BUENOS AIRES – DNSSEC Workshop
Wednesday, June 24, 2015 – 09:00 to 15:15
ICANN – Buenos Aires, Argentina

JULIE HEDLUND: …panel, the regional panel is welcome to come up now, because we'll start with a short introduction by Dan York, and then we'll immediately go into our first panel. So you're welcome to come up. And we do have all of your presentations all set and ready to go.

So welcome, everyone. Please take a seat. And I must apologize for the seating arrangement. It's not as ideal for the workshop, but it will come in quite handy when we have lunch in the room. So that part is good. Anyway, thanks, everyone.

DAN YORK: Perfect, all right, there is an on/off switch. So I think we're ready to get going, right? We're at the time. We should start. And we're all good with remote?

JULIE HEDLUND: We're all good with remote.

DAN YORK: All right. So welcome. Good morning. My name is Dan York, and I'll be beginning this presentation. First of all, thank you all for coming to this DNSSEC workshop and our unusual configuration for the room

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

here. We did have a breakfast meeting in here before, which is why we're set up this way.

So let's begin with talking a little bit about what's going to happen today. But first, we do need to say a round of congratulations to the great folks at .AR, who were signing .AR just last week.

So where are the .AR folks? Oh, here's Luciano, okay. Where are some of the other folks who are here? Come on, you guys, stand up for a minute here, you know?

As somebody creating the DNSSEC maps, it's always kind of cool when you get a large country to sign like this, because all of a sudden a lot of the map looks green, which is neat. Anyway, congratulations to NIC.AR. And we're looking forward to seeing more of that deployment happen on that.

So this workshop is brought to you by a Program Committee that consists of a number of folks. Actually, Program Committee members, could you just stand up for a minute to be recognized, as far as the folks who are here? Okay, we've got a couple here. All right. Good, all right. The folks that are here are part of the team that puts this together. We are always looking for new presentations and new things that are there. So you guys can sit down again. Thank you. But Russ, there's Xiaodong, Yoshiro, Jacques. All right. And we have a number of other folks who participate at different times, as well.

We also have five sponsors, who we need to thank for the lunch that we're going to have, because we will be bringing in lunch into this

room here, and they are Afilias, CIRA, Dyn, .SE, and SIDN. And are our sponsor folks here? I see Christian, all right, and Jacques. All right. [Jim] is probably in the SSAC stuff.

So we want to thank these sponsors for lunch. So let's thank them right now.

I also note on here, [Anne-Marie] let me know that .SE, after being a sponsor of these for ten years, has decided that they'd like to pass that on to somebody else. So if anybody else would be interested in helping sponsor this for next year, we'll be looking for somebody to join the ranks of the other four that are up here. So please talk to me if you're interested. It's a good deal, and it helps make people in the DNSSEC community happy. So it's a good thing.

The implementers' gathering that we had on Monday night, how many people were there? All right. We have a nice picture here to show some of you. It was hosted by CIRA, NIC.AR, and SIDN. We have this ongoing two questions.

One is who can sponsor the gathering at the next event? Because we will need some sponsors for that. So if you're interested in that, what we're typically looking for are some folks who can find a restaurant or pub and do that.

The other question we have is we've been to Irish pubs now in Singapore and Buenos Aires. So what do we do when we go to Dublin? Do we continue and find another Irish pub there, or do we find an Asian fusion place or something? I don't know.

UNIDENTIFIED MALE: Moroccan.

UNIDENTIFIED MALE: Mexican.

DAN YORK: What?

UNIDENTIFIED MALE: Moroccan.

DAN YORK: Moroccan, yes, that would be appropriate. You know, we need to do that. So is somebody would like to step forward and help sponsor this, they can help figure out the restaurant.

Anyway, thank you to CIRA, NIC.AR, and SIDN for doing that.

This workshop is a program that is organized between the Security and Stability Advisory Committee, of which we have a good number of members in this room, as well as the Internet Society Deploy360 Programme, which employs me and some other folks to be part of that.

You've all got the program there. I think we've got a great session of things this morning. We'll begin with our panel, obviously talking about DNSSEC in Latin America. Then we'll have Ed Lewis coming up

and talking a bit about the root key rollover. Yes, Ed wakes up. What? What? Root key rollover, yes, that one.

Then we've got a panel on DNSSEC automation. And one of the ongoing questions we have is how do we make it easier to do signing and how to do pieces? And we've got some folks who will be talking about that.

Also, we're bringing back The Great DNSSEC Quiz. You've seen your forms on here. We have to give a special shout-out to Paul Wouters, which is right here in front of me. Okay. So Paul took on the quizmaster role this time. And so we'll see how we do with whatever Paul throws at us.

We have lunch, obviously, in here. And then after that, we're going to have a number of presentations around some new innovations with DANE and some new ways to do some cool things with e-mail and OpenPGP and other different kinds of stuff.

And I'm going to wrap up with a session about deploying new DNSSEC algorithms, both some of the challenges we've seen and pieces with that.

So that's a bit about what we're doing today. Let me just quickly run through some of our counts and the pieces that we have. If you've looked at Geoff Huston's APNIC graph lately for the rise of DNSSEC validation globally, we're up at about at about 14% of all DNS resolvers around the world currently validating DNSSEC. And that's the count we're seeing from him. It's obviously significantly higher. If

you go down the statistics on the page, you can find that some countries are up at 70-80% of all DNS queries coming out of that region being validated. And others are obviously less. But it's good to see that continued ongoing rise, and we'll need to look at how we continue to move that on.

Yeah, here was an interesting – if you've not seen his stats, if you look down this, you'll see that some of the regions are quite high, DNSSEC validation seeing 30% in Eastern Africa, 28% in Southern Africa. Now, Geoff also includes sample sizes, some of these. There's a column on here on using Google Public DNS. There are some countries that have 80-90% measurement of DNSSEC validation. But when you dig closer, you find it's because the ISPs in that country have basically sent all their DNS out to Google for their Public DNS. So it's some interesting stats that Geoff has in there to go and take a look at.

Some of the top countries. Again, you can see some in here. Again, this is what I mentioned, like Saint Pierre has 89% validation, but 99% of those are using Google's. But the other ones, if you look down a little bit further, like Mayotte in Eastern Africa, they're doing 84% validation. Only 4.5% of that is from Google. So what that means is that the rest of that is going through the local ISPs, which is great to see. And it's ideally what we want to see, is a lot of local ISPs doing the validation.

Rick Lamb continues to provide a nice tracking tool for the rise of the signing of TLDs. And this one shows that continuing chart going up,

where we're now at about 82% of all TLDs being signed. A lot of that, obviously, is the new gTLDs that are providing that huge rise in there.

So looking at those numbers, right now, as of June 19th, we had a total of 788 signed domains out of the total of 968 that we're tracking through this measurement.

Let's look at a couple of maps that we've seen here. Overall, this is what we look at, like today. There's an awful lot of green out there, which is awesome to see.

Diving into the picture a little bit deeper, here's what Africa is currently looking like. Here's Asia-Pacific. In Europe, we had one change since the last time, which was that Hungary signed. They're .HU.

And then in Latin America, woo-hoo, we've had two in this last bit. We have the Cayman Islands folks – yay, over there, okay – who told me that they went to the last DNSSEC workshop in Singapore and went back and signed it after that. So, all right, let's hear it for Cayman Islands!

And we already mentioned the folks at Argentina. Thank you guys for doing that. Let's look on from here.

And North America is North America.

All right, DNSSEC maps, we know this. Let's go on here.

I want to mention, there's two more sites that are now providing domain stats on the next level. Because, obviously, TLDs, it's great,

but we really want to know what's happening at the second-level domains.

One, Rick Lamb's site that we mentioned earlier has put a column on there for the signed versus the total. And you can go in there and find out the number in there, and you can see that.

The other, also, the folks at nTLDStats, which provides statistics around the new gTLDs, have put up a page on DNSSEC, although when I looked yesterday, it was broken. But anyway, that should have some stats on there for what's going with the new gTLDs.

Some nice percentages that are here. If you look at these, 43% of .NL, 62% – I think it's actually 65 % now – of .CZ. Some other different statistics that are down here. This is from Rick's site. Great to see this kind of growth that's going on inside of there.

It doesn't include all the TLDs. It's only the ones that Rick can get statistics from. We're missing some, like .gov, which is 88% signed right now. And Norway just recently launched DNSSEC, and in a couple months, they're now at about 50% of all .NO domains.

This was what the other one looks like.

Two other quick items. We started to put together a little event calendar of DNSSEC/DANE-related events on the DNSSEC-deployment.org site. And so there is an event calendar that we have up there. If you've got events that are related to that, which could be conferences, it could be items, or it could be webinars. We're open to

putting whatever. This is generally meant to be a place to promote stuff that's happening with DNSSEC.

And I want to mention one specific event, which is that at IETF 93 in Prague, there is a hack-a-thon on the weekend before that, where people are working on different tools and projects, and a couple of us are going to be there and going to be looking at ways to work on DNSSEC and DANE-related tools. So if you're interested, you can follow these links. This slide deck is up on the webpage to go and do that.

So I think that's all I'm really going to mention. The DNSSEC History Project is around. We're always looking for people to help contribute to that.

And I want to just end with two quick notes. We do have remote presenters. And so we would ask, when you come to the microphones and ask questions, to please state your name. Also, if you would speak a little bit slower, in terms of as I'm trying to speak. I'm trying to speak slowly. We do have translation happening over here. And for the sake of our translators, we need to help them and not speak super-fast, like this.

Anyway, that's all I have. I'm going to turn it now over. Oh, Julie's got something else.

JULIE HEDLUND: I just want to note, you have a program. If you turn that over, there's a ticket. And that ticket is your ticket to lunch. Now, if you stay in the

room constantly, all the way up to lunch, your prize is that you don't have to show a ticket. You'll be here. But if you leave the room, take your ticket with you, because there'll be someone at the door checking tickets. And I'll be there too, but I may not always recognize all of you. So have your ticket with you if you want to have some lunch.

DAN YORK: All right. And thank you all for being here. And please do feel free to ask questions, raise questions. And also, I will say too, as you go through the day and you're hearing these presentations, if you think about an idea you will have, if you've got an idea for, "Oh, I can do a lesson learned like that," something like that, we'll be looking for submissions for the Dublin event soon after this. Within the next couple of weeks, we'll put out the call for papers on that. So please do think about how you might like to contribute and be part of this session in Dublin. Thank you.

JULIE HEDLUND: Thank you very much, Dan. And we will move now to our first panel. Let me then turn things over to Luciano Minuchin, from NIC.AR, who will be moderating the panel. Thank you very much, Luciano.

LUCIANO MINUCHIN: Hi for everyone. Thank you for this invitation, surely. Sorry for my English. This is a Latin American panel, and we speak in Spanish. If you vote for the headset, go ahead.

Good morning, ladies and gentlemen. We intended to have this presentation commenting what Dan was talking to you about the signature of DNSSEC of NIC Argentina. It was a great challenge that we had set for us. And perhaps we will not give so many technical specifications. Most of you are specialists. But we wanted to share our experience with you, especially to encourage those who have not joined this world and how may use the experience we have, the lessons learned.

Many people in Latin America came over to ask me, so it is pretty fresh in our minds. We can tell you many details which can be useful.

I wanted to tell you the story about DNSSEC. In the last ICANN in Buenos Aires, after that, we made the decision to sign the DNSSEC. Other projects that were overlapped delay the signature. So it was a bit delayed. But we had it in our minds.

In December 2014, there was a chance to hold ICANN in Buenos Aires again. That was a major trigger for us, was set an objective for us to do it. We knew there were a few months. Many people had told us that it takes quite some time to do it. But the reality is that we took on the challenge and move forward. The deadline was this ICANN, right? So we got there pretty tight. We managed to sign last week.

In January, what we did was to update our master servers in our areas so that all can respond to DNSSEC questions. Definitions were made about times, keys, architecture, equipment, and algorithms.

In February, we put together the DPS document, which was quite a challenge and took so many meetings. But with that definition, we managed to move forward.

In March, we held many ceremonies. There were many issues.

In April, we had more ceremonies, more failures, more setups. That was a kind of growth for us.

In May, after this number of trials and tests, there were definition of dates, sizes, keys, architecture, hardware, and algorithms. We had so many ceremonies, ceremonies, ceremonies – over 20, I think – testing to fine-tune the process of the scripts and the ceremonies.

And on June the 8th we had the first Offline Keys Ceremony Generation for the full ceremony. And June 18th, we took the DSs to IANA. And in 48 hours, we went on to production. The process with the IANA people was pretty happy and fast.

Overall, the total project time was five months. But we can say that the full dedication time was the last two months. We invested all the team time full time to achieve the signature. So we want to support people who have not yet done it to go for it. It's dedication. It's time. And I think that two months is a nice time to do it.

Here, we say a bit what we used for the key generation. We used TPM technology, the RSA256 algorithm, KSK 4K and ZSK 2K keys. We had RAM storage for action. The hard disks were encrypted. Then everything was taken from the RAM to pen drives and encrypted with PGP. That was part of the process.

Then we built the automated sign zones. This was done, dedicated redundant hardware with BIND 9.9.7, with NSEC 3 OPT-OUT. And then we transferred to other services with TSIG.

The ZSK signing with KSK was done offline, a whole ceremony. That was one of the issues that came up at the beginning, to do it on or offline. We decided to go offline to actually preserve the keys. We have the zone signing with ZSK with KSK. Then the KSK was stored completely offline on dedicated hardware and then secured.

The ZSK in online computer with the [RR] sets, only operational keys were in the hardware. We rolled out previous testing keys. Once the area was checked, there were the reloads and notified to the zone DNS servers, the master servers. And as we said, the master to slave transfer used TSIG.

This is small distribution and classic format that many have. We added the jumps where you check the zone. We have a zone [verificator] before and after the signature, where we check different elements. What we added was the format to upload the DSS. Right now, it is direct with us by providing us the [inaudible] we have are ours, be can sign third-party domains. We will do it on a person-to-person or encrypted email. But we are working already for people to be able to upload their signatures to the application.

An important topic that use was the physical safety of the keys. We used duplicated pen drives encrypted with PGP. We used security [bags] with bank specifications in case they had been altered. We could check by watching them, because they bore indication saying

that they had been opened. A safe with double door and double security system. At the place where the safe is and at one of the buildings where the safe is with the key, we have double closed-circuit video. We have three access controls with magnetic doors, and we have federal police in the access control and in the cameras.

Finally, we managed to achieve our mission. It was hard for me to do this slide, because [ZZET] plugin was not working well for Chrome. We managed to make it work on the Internet Explorer. Quite weird, but it worked.

What are our new challenges? We wanted to see, now that we had signed, what we are going to do with the DNSSEC. We believe it may be important to [find active] momentum at government, since we are part of the national government, with a main objective to make government agencies have DNSSEC signature. We believe it's an important objective and one of our main challenges.

We are also analyzing to do it with financial institutions and transactional WEBs.

Another of the tasks we are doing is working with small and medium ISPs to help them with DNSSEC and seeing if we need to help them understanding how it works and with their signatures.

We're also working on key monitoring tools to have automatic control of expirations and an alerts system.

We are thinking of signing new zones. We were working with the .AR zone, but we are analyzing whether we are going to move forward

with the rest of the zones that we are using: .gov, .com, .net, all the others we have.

We're also thinking whether we're going to change any signature format, whether we're going to HSM. Or we may do a modification. Yesterday, we had a meeting with Richard Lamb and he gave us some smart cards, which we were not able to get here. Maybe next week we'll start testing those cards.

Thank you for listening to my presentation.

UNIDENTIFIED SPEAKER: We will now move to the rest of the panel. We will start with Diego Espinoza, who is consultant from Costa Rica. He will tell us about the activities of DNSSEC in Latin America.

LUIS DIEGO ESPINOZA: We will be all speaking Spanish then. Keep your headphones.

Good morning. I am no longer related to a ccTLD, but I have been for many years. So I still feel the commitment to continue to collaborate in whatever I can and help in whatever I can.

What is my experience in this case with DNSSEC? Continuing with the LACTLD workshops in September 2011, I went to a workshop in Santiago, Chile, where a key ceremony was held. It's important to take note of the dates, because this is something I want to highlight. It's taken a lot of time to get this going.

In September 2012, a year later, I was at a workshop in St. Maarten, contributing to the DNSSEC signature process, then in Paraguay. That is where I met some of the guys of .AR and others from the region.

At all those workshops, the issue of DNSSEC, which was the main thing, there was a ceremony process, a signature process, so that everybody should leave with all the intended tools they needed to go sign their ccTLD .This didn't happen all the times.

LACNIC, on the other hand, also wanted to promote DNSSEC. At least my involvement in Medellin, Colombia, in 2013 in May, and later in Curacao in October 2013 at DNSSEC workshops.

In March 2012, .CR signed with DNSSEC. Then I was in charge of .CR. It was something motivated by the meeting held in Costa Rica. We needed a little running to make it for the ICANN meeting, and we managed to do it. We wanted to go little further, and we managed the most important bank of the country to post their website, which was under .fi.cr, which was the zone for financial sector, to obtain a signature with DNSSEC. And we have maintained it so far, something that I find pretty good. They've kept it.

At the ICANN meetings, we've been talking about DNSSEC for years, many years. I have mentioned it because it's been many meetings.

