENTIFIED MALE: Okay. Second question is on the slide, the KSK can be automatically rolled over. How does it mean?

KUMAR ASHUTOSH: Automatically rolled over.

UNIDENTIFIED MALE: Yes, because the KSK Rollover by the carrier's DS registration to the parents. But that process is not automated, I believe. The automatic KSK rollover is somewhat confusing for me. So how does it mean?

KUMAR ASHUTOSH: Okay. This goes into DNSSEC definition. There are two parts of this. Whenever rollover happens, KSK – in our case, it happens, rollover happens by double signature. There are two process. One is the pre-published and one is the double signature. In those DNS server, KSK rollover happens by double signature method. There on the server, you specify that, okay, this KSK will roll over after some time which means after some time, that double signature process comes into picture. This is the DNS server setting.

But the other part is where you say the parent delegation has to be updated, and wherever the trust anchors have been put, they

have to be updated. Right? Have I got minute to show him something or…?

JACQUES LATOUR: No, not really.

KUMAR ASHUTOSH: Not really? Okay.

JACQUES LATOUR: Do it offline.

KUMAR ASHUTOSH: Please just connect with me offline. I'll show it to you. Thank you. Any questions?

JACQUES LATOUR: Any question? Are you planning to support CDS?

KUMAR ASHUTOSH: Just serious. When those DNS are already, there is a functionality called DS polling mechanism where the parent polls the signed delegations. It already updates.

JACQUES LATOUR: Perfect.

KUMAR ASHUTOSH: This is called DS polling mechanism. If you have been those DNS server at the [archive] delegation and there is a parent, when those DNS server is signed, it automatically poll and find out. Yes, please.

JACQUES LATOUR: Last question from-

KUMAR ASHUTOSH: Please talk to me offline.

JACQUES LATOUR: Talk to the mic.

[MOHED]: [inaudible] from Nixi. My question is does your Microsoft DNS server run in authoritative as a less re-considered [inaudible]?

KUMAR ASHUTOSH: Yes, all modes. I showed you. There were three machines.

[MOHED]: All of them are Microsoft only, I guess.

KUMAR ASHUTOSH: Yes, all of them are Microsoft.

[MOHED]: I suppose the source code is not public.

KUMAR ASHUTOSH: The source code is not public, yes.

[MOHED]: Okay, thank you. As expected.

KUMAR ASHUTOSH: Yes. Microsoft loves open source.

JACQUES LATOUR: All right. Thank you. All right. Yes. Go.

[inaudible]

All right. Next up is Rick Lamb and he's going to talk about the DNSSEC-S/MIME-DANE Package Integration in Microsoft Outlook. He's going to be doing demos. Right?

RICHARD LAMB: Yup. I'm doing a demo, too. I'm glad someone else are doing the demos.

JACQUES LATOUR: Good. Try to increase the font so we can see it.

RICHARD LAMB: Okay. Next slide please. Thank you. All right. Problem has always been, okay, there's a slow uptake in DNSSEC. My job, actually, at ICANN is DNSSEC deployment, trying to increase deployment. This is a very painful thing for me. At work, it seems like we can't seem to make it get passed this number. At the second level, how many domain names like Google.com are assigned? It's 2 or 3%. It continues to stay that small.

Of course, along comes DANE. Yipee, great. SMIMEA. SMIMEA, for those of you who know don't, is a way to put certificates, S/MIME certificates, into the DNS and protect them with DNSSEC and be able to then, ideally, be able to send end-to-end encrypted e-mail.

But it's been a slow uptake. I feel some of that is because we're very much of an open source community. We have not addressed the huge installed base of outlook and S/MIME

capable setups that are out there. U.S. Department of Defense, for example, and all the government employees there, I was one there for a while. We all are forced to carry an ID Card. It has a digital certificate in it. We're all forced to take a class on how to send encrypted e-mail using Outlook and S/MIME. This is just sitting there. There's this installed base of capability.

However, if someone within one of those organizations wants to send an encrypted e-mail to somebody else, it doesn't work. Initially, you'd have to typically exchange a signed e-mail with a certificate in it or some way, get the certificate into that person's hands before you could do this. This is where SMIMEA and – it's not quite an RFC yet, but something that had been worked on by Jakob Schlyter and Paul Hoffman in the IETF. It would be a wonderful example.

Problem is, how do I get this in the Outlook. Well, it turns out, Outlook has an Address Book function. It turns out that Address Book function talks LDAP. Actually, this is an effort that I did myself, not with ICANN. I funded some friends of mine who are windows programmers, to write from scratch an LDAP to DNSSEC validator. Okay.