Here I wanted to highlight the countries in the region we have DNSSEC operational. Why am I considering the operational DNSSEC? The ultimate goal of DNSSEC, although, it is a playground which is very

nice for [digs]. In fact, its purpose is to make a better Internet, to increase the users of the Internet security.

So having a TLDS as a TLD be signed is not sufficient. We need to have all the sites signed, all the websites that people access to. Why? So that that name resolution will be protected with a signature.

So where are we at this point? Nine out of 22 countries in Latin America have signed and are operational with DNSSEC: Brazil, Chile, Puerto Rico, Honduras, Colombia, Costa Rica, South Georgia and the South Sandwich Islands, Trinidad & Tobago, and the Saint Martin Island.

But beside that, even those countries where it is operational, the percentage of sites that have signed is small. In many cases, the names are experimental. In fact, they are not a transactional name.

At the Costa Rica meeting, some people from .CR came and asked me, "How did you manage a bank to make its transactional website signed with DNSSEC?" Well, we managed to convince the chief security officer, not the chief technology officer that it was important to have DNSSEC operational. And he embraced the issue.

What this means to me is that besides the fact that some banks already have DNSSEC, they are not using in their transactional website. In the case of Costa Rica, I can tell you, only the national bank (BNCR) has signed DNSSEC, because the others, their DNS name for the transactional website is a .com. This is something that is maybe

uncomfortable, but it's the reality. And in the end, the end user is not receiving the protection that we want to achieve with DNSSEC.

So what I want to discuss, it's something I just want to state, and we may discuss it a little, is there's still a long way to go, not only in Latin America, but in particular in Latin America. There's still a long way to go to achieve our commitment to obtain a better Internet, protecting the names with DNSSEC.

Some of the elements I would like to leave you and the reasons why I believe that DNSSEC hasn't been deployed completely may be elements which are reasons are for deployment. Why hasn't DNSSEC been deployed in the same manner as SSL? Maybe there's awareness about the security impact of DNSSEC. Maybe there is lack of this awareness about its security.

Or maybe at the time of evaluating impact versus cost, some people believe it's quite complicated, quite costly, and maybe the impact is not enough. Or maybe complexity versus the benefit obtained. It's relatively complex to implement DNSSEC. And not only implementing it; it's complex to maintain it. Many tech people know about this.

Lack of technical skills, I don't know. I know many of the persons in charge of ccTLDs. I know there is lot of technical skills there. But is there enough technical skills among the clients?

Marketing interest, I'm going to be honest here. One of the reasons why .CR signed before ICANN meeting is because of marketing interest. I want to be honest. They said, "We wanted to show that

we're signed." And that's marketing interest. There was one further motivation. It worked.

Or political decisions. Sometimes administrative or managerial aspect of ccTLDs, or those who manage the Internet, do not make the decision for that to be implemented. I would like to discuss this with you at some point.

I'm going to leave my other colleagues continue.

LUCIANO MINUCHIN: Another speaker will discuss with Diego about his presentation later. We'll now move to the presentation by Carlos Martinez on the DNSSEC in the reverse tree at LACNIC.

Carlos Martinez, thank you for your presentation.

CARLOS MARTINEZ: [inaudible] the wrong presentations all the time.

Don't worry, I will be speaking in Spanish. This presentation, for those of you who were at the workshop 2013 ICANN meeting, will you find it familiar. I did it as a continuation to my presentation back then to highlight what my colleagues that preceded me said before. This is a work in process in which we learn as we progress.

I'm not going to tell you why it is necessary. We signed the root in the 2010, and it's important. It's the moment to take advantage of the signed root.

To talk about the timeline, what was the process like for the signature? It took us about two years since a decision was made to sign the reverse zones of LACNIC until we managed to achieve it.

For those of you who are not aware about LACNIC, you may have heard of LACNIC. It's the registry of addresses for Latin American and the Caribbean. We have the role of assigning IPv4 and IPv6 for Latin America and the Caribbean. Among the associated services we need to provide, one of them is being on the road to reverse zones. Once you make a query, in the case of IPv4, it becomes [inaudible].

For example, LACNIC has administration of 200/8. When you do queries for an IP address within this block, one of the intermediate zones through which you need to go with 200. Those associated to the /8, the servers that are authoritative for that zone are LACNIC servers.

When I talk about LACNIC reverse zone signature, I'm talking about those zones that we call the large zones. For IPv6, something similar happens, although it's more difficult to say it because it's a bit more burdensome.

What is the current situation? We have the large zones signed from almost two years now. The good news is that we haven't had major problems. We've had some hardware failures at one server. Once the software made the mistake, and there was two minor events in two years. So I think it's quite successful.

Interestingly, those events were never seen in the outside because the configuration of the system caused there to exist some time so that this was not seen by the public, by clients.

Our pending activity is to start accepting DS records for LACNIC reverse zones. We are doing it, in fact, in an experimental manner consisting of somebody coming to talk to me and bringing their DSs, at least signed with PGP.

We have had some experimental situations in that scenario. What I can tell you today is that in these days, we're completing a modification of the LACNIC registry where we're going to try a method in which instead of you uploading your [inaudible] the LACNIC record system will checking the delegations all the time to reflect them on the WHOIS, if it exists.

Part of this check is going to be whether if the root zone you've delegated, there is a DNS key record. If there is, it will suggest you generate a DS based on that and to load it on the reverse zone. You will need to enter the system and check the self-generated DSs, and that will be reflected on the reverse zones. The idea is that it should be quite simple, going from having a reverse zone signed to having all the chain signed.

This is the architecture of the signer. This is quite typical. Although this came, the icons are different, it's quite similar to what Luciano showed before. There's a zone supply system, which are called the LACNIC record. The computer sends to the master servers through walls, so through a [dance] of copy signature and transfer zones.

In association with this, the presentation I made in 2013, I remember I told you how we had made that computer, what is called the then signer. The first version of that computer was quite low budget, which led me to think that it might be interesting to propose architectures or mechanisms to sign zones for smaller zones or with organizations with lower budgets. Not everybody is a ccTLD. Not everybody has the same resources of a large ccTLD. I believe there is a need to propose good signature mechanisms for organizations with lower needs.

When I put together this presentation in December 2013, I offered the audience the document with the recipe for the construction of the server. And some people came over to tell me that they had implemented it. As a way to provide an extra edge to this, what was the most expensive link in that recipe, so to call it, they needed a physical hardware.

What I tried to do, I tried to do away with a dedicated hardware requirement. So the question was what happens if we sign in a virtual machine in the cloud? Does it work? How hard is it? Does it work properly?

The responses that I could show you, if I could, I have a virtual machine in a cloud server that is signing areas. And what I can share with you all is a script that [bears] that machine. Effortless. With a technology that's called Docker, that you may heard of to build virtual or [container] machines, the machine signs areas quite quickly. It's not for large areas, of course. But for smaller zones, for reverse and even direct zones that are small, it works very well.

There you have the [areas was] signing with that machine. It's called secure.xt6.us. I don't' want to create any confusion. If you look for that area, you will find records called A, B, C. All of them have fortune cookies.

The interesting thing about it is that it's signed with a hidden signature machine in the cloud. It costs $30 a month, more or less. And those who want to set up something just like that can do it in half an hour. I think it's an interesting way to give smaller and smaller organizations the possibility of signing.

It's not accepting for some issues. Someone can say, "I'm leaving my keys at a data center. That's not under my control." I have two answers for that. Not everybody has the same adversaries. Smaller organizations have other types of risk. They are more exposed to the operational risks, rather than the dedicated [foe] trying to use their signatures.

But there's a lot to be won if you do it in a way that you can maintain. You help with the operational risk. And if there is any concern of the keys being in a place that's not under my control, you can rotate them more often.

So wrapping up, I go back to what I said in 2013. If you are interested in these low-cost signing formats, just talk to me after the panel. Thank you.

LUCIANO MINUCHIN: Thank you, Carlos. Now we will go to Gonzalo Romero from [.CO]. He will talk about his experiences and challenges in DNSSEC.

GONZALO ROMERO: Good morning, everybody. Thank you very much, Julie and the DNSSEC Committee, for bringing me the opportunity to be here. I'm going to talk in Spanish, so keep your headphones.

Good morning, ladies and gentlemen. Thanks to Julie and the DNSSEC Committee for giving me the change to share my experiences and challenges for the Colombian domain.

In this ten minutes, I would like to share with you the experience of the technical deployment in relation to the awareness strategy in DNSSEC, the status of the domain signature, and the number of domains signed and the DUM, the challenges to increase the number; and finally, a number of questions and answers if that is the case.

At the end of 2010, we had a chance to be involved in ICANN 45 in Cartagena, Colombia. We were receiving the administration of the domain as .CO Internet and ran an exercise of publication, disposition, and attitude to sign that in ICANN. The exercise was based on the American-based domains, and three months later, in March, we ran the press release saying that the .CO was ready for DNSSEC.

The policies are there. KSK 2.048 rolled over annually, and 1.024 ZSK renewed monthly. The signatures are generated by RSA and SHA-256 and they are refreshed monthly. We have NSEC and NSEC3 capacities. We have no restrictions on transfers. Our WHOIS indicates when the

domain is signed or not, and we do not require certification from registrars. The DS records are submitted via EPP updates.

Between 2013-14, we had the EPP implementation update to migrate from the secDNS-1.0 (RFC-4310) to secDNS-1.1, associated to RFC-5910. All the information associated to the technical deployment of the Colombian domain can be found in the website.

What have we done in relation to awareness, especially in our country? In 2011 to 2013, we had a number of annual events associated to technology and security in the DNS. We were able to share with Internet Society people, with ICANN, LACNIC, LACTLD DNSSEC subject and also security, stability, and resiliency in the DNS.

Based on those events, we build the CO-DNS virtual community that we are still disseminating. Any of you can become a member. We also have a blog associated to the .CO domain, how to sign a domain in the area, if you want to.

Currently, we are engaged in this type of activity working with the government so that requirements from the technical standpoint can be added to governmental contracts and requests for proposals of a higher level technical associated to information.

With the national SCR, we had issues with the WHOIS identity, and we would like to sign the military and governmental areas. We want to work also with the Academy to sign the domains associated to the high-speed network called RENATA in Colombia. It's 200 members.

And of course, we're supporting local ISPs so that recursive resolution services can be provided and to have the possibility of having the signature services to the DNS customers of their areas.

We are also supporting National Banking Association interest, that have showed their interest in the .bank domain. I believe it would help a lot, the DNSSEC, because it's assigned [inaudible].. I think that as front to the sunrise process is over, with 700 organizations expected the domain. I think it's a major leverage for ccTLDs to be able to use it, because there is some good noise as to the subject that we can use the ccTLDs in the region. We are also signed and we can provide advantages in security.

In line with Luis, that is our status. We wanted to share with you this rather complex scenario we have been following through the different ICANNs. In February 2012, we have 1.2 million domains; 59 were signed only. Before ICANN 46 in China, of the 1.5 million domains, we have 139 signed. In 2013, before ICANN 48 in Argentina, we had 200 domains out of 1.6 million. And before this ICANN, again in Argentina, we only have 150 out of 1.8 million.

When we asked these 150 domains that have signed their domains in relation to DNSSEC, none of them are banks or financial institutions. All of them are experimental. They tell us that actually they did it because it's a bundle of the registrar. It's a DNS security matter. A few of them have identified or seen this as a reactive solution to a website compromise, and many of them don't even know what this DNSSEC

means. No registrants surveyed said they signed by themselves without promotion or support of a registrar.

Challenges, it would seem it's an issue of cooperation and collaboration about multiple stakeholders in the security, safety, and resiliency of the system. It seems that there would be a need of the relevant players – registry, ISPs, the CERTs, Academy, government and private sector – even will need [same series] of growth.

There is a security issue in the public sector as well and you see better and better practices in stability, security, and resiliency. And, of course, the knowledge associated to domain names industry is growing.

Now we're talking about Colombia, of our own security. There are more awareness, and there are more incident reports that can support developments in security and we must make the best of a public strategy in cyber-defense that has five years.

Now talking about automation. That will be discussed today. I believe are very important for the growth of DNSSEC. I also believe that such as IPv6 is quite relevant for the structure of the development of Internet. Things such as DNSSEC and DANE are required to preserve DNS security, safety, and resiliency. Thank you.

LUCIANO MINUCHIN: Thank you, Gonzalo, for the presentation. The coordinator now. Now we will pass the floor to Rubens Kuhl – I don't know whether I have pronounced it properly – of .BR.

RUBENS KUHL: [inaudible] headphones. And more people need to go to headphones now, as this presentation will be done in Portuguese. And there are probably two or three Portuguese speakers in the room, so. Next slide, please.

Good morning, everybody. I came to tell you about the operational experience of .BR with DNSSEC. And you will see that this presentation will touch upon two other items strongly approached by this DNSSEC meeting: automation and DANE.

We will start back in 2007, when we signed .BR for the first time, even using [DLBs]. We didn't have any root sign, and we started with a small number of second-level zones. In the case of .BR, the records are in the second level. And so the categories there – .com, .BR, etc. – they find [that are] a registrant we are dealing with.

In the small areas, we have two where it was mandatory to use DNSSEC. One of them was the judiciary that became quite used, actually. Any citizen today that needs judiciary information can resort to this domain that is DNSSEC signed.

So we have a second-level zone for banks where only banks can have their safe haven, and it also demands DNSSEC. But they have never used it even. They continue to use .com, .BR, even when there is registry category with those restricted characteristics.

In 2009, we signed the large zones. Millions of domains were .BR. These zones were signed thanks to the NSEC3 technology.

Up to 2010, we still had the signatures with the keys directly stored in the computers. And as from 2010, we started using HSMs. When the key was added to the IANA root, this happened when the key generated in the HSMs, which is only in the hands of the HSMs, and so we went on for domains. Then the necessary domains signed. And in 2010 we started DNSSEC hosting for limited-sized zones, which supported increasing the number of zones signed with DNSSEC.

A DNSSEC policy specified that we would have a KSK rollover between two and five years. This happened up to 2014-15. But actually, the rollover is still going on. This key continues to use our site, and even when the DNS uses key 256. And now we are using KSK and ZSK, with the size on the screen.

This rollover started without any issue, even when there was actual sign. There is a kind of risk depending on the understanding of the use. Actually, it did not create any issue, at least that we have seen. The rollover will be completed in July, in a few days.

By looking at social networks and others about DNSSEC, we can see that there are a number of comments on scalability, whether it's scalable or not, if it cause any problems or not. And what we want to show is transparently things to do second-level zones in .BR that use DNSSEC.

The machine is simple. It has four-core processer, four gig of RAM, and a single machine does the backend zone editing, key generation. There is one key for each zone. And today, this feeds 700K zones

signed with DNSSEC and creates zone transfer to 12 authorized servers that respond for all of those zones.

The software that we use is available in the public domain, open code, open license. It may be downloaded from this URL to enable the automation of all zones. If somebody needs a large number of zones signed with DNSSEC, have an availability of public domain software. The software we use is exactly the same that is published here.

Besides, this year we started doing [DUM] experiences with DANE and to make it available for users. In Brazil, we hold meetings of operators, which are similar to the operators' meetings, as [RIPE] explained. And we launched a wizard that auto-generates TLSA records. This wizard obtains from servers both HTTPS and SMTP, the keys, calculates the regions and generates automatically TLSA regions for the users. We initially launched with HTTPS, and then we started even using for e-mail and for other [particle] processes.

We are moving forward. Users are more ready to use these processes, and this is advancing rapidly. Many people don't like the idea of validating keys with DNSSEC.

This is what I wanted to tell you about our experience. In .BR, we have a large percentage of regions signed with DNSSEC. Over 600,000 out of 4 million. We believe that much of this happens based on the availability of users. If users want simple things to solve problems, we also want to solve the users' problems. We want to bring DNSSEC to users. This is an important benefit. And what we need to give users is

simplicity. We believe that we are growing and we have good figures, but we want to continue growing. Thank you.

LUCIANO MINUCHIN: Thank you, Rubens. We will now move to the presentation by Hugo Salgado, from NIC Chile, who will give us an update of the status in his country.

HUGO SALGADO: Good morning. We would like to present our status. We signed in 2012. We presented at the ICANN meetings our experience. We would like to update the situation.

NIC Chile is part of the University of Chile, which is the largest public university in the country. So far, we are the only registry and registrar available for .CL domains. We are in the process of launching registrars within our scheme. We had a large redesign in 2013 of the registry and domain management architecture. We implemented [DPP]. So now we are ready to launch the registers. We have almost half a million domains. An important part of the redesign in 2013 is that now almost anyone can register .CL, not only Chilean nationals.

As I was telling you, since 2011, we've signed .CL in full production. We started two or three years before doing tests and development. Due to the lack of tools then, much was done internally, and we have [quite] in-house solutions for signature.

For NIC.CL, we had more flexibility in doing changes. We did OpenDNSSEC a couple of years ago, which we used for the signature of .CL. Those are the [NS for .CL]. We used it for reverse and for other zones, small zones that are internal to our operation.

Also, we were in conversations with people from the Ministry of Finance of Chile, which wanted to sign with DNSSEC and promote it for national banks. Some meetings were held. There's a work panel there. And so far, no bank has signed, but we are working on it. And there is local interest.

An important issue is that the largest ISP, from the point of view of residences, in the country, what is called VTR cable/ISP, activated validation last year. This gave us in the statistics, such as APNIC, to be the country that did more validations in proportion to its population. It was something very interesting, because they did it on their own and [inaudible]. People who did it to tell their experience to the people who were working in validation. They were at LACNIC presenting their experience.

Another task in the research area, we have a laboratory which includes NIC Chile and part of the university, did an important work on distributed signatures. This has been presented at ICANN and at DNS-OARC.

This is interesting, because normally there is key distribution. You can segregate private KSK. But the laboratory separated the signature. So normally the private key is divided into different players. They can take them to their own sites or infrastructures nd they sign the zone

separately so that you never need the ceremony of getting the keys together. That signature can be distributed securely and remotely, and it can be mixed. It enables a group of [in chunks], you can have a minor number, and they can vote to detect whether there is fraud. A mathematical paper from the beginning of the year 2000, and this is in the prototypes phase, has been implemented.

Besides this, talks and classes have been given at universities, following invitations we received to speak about what DNSSEC is.

At the regional level, we've always been interested in participating as much as possible, telling our experience, helping in whatever we can.

Some of the ideas that came up from the LACTLD courses were having monitoring of signatures so that people could receive warnings by e-mail when their signatures were running the risk of expiring.

There was an idea given at one LACTLD workshop. Thanks to the work of Rafael Dantas from .BR. They have a monitor operating, and receives a list of domains and it's checking them regularly to check that everything's fine.

Besides, at the community level, there were several talks and presentations on the distributed signature work by the lab. We are helping other ccTLDs, in terms of delivering DPSs and collaborating via private e-mail. And at different conferences, we share scripts and we help with our experience.

There's also support work. LACTLD is hosting an e-learning course by the end of the year, given by Richard Lamb. We were helping on the agenda for the course and the content, based on our experience.

Finally, I'm part of the Program Committee for the Tec@LACTLD, held once a year. I'm in charge of the track for DNSSEC. We have had a lot of local involvement, and the whole experience helps. The people from .AR have been invited also to tell us about their experience. This is going to be held in August in Santiago, Chile.

What's next? This is news we are breaking to you. DNSSEC is signing a new primary DNS service, which we hadn't so far, and we have a local demand from our local communities.

From 2002-2003, we have provided a secondary level, which was free of charge, to improve the robustness of national Internet. But now we are going to give a primary service also. That's going to be signed with DNSSEC. We believe it's going to be a huge leap, at least in number of domains.

To continue to improve our relationship with banking and the government, the Ministry of the Interior is very interested in this. We've had a lot of conversations and support for them to sign the whole government infrastructure. There are plans for them to require it at the level of all their departments.

Continue to [port] validation, which is the other side of the DNSSEC equation. Supporting the work that VTR has done, and supporting other large companies in the country to copy their experience. We

know we expect a lot from the authoritative part of DNSSEC, but the validation part, we believe that the experience that they have is important. So we are aimed in that direction.

The expiration monitor from .BR, I want to bring it to full production and deliver it as a service to the people from .CL who've already signed.

The other issue, distributed signature, we want to bring it to full production to have real data, because when this was presented at different events, the second questions is always, "How does it work in the real life?" So we want to have some certain test zones to collaborate with more data.

Finally, one item, something we have a doubt with our community, we need to give talks and conferences to promote this signature. This is something we had in our original roadmap. But all this changed thing, all the full system we did in 2013, required a lot work from our side. We are not such a big team. But now we are beginning to do awareness.

This is it. Thank you very much.

LUCIANO MINUCHIN: Thank you all very much for participating in this panel. I would like to thank Julie and the whole ICANN team for having the simultaneous translation service, which for us is very important.

JULIE HEDLUND: So at this point, I'm going to open it up for questions. We have at least ten minutes here. And, Luciano, I'll ask you to continue to moderate. But please, people, there's microphones here on each side on stands. And please do come up to the mic if you've got a question. I'll also encourage people in the chat room on Adobe Connect to ask questions.

ROBERT MARTIN-LEGENE: This is for Brazil. Oops, sorry. Have you had any feedback on the methodology you're using for storing and fetching certificates from user sites? Because what you're doing is you're going out there to get a certificate so others don't have to rely on the answer they are getting back themselves. I mean, at some point, you have a bootstrapping process in actually getting the certificate from the SMTP server and whatever they have, right?

RUBENS KUHL: The system by the domain registrant doing the change to the domain. So this is not an automatic tool. It's just an assistant so their hash information gets right. But the user still has to apply the configuration to that domain. So we don't have to rely on that information being correct or not if the user can validate it. So the user can look at the hash and say, "Oh, that looks right," or, "Let me see if it's right or not." But this not automatically updated to production configuration. It has to be in the user confirmation.

ROBERT MARTIN-LEGENE: And has anyone shot themself in the foot? Do you know about that? Maybe they changed the certificate on the mail server and suddenly things stopped working.

RUBENS KUHL: After 70 that did it, so far no one complained. But 70 is not a lot in 700,000 zones. But so far, no problems.

JULIE HEDLUND: Thank you. And could I just ask people to be sure to state your name and your affiliation when you ask a question? Thanks.

ROBERT MARTIN-LEGENE: Sorry, Julie. I'm Robert Martin, from Packet Clearing House.

DAN YORK: Dan York from the Internet Society. A couple of questions. One, I would just like to give thanks to the .BR folks for the TLSA tools. Those are great. There'd been another thread about how useful those are for generating the record. So thank you for that.

One question for Hugo. This Tec conference that you mentioned that had a DNSSEC track, I guess I would just say I'd love to hear more about that, if you want to send a message to one of the mailing lists or send it to me and I'll forward it. That's the kind of thing I'd love to put into this event calendar we're talking about to let people know. If

there is a DNSSEC track specifically, that it'd be great to know about that. So please feel free, yeah.

HUGO SALGADO: The problem is that they are closed conferences for the TLD community in the region. They are not for the public in general. They are closed meeting for TLDs, ccTLD for the region. We have invited people from outside. We do streaming. But for a question of logistics, I believe it's not possible to include people from outside.

Anyway, the presentations are public, and it's something that we are going to disclose better.

DAN YORK: I guess I would just say if they are public and if you're doing live streaming, we'd be delighted to put it up on the list so people could at least view it, even if they can't actually attend.

HUGO SALGADO: Okay, will do.

DAN YORK: And my other quick question was, Gonzalo, you mentioned that you'd seen a decline in the number of signed domains from two years ago to now. Have you had any understanding from some of the people who let it drop why?

GONZALO ROMERO: Yeah. To be honest, we haven't seen any progress on this. But I think I would like to answer you with some questions to these cues as well.

The Alexa.com has a list of the top-25 global websites and not a single one of those domains is signed. The Federal Financial Institution Examination Council has a list of large US financial institutions holding over 10 billion in assets. There are 104 domains on that list, and exactly one is signed.

The Federal Procurement Data System has a list of the top US defense contractors. There are 103 domains on that list, and not a single one is signed.

DDoSattackprotection.org has a list of computer security blogs and resources. There are 126 domains on that list, and only five are signed.

ICANN has a list of accredited registrars. There are 1,289 unique domains on that list, and only 16 are signed.

DAN YORK: Yes. That's coming out of a CircleID article that actually went up yesterday. And I actually replied back to that. It all depends on which stats you pick. The gentleman who's standing over there can talk to you about a large number of domains in his region that have been signed, as he's next to the mic.

So, yeah, I certainly agree with that. I was just more curious if there were any lessons that had come out of those who had stopped that. But I understand, from your perspective too, a lot of that was driving

by the registrars and DNS hosting operators. So the customers, themselves, may not have actually really had much involvement with that, yeah.

GONZALO ROMERO: Yeah, we are really concerned on that, as well.

DAN YORK: Yeah.

GONZALO ROMERO: Because I think that DNSSEC is part of the DNS security, stability, and resilience of the Internet. So this is a market strategy.

DAN YORK: Yep.

GONZALO ROMERO: We need to show an example, what were are doing. Not from the marketing perspective, but from the technical perspective as well.

DAN YORK: Yeah.

GONZALO ROMERO: So the security is like some kind of [inaudible] as example. And we need to show example. We need to show example from our technical

community here. So I would like to be more concerned in terms of our community to show more real numbers of what we are doing.

DAN YORK: Perfect. And I agree with you on that. I think we need to do a better job on that. And also, I think the key part is what we've heard here a number of times from you folks about the automation and the need to simplify it. And I think that's really key point that we have. But I'll turn it to Cristian.

CRISTIAN HESSELMAN: My name is Cristian Hesselman. I'm with SIN. We're the registry for .NL, the Netherlands. And as Dan already mentioned, we have quite a few signed domain names, 2.2 million at this point, so out of 5.4 million domain names in total. Our main problem though is that we have a large number of signed domain names, but there's hardly any ISPs to do the validation.

So I was actually very impressed by what you achieved in Chile, and I'm really curious to learn what you guys did to convince these ISPs to turn on validation, because we'd love to know.

HUGO SALGADO: We would love to know what we did, because actually it was just the other way around. They signed on their own, by their own motion. They changed their infrastructure a lot. They went from old machines, the typical things that are out there for ages doing DNS resolution.

They went to an internal Anycast cloud and started validation, because they saw it there and they went for it. It was not something planned. And that is good, because somehow it didn't have an impact on that.

That is the experience we wanted them to share with the rest of the ISPs. It was at that time that Global started validating and somehow they felt afraid of that. And I believe that right now this fear of being the first comer or doing something wrong should be done with. At the present time, in conversations with other ISPs, their main concern now is performance, knowing whether their machines would put up with the load. But we have to do away with it.

CRISTIAN HESSELMAN: It's kind of interesting you mentioned that, because in the Netherlands, the ISPs are not so much concerned about the performance of their infrastructure. They're concerned about the support calls they might get when there's validation errors.

So if a registrar makes a mistake, then they don't really feel the pain because the ISPs are afraid that they well feel the pain, in terms of that their customers will be calling their support desks. And as a result, there is a cost for them of about 50-60 euros per support call. So they're afraid that this will basically kill their business or something like that.

So it's interesting to see that they come from a different angle in your country. Thank you.

HUGO SALGADO: I think one of the best experiences on ISP signing domain is the Comcast experience. So I think you can talk to him, because the Comcast experience was very, very nice. Talk about him in regard to the NASA experience last two years ago.

[PAUL ABRISMUTH]: [Paul Abrismuth], Comcast. We do have validation failures. They currently do go to our DNS engineering team. We do contact the domain [enterers]. We go through the negative trust anchor draft process. So it does cost us money. And because it is a senior engineer instead of a standard 800-number call, it probably is $100-200 to process that.

We're seeing three or four failures a month, so enough that we notice it. But it's certainly not something that shows up as a line item and my boss starts screaming that we're spending too many hours doing it.

So across 23 million customers, somewhere around that, that level of failure and the domains that they're actually interested in that are signed, I think it's something you need to plan for and have process for. But it's certainly not the financial burden that everyone assumed would be a disaster.

UNIDENTIFIED MALE: Congrats.

[RAY MESETARIO]: I will speak in Spanish. Good morning. I am [Ray Mesetario]. I'm a fellow first-timer in ICANN. I have two questions, first to LACNIC and then NIC Chile.

The first part, when we were talking about to take costs down, we were talk about cloud and [inaudible]. For instance, in Venezuela in the local chapter, one of the members at the university wants to certify with DNSSEC for traffic generation in the university. Is it possible to do it differently with devices that are low performance that do not depend on the cloud? I'm talking about cost, basically.

CARLOS MARTINEZ: Let me see if I understood you from the table. There are some domains at the university that want to sign, and they are concerned about the cost of the clouds and [inaudible].

If it is a university, they can use a server, almost anything. The requirements to sign zones that are not too big and not that large. You can sign quite large zones even with virtual machines. It's not something that requires large things. I'm talking about the smaller, business-size zones. It's not something too costly as to computational requirements.

I have not gone through this, but I think that zones with millions or tens of millions of registries, it is different. But in this case, with relatively small, a modest server should be all right.

[RAY MESETARIO]: Now, to NIC Chile, I don't know whether you have helped universities in Chile to do something similar or something a bit larger. I would like to know whether you had done that.

HUGO SALGADO: Not. No, unfortunately, up to now we have that with the University of Chile. We are part of it. That is part of the dissemination that is still outstanding.

Now, in relation to what Carlos says, you can sign using the same software that you use for an authoritative DNS. BIND has tools to sign internally. I recommend OpenDNSSEC that is in one of the slides. That automates that a lot. So I would recommend that path.

You can also have a virtual HSM, and you don't need hardware for that. Thank you.

JULIE HEDLUND: So [inaudible].

ISAIAS MERCADO: Now talking about DNSSEC. I am Isaias Mercado from the Dominican Republic ISOC. I asked myself, [in territory] companies, private companies such as banks or other organizations can be interested in DNSSEC. But as it was said before, the fellow who spoke before me, there can be the case of smaller or larger companies that have one, two, three DNS domain names, but they are not service providers but may be interested or would ask themselves what's the benefit for their

world? A private company, what benefit can it get? Does it depend on ccTLDs or some organization? What benefit can they get from this?

UNIDENTIFIED MALE: Good morning. I am your brother, so I am going to talk in Spanish. Recently, there was a great interest from financial organizations mostly for the opening of ICANN, in terms of new generic domains. This .bank domain that has all the specs for security associated to the new generic domains. This big interest from banks and banking organizations in a country like yours, they see that there is value added in security. For instance, preventing phishing, some concern for banks. When they are commercial domains that manage registrar schemes and they see added value, such as DNSSEC, they go for it.

So there is a market, competitive edge with the ccTLDs as an added value they have not found in their country code. There, we need to start working and make use of that big opportunity for ccTLDs, as well as signing and the capacity and security for the domain.

These are interesting times in the industry of domains, from the area of security that are being developed in the financial world, and also in the industrial world.

JULIE HEDLUND: Thank you. I did have one question from the Adobe Connect chat room. This is a question for Luciano for NIC.AR. It is from [Rafael Kanagusuku]. And he says, “Have you started signing .AR domains? I

work for the AFIP and would like to start using DNSSEC. May we contact you via mail for technical assistance?"

LUCIANO MINUCHIN: Sure, we can get in touch. We first intended to start signing. We can sign the domains under our control right now. That is NIC.AR and IPv6.AR. As an example, we want to sign a few domains more in the next few weeks and we want to move forward mostly with government agency to reach the relevant agreements and go on with the signatures. The presentations include my e-mail, and we can be in touch.

JULIE HEDLUND: Thank you. Please join me in thanking Luciano as the moderator and all of our panelists here for very, very interesting presentations.

And now I'd like to welcome Ed Lewis. So we're going to move now to a presentation from Ed Lewis, from ICANN. And that is going to be an update on the root zone KSK after ICANN 53. Thank you. And I'll just go ahead and turn things over to you, Ed. And welcome.

ED LEWIS: Thank you. My name is Ed Lewis. I'm from ICANN. I'm here to help. Sorry. I'm going to keep my headphones here. I'm hoping to hear questions from people that I need to have translation. So I really want to encourage some feedback here. We'll try to catch up time on the agenda, too, while we're doing that.

UNIDENTIFIED MALE: Give up the break.

ED LEWIS: Give up the break? Well, who's for that?

Okay, so my agenda. A little bit of background. There are two things I want to cover right now. One is something about the HSMs, and I'll explain that stuff later; the KSK change we're talking about; and then I have a big finish, which is not that big. But it looked good on paper.

The root zone KSK, it's the thing at the top of the DNSSEC hierarchy and validation. It's been in place since 2010. We have used the same key for the last five or so years. It's probably about time to change that.

We also have been using the same hardware, the HSM, since that time too. Although now that I'm giving the presentation this time around, we actually have changed some of the HSMs.

And after five years of the operation, two of the major themes here is that there are some concerns over the HSM, whether they can continue to work at that age. Their battery life is the particular rumored problem they may have. And also, there is a requirement – and I use "requirement" as a loose word – to roll the KSK. Next slide.

Now, the players involved here, first are the root zone management partners. That includes ICANN, that includes the US NTIA, and there's also VeriSign are the three major parts.

We've also engaged an external design team to look at the KSK roll. These are people from the community. Volunteers were sought. We picked a group of them, and we've been working over the past couple of months to review our plans.

Now, ICANN is doing this work under the IANA functions contract. And the ICANN responsibility is specifically the KSK functions. ZSK is managed by Verisign in coordination with NTIA. Next slide.

"What is a…" What is a KSK? I've use these slides in many different venues, and I'm sure most people are a little more familiar with this here than other places. But anyway, a KSK is a key-signing key. It signs the DNSKEY RR set in any zone, in the root zone in this particular case.

The KSK is public-private key pair. The public part of that key is what is distributed everywhere. If anyone is doing validation of DNSSEC and they're doing it from the root down, they have to have a copy of that key. That key has to be somewhere stored, copied in their local configuration so that they can go forward and do the validation from the top down.

The private key, on the other hand, is kept very secret. It's actually kept inside this HSM, a box that nobody's actually ever seen the private key in the raw. It's only in the HSM.