It does all the ASNN1, DER1, all the yucky stuff – converts it into a DNS lookup, validates the response and brings it in. Yipee. Now, we have encrypted e-mail. Next slide, please. Pray.

If this doesn't work, I have a bunch of slides there that that will work. Okay. Let's see. Tell me if you see this. Yippee. Okay, so let's do this. I would like to increase the resolution of this thing. Nope. Too far. Worked? Okay. Thank you. All right. Good. Excellent.

I got my little Linux laptop here running two versions of Windows 10. That's weird. Okay, so I have to look at the screen, too. That's a pain in the ass. Okay. All right. Here we go. All right. Thank God for VirtualBox. Okay.

I'm going to try to send an e-mail here. I'm going to try to send an encrypted e-mail to someone. dtest01. This is hard because I can't see it. dtest01. I'm pretty sure it's that first one so I'm going to go for that. If I can't see it, you can't see it, so this is unfortunate. I don't know how else to make this any bigger. All right.

Test encrypted e-mail. One, two, three. All right. Now, I'm going to pick up here the encrypt figure. Then if I try to go send, of course it doesn't work. It does not know where the certificate is. Fine. I cancel out of this, this, and this.

Okay. I say, all right, I'm going to download or, in this case, I'm just simply going to execute this little plug-in or this program that I have that will perform this LDAP to DNSSEC conversion. It's

called lvdt.exe. Okay. There it is. It's done. I don't know if you see it, but it shows up down here in the tray. Fine. Done. All right.

Now, I then also have to tell Outlook that there is this new address book. It didn't work. Let's see. Where is it? Where is it? There it is. File. File. All right. Do this. This is all standard. I haven't modified Outlook at all. I haven't done anything here different. I'm going to add an LDAP Address Book. It needs an IP address. This thing runs locally so 127.0.0.1:390. Next.

Okay. Fine. Hopefully, I got 390 in there. Right. I forgot that I couldn't. This is hard to see. All right. It needs me to restart this, so I'm going to restart this. Hopefully, I think on the bottom is Exit. Yes? Okay. All right. Blah, blah, blah.

Huh? It doesn't? Robert here made a very good point. This thing that's sitting here running locally, the reason I want it to run locally is I want end-to-end validation on DNSSEC. This is a validator, too. But it does not have to run locally. I could run this, say, in my corporate setup and have everyone just point to this address book and it worked just as well. In fact, if you look at the references at the end of this presentation, you could do that. I have one running in my basement that you can run. You can do that. All right. Let's see.

All right. I'm going to try to just kick off Outlook again. You know what I'm going to do. I'm just going to try and try again. Okay. All right. This shows that I already have a certificate installed for my account. Remember to send an encrypted e-mail, I need the certificate of the other end. All right. I'll try to do a new e-mail. Send. Blah, blah, blah. Let's try dtest01. Looks like it's already there. Let's hope that's the right one. All right. Testencrypt@icannmeeting. Okay. 112233. I don't know, random characters. It's always hard to be random.

All right. Now, I want it to be encrypted so I'm going to say Encrypt. Okay. This is where the demo usually fails, so let's see. It worked. Okay. Sorry. Anyway, that's better than a [steak]. All right.

Now, I just sent that to an e-mail account, dtest01 on another machine. Well, because I have the magic of VirtualBox, here's another Windows 10 running on my VirtualBox. All right. I can even run Mac OS on this thing. I just think this is really cool. Well, there it is. There's the e-mail message, encrypted. It came across just fine. This worked. That's really the crux of my demo. That's it. Right.

This was – for the sender, it was completely transparent. They saw nothing. It just worked. It looked up in DNS to find this information. It's a bit too hard to see on the screen right now, so

I'm not going to go through and show you the logfile. There is a logfile that allows you to see what is going on.

But what I will do – and I will make this screen bigger but this I do know how to do. Okay. Just to prove to you that there is – if I do the DNS lookup for the certificate associated with that e-mail address – there it is and I do this – and there it is. What I have stored on one of my servers is this long blob which represents the SMIMEA-encoded e-mail address on the left here. It's a Type 53 which I think is the SMIMEA-type record. And there it is. All right.

That's it. We're done. This is the killer app I think for DNSSEC because now, we can exchange e-mail everywhere and all we need to do is get this little small executable and throw it on our systems. My hope is maybe somebody at Microsoft is here, maybe, I don't know, find this interesting and want to put something, this sort of functionality into Outlook.