The HSM is a hardware security module. It's been mentioned today already today a couple times. It's specialized hardware. They are boxes built to manage private keys and keep them private. They operate the KSK's private key functions. We send data to it. It signs

and sends it back. And the chief job of an HSM is to keep the KSK from being viewed outside anywhere. Next.

Now, in terms of public impact, this is part of, "What should you care about all this?" The HSM change, you shouldn't care about that. Unless something goes horribly wrong, you won't even notice we did it. It's basically just changing out the mechanics of how we do things day-to-day right now.

The concerns about the battery life, that doesn't mean we have impending doom. They're just getting old, like me. They still work, so they shouldn't put me out to pasture. I'm talking about the HSM now, I guess. They're just getting kind of old. In the sense that they may actually wear out, we're replacing them.

The KSK roll, though, on the other hand, is something that's going to have a lot of public impact. Everybody who sees validated DNSSEC right now is coming through that place. Paul over there will be hearing a lot of support calls at Comcast if this goes badly, or if Comcast doesn't know this is going on.

All these copies have to be updated, and it's not exactly a well-automated system for doing this, which is what we're concerned about. We have mitigations for this, but we don't have a seamless way to do this. It's not designed to be seamless. And trusting the new key is basically the work to be done.

So in the presentation here, it's first to inform you, to let you know what's going on so that we can't say you weren't warned, at least in this venue.

What I [also had in here too] is a stir of feedback and comment. And depending on how much time we have, I'd like to stir some feedback here.

But also, I want to advertise that we're going to have an ICANN public comment coming up soon to review the draft document that has come out of Design Team work. That should come out next week. I'm not sure exactly what day, but I'm hoping for Monday. That's the formal way to provide feedback for the work that we're going through right now. And as I say, I'm going to stress *formal way* to send back feedback. If it gets there, it'll definitely be seen.

There are also informal ways to participate in this. And this is to talk to anyone who's involved and use any mailing list out there that anyone is attached to. Likely, we'll see things and pick that up. And we do work on what's going on out there. Next.

So one slide on the HSM change. The HSM change really is minor, so I'm going to spend just one slide on that. It's a straightforward replacement with the same brand, a newer model of what we've been using for the last five years. ICANN uses these in two different facilities. We have the Culpeper facility, and we have an El Segundo facility.

The Culpeper facility already has the new HSMs installed. They went in, in a ceremony on April 9th. The ceremony actually went flawlessly.

The script was written well. We followed the script. We have the new HSMs in there.

The El Segundo facility will get its HSMs put into play in August, in about another month and a half from now. The plan for this is documented in a web page. The URL is listed down at the bottom there if you're interested in looking that up.

Now, the KSK roll, compared to the HSM change, it's a much greater public impact and there are various options to consider. So because there's many more degrees of freedom in doing this work and it has a much bigger impact, we've gone through a very slow process to come up with a plan for changing this key.

Initially, in 2012, there was a public consultation. People were asked for input about what should happen, and that went in 2012. In 2013, there was an engineering effort following up to that, where a plan was drafted to follow for the actions. And then the effort just went on hold.

And then in 2015, we took all the stuff off the shelf, everything that had been planned out, and called an external expert to say, "What do you think about this? What are the things we should look at? Are the plans we have okay? But also, what has changed in the last couple of years?" Because we're in a very rapidly changing environment with cryptography, hardware, the state of DNSSEC. Everything has been changing so much in the last five and ten years in the entire industry.

Next.

So the current Design Team plan was to do a study, to work on this through the month of June, which we are now in. Present a report for public comment. That'll be open for 40 days. Opening it right after this ICANN 53 comes to a conclusion. And then after that's done, the Design Team will come back and respond to the comments, work some more on it, and have a final report about a month after they reconvene for this. The root zone managers will then develop a plan and execute the plan. Next.

Now, the Design Team roster, the people that you can track down and present comments to, I'm inviting you to do that. Joe Abley; Paul Wouters, behind Joe. Yoshiro was, I believe, here earlier. And Jaap Akkerhuis is here. John Dickinson, Ondrej Sury, and Geoff Huston did not attend ICANN 53, but they're also part of the team. You can contact anyone there, send an e-mail to them. You can go to their house, have coffee, cake, and all that too. You notice they aren't listening to me, so. I love it when that happens.

And also, anyone else involved with the Root Zone Management Partners, including me, you can come to me with comments. In fact, every time I've given this presentation, I've had someone say, "I have a dumb question," which turns out to be, actually, a pretty good idea we hadn't thought of. So fire away. Next.

So in theory, on paper, [to roll] a KSK is pretty easy. We've screwed it up a lot. Paul knows that. And we've also done it correctly a couple times too. So we have an idea of what's good and what's bad about that.

The root zone is different, because in all the other cases, the steps were basically you do some work on your own and you tell your parent, "I have a new KSK. I want a new DS record." We don't have that luxury at the root zone. There is no parent to give it to. So we have to figure out how to get that KSK out to everybody.

Now, fortunately, there is an RFC in the [IETF]. We through around the word "RFC5011." It's for automated trust anchor updates. It's a means to learn the key through the system, and we really are hoping that that will do a lot of good for us. Next slide.

However, any plan we come up with will have big challenges. This is a very multi-party process out here. No matter what anyone does, will the other side follow along?

Will the validators out there be able, first of all, to even see the messages? We're going to be changing the size of some messages, and DNS is very size-sensitive. Big messages get dropped by firewalls. It's too big. EDNS0 is a concern, and so on. Fragmentation is becoming to be a growing concern about how that's being done on the Internet.

Is the entire process of automated trust anchor updates, is it working? Just because it's been defined in RFC and people have written the code, does it actually work? So one of the things we're doing is calling up all the vendors and saying, "Did you try it?" And we get back, "Yes." So at least we've got that going for us.

Will the operators know how to prepare and how to react? And this is my specific call out to Paul, that we're going to try to make sure you

and your kind know what to do when you get trouble ticket calls, because that's usually where the brunt of DNSSEC failures hit is the ISP NOCs.

And finally, we've written a lot of DNSSEC code out there. It's been around for a long time. Will they all execute correctly? Will the specialized code for the root zone kick in everywhere? So we want to make sure of that.

So on this slide here, this is my last major content slide. This is a rough outline of the document that's going to be out for review in the next couple of days. And I'll walk a little bit through that to give you an idea of what's going to be in the document. So you might think now about what you might want to come up and say.

First, there's some history. There's scope, motivations, explaining a little bit more detail what I've highlighted in this talk about how we go to the point where we are today. Not necessarily a tutorial on DNSSEC, but a tutorial on the process of coming up with the plan that we have.

We talk about cryptographic considerations. There's been a lot of concern, like should we keep the same algorithm? Should we go to a different algorithm? Do we need a different algorithm for size differences and all this other issues out there? And we go through some of the rationale there and some of the studies that went on behind that.

We look at the protocol. Now, DNSSEC changes in the protocol are a little bit special at the root zone. The idea of prime inquiries, the idea

that we have to keep things small because this is the bootstrap for everything else you do in the Internet. Whether or not TCP is going to be good enough, if that's a fallback. What do people do about validation errors?

Operational coordination, which, in my personal opinion, is probably the biggest part of this. This is an operational issue. This is not a protocol or a science issue or mathematics. This is all about operations. It's about changing a configuration number somewhere.

We want to make sure that we're reaching to the right places. Giving talks like this are nice, but I don't think that that necessarily translates into the NOCs getting prepared for things out there. We have to know what else has to happen. Who do we contact? Who do we specifically need to tell that, "Hey, this key is coming," and, furthermore, that this is really right key. Just because a key is coming, you want to find out that you have the right key. You don't want to be misled into following the wrong keys out there.

The impact on DNSSEC validation. Right now, validation is actually rising. I think that one of the surprising results in the studies we've been doing is that there are more validating than we thought. That was surprising. Not everyone is relying only on validation. Some were validating, and then when it fails, they go back to regular DNS. But still, there's a lot of DNSSEC validation happening out there.

I should step back. The criticism about the lack of signed zones, I remember back when we were signing zones, and they were saying, "Well, we're signing so many zones, but no one is validating." Now

we're hearing people are validating, but no one's signing their zones. It's an interesting switch we've had in the last couple of months.

So there is a lot more validation out there than we had anticipated. And that actually creates a higher risk that when we change the keys, that things, if they go badly, will go badly on a bigger scale. We don't want that. We want to avoid that.

Trust anchor publication is something we're looking at. What's the way to get the trust anchors out there? There are a few different methods out there. And surprisingly, not many people have been using some of the ones we had out there. We were surprised to find out that almost nobody's actually accessing the stuff that's out there. So we want to make sure that that's a valid way of doing.

Besides RFC5011, which is the automated, in-band way of doing this, not everyone is going to trust an in-band mechanism for giving the new keys. So we have keys published in other ways. And again, how we're going to distribute them in a way that you know this is *the* key, not just some new key.

We have a little bit of testing in there. It's been said that we have to make sure testing's important. We've discussed it. I will say, frankly, in the document that's going to go out there, we don't have a lot written about testing. Not that it hasn't been discussed; it hasn't been written about.

So we're leaving it there, in a sense that if people have ideas of what should be tested and how, we're open to hearing that. We've actually

thought about a lot of things, but it doesn't hurt to say them again. And there are some [test bits] out there that are actually functional and available, and we've been using them to test some of the implementation. So there's work out there, and we want to make sure it's known.

Finally, we're also going to talk about the plan itself. The plan itself, I mean the actual steps that were being proposed, given the work in the past and some of the tweaks put in there more recently to try to optimize this.

We're looking at RFC5011 to see what it actually says. We're trying to interpret it in a way that is very advantageous, and we want to make sure that others have implemented code in the same way. RFC implementations generally tend to be a little dodgy for a while. So we're a little concerned about that.

And finally, at the end of it, we have an analysis of risks out there, which I believe is kind of a stub. What could possibly go wrong is listed there, and then whether or not this is going to happen, how big would it be if it happens. And then what do we think we're doing to avoid that being a problem? And I would like to see a review of that, from that point of view, because that's a good way to catch, are we doing everything we want to do in our plans?

So this list that I've gone through somewhat rapidly is meant to raise your interest here. Pick up your favorite thing that you want to mention about this. Is there a concern that you have about this? And we have some time for questions, I suppose, here, and especially

addressing to the people in group here. And look for the public comment period coming up. Next slide.

And my last slide, I just have these links up here, just to fill the screen while we talk, and we can go back to the previous slide if we want to.

On the IANA website, there's a DNSSEC page which has the DPS for the KSK for ICANN and the other operations there. There's other documents. There's all the histories of the key ceremonies and such on there. Root-DNSSEC.org has some more information.

And the last one I have there is the DPS for the VeriSign operation of the ZSK. Is someone from Verisign here? I'm just curious. All right. Okay.. I just hadn't even though to look for anyone from VeriSign. I see you.

All right. So, with that, I'll throw the floor open for comments, questions, and anything that you want to raise up with this. And I believe we still have 13 minutes, roughly. We have time, so yeah. Break is next, though.

JULIE HEDLUND: Any questions for Ed? And please do step up, nd be sure to state your name and your affiliation.

ED LEWIS: All right, Dan.

DAN YORK: Come on, guys, we can't let Ed off this easily. Come on.

The question really is what do you see as the time frame? What's realistic for all this?

ED LEWIS: Good question. Okay, so the time frame is a good question. I asked this question myself internally because we've been doing this process for a while, because it impacts on how much time is going to be spent in preparation.

And the rough idea is that I believe that we will do the key change in the next calendar year, meaning that if there are things that come up that we want to have months to prepare for, we're not going to shy away from that. We're not going to rush into this. And that's an important point to hear, that if the [inaudible] come to us saying, "We want a test bed. We want to have testing." We want to make sure that we take the time to prepare for that, to be able to have that out there. And I'll leave it at that for next.

DAN YORK: Thanks.

RUSS MUNDY: Are we alive here?

ED LEWIS: I can hear you.

RUSS MUNDY: Is there any relationship between this activity and what's being looked at and studied extensively and talked about extensively in this meeting? And that's the IANA transition process.

ED LEWIS: I don't really know, to be honest. I'm not up on the transition process, to be honest, to give you a good answer. So, yeah. Mark?

MARK ELKINS: Mark Elkins, [inaudible]. Do you think there's going to be any change in the zone-signing key, key size? Or are people seriously looking at changing the algorithm of the protocol? Or are we going to basically be doing the same thing again?

ED LEWIS: Okay. So for the ZSK, that's totally the responsibility of VeriSign. I'll put a blanket statement out on that.

MARK ELKINS: Sorry, KSK.

ED LEWIS: Oh, KSK. Okay. And I didn't mean it to be an excuse. It's just to point that out.

For the KSK, right now, the KSK is at 2,048 bits. In terms of cryptographic reasons, I've never heard anyone question whether that's a good idea or not.

In terms of packet size, there was a question of whether or not we needed a different algorithm to go to, because the RSA 2K signatures are like this big, and you can get elliptic curved ones that are like this big. And in some of the background research, we've discovered that, from what we can tell, we don't believe that that is a bottleneck.

Did you want to answer the question, Joe, or should I keep going?

JOE ABLEY: Either way, up to you.

ED LEWIS: Well, I'll defer to you as a Design Team member.

JOE ABLEY: Okay, well, I think the idea here is to try and provide the functionality that we need, the behavior that we need, changing the key for all the good reasons, and cause the minimum amount of disruption on the Internet. And this is really the principle concern that we have with this design. We can't characterize what's going to happen. We have to try and be very conservative.

So I think what we've found out so far in the experiments that Geoff Huston has mainly run is that the impact of a larger response size on

the ability of validators to actually serve their end users is minimal. We don't really observe any breakage caused by larger responses.

We also only observed a relatively small amount of breakage from using a different algorithm. And the one that was tried was ECDSA. But it's bigger than the breakage we see from the larger responses.

So the conservative approach in the first key roll is to not change the algorithm, to tolerate the larger responses, because the evidence seems to suggest that that will be benign. But leave the door open in the future for algorithm rolls when we see ECDSA better supported. Paul may have other insights here as well.

PAUL WOUTERS: No, obviously, I agree. I just want to point out that most of the TLDs have much bigger DNSKEY sets than the root zone, and so we wouldn't expect any problems in the root zone, because those domains, the TLDs don't see any failures either.

Additionally, the packets of the TLDs are a little bit bigger because they have the TLD name in it, which is bigger than the root name, which is only a dot.

So there's enough reasons to think that it would not be a problem. Or otherwise, we would have TLDs that accidentally published eight DNSKEYs by accident, say, "Oh, resolving is a problem for us."

ED LEWIS: Over here. Mark?

MARK ELKINS: Which brings me into another question. If everyone was keeping the same algorithms and stuff like that and everything else was equal, is there any reason to actually run longer keys than what the root is running? Because isn't the chain weakest at the weakest point? So is there any point ever having longer keys?

ED LEWIS: Okay. That gets into design philosophy of the protocol. You're always welcome to take any key and make it a trust anchor point. So say you're four levels down and you want to have longer keys. You can get that key into all the validators that you care about.

So in a sense, it doesn't make any sense. It makes sense, if you're someone who really wants to go through the effort of having higher security, it can make sense to do that. In general operations, you're also right though. The weakest point in the link is going to be the worst part of this.

And I'll leave it at that, because really, I can't come up with a definitive. Because we actually discussed this back when we did the research on this. And you're right. It's a toss-up. I'll say it's a tradeoff. If you want to go through the effort of promoting a stronger key at some point in the hierarchy, you can do that.

If you're saying the 2,000-bit KSK is the weakest point of everything, then why build beyond that? The next divide is maybe you want to be

stronger in case that gets changed, or you just want to live by it. So it's where do you want to put your bottleneck.

ROSS MUNDY: I'd like to just add a little bit. It's an excellent question, Mark. I believe that where it would come into play is if a particular set of activities. We had a lot of financial institute discussions on the regional panel. Whether it was something like that or, say, a given set of companies got together and purchased their new TLD and wanted to have a higher level of trust. Because as Ed well points out, you can use in your validator your preferred trust anchor. And you can go down for just the general use of DNSSEC.

But in that particular community, if you want to achieve a higher level of trust, that's one instance in which a single, larger use of a key by a particular TLD might be useful.

ROBERT MARTIN-LEGENE: So the key size would reflect how long you want the key to actually live. So if you have a ZSK that has 1,000 bits, you might want a KSK that would change in 20 years, and maybe you might want 4,000 bits.

ED LEWIS: Yeah, the sizing of this is a matter of what are you protecting in this message, is a good question too. Also, I'll say this, caution people again. DNSSEC is not the solution security. It's just there to make sure the messages get through the DNS. Even though you may use DNSSEC

at the root chained down to somewhere low, and then it signs a DANE, a TLS record, that's used to do something else, so on and so forth. This can't be the only security you have in that area.

So that's one thing to keep in mind, that the DNSSEC is meant to just make sure the DNS messages come through authentically from the source, source integrity, and you get the whole answer. And that's the real goal here. So we have to keep that in mind as the mission of the protocol.

DAN YORK: I guess I would just say, I appreciate you coming here and giving us this update and to do that. I look forward to more info about the time frame. I really do hope we can do this sooner, rather than later, if we're going to do it, because I do worry that every time we hold one of these workshops and we encourage more people to do more validation and signing, we're setting ourselves up for situations where, if there is breakage, it could be worse. So I think the sooner we get this done, the better we can move on with this. So I wish you all well with figuring that out.

ED LEWIS: Thanks. Thanks.

JULIE HEDLUND: Well, thank you very much, Ed. Lots of interest there. So we can't wait to see this report. And I'm sure that people will be getting in touch.

So, please, everybody join me in thanking Ed.

And now we did have a 15-minute break scheduled. Perhaps just to make sure we stay on schedule, we'll give you ten minutes. If you could come back at 20 minutes after 11:00, 20 minutes after the hour, then we'll start back up. Thank you.

[break]

I'd ask you to finish up your conversations please, and please go ahead and start taking your seats. We'll start up in just a couple of minutes here. Thank you. We're going to start now, if folks could take your seats.

Again, this is Julie Headland, and we have the DNSSEC workshop here today. We are now starting up with our next panel. This is a panel discussion on DNSSEC automation. I'll go ahead and turn things over to Russ Mundy from Parsons who will be moderating this session. Thank you.

RUSS MUNDY: Great. Thanks. Paul, if you could start our clock, that would be wonderful.

We have a panel on DNSSEC automation. We have a set of different activities that we're going to talk about today. We're going to go ahead and jump right into it.

I believe Eberhard Lisse is our first presenter. Eberhard, why don't you just go ahead?

EBERHARD LISSE: Thank you very much. It's quite a pleasure to be able to talk to some real people and not having to have this nonsense with the accountability all day long.

Last time, in Singapore at tech day, Diego Espinoza from Costa Rica and I presented our work that we've been doing on smartcards, and we managed to get SmartCard-HSM to sign. We managed to get the keys into the smartcard. We managed to get this working, but now how to put it into production?

Turns out these things are not as easy as it looked from the outside. Just for completeness sake, I have a few introductory slides. You all know this. This is more geared to the starter end of the spectrum. Probably not represented here, but I think it's always good, not only to hear from those, but also to hear some failures, and what we think is causing these things to fail. We can learn from failures almost as much as from successes.

As we all know, DNSSEC is very easy. It's easy to do. It's easy to fail. The question is is DNSSEC actually secure?

Lots of people are saying it's not. It is. It doesn't really matter. It's the standard, so as far as I'm concerned, as long as it's the standard, I will try to support it, and I will also try to encourage other smaller ccTLDs or TLDs to do it.

The big hamper is the expense. My ccTLD would be able to afford three HSMs at 10,000 US a pop, but at the moment, the cheapest offer we

have is 20,000 US. Probably, that makes it a little bit much. We wonder where there isn't it cheaper, easy, off-the-shelf solution that is secure. In other words, hardware based, it's cheap, and that we can use for small TLDs, but also for users.

Why must a small company, Internet related, computer support [signs] ISP or whatever, why must they buy an expensive machine if they could sign their own domain in hardware? This is also for completeness [sake]. The registry system has a database. The database throws out BIND tables. They get signed.

At the moment, the two common methods are using BIND DNS sign zone or open DNSSEC. Or if you really want to be courageous, you put both together, and if you then turn the automation on on both sides, you get very interesting results and surprising results.

Then after the zone is signed, it updates the serial, and it loads it. We basically sign it on a stealth server, load it on the open master, and so I think it's easier to handle if you have two separate things.

Our top level is basically signed. .NA is basically signed with a software key. We have a [share script][that monitors every single step and squeals if something happens, and then SCPs it to our primary with the serial number on the file, so if we have a problem, we can work back several steps.

We keep at least 20-30 generations of the file, and we have a lot of checks in so that doesn't work. But still, you want to have a hardware key because if the key remains in [inaudible], it's a security issue.

Diego Espinoza has done some interesting work with Rick Lamb about using a TPM chip on the hardware to use it for signing. Can use the HSM. You can use a SmartCard-HSM, which costs you $20, and if you flirt with the guy, they give you a 10% discount and put the presentation from Tech Dy Singapore on their website.

Card readers. There is a number. You get one for $10 at a bank in Costa Rica, and you can get one for 20 bucks at any decent window of your choice. But there are some issues with that that are not related to the card.

There are many brands. Currently, I like most the German one. It has something to do with my cultural heritage perhaps, but maybe German engineering.

On the PDF, every link that is clickable is in blue. If you download it, you want to have the address of their website or the address of an e-mail of one of the protagonists involved here, then you don't have to ask me about it.

That works quite well on Linux and on OS X. Rick Lamb did very excellent work on creating a DVD, which has a complete bootable system to do this. Diego and I took this and adapted it to work with a little graphical or a semi-graphical from them on the Macintosh, but basically, it's important to see the work that he did and pick that apart.

You can have a flexible number of crypto officers. In other words, if you need to clone the card, you have at least two or three people

being present so all the security measures are there. It signs in the card.

If you have the key size big enough, it can do about 7,200 per hour. If I needed more, I could increase my reload time to two. If I really had a problem, I could then have two cards, and if it really, really, really started a problem, I would probably have enough clients to buy me a proper HSM.

DNSSEC sign zone works very well with the software key. This is absolutely rock solid since 2009. We have never had an issue. But the card, the key has to be on the system.

Our system is credit card compliable, so we have really tried to plug every hole we can find. We have several security services probing the system, and any hole they find, which is really rare, we plug immediately. I am fairly confident that for the time being, we can carry on like it, especially since we don't have clients.

In order to run, to use it on the smartcard system, it requires a pitch. Rick Lamb has written the pitch. It works well, but the pitch has not been accepted by ISC into their standards, which means it doesn't go into the repositories.

There are technical issues, logistical issues and political issues, which I accept actually, but in the end, it's not possible for me to run this in production because I want to run it with the normal repositories. We're on Ubuntu.

I see Paul Wouters. They're frowning. But whether it's red head or Ubuntu, doesn't matter.

PAUL WOUTERS: I thought BIND 9 actually added support for PKCS 11.

EBERHARD LISSE: It's not complete, and it doesn't work. We have discussed it. I think this is something that you want to discuss with Rick and Vicky. They have had some e-mail exchanges.

As you all know, I'm a gynecologist. I don't understand the deeper stuff on this. I'm not an obstetrician any more, by the way. The insurance has become too expensive.

But there is a reason why ISC cannot put it into their [inaudible] tree in a way that works on that smartcard. Some cards work, but that one doesn't because it doesn't implement a full spectrum or something. If you want to discuss it, talk to Rick and to Vicky. They have exchanged e-mail.

I'm not the person dealing with this. I find the reason from both sides to put it in and from ISC not to put it in reasonably compelling.

We then looked at open DNSSEC. It's not part of the standard Ubuntu 12.4 or 14.4, but Ondrej Surý, who we know very well, retains a very good repository, so you just plug that [N run], push the button, and it comes in there.

It also needs OpenSC. The interesting thing is 14.0 comes with Ubuntu 14.4. Ubuntu 12.4, which we run in the production machine, comes with 13.4, which doesn't really work so well yet. Recently, 15.0 has come out, which I've compiled on my home machine, works exactly like that.

Then we come to the problem. Daemon on the Ubuntu that talks to the reader. Not to the card, but to the reader is called PCSCD, and that's a bit of a nuisance.

You [inaudible] SQLite and MYSQL. I find MYSQL works a little bit better.

There is a significant learning curve. It took me about a week to figure out which words on the card you must put in the token label. It was not easy. I've put the exact strings that come on the default. If you just put the keys in the card, it gets this label SmartCard-HSM and user pin, and that's what you must put in in that particular way exactly into the configuration file.

But I think I have heard I'm not alone in struggling with this XML stuff. Then the RRSIG validity surprised me occasionally because it's much shorter than I expected.

The cards, we tried three different [kinds]. My cleaning lady could toss it around when she cleaned the place. There's a desktop standing next to my desk. It fell on the ground. The usual excuse is the dog ate it. No problem. No contact problem whatsoever. I never had an issue.

But this reader [daemon], that PCSCD, that looks at the reader – not at the card – that stopped working all the time. It didn't crash. It didn't go zombie. It just didn't respond any more.

We tried different readers. We tried different cards from the same brand. We couldn't find what's going on. We haven't spoken to the developers.

Now, Diego and I have spoken about it, so he will reproduce exactly my set up and run it on his hardware. Maybe it's a hardware issue of the USB set up that I have. Maybe I must buy me a new computer. It's a bit elderly. I don't know.

If he can reproduce the same problem on his machine, then it's not a hardware issue. Then we shall go talk to the people. Maybe they can reproduce the same thing and try to find out where the issue is so that they can find this thing, and then they can fix it.

Then, of course, open DNSSEC failed to [find] at short RRSIG validity, and whoops, my e-mail wasn't working. My son started to squeal because the girlfriends couldn't communicate. Most of them use Facebook nowadays, but some even use e-mail.

Then I wrote a heartbeat script, which figured out at least where the problem was, but of course, you can't kill your daemons in production on a regular basis and run a ccTLD on that.

My last slide is interesting. The weekend before Julie pressurized me into submitting my presentation – and I even got an extension – I found a link on Google. Warren is my friend here.

Somebody in the Netherlands has used PowerDNS and a smartcard, and found that there is an experimental feature. I haven't played with this yet. I will. But it's probably possible to run a stealth server on a different port, which pulls the data out of CoCCA tool. CoCCA tools has support for PowerDNS in already, so there isn't much configuration to do, and then notify the master on the proper name server and push that. It may be what the doctor ordered.

I, personally, would much more prefer to see OpenDNSSEC pull out all these daemon stuff, pull this all out, leave it for the people who have got time on their hands to play with this and to look after crashing software all the time, but get just the pure signing program that you can plug it into a shell script, and then be the master of your own destiny by controlling exactly each step, and if it fails, then you know it and do manual all over of the keys once a year or whatever, how often you do it. But you are involved in every step of the way.

So, it failed, but we are having a plan. That's it.

RUSS MUNDY: Thank you so much, Eberhard. As always, a very interesting presentation. We'll try to collect up the questions for the end.

Our next presenter is Robert Martin-Legène, who is going to tell us about the PCH signing service. Robert?

ROBERT MARTIN-LEGÈNE: Thank you, Russ. I will say my name probably once at least. I try to avoid the troubles. I'm Robert Martin-Legène. It's a French name, and I'm not, so I probably screwed it up, too.

RUSS MUNDY: I don't feel so bad then.

ROBERT MARTIN-LEGÈNE: Right. I was asked to give a little talk about the DNSSEC signing service that PCH has for primarily ccTLDs. This is not so much a new thing. We've actually had it since 2011. We've introduced it in ICANN Singapore in 2011. Since then, we have signed up almost 40 TLDs to use the platform, and that's 40 TLDs that use it in production where they actually have the DS in the root zone. We do sign for most zones, but some of them may be in extended tests or that just never got around to do more about it. Next slide, please.

The PCH signing service uses key ceremonies like the ones that ICANN performs. We don't have the same amount of register representatives that comes in every now and then, but we do have external witnesses. We do have notaries. If somebody wants to come, they are very welcome to participate, but as everybody has learned by now, the key ceremonies are not the most entertaining thing in the world. But if somebody comes by one of our locations, they are welcome to join.

We do about three or four of these a year depending on demand. Sadly, the effect of this is that if somebody needs a domain name signed, we need to know the name to put it into the key ceremony

because part of the things we generate in the key ceremony, well, you need to put the domain name in some signatures. We cannot pre-generate a lot of keys and just use them as we want.

The keys – as I think everybody here knows or should know – are stored in a hardware signing module. It's one of those big boxes that Eberhard wants, and they are not cheap. That's true. They perform really well. We use also the same as ICANN does I think, and as many others do the [AS Keeper].

When you create the way we have configured it, you cannot extract the keys once you've created them, so you create the keys inside the HSM. You hope that it's a random key. You have to trust that it's not breakable because we are not really able to tell if it's a [valid] certification.

We trust FIPS is able to do that. The platform has been certified to FIPS 144 level four. Is that 144 or to 142. Anyway, it's the highest certification you can get for an HSM. The root zone does the same.

When we do the keys, we use to do 2k KSKs and 1k set as Ks. But recently, we switched. Because of some discussion on some mailing lists, we realized that there wasn't really any reason not to do 4k and 2k, so now we doubled the key sizes for each one of them. That's also the recommendations that we are giving to DNSSEC partners that want to do their own signing.

The 4k is supposed to be a little bit more burdensome for a resolver to work with, but we believe that you only need to validate the KSK once

before it expires depending on how your cache is configured. We trust that's something people can live with without getting too upset.

In terms of security, we think it's a valuable tradeoff. On the same note, I think the root should also go up.

We use NSEC3 with opt out, which most TLDs do. The reason for this is that many of the domain names in a TLD is absolutely insecure. There's no DS record that secures it, so you can skip a lot of signatures, and your zone size actually becomes very manageable in that sense. We use NSEC3. We only sign what needs to be signed – what BIND does for us.

The disadvantage of NSEC3, of course, is that it is extremely difficult to debug. The first few months you are trying to figure out what those hashes mean.

Another thing is that some companies believe in security through obscurity, and if you don't use NSEC3, but use NSEC instead, then you can use zone walking. People are not too pleased with that.

Part of the service, we also automatically roll the keys. Usually, just about six weeks, we roll the ZSK. The KSK, we don't really plan to roll, but we probably roll it every five years. That's what we have been hinting that we would do, so I expect we'll be doing that. But it requires a lot of coordination with the TLDs.

We, like Eberhard, sign with the BIND. Not old BIND, but old enough because we know that it works. We have a lot of experience using that

now. As long as there's no reason to upgrade for security reasons, I think we will stick with that. Next slide.

How do you get onto a platform like ours? I suppose it's much the same for many others that would provide the same service. Basically, we would transfer the zone from your hidden primary. We would sign it, and we would verify that the data is valid, and then we would be sending it back to you, or you could tell your secondaries to pull it directly from us.

Finally, of course, we can also add it to our Anycast [servers] if you are interested in that. The Anycast [service] PCH is very known for the Anycast [service] in the ccTLD community since we have many nodes and many happy TLDs.

Anyway, those things are not connected. We can easily sign and hand it back to you and not tell anyone that we are signing your data. If you want it to be a secret, that's fine. Next slide. Thank you.

The ccTLD: what a ccTLD really needs to worry about? If somebody else takes over the signing is that they need to collect the DS records from the children that are interested in that. Usually, that requires some kind of modification to the database, some user interface, or maybe some scripts that goes out and fetches something. But in reality, what we're seeing is that the take up so far is slow enough that you can use a file that you just include manually and maintain that by hand.

If somebody needs to change, well, then you have some manual process. You can do that until you get tired of it, and then you will eventually automate it. That seems to be working for many TLDs.

I recommend that approach, and in the meantime, you would get a lot of a feel about how DNSSEC works, and you try to verify keys and everything. So, getting on a DNSSEC platform until you're ready to sign yourself is a good way of getting familiarity with it and getting a soft approach to the learning curve of DNSSEC.

It's like DNS. It's extremely simple until something breaks. If you do every single step correct, it's okay. But if one of them fails, then it's sometimes a little bit difficult to clean up.

We are happy to work with registries to help them with their own DNSSEC signing service if they want to do their own. I talk to a regional ccTLD just yesterday, and they were very, very eager to hear what we had to say on that.

Part of PCH's mission is to help strengthen the Internet infrastructure of the different countries. I have much more to say. I will ask for the next slide.

That's a map of the world, and we are everywhere.

UNIDENTIFIED MALE: No. You're not in [inaudible].

ROBERT MARTIN-LEGÈNE: Okay, we are not in all parts of Africa and Antarctica.

What we have is three locations where we have HSMs. We can sign in Europe, we can sign in the US, and we can sign in Singapore. The Singapore facility is a key ceremony facility where we do not actually sign with ZSK until we really have to. It is a possibility, but we mainly use it for a KSK signing facility. The other facilities can be used for either. Next.

A quick sales pitch. We do Anycast DNS, and we have more than 250 TLDs on our platform and more than 100 locations around the world.

We are very happy to install new nodes at any IXP that we consider an open and fair IXP. We connect directly to the IXP. We connect to every ISP in the IXP without setting behind some other [inaudible]. We might connect to a route server if there is one.

If there is no IXP close to you, we will be happy to help in creating one. We do that many times, and we even donate equipment.

I think that's it. Questions or none? Later?

RUSS MUNDY: We'll try to do the questions all together at the end. Thank you very much, Robert. Next we'll go to Joe Waldron from Verisign.

JOE WALDRON: Thanks, Russ. I'm Joe Waldron from Verisign. I'm responsible for the registry product management within our registry business.

The DNSSEC signing service that I'm going to talk about is something that, like PCH, is a tool that we implemented many years ago when we were first going through the processes to sign the root as well as .com, .net, and the other top-level domains that we manage. We realize as you look at the whole ecosystem that it does add a lot of complexity to the DNS.

At one point, prior to implementing DNSSEC, if you look at it as a fire and forget system, once you implement DNSSEC, it's no longer fire and forget. It adds a lot more complexity, and it makes the DNS more brittle, so how do we help the registrants implement this?

So rather as a kind of complimentary to helping TLDs sign, this is really a service focused at the registrant level for the domain name management. Can we go to that next slide?