Anyway, I'm going to do one more demo here. I think this last one is something you could all play along with and you might find fun and interesting. These will be at the end of the presentation, but I also created a [mail] listener that sits there and does an analysis on you and tries to give you back some information. If you send it a signed e-mail, it'll, for example, give

you back the SMIMEA record that you need to put in your DNS. If you have something signed already, it'll do other things.

If you send an e-mail to SMIMEA@zx.com. Yes, I'm old so I have a couple two-letter domain names. Haven't sold them yet. All right. Test, "1 2 3", blah, blah, blah. It doesn't matter. It's not reading the contents of the e-mail. I send this and I wait.

All right. Here is the response. I know that was impressive. Thank you, [Warren]. Okay. All right. Okay. All right. It does two things. First, it gives you back a response. God, I wish I knew how to make this bigger. It gives you back a response with a bunch of information that says, "Okay, I found an SMIMEA certificate for you and here's a fingerprint of it. Here's some other information I found about you." It gives you that instantly, which is nice.

Then it also, if it finds this SMIMEA record in the DNS, it says, "Well, I can send you an encrypted e-mail." It sends you an encrypted e-mail. If you can read this, two-way encryption words for you so you're all set.

The other way to use this, I'm not going to demonstrate that, is if I sent a signed e-mail to this thing, it would say, again, "Here's the SMIMEA record you should put into your DNS to make this work."

Okay. I'm done. That was the end of the demo. It all worked. I'm going to switch back to the slides and there's just one more slide.

Huh? I have lots of time? That's not usually true for me. Something's wrong. Yes. Okay.

Okay. Next slide, please. Okay, so what happened? All right. Outlook queries its address book. It went looking for dtest01@dnssek.info. That's who I was trying to send this to. One of the LDAP Address Book entries points to this local server, 127.0.0.1:390, just picked out of a hat.

This little lvdt.exe thing is really lightweight minimal little LDAP server written from scratch from RFCs. It listened to the LDAP request, converted it into a DNS request, sends that out, and then receives the response. The response is, in fact, DNSSEC validated. It's converted back into LDAP. The address book says fine, got the certificates. It can encrypt the e-mail. Next slide, please.

That's it. Done. These are the things that I used in this thing. If you want to try this, it's free to download this little beta thing, this exe file from there. It's an exe file. I know, you're never supposed to download and execute an exe file. But, hey, in this case, you just have to trust me.

But you can do that. It's all based, of course, on this draft that I'm hoping at some point is going to turn into an RFC. That's the e-mail address you could send your little tests to, smimea@zx.com. That's it. Thank you.

JACQUES LATOUR: All right. Thanks, Rick. Do you have any questions?

ANDREW MCCONACHIE: Maybe this is a dumb question because I don't know how Exchange and Outlook work but does this work with multiple recipients? If so, how does that work? If multiple recipients have different certificates.

RICHARD LAMB: Outlook simply uses the service as an address book. If they're multiple recipients, it's just going to pull the certificates for every one of those recipients and then do some SMIME magic which I always get confused about.

JACQUES LATOUR: Any other questions? All right. Thanks, Rick. Next up, Jaap from NLnet Labs. He's going to present the Secure Mail Server using DNSSEC and TLSE. Another demo? Yes?

JAAP AKKERHUIS: Yes, and that's me. This is actually a similar thing as Rick was telling about. Notice that I'm just proxying the people who did the work because they just happen to be there. So, a lot of details I cannot answer. What is it all about? Next please.

Well, it is actually trying to catch a secure mail implemented by different systems and different people and trying to get interchange between [those].

We've got the Fraunhofer IAO. I forgot what it stands for – the German-some research institute. ISC, well known for BIND [inaudible]. Microsoft, also well known for some slightly used software. The [NCCE] which is – actually, I forgot what it stands for. I'm sorry.

The NIST is actually the driving force behind it [inaudible] it. It's [inaudible] It's National Institute of Standards and Technology, I think. NLnet Labs, that's us. And Secure64. Secure 64 is a provider of applications which is doing security analysis. These are basically the providers, the players. Next one.

There are standards being used there. Well, there is the SMIME, TLS DNSSEC and various CERTS, which is actually known as more or less as Dane that Rick was talking about. The CERTS got divided into three categories – Self-signed, Well Known Certs, or

Private Certs which are now private for a single company or things like that. That's the three different types of certs that they had. Next, please.

What are the Mail User Applications for ACC parts? There's Microsoft office and the other one was Thunderbird. Thunderbird is also on the Mac with a special utility delivered by Secure64 to make it work with Mac mail. Next, please.