This is a service that is really a cloud-based architecture that takes unsigned zones that registrants have, working through their registrars to opt into the service and signs those zones. It's intended to make the process as simple as possible so that it's a one-time configuration, and then we manage the signing and re-signing and updates going forward. You can see some of the features in terms of signing the zone. I'll show that, I think, on the diagram on the next slide. I'm more visual, so this helps be a little bit clearer.

So, a registrant. In a typical registration, goes to a registrar that will register a domain name, and then create an unsigned zone. In this model, I'm assuming that the registrar is providing that hosting. But that is really not necessary. It could be hosted through any third party.

Then that unsigned zone is then what would be available in the public DNS. What our service allows is that registrar to have the registrant make one configuration, which essentially opens up a access through their firewall so that we can access that zone file. We bring it into our signing service. We have all of the standard HSMs and signing processes. We sign it within our data centers, and then ship back to that signed zone master a signed zone.

Then we monitor the service throughout the life cycle of the domain name. We regularly go back and check and see if there are updates, anything that requires re-signing. If that's required, then we update those signatures that are required, and then that keeps the zone updated and current.

From the registrant perspective, they don't have to worry about how their managing all of the mechanics on the back end in order to take advantage of DNSSEC. Next slide.

This is really, again, intended to help address that perception that implementing DNSSEC is difficult. It does add complexity to the management of domain names. That was an objective of ours to overcome that for both registrars that were going to be providing those DNSSEC services as well as their customers so that they would have the ability to take advantage of the additional security features as well as some of the other services that will rely on DNSSEC. I know Danny McPherson, our chief security officer, is going to talk about DANE later this afternoon as one of those services.

Implementing DNSSEC really is an enabler for other opportunities, and we wanted to make that as simple as possible. Again, if some of these issues that a registrant would face in managing the DNSSEC themselves, if you have a failure, it becomes very difficult to diagnose and troubleshoot, so this really takes that out of their hands and makes it as easy as possible for the registrant to manage that. And we go to the next slide.

In summary, this is a service that we decided at the very beginning to offer for free to our registrars. Registrars can include this in a hosting package and implement that in any of the services that they're providing to their registrants. It is available for free.

I will say, in full disclosure, that the adoption rate is very, very low. Many registrars don't offer DNSSEC. Many registrars, if they do offer DNSSEC, don't provide these tools.

But these are available, and we're trying to make that as simple as possible as I keep saying. But I think that it really is a challenge to get the demand for this type of security and the complexity that is expected in implementing DNSSEC is one of those obstacles.

Again, we're going to continue to offer this service. I think that as more applications come online that expect and rely on DNSSEC, we'll see more adoption.

But it is something that if anyone is interested, you can contact me directly or by the e-mail address that's there. We've also published the

DPS URL, if you're interested in some of the technical specifications of how we're managing the service. Thanks.

RUSS MUNDY: Thank you, Joe, Robert, and Eberhard very much. We have left specifically time for questions in this session, so please start looking at and walking up to the mic with the questions that you might have. But while people are doing that, I have one to kick it off.

Eberhard's presentation was really focused in and getting a hardware-based solution for anybody, everybody, or the common man so to speak. Whereas, what I heard from Robert and Joe was more focused at higher levels in the organization. I was wondering if Robert or Joe would comment on whether or not your service is available to an individual zone holder if they wanted to come to you and ask for this service.

ROBERT MARTIN-LEGÈNE: We do offer a signing for all the TLDs if you're interested. We don't only do it for ccTLDs, but the take up time, because it requires a key ceremony, it's going to take a little while to get onto the service. Whereas, when you use probably soft keys, it's a little bit faster.

RUSS MUNDY: Go ahead, Eberhard.

EBERHARD LISSE: Two things. I noticed you greeted us as gentlemen and Eberhard. That's not the first time that has happened. One of my colleagues in the hospital always comes to the tea room in the hospital and says, "Gentlemen, ladies, and Dr. Lisse."

I also must say PCH has an Anycast node in Windhoek since about two weeks or so. It wasn't really true that I was saying they were not there. Now I forgot what I was going to say.

ROBERT MARTIN-LEGÈNE: You were going to talk about key sizes on [inaudible].

EBERHARD LISSE: Yeah. I was also saying we do our top level the .NA ourselves. But the second level com.na and net.na., net.na only has about five zones, PCH does for us, and that works very well. Com.na has got about 2,000. It's peanuts, but even smaller zones.

I think the workload for PCH – like he said – is the same. Put it in the queue, get it done. I fully agree with what he said. If we want to push acceptance, we need to find a way also for the end users, the banks and so on to actually do this at a low cost.

JOE WALDRON: Yeah. The signing service that we provide is available through registrars. We don't have any mechanism for end users to come directly to us.

I realize that there are cases where you have hosting providers or individuals who may have a difficult time working through their registrars, just because of some of the tools, especially if you're looking at larger volumes. I know there's some work going on to try to address that shortcoming, but right now, we're just exclusively providing that through the registrars.

RUSS MUNDY: Great.

JACQUES LATOUR: Two questions. Jacques Laotur with [inaudible]. First question for Robert Martin-Legène. That's how you pronounce your name. Just saying. Is your service free?

ROBERT MARTIN-LEGÈNE: Which one of them?

JACQUES LATOUR: Your DNSSEC signing.

ROBERT MARTIN-LEGÈNE: Oh, the DNSSEC signing. For ccTLDs, it's free. For new gTLDs, we haven't charged anyone yet, but the price currently is zero. It might see some inflation. For country codes, it is free and it will remain free.

JACQUES LATOUR: Second question is for Joe. In terms of your signing service, how do you handle the DS record, or does it make its way back to .com? Is that the challenge you're having?

JOE WALDRON: The registrant still has to take the DS record back to their registrar to have that entered into the registry. We can only take updates to the com registry or any gTLD registry from registrars, so the registrant still has to take that back.

ROBERT MARTIN-LEGÈNE: Can I ask a question? What I understand is that since the signing service is not directly connected to the registry, it seems that it's a kind of generic service. Why can't you engage directly with any customer of any TLD instead of having to go through their registrar channel? Why is that?

JOE WALDRON: Well, to get the DS record into the registry still requires a [mod] that's processed by the registrar to get that entry into the com registry so it'll be in the zone file. But you're right. It is independent.

I will say that there is one TLD that is not a gTLD that we're working with where we have completely integrated that where it is all done at once within the registry. There are some options, but there are also some restrictions just because of the registry/registrar model requirements that we have within ICANN.

JACQUES LATOUR: Is that requirement a documented fact? Does it say that it needs the DS has to go through the registrant, or is it something that we all assume it's like that?

JOE WALDRON: It would work the same. Whether you're using our service or any other signing service, the registrant will still have the requirement to provide that. If the registrar is doing it all themselves, then the registrar is handling that. That's why if we're offering a service through the registrar, typically, the registrar will handle that complexity because the registrar is offering the signing service, the registrar manages the customer relationship, and the registrar is passing the EPP transactions to us.

RUSS MUNDY: This is a very interesting topic. I think one of the reasons it may have been also driving Jacques's questions here was at the last ICANN meeting DNSSEC workshop in Singapore, we had a panel that was trying to discuss and address and get the discussion going about how can we make progress for some of the DNS service providers – some of the large service providers CloudFlare and Akamai, not their content providing side, but their DNS providing side – to be able to accommodate this challenge of having the need to get the signed information into the registry and done perhaps in a way that doesn't follow exactly the current established traditional model. Have any of the three of you thought about that problem at all, and if you have, would you comment about it, please?

EBERHARD LISSE: I haven't thought about it because we have no clients. But I feel you have to have your house in order before you can start going for clients.

The market in Namibia is extremely small. We have a total of 3,800 domain names and perhaps ten banks. If I go to the bank, I want to be able to say what we're doing without being laughed out of the room, so therefore, I first see that we get the infrastructure properly working, and then, for us, it's a small thing.

CoCCA tools has got facilities. We can do it automated, but it's so few, we can do it manually. It's not a bother.

JOE WALDRON: Yeah. I would say that we have thought about this. I think that there's a bit of a chicken and an egg issue here.

One is to have some mechanism for a non-registrar to be able to update authoritative records within the registry is not a trivial task within this community. This is a change to the existing registry/registrar paradigm, and where we see an opportunity that has such low volume, that's a tough issue to take to the GNSO to tackle an issue when they've got a very full schedule of things to work on. So if there's demand, I think that helps build the case. But I think that's probably the biggest obstacle that I see right now.

RUSS MUNDY: Interesting that you mention the volume aspect. Clearly, that's something that needs to be considered. At the panel last time, some of the participants in the panel were talking in terms of millions of names, so the quantity of activities at this point that want to do this may not be extremely large themselves, but the quantity of names that at least they're claiming that they're handling is very, very large. I wanted to stimulate a little discussion on that. Jaap?

JAAP AKKERHUIS: Jaap Akkerhuis, NLnet Labs. This part of the discussion reminds me of an attempt from Oliver [inaudible] and friends of CloudFlare, which also want for other people to deal with just the DNS echo [inaudible]. What this actually boils down to is that there has always been a silent partner in the registry, registrar/registrant relationship, and that is actually the DNS operator. It's not necessarily that a registrar is also the DNS operator or the other way around.

Now this is coming to attention to more people in more occasions, and there is actually some push to try and to see whether this [key] and recognize in the system can change, then it will be much easier to do that.

JULIE HEADLAND: I have a question from the Adobe Connect chat room. This question is from Brett. Brett asks, "Does Verisign publish a list of registrars that support their DNSSEC signing service?"

JOE WALDRON: I don't believe we have one published.

JULIE HEADLAND: Thank you very much, Joe.

RUSS MUNDY: It looks as though the line has subsided. Anyone else have any questions that they want to ask? Robert?

ROBERT MARTIN-LEGÈNE: Hi, Eberhard. I want to know if you have any experience with different key sizes on those smartcards. Is that something that can go beyond 1k, 2k? How much can they handle?

EBERHARD LISSE: I must say, Diego Espinoza has left the building, so I don't know. But this you can look up. We are experimenting very earlier.

At the moment, we do 2k, but I think it can do 4,000. But I'm not sure what the speed implications are.

ROBERT MARTIN-LEGÈNE: Probably heavy.

EBERHARD LISSE: Yeah. With 1,000, you can do five signings or eight signings a second. With 2,000, you can do two a second, so if you take four, then you can go and take a coffee and smoke when they do the signing. But it

doesn't matter because if it's for a small company or for a really small TLD, it really doesn't matter.

ROBERT MARTIN-LEGÈNE: I Agree. It's just for some TLDs that don't care about the big HSMs, sometimes I recommend that they start out with a smartcard, at least for the KSK.

RICK LAMB: I was wondering, Eberhard, if you had a chance to look at any of the ECC support on those cards? I think those cards claim they support elliptic stuff as well. Have you played with that at all?

No. All right. Thanks. Those are really great cards.

EBERHARD LISSE: I first would like to figure out why it's crashing and find a solution to that.

But I must also say this work has depended a lot – and you see it on my presentation – on work that Rick has done, and it's in production, for example, you can use key bundles. You can generate key bundles with these smartcards and use that. That's being used, for example, at nic.cr, so there is really a wide spectrum of possibilities for very little cost.

RUSS MUNDY: Well, if we have no more questions, I think it may be time for your great DNSSEC quiz. But before we do that, I want to thank all three of our panelists for a very interesting and stimulating discussion. Thank you.

EBERHARD LISSE: Since I recall the embarrassment from my last participation at the great DNSSEC quiz, may I be excused?

RUSS MUNDY: Paul, I think you're up now.

JULIE HEADLAND: On just a note, you should have on your chair a form where you can fill in answers for the quiz, assuming you want to play. I did notice just now that the form has space for 12 answers. There are only ten questions. I guess you could always try for extra credit or something like that.

But at any rate, please find one of these. There are probably some extra ones around. In fact, I see extra ones around on the chairs. Go ahead and get your answer sheet ready, and then I'll bring up the quiz.

If you'll give me a moment, Paul, I need to let folks in the Adobe Connect room know that we're doing this and that they can't really participate remotely, but at least they'll be able to see it.

PAUL WOUTERS: Welcome, everybody, to the great DNSSEC quiz. This is the first time I'm doing this. Depending on how it goes, it might be my last time doing this.

I slightly deviated from the rules but not very much. People who are comfortable with the previous rules will quickly follow up. I guess you all have to do this on an empty stomach. I thought we were doing this during lunch, so I'll make it quick. Next slide.

The rules: these are all the same as before. Use the form. Put your name on the form. When you're done answering, find someone next to you and they will go through the questions and evaluate it, and you get points. Next slide.

Sometimes there's more than one good answer to a question. Like an A record, you can have multiple answers that are all valid. You score a point for every valid question that you put in.

However, just like lame delegations, if you have one lame delegation, if you have one correct answer, you score nothing for that question. You either have a lame delegation or not. Be careful. You might want to not guess too many parts of a question if you want to score some points on it.

Then one last preamble slide. I find that the previous times when I was here that it was a bit unfair, so to level the playing field a little bit, I decided to hand out some handicaps. When you play Go, you get stone handicaps. I remembered high school. I got nine stone handicaps against my teacher and still lost.

Minus one point if you're on a DNS ops mailing list. Minus one point if you ever had or have an ICANN.org e-mail address. Minus one point if you have root access on a TLD server. Minus one point if you're a listed author in a DNS RFC.

And minus one point if you've ever used the nslookup or host command in the last five years. I have to say this has been obsolete for ten years or more now, so you should really stop using it. This is a point you really shouldn't have.

So, up to minus five points for people.

Question number one:. Next slide please. Which of the following are true?

The KEY, SIG DEL RRTYPE were replaced by the DNSKEY, RRSIG and DS RRTYPe.

Many countries have legal requirements that require DNSSEC to always use RFC-5155 opt-out.

And C: Dig, drill, unbind, bound, delve and knot are names of open source DNS software.

And D: Every key with the SEP bit set in a valid trust chain must have a corresponding DS record published.

I'll give a minute for people to think about these questions. No one is cursing yet, so it's good. We'll go to the next question.

Question two: which of the following situations could lead to a DNSSEC validation failure?

Expired RRSIG records, a melted HSM card, RRSIGs that are only valid an hour from now, a disk full on your signer machine, or a cable cut causing identical backup DNS servers to take over DNS resolution. Next slide.

Question number three: which were the first DNSSEC signed countries on each continent?

For the record, I used continent as in how Wikipedia defines a continent, which it might not be the correct way of doing it. I won't read all the names, but according to Wikipedia, there are seven continents.

I already notice a little bit of an issue. On a previous slide early in the morning, I saw that one of these countries listed was listed on a different continent, so I blame Wikipedia on that. Next slide.

How many times has the Root KSK visibly changed, excluding any TTL changes?

Never, once, twice, or three times. Next slide. We're halfway through.

Which of these TLDs was signed before the root, but is no longer a signed TLD?

.test, .um, .example, .aq, or e164.arpa. Next slide.

When deleting a delegation from a zone, what should be done with its glue records?

Remove the glue if not used by any other zones, remove the glue regardless of other zones, keep the glue and do not sign it, keep the glue and sign it.

Remember more than one answer could be right. Next slide.

Did the well-known open ssl random "Debian bug" impact DNSSEC?

No, because DNSSEC signed zones are served statically.

Yes, and various TLDs had to perform emergency rollovers.

C: No, because Open DNSSEC and Bind do not use open ssl to generate keys.

Or D: Yes, about 65 vulnerable keys were found, but none in TLDs. Next slide.

What was the .nl.nl zone?

Was it the first DNSSEC TLD zone, a missing dot leading to a large DNSSEC outage, an early experiment that took the .nl domain and republished it using DNSSEC, or an active delegated zone owned by Olaf Kolkman who uses it for IETF DNSSEC experiments.

I don’t know what it is with Dutch people and DNS. I don’t know how we ended up being so overly represented. That’s nothing to do with water. Next slide.

Which one of these DNS keys will work best on resolvers throughout the world?

I'm clearly not going to read out these blobs. Remember the word one is highlighted in bold for a reason, so on this question, you can only have one good answer.

Then the last question is for those people who think that they've not done so well up until now. This is where you can really score a lot of points because each good answer is one point. Which TLDs were signed before the root was signed?

Now Wes is looking up. Do the next slide just for Wes. This I will give a couple of minutes because clearly everybody has to go through their atlas and figure it out.

Anyone still guessing or has everybody settled down on giving up?

So, the answers. Next slide please.

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: Oh, yeah. Sorry. You should swap your paper with a trusted person next to you. Also, don't forget your handicaps. Maybe write your handicap on your slide as well, so we can discount those points properly.

The first question: which of the following were true? None of the answers are correct. If you have none of the answers, you get one point. I went to teachers college, so I learned to be mean to my students on tests.

UNIDENTIFIED MALE: [inaudible].

PAUL WOUTERS: That's right.

Second question: which of the following situations could lead to a DNSSEC validation failure? All of these have happened to TLDs.

I'll explain the last one. The last one the TLD automatically switched over to their backup DNS servers and somehow, they got their [DO bits] stripped out of their answers. So, even though the machines were identical, the transport was still mangled enough that it didn't work.

One point for each answer. You can score five points on this question.

Next question. If anyone has a question or thinks I'm wrong, you should definitely interrupt me. Go back one slide.

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: You're sort of saying, if I'm walking, I can't get into a car accident.

UNIDENTIFIED MALE: [inaudible]

RUSS MUNDY: The moderator is the final authority in this game.

PAUL WOUTERS: Next slide. This is the slide I feared most because I might be wrong. I think not, but clearly, someone earlier demonstrated and said that Puerto Rico was actually not in North America, but in either Central or South America. I am definitely not an expert on this. Again, I used Wikipedia to determine if it was North America or not, and it told me it was North America. Someone who edits Wikipedia should update this stuff.

If that's the case, if Puerto Rico is wrong, then I guess the first one in North America would be .US I think, Ed?

ED LEWIS: I think so.

PAUL WOUTERS: Yeah. If you had none of these, because you thought US was the one, then you will also get a point. Next slide.

How many times has the root KSK visibly changed? Three times is the correct answer. Did anyone say three times?

Wes said three times. Wes remembered the outage on January 10 when the root key briefly revealed itself by accident, and then quickly masked itself again through all zeros. Next question.

This was the midway question, which in case you read the title was a dead giveaway because the answer is B, Midway.

I was tracking this because this was one of the first ones when I was still doing my Google-based DNSSEC maps. At some point, it just vanished. I was like, "What went wrong?" Then I talked to a few people and they told me, "Yeah, yeah. Just don't talk about this too much. Let's just forget about this."

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: Not when I checked it a couple of days ago. Really?

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: No. You're getting an NESEC.

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: The root validates. But you're getting an NSEC because the entire domain doesn't exist. Next one.

What to do with glue? Basically, people haven't decided what the best solutions are, so all answers except C is right. Obviously, if you keep the glue in your zone and there's no more delegation, you're obliged to sign it. You can score three points on this question. No disagreement here. Next question.

The random effect. The open ssl bug. Apparently, 65 keys were indeed found that were weak. But as far as I could trace back, there were no TLDs with it. No corrections from people. No TLDs. I was actually right. Good. Okay, next question.

The nl.nl zone was the early experiment where they actually took at TLD, copied it under the .nl.nl zone, and then signed it. This was still back in the days when I was living in [inaudible] close to SIDN, and we did the [inaudible] l signing with the old records, still. This was still with the key in the [SIG] records. Next question.

Anyone disagrees? I'm open for arguments. But I'd like to see if someone can tell me why D is wrong.

UNIDENTIFIED MALE: [inaudible]

PAUL WOUTERS: Yes. It doesn't start with AW. That is a very good observation. Do you know what that means?

UNIDENTIFIED MALE: Yeah. It means it doesn't validate.

PAUL WOUTERS: That is incorrect. It validates fine, but it will use a little bit more CPU because it's actually using a larger public exponent. Google doesn't validate the larger exponent, so for Google DNS, it doesn't validate. There's no reason it shouldn't fail more, but because Google doesn't support it, it actually will fail more. Warren [was at] another meeting I think. I was safe there.

Then the last big question. Let's see how many mistakes I made here.

So, CL, I'm not sure if they actually managed to win or not because it was on the same day that the root was signed according to my data, so I don't know if they win or not. You can have it.

UNIDENTIFIED MALE: Which TLD is the PTR?

PAUL WOUTERS: PTR?

UNIDENTIFIED MALE: It's on your slide.

PAUL WOUTERS: Good question. Sorry. That's Puerto Rico. That should be PR. If you have PR, it counts as a point. If you have PTR, it does not count as a point.

Did I miss any TLDs? Any claims?

You have all the questions, so you can add them all up. Next slide.

Give you the score card. If you are from minus five to zero, you're a DNSSEC skeptic.

On the other side of the spectrum, if you have anywhere between 32 and 37 points, it means that you scored a perfect score. Yet, you get no handicap to start with, so you're extremely lazy. You know everything, but you've not written an RFC, you're not on any of the mailing lists.

I should really want to be in the section one to four, which means that you're really enjoying the world out there. Do we have any DNSSEC ninjas? Well, I guess, no procrastinators, right? No.

Any DNSSEC ninjas? No.

Any DNSSEC historians? Oh dear. Good thing I kept all those names so positive.

DNSSEC experts?

DNSSEC enthusiasts?

UNIDENTIFIED MALE: I don't think we're equal to the titles.

PAUL WOUTERS: DNSSEC users? One. We're all DNSSEC fans then at least.

Well, thanks, and if you don't hate me too much, I might do this again next time.

JULIE HEADLAND: We have lunch now. I think we should let the winner get to lunch first. What do you think – along with Paul? Lunch will go for an hour. It will go until 1:30. Please go ahead and help yourself. Thank you very much.

UNIDENTIFIED MALE: I just want to say thanks to Paul for stepping up to go and do this. Maybe next time, lose the Dutch answers, though, or something.

[Break]

RUSS MUNDY: So folks probably ought to think about finding a convenient end to their conversations for a little bit and getting your last set of drinks for our big session here. I think Dan already asked the next panel folks to start moving their way up here, so we could get started on time.

DAN YORK: Wes. That would be you, Wes. That would be you. Mark, you can end your conversation with Wes now, okay.

Hey, Mark, where's the tie, too? There was a picture of you that was tweeted out today that has a picture of you looking very sharp in a tie. I wanted to see that here.

MARK ELKINS: [inaudible]

DAN YORK: Wherever you wish to be. I'm sure there is. I'll tweet pictures of you. Don't be scared.

All right, so let's get going. Thanks again to Paul for the DNSSEC Quiz. Thank you as well to our sponsors, which we should mention on the back of this page. That lunch you just had is courtesy of Dyn, .CA, Afilas, .SE, and SIDN. We do have to just say thank you to them for paying for the food which allowed us all to eat that. Thank you.

RUSS MUNDY: The lunch wasn't free for them, but it was free for all of us. Thank you, guys.

DAN YORK: All right. This afternoon we have our session where we want to talk about what we can do now with DNSSEC. Now that we have the DNSSE infrastructure out there and the pieces are there, what can we do next?

The answer to that question is going to be brought to us by a number of speakers who will be talking about what we can do with DNSSEC and specifically DANE.

Actually, I realized – Jaap, are you going to talk about what DANE is? All right.

JAAP AKKERHUIS: [inaudible]

DAN YORK: Yeah. We got some dames floating around, too. There's more jokes. Okay.

Anyway, we actually have four speakers. We have Jaap Akkerhuis from NLNetLabs here. We've got Wes Hardaker from PARSONS Technology. We've got Jacques Latour from CIRA, and we've got Danny McPherson from Verisign.

Oh, why. Am I – are you something else?

UNIDENTIFIED MALE: There's no Technology, but that's okay.

DAN YORK: Parsons. Sorry. Okay. So first up I'm going to turn it over to Jaap.

JAAP AKKERHUIS: Yes. This is a story about one year experience of DANE. I do want to explain what DANE is. Next slide, please.

A lot of this work is actually done by our German friend who is part of the – and all errors are mine. You noticed that I just checked and it seemed that a couple of the slides have a very odd format, somehow. But that's my error, of course. Anyway, let's go further. Next one.

DNSSEC and DANE. As you realize, the DNSSEC is not really an application. It is just part of the infrastructure. What it really does is it gives you authenticated data. But it enables use of DNS for all these types of applications, such as DANE.

DANE is the DNSSEC Authenticated Names Entities. Basically, what it tries to do is it doesn't give you security. It allows you to verify how the security is being made. Next please.

As we know, we have two different encryption models. We [inaudible] a lot more about it later on. This has more or less opportunistic when you expect anything. You downgrade to non-security when there is no security. I most of the time [inaudible] failure while with the

mandatory encryption you really expect is mandatory. You force the encryption. You do alarms.

To summarize, actually opportunistic encryption actually the message has more priority of the security, while on the [mandatory], you really want the security and that's the first priority. Next, please.

Opportunistic TLS issues. There are quite some issues with it. One is the CA model .You can do downgrade attacks and these man-in-the middle attacks or the monkey-in-the-middle, what it's also known as.

The incomplete automation for the certification roller. If you have certificates and they expire, then you always notice that at the moment you are using it, and people seem to forget to update this stuff.

The broken certification model. Well, it's just a matter of trust if you trust the certificate agent or not. Well, and that's it. It's like trusting someone with blue eyes.

The certificate has been compromised in the past. They issued the wrong or unauthorized certifications. There's also in America the declining trust in root certificates since Snowden. It was there before, but Snowden really put it on the front page. Next, please.

Here's some interesting examples: Turkstrist/Diginotar [inaudible] whole certificate agent going under in flames. Next, please.

Man-in-the-middle attack. It can intercept TLS-secured conversations with a matching certificate by just pretending to use the same

common name. It is easily done since everyone really accepts self-signed certificates. You basically click, “Yes, I trust this guy,” and there we go. Next one, please.

The session downgrade. This is a quote from Electronic Frontier Foundation: “20,000 EFF were discovered that there were a lot of ISPs which actually move TLS on the conversations and nobody will notice.” Next please.

This is one of the broken slides. What we wanted to say here is that the man-in-the-middle can actually say, “Well, let’s move this [inaudible] in the initial handshake and just continue with the mail.” So you’re not doing TLS anymore. So this is not a real separate policy channel. Next, please.

Automation is not there. I mean, really the guarantee is that the certification authority is the one who certifies that the [decision] is secure. All the verification needs to be manual. You really need to know a lot of stuff. The need for [inaudible] certificate change is something you really want to do. Next, please. Next, please.

You can trust certificates, no problem, but wouldn’t it be nice that you verify that they’re actually done the way you expect them to be done? That’s what DANE gives you. Next.

So you add a policy planner channel. You add a trust layer. You indicate what I prefer – encryption, too – and the identity you expect. Next, please.

That's where DANE comes – DNS-based Authentication of Named Entities, RCF – the number just fell off the page. DANE uses and actually requires DNSSEC. So DNS becomes the policy channel, a separate channel for how you do policy. And it adds a trust layer.

How does it do that? Well, new resource records. Well, if the record is there, it shows you that the service is there. It also carries specific data for the service you do. Next, please.

The current use cases are HTTPS, SMTP, OpenPGP, and S/MIME, but the last two are actually still under discussion, very hefty discussion. Let's first look at HTTPS. Next, please. There we go. Yeah.

This is the [broken] format, but basically you have extra records, TLSA records. It gives you what type it is, what type of use it is, the service types, and the data associated with the servers, which actually has the certificate.

I will actually give better slides so they can put it online and fix all those errors. It makes it so much easier. So that's what's happening. Next, please.

What you do in the browsers – this is 14, but what you see, the little thing up there – comes from our friends from Czech, and the key says, "Yes, this is actually a DNSSEC-secured site and the certificate is actually correct according to the TLSA records." So you can actually trust that this comes from the site that it comes from. Next please.

CZ.NIC here is the TLSA validator and you go out and install that [inaudible] Next, please.

SMTP. This is actually the SMTP and it's not a person-to-person, but it's server-to-server security. Next, please.

Ah, this one actually worked. This is similar, accurate. It's Port 25. The protocol is TCP. The name is open. The host is NLNetLab. This is a TSLA record and resource type is 3. There are a lot of simple differences in what these [inaudible] mean, but there's selectors, [matching] type and then the data associated with the cert. NLNetLab is using that. Next, please.

The initial draft is by Wes and Viktor Dukhovni. They kind of finished it. It currently is in the Internet Steering Board waiting for the final step of approval. I think maybe even in the 48-hour period.

UNIDENTIFIED MALE: [inaudible] editors. It's not in 48.

JAAP AKKERHUIS: [inaudible]. But it's basically done. The first implementation are in Postfix, Open SMTP – I did something on that – and [Exim]. They do have implementations of that. Next, please.

The guys, sys4, have an SMTP validators. You just type in whatever domain it is. You'll see the result on the next slide, I hope.

Here you see it for NLNetLabs and without the gory details, the server is open in NLNetLabs for IP addresses. You see that there are two TLSA records. One is called a [inaudible].

Why is that? Well, that's a self-signed cert record, so it's not known by the TLSA validator in Germany. But if they added to their chain, they will validate it properly. It's actually from the CA cert guys from Australia, the non-profit stuff. So that's how you see the details of this thing. Next, please. I may be running out of time. I [inaudible] out of time.

As I said, there's still work on S/MIME and OpenPGP. Next, please. And it's under construction. There are a lot of problems. It has to do with how you deal with all the people who are doing SMTP but don't adhere to standards and introduce variance in the local part of the mail address. But if this is going to work, you have to have security directly from person to person and not only from server to server. Next, please.

So what are actually the lessons we learned? DNS is an infrastructure to build upon, it's a security-enabling technology, and DANE verifies the trustworthiness level of your communications. I think this is the end of the lesson. Next, please.

Ah, yes. There are a lot of stories why you should not do this. DNS providers with incomplete DNSSEC-support. Well, [inaudible]. With DNSSEC, issues become mission critical. Well, that's not true. DNS is actually mission critical, but with DNS, you see all the errors so it's easier.

So there are some more of these things, which actually can easily be fixed if we want to work on it. Next, please.

DNSSEC is actually a one-time cost. If it's there, you can build a lot of stuff on it. It's an open standard. DANE allows scalable and secure trust management. It reduces the management cost in the long run because you can automate things like certificates and all of this various stuff. Next, please.

Questions, or do we leave that for later?

DAN YORK: Well, let me just ask. Are there any questions that you have for Jaap or any of the panelists about DANE in general? We're going into now some more specific use cases of it.

I'm not seeing anybody rushing for the mics, so if you do have more, we'll go on and have Wes talk a little bit.

Also, I would say to any of our panelists, too, if you also want to get up from behind the table, we do have handheld mics if you want to walk around. But you can also just sit here.

WES HARDAKER: All right. I'm Wes Hardaker, and I'm going to talk today on Opportunistic SMTP and security. I'd be happy to get up and walk around and do a dance if it's more entertaining because this is not exactly the most lively of subjects.

DAN YORK: Up to you.

WES HARDAKER: Okay. So let's go on because you don't want to see me dance. Really quickly I'm going to go about what e-mail is, where it can go wrong, how DNSSEC helps, and then securing SMTP, using DANE and DNSSEC together. We'll find that that's really the only solution.

In the beginning I'm going to go over a little bit of a scenario. Let's pretend that we have this typical situation. We have Alice needing to talk to Bob. Alice has an ISP and Bob has an ISP. Next.

What happens is Alice talks to her ISP first, and she talks to her mail transfer agent in particular. Then – next – Alice's ISP actually talks to Bob's ISP, and they exchange mail. So Alice sends the mail to her mail transfer agent. The mail transfer agent says, "How do I get to Bob's ISP?" and it goes to Bob's ISP. Finally – next – Bob actually pulls it down using IMAP or POP or something like that. Next.

The only part that we're going to talk about with DANE today is that middle piece. It's the ISP-to-ISP communication. Bob and Alice usually already know how to talk securely to their own ISP (subject to some debate).

So e-mail server to e-mail server is really how DNS gets involved. Next. Let's talk about actually what happens underneath the hood a little bit more between those two ISPs. Well, what really happens is the mail transfer agent says, "Hey. I need to send mail to Bob's ISP.com. Where do I do that?" It talks to Bob's DNS server first. Next.

Then the DNS server responds back, saying, "Well, if you're trying to talk to mail for Bob's ISP.com, you really want to go to mail.Bob'sISP.com. This redirection effort is really important because this is actually where attacks come in later that we'll talk about. Next.

Finally, the mail transfer agent, once it knows where to send it, actually sends it to the real mail transfer agent for Bob, which would be mail.Bob'sISP.com. Next.

Unfortunately, that's like the simplest possible diagram I could draw that made any sort of clear and easy sense. The reality is it's a lot more complex than that. There could be multiple DNS servers. Almost everybody should have at least two DNS servers.

Alice's mail server actually asks for ISP's resolver. Alice's mail server does not actually talk to the DNS server directly. He talks to his own DNS server in his own ISP, which then does the negotiation. It's actually a much bigger web of problems. There may be multiple resolvers that Alice's ISP is talking too as well, her mail server is talking to within her ISP.

So what does it really look like? It looks more like this. It's even worse than this. I'm not going to go through this step by step, but I only have one DNS server in each of those cases.

So you can see that the number of possibilities for all these machines talking to each other actually gets rather complex. This is about the simplest you can make the more complex diagram, but as I said, there's actually multiple servers that you may be falling back to. Next.

Back to this slide of showing the complexity a little bit. Next.

What can go wrong? First off, there can be multiple DNS servers. They can be compromised. That's where DNS attacks occur, through cache poisoning. Between the two ISPs, there could be DNS problems.

Alice's mail server actually talks to her ISP's resolver, but that could be compromised and cache poisoned. There are multiple mail servers, and they could each be individually compromised as well. Well, I'm going to lay that one of the table because if a mail server is compromised, there's nothing DNS can do to fix that. That's a routed machine, so that's the one thing that we can't fix here today.

There can also be a man in the middle. The man in the middle is somebody redirecting, say, Bob's mail server to somewhere else though these cache poisoning attacks. If you look a MX record for "I need to go send mail to Bob. How do I do that"? it could redirect you very easily to EvilHacker.com instead. The mail system is designed to do that, and that's really where DANE comes in and solves that problem entirely. Next.