The transport agents being used was Postfix, a well-known sent mail replacement, Dovecot and Exchange. Also, there's IMF and so on. Exchange is well-known for the usual suspect, Microsoft. Next, please.

The DNS parts, which is actually – that's how we got defaulted in this because we're doing it DNS and not mail. But ISC is, of course, doing BIND. Microsoft was doing the Active Directory and DNS Server secure. Next, please.

We were doing NSD4 unbound and OpenDNSSEC together. Secure64 has the three different parts – Signer, Cache Manager, and then the Keychain Utility. The idea is not to stick to one single system, but to see whether you can interchange more or less secure mail. Here we go. Next one, please.

The product. What we actually delivered in the end is an NIST Practice Guide [program] basically of how we do these things.

It's a HowTo guide with a lot of detailed information and tested examples. Now, it is actually in Public Comment Periods. It got published two days ago. That's why I added this to the slide. Public Comment Periods for people who want to comment on what it is, I think 14th December if I remember correctly. But here below, you find the URL to find this.

The problem with the HowTo is it takes endless amount of detailed stuff which is very boring as well for the presenter as for the public to go over. So I just limit myself to some high-level remarks. Next, please.

This is the testing environment. On the left, you see Outlook. We talk to as well as – I cannot read it myself – Dovecot or Postfix and Exchange, depending on which mode is being used.

Then on the right of this left block, you see the various name servers which have been used in the experiment. On the right you see there's two other parts who are actually playing with new implementations. Here, the yellow lines, you see how the mail information went. The other one is how, in this case, for this experiment, the DNS information went and how they combine together.

Actually, what you see here is there's two lines in between the blocks. That is why you see that you have two different parts and

you have to, can verify what's happening with the mail and the other way around. That's the basic part. That's really what DANE does for you, verify what's going on or being able to verify what's going on. Next, please.

In this drawing was just one of the scenarios that's done. But a couple of the main scenarios was Transport Security. That's, of course, TLSA DNSSEC. The end-to-end security, the S/MIME signed mail, and there was an experiment which encrypted mail as well from end-to-end. But the problem there is that S/MIME is still a draft and [getting], so not everybody who [inaudible] for doing this fully. That's why it's carried out with some assistance data because it went the extra mile. Some said, "Forget it. We wait until the draft is finished." Next, please.

Then what we did was well defined test. I think the numbers there on the left is which number of tests. This is just one of the examples. We have pages of this. Basically, so trying to find out all the combinations and see what works and what doesn't, and really testing out the interoperability of the various systems. Since, of course, [we upped the] standard, now everybody should be able to do this. Ha!

Actually, in the end, what they also did was trying man in the middle attacks on various occasions and see whether you could

detect them or not, whether or not complications work. This is an awful lot of details which I spare you. Next one, please.

Now, the [inaudible] there were no surprises. Everything worked according to plan. The standards worked, the interchange, and all the tests met expectations – even the failed ones because that was of doing the analyze of tampering attempts and just basically done from logfiles. Of course, that's for\ a system administrator to look whether or not people are trying to do weird stuff. Again, the nice thing is it does work. We just need to do it. Next, please.

I think I've got it. Really, the role of DNSSEC in this case is actually the enabling of the verifications of trust in applications. That's the really part of DNSSEC. Some people are doing DNSSEC just because it's an application tool. No, it's an application. It's just part of the infrastructure to grant applications on, and it shows here that it does well. This is actually interesting. Just maybe next, please. I'm done.

I have an extra comment to make and I forgot to put on slide. It's interesting to notice that this is actually going to be a new hot item. The [Dutch government faces] have just ordered, a couple months ago, that everybody should be using DANE for the communication between government [sides]. They should comply to using DANE and DANE-enabled applications or they

should official tell why the people cannot do it. So it's comply or tell, it seems we have.

Actually, we hope – probably will see DANE-based applications move along –and DNSSEC applications – move along in the short future, at least for–

And this government does [inaudible] customers [inaudible] and things like that.

As far as I know, in Germany, they're actually doing something similar – and I guess the time stopped [for Peter]. This is going to be. If now, the S/MIME or P2P encrypted mail becomes final [inaudible] idea, then the e-mail can get more secured and more difficult to steal. Of course, if you just shove money on it, they can always back into your machine and catch your keyboard, but that's not a part of the puzzle. Anyway, any question.?

By the way, the URL Warren gave, you can actually just [shut] down the P2P with the document, so that's… [inaudible].

JACQUES LATOUR: Any questions? We've got lots of time. All right. We can do P2P. Yeah. Right. Thank you, Jaap. That's it.

All right. Next up is me. We've got our DNSSEC - How Can I Help? Typically, this is Dan York's show, so I'm not sure I can do exactly as he does. Next one.

So, a couple of slides. I'll talk about getting DNSSEC out there, more of it. As a TLD operator, you want to sign your TLD. I think most of us are signed, but some are under way so we're making process. Those are available to get there. We need to automate more processes. We've seen a little bit of that today.

TLDs need to accept DS records through the registrar through different interface like DSAP or stuff like that. It's really important to accept DS to increase the DNSSEC out there.

Working with registrar, trying to get them to do DNSSEC – to offer signing services, to get DS from customers, and all of that.

Then Stats. It's important to know who's signed, not signed, and to show progress on DNSSEC. Next slide.

Zone operator. You need to sign your zone. There's more and more tool. Pretty much everybody support DNSSEC. Microsoft, although it was small, but they have a nice implementation of DNSSEC. It'll be nicer if there's CDS in there but we'll get there.

Again, you need – so you're on the other side, you've got to make sure your registrar supports DNSSEC. That's an issue. A lot

of them are not supporting it, so we need to work on them to do more support or use alternative means of getting your DS out there – and more statistics. I guess [Dan] likes statistics. Next one.

Network Service Provider, ISP. It's missing a bullet here. Deploy validating DNS resolver, that's important. You need to enable the validation, and to sign their own zone.

Also, upgrade your software. There's the key rollover happening, so you've got to make sure you're ready for that. As a TLD operator, you need to tell your ISPs in the region to look at this, make sure it's enabled to avoid failures. Next one.

Everybody, use DNSSEC. Learn. Today, you've seen a lot of stuff – a lot of different DNSSEC implementation. Learn, play with it, share your lessons. If you play with it and discover something new, share that with everybody. There's lots of mailing lists. Then participate in workshop, local, and promote DNSSEC. I want to thank everybody today for participating and presenting, and Robert for all his questions.

ROBERT MARTIN-LEGENE: It just dawned on me that this thing of disabling DNSSEC when everything breaks. I noticed that at home when my ISP breaks, the first thing I notice in the logfiles is that DNSSEC is

complaining that the fail should validate. Then, of course, the first thing you would do is to disable validation which is basically not the problem. The problem is that the default gateway just went away. Of course, the DNSSEC doesn't work. But you get confused if you read the logfiles and then you think that, actually, you misdiagnose a problem very easily.

JACQUES LATOUR: So we need better tools to monitor.

ROBERT MARTIN-LEGENE: [inaudible]

JACQUES LATOUR: There you go. Thanks to all the participants today. It was a great session. Next one. Oh, question.

[PETER]: Jacques [inaudible], Peter [inaudible]. I've been quiet all day and, since you appreciated Robert's comments, I hope I can confuse you a bit. I have two things. First, I'd like to nitpick on one of your first slides when you said "accept DS records". I urge you to change this wording into "Accept key material" because the majority of second level domains in the world, still assuming

that .nl is leading there, is running on DNS key rather than DS records. That's just a small suggestion.

JACQUES LATOUR: I agree.

[PETER]: And one request for this. This is addressing TLD registries for the most part here, but you've also brought the registrars into play. I might have missed that point, but it's important to talk to the ISPs as well – and to enterprises. If that could be included there. We've done that in part. It is also watch who your validating resolvers are and go talk to them. That would involve the operational side on the registry side as well, like for DNS operative side. That helps a lot knowing who your consumers on the DNSSEC side are. Thank you.

JACQUES LATOUR: Okay, thanks. I just updated my slide, so the next one will be there. Okay?

[PETER]: You won't regret that. Thank you.

JACQUES LATOUR: Okay. Next slide. The sponsors of the Luncheon date, thank you. It was a great lunch, probably better than the free stuff. Yes. Afilias, CIRA, Dyn, SIDN. We're looking for sponsors for the next DNSSEC workshop. You can e-mail Dan, york@isoc.org. Then if you're willing to contribute, we always need more people. You get a great lunch, but sponsors help for that. Next slide.

ICANN, the DNSSEC workshop is organized by SSAC and the ISOC Deploy360 Programme. Just so you know, when we have lots of time, but we actually meet on a weekly basis to plan this meeting. We have a planning committee and then we spend a lot of time talking about this. We'll do a lesson learned after this meeting, so it's not just an ad hoc thing that happens. There's a lot of planning and work on the backend from the planning committee. That's how we generate great content like this. So thank you, all. Next slide.

Thank you. Those are links and tools to help you with DNSSEC. That's it. Thank you.

[END OF TRANSCRIPTION]