For the first two, when there's multiple DNS servers that can be compromised or you're not sure where you're getting the answers from, DNSSEC makes sure that you're getting the right answer.

This is kind of important because even if the DNS server is compromised and the data was created offline, there is no way that DNS server can convince you that the data is right, even when the

machine itself is compromised. That's one of the benefits of doing DNSSEC with offline signing.

The resolvers have the same problem. If you're doing validation all the day to the end application, even if the resolver is compromised and serving bad data, you'll detect it. That's the importance of DNSSEC.

Now DANE comes in to prevent man-in-the-middle-type of attacks, where you can't be redirected to EvilHacker.com, and even if you are – that's actually possibly okay if you've outsourced your mail to EvilHacker.com. A lot of people outsource their SMTP servers to huge infrastructures that handle hundreds of hundreds of thousands of ISPs' mails, like Google, for example.

How do you know that you're getting to the right place and you really did trust all that? Between DNSSEC and DANE, that's exactly how it happens. Next.

There's SMTP vulnerabilities as well in that the MX and the A records in the DNS can be spoofed. I just talked about that. It redirects the SMPT clients to somewhere else. Where that somewhere else could be is a problem DNSSEC detects that and it won't be perceived, as I mentioned.

Eavesdropping is incredibly easy. If you are in the middle or if you are listening to it, it is unencrypted by default. Anyone listening to the traffic, it's unencrypted. If you can spoof it, you can actually put yourself quite easily, if you can spoof the MX or the A records in DNS.

Opportunistic encryption helps. Opportunistic encryption at least prevents sniffing along the side, but it's so easy to actually insert yourself in the SMTP chain that you need to do something better than that.

So you may only be just encrypting to – let's go on – a man in the middle. A man in the middle, if DNS is spoofed and things happen, you could end up talking to a man in the middle when you didn't know it.

SMTP as I mentioned is authenticated and unencrypted by default. The problem is that with opportunistic encryption, you can actually say, "Hey. I do encryption. Do you do encryption?" Both sides say yes and it gets encrypted. Well, that's great.

Well, a man in the middle actually says, "No, I don't do encryption. I'm not going to give you a certificate," and you have no way of verifying whether or not they should be doing encryption and should be doing authentication. There's no way of knowing that through the SMTP protocol.

CA solutions don't help. Certificate authorities really can't help us here because the man in the middle says, "I don't do security," when the reality is that it's supposed to, and you've been redirected through DNS in the first place. You're redirected right to the man in the middle that has a signed CA for EvilHacker.com because they can go out and register that. Next.

This is where DANE and DNSSEC come in for the win. It solves all of these problems. With DNSSEC, you can trust the MX record. You know

it's correct. You can trust that the TLSA record that you're getting that talks about the certificate that you need to talk with is correct. It has not been tampered with.

With DANE's TLSA record, it really states, "This is my certificate," so you know you're talking to exactly the right one, or, "This is the only CA that's authorized to issue me a certificate." You must expect security.

Here's the important thing. If you publish a TLSA record, any DANE-enabled SMTP server out there won't talk to you if you say, "I don't do security anymore." That gets around the whole man-in-the-middle problem where the person in the middle says, "I'm sorry. I don't do security." You have to expect it at that point. So you refuse to talk to people who won't do TLS if you publish a TLSA record.

The result is that you end up being connected to the right place, period. You can guarantee that. And it's encrypted. Problems solved. Next.

How do you do this? How do you pull this off? It's actually not that hard. Postfix 2.11 and Exim 4.85 – you mentioned Open SMTPd, which I did not know about.

JAAP AKKERHUIS: Okay. So apparently there was another one that I was not familiar about. The configuration. There's five lines of configuration to basically do [inaudible] DNS to publish your TLSA record, and there's

really only two lines that need to go the SMTP server. It's actually quite simple to set up.

Viktor Dukhovni, who is the co-author of [inaudible] draft to be honest has done much more of the work than I have – I've put a fair amount of effort into the draft, but he's been the primary author. He put a whole lot of effort into the Postfix implementation to make it very easy to use. Next.

The standardization, as Jaap mentioned earlier, is almost an RFC. It's in the RFC editor's key right now. What's more important, there's 1400 domains already using it. It's actually, as far as any of the rest of the DNSSEC deployments have gone, way high up compared to anything else. It's been fantastic.

JAPP AKKERHUIS: In Germany, there are ISPs. Big ISPs.

WES HARDAKER: Yeah. In Germany, there's a huge – there's actually another listed in a second of a lot of places that are using it – there are 2o of those ISPs listed in Google's Transparency Report. So they're not small domains.

That's the website on the bottom that Jaap mentioned earlier where you can go plug in your own domain and see how it comes out. When you're doing it, you can go plug in your domain. Next.

Here's some large early adopters. You can see that a lot of them are from Germany. The IETF.org has a SMTP server that's compliant.

[inaudible] has it. The NLNetLabs folk of course have it. CZNIC of course has it. There's a lot of the standard faces, but Germany in particular is really ramping up. They have a whole conspiracy within the government to actually make that really push out, which is a really wonderful thing. Next. Sometimes there's good conspiracies.

Any clarifying questions on this at all? That's actually a picture from Singapore, where we were last.

DAN YORK: Thanks, Wes. I think this is fascinating to see that DANE is taking off as well as it is in SMTP. On the note of Germany, it's something that was going on in social media today, but I sent a note to [Peter Caulk] at DNIC and they're actually doing what they're calling a DNSSEC Day on June 20th in Germany, where they're going to be working with a lot of folks and promoting DNSSEC specifically around e-mail. They're doing it the government security agency and with DNIC and with [Hiza], one of the local media outlets there.

Again, I think we'll see even more of an uptick of DANE usage, well, certainly within Germany, for SMTPs, so it's great to see this.

Questions from the community. How many people have implemented DANE with SMTP? Okay. I see a number of folks here.

Anybody got any questions for Wes? This is your time to put him on the spot.

WES HARDAKER: One final comment is that I did this in about 10 minutes just on SMTP. There is a 30-minute long video on YouTube that I made that is all about DANE and SMTP both. It goes into even a little bit more detail that you're welcome to look up if you'd like.

JAAP AKKERHUIS: The .PR registry actually has a website where you can very easily generate a TLSA record. You just type in your MX server and out comes the TLSA records. It looks up the certificate. It does all the stuff. Even putting it into DNS server [inaudible]

WES HARDAKER: One last word of warning. If you do implement this, make sure that when you roll your certificate in another year you make sure that you go update your TLSA record. That is the number one failure. It occurs about a year later when people go pull a new certificate from their CA.

UNIDENTIFIED MALE: Do they send a warning e-mail?

WES HARDAKER: There are monitoring sites you can do that. You'll get a warning e-mail, but an unsecured warning e-mail.

DAN YORK: You're seriously not going to ask Wes any questions? Come on. Somebody.

UNIDENTIFIED MALE: Go back two slides to that URL. One – yeah.

WES HARDAKER: Oh yeah. The DANE.sys4.de

DAN YORK: Anyone else? Come on. All right. You answered one of my questions that I was going to ask you, Wes, already in your slides, so I don't have a chance to ask you that.

WES HARDAKER: Then I succeeded.

DAN YORK: You succeeded. Actually, it's this point here, the 1400 domains. Look at DANE usage. One of the things that people mention is they say, "Well, how come websites aren't using it or browsers aren't using it?"

Well, look at what's happening out here. In other places, we're seeing it here. The other space that we're seeing a lot of DANE usage is in the XMPP space, where there's a l0t of the public Java servers are all using it for a similar kind of server-to-server kind of communication.

All right. Well, if you're not going to ask questions right now, we will go on to – I think when we looked at the sequence, I think Jacques made

sense next, and then having Danny coming back at the end with – I want to have Jacques come here and talk about…

JACQUES LATOUR: DNSSEC automation.

DAN YORK: Right.

JACQUES LATOUR: All right. I'm Jacques with .CA. Today I just want to go quickly. There's a lot of new stuff happening with OpenPGP and DANE and S/MIME encryption. I think pretty soon there's going to be a demand for people to register their domain.

Right now with .CA that process is not very efficient. That's what I'm going to talk about here in the next ten minutes I guess. Next slide.

At .CA, we have about 140 signed delegations. This is pretty sad. The reason for that is the registrars for .CAA don't necessarily support DNSSEC to EPP or the web interface.

They're not interested in doing it, and they say it's a DNS operator function. We believe it's a DNS operator function. Every time I go to talk to my registrar about DNSSEC, they run away. They don't want to talk to me. But they think it is a DNS operator function and we should do something around that model.

This presentation is about talking about a new model of doing DNSSEC registration using DNS operator. Next.

I'm not going to cover this, so next one. Okay, go back. There is a sacred cow. The issue that we have right now – and I don't necessarily believe that is true – is that everything has to the Registry, Registrar, Registrant model (the RRR) for every DNS information that has to go in the registry.

So the registry is authoritative for information, but the source is enough to all come from the registrant. In this case, I'm proposing that the DNS operator is actually allowed to put stuff in the registry. That's what this is about. Next.

This is usually a built slide, but typically if you look at a registrant in Canada, you can have a registrant that gets a domain to HostPapa – that's a hosting provider. The registrar for HostPapa is Tucows, which is directly connected as a registrar. Then with HostPapa you can use CloudFlare. So CloudFlare is performing the DNS operator function on behalf of HostPapa, on behalf of the registrant, me, on behalf on the registrars [inaudible].

So if they assign the domain, they need to get the DS record technically through the food chain to the registrant or the registrar or the hosting provider. It's not clear how to do that, and that's where DNSSEC breaks the registration piece. Next slide.

So we're proposing is that one, the Legacy interface, if somebody wants to use EPP in the standard mechanism, it's there. It exists. I'm

proposing that we build a registry-based bootstrap process and ongoing maintenance interface for the DNS operator.

In this instance, CloudFlare, if they operate the DNS, would have access to the .CA registry to update DS records, or do DNSSEC maintenance ongoing for domains, and not have anything to do with the registrar or the registrant. So they run the zone on behalf of multiple parties, and they have access to update a registrant. Next slide.

The issue is that you need to set up the bootstrap process for a domain, and the way we figure it out is that you need to prove you control the zone, and you need to prove that you operate the zone. If you have these two things, then we'll allow you to submit to put a request in to create a bootstrap for DNSSEC.

The control is done by adding a TXT record, _delegate, with the TXT ID of the KEYID for your DNS key that you want to put in the registry. So that's the first piece. You go in your zone and you put something to say, "I want it signed." Then you to web interface or a RESTful API and you put a request to sign that domain to have it inserted in a registry. Next slide.

The validation is done over TCP. You check to make sure the domain that needs to be signed is properly signed, that DNS is good at the child and parent, everything matches. There's no lame delegation. Otherwise you lose a point or you get no points.

Then the TXT record actually matches the KEYID in there. So if that's all there and it's over TCP, then you prove you control the zone. And that's it.

If somebody goes in and wants to re-bootstrap a domain that's already bootstrapped in the system, you ignore your request. If the domain is not signed properly, there's errors. You just dump it to the user to fix. Next.

So the stem looks like this. People that will do it infrequently, we have a web interface, like a registrant. You sign your domain. You go to the registrant web interface and you say, "I want to sign my domain." If you're a DNS operator, a registrar, a hosting provider, or a content provider – any one of them – we have a RESTful API with an ACL. Then you can do bulk transaction.

The validation maintenance is what I talked about. That's where it does a TCP checking. If everything is good, then it talks EPP to our registry to insert the DS in the registry. That's how we bootstrap a domain. Next one.

We actually have prototypes of this. If you go to CIRA.nohats.ca, you can put a domain name in there. All it does is generate DS in the end, but it actually shows in the debug all the steps you need to do that were done to validate that you control the zone. There's a RESTful API you can play with. Next slide.

This is where it's simple. I like the simplicity here. The first little box there, you go to the web interface. All you do is put the domain name,

like in there it says nohats.ca. So you put the domain name you want signed, you click go, and that's it. That's your intention that you want the domain signed.

In the back end, it checks everything. It checks DNSSEC, the [RFC] to make sure everything is good. Then if it is good, it goes in the zone file. So you don't have to copy DS. You don't have to copy DNSKEY. There's no cryptographic material because the DNSKEY is already in the zone. If it's valid, we'll take it, create a DS out of it, and get it done. Next.

The RESTful API is the same thing. The idea is to allow large-scale DNS operators with access lists. They can do this automatically through an API. Next.

Then the idea is that, well, if we're going to bootstrap through this process, then we might as well maintain. This where we want to use the CDS and the CDNSKEY. That protocol automatically manages the key rollover with the signed zones.

We're still working on that. I'm not sure exactly what we need to do, but we know it's feasible. The concept is that we replicate whatever DNSKEY that have in the registry, but we don't allow un-signing of a domain. Next.

Right now we're building a framework to do this. There's a lot of questions. There's a lot of issues. Certain people have different environments than we do. Feedback is important.

Right now we have a couple of partners, registrars in Ottawa, that are willing to work with us to test this out. Some of the registrars have

hosting businesses and DNS operator businesses, and it's much easier for them to use this RESTful API to sign domains than to use their own EPP back end to submit a DS. So it's much simpler for them to do this and automated maintenance. It takes a big headache away from them.

We're going to make the code open source. Eventually, we'll develop a new RFC.

Then there was a discussion at the CENTR meeting in Stockholm a couple of weeks ago that potentially, if you separate DNSSEC information in the registry from standard registration, it makes the registry lock better. That [inaudible] compromise the domain and they change the name server to point somewhere else. If they don't change the DNSSEC keys, then the domain will fail resolution, versus being rerouted.

So that was something to look in there to see if it was really useful or valuable.

Make the Internet a better place. That's it. 54 seconds.

DAN YORK: And Jacques finishes up with 54 seconds left to go. In those 54 seconds, or 46 seconds or whatever else, anybody have questions for Jacques? Anybody else interested in working on this kind of project?

Wes is. Okay. Rick Lamb is in the back. Anyone else? All right. Cristian is. Yeah, okay, Paul. Paul owns the nohats.ca, or rents it or whatever we ought to say these days.

Anybody else? Questions? Thoughts? Anybody see this as a solution to the problem? Anybody – all right we got a few – yeah, we'll hear from CIRA. Okay.

DAN YORK: [inaudible. I have question to Jacques. Have you thought about what you want to do with the NS records and the [glue] and are you thinking of using CSYNC or one of the other records to even more than not use the Registry/Registrar model and go direct from DNS hoster to you?

JACQUES LATOUR: We need to start small and grow big, but the idea was a lot of content providers, like CloudFlare, Akamai and I guess Dyn, when they host a large amount of domain in a certain portfolio and then they want to move domains quickly because of a DDOS – they want to bulk change, I don't know, 10,ooo domains – they need to change DNS and the name server and the DNSSE keys quickly to do that.

Today they can do it with the standard mechanism we have. So the idea was that if there's a way to authorize the registrar without the [right] DNS operator to perform name server changes in the registry through this API.

So it'd be more agile, more responsive for a DNS operator as a registry to respond to large-scale attacks.

DAN YORK: Okay. One more question. I was actually talking to a registry earlier today and they said it's really confusing. If you're updating the DS record based on this mechanism, now the registrar doesn't have up-to-date information anymore because normally it goes through the registrar and they know what DS record has been sent.

Do you think that that can cause problems?

JACQUES LATOUR: To the registrar I talked to, the DNS keys or the DS, they don't store them.

DAN YORK: Well, they might, actually. I think mine does because it's in the GUI interface. When I go back in there and they show me what's there…

JACQUES LATOUR: They pull that from the registry.

DAN YORK: You have greater faith in my registrar than I do. So I don't know. I think my registrar, one of the ones they use, probably has that stored in some local database, and they pushed it up the parent TLD.

But anyway, Russ. Actually, Wes had a question first.

WES HARDAKER: No, go ahead.

RUSS MUNDY: Go ahead.

WES HARDAKER: I'm on the panel. Let him talk.

DAN YORK: All right. Well, while you fight it out, I'll say, Russ, you ask yours.

RUSS MUNDY: Okay. Primarily for Jacques, the concept of separating the source of the information that's in the registry that's associated with I'll call it the glob of this name would seem itself to introduce an additional threat possibility because you're getting some from one spot, some from another spot.

Is the general concept as part of this that you'll have a name server operator functionality that it may be residing with a registrar but it's, if you will, operationally separate?

The equivalent is they're running your own name service or they're using CloudFlare so that all of the actual operational running part of the DNS name that served on the Internet is coming from the same

spot. It's just going two different routes, where some of it goes through the registrar and some of it comes directly through this interface.

Is that kind of the picture in your mind?

JACQUES LATOUR: Yeah. For whoever wants to use a Legacy interface EPP, then they can manage it that way. Whoever wants to use the other web API or directly access us, the DNS operator needs to talk to us. They go different channel.

For .CA, we have eleven registrars that are DNSSE accredited. None of them do EPP. So we have an [inaudible] interface brand new for anybody to use. Right?

UNIDENTIFIED MALE: Yeah. I'll suggest that the effort going through the IETF should be a lot of fun because we'll also have to I think address some of the architectural use cases involved to sort of help people scope how this is expected to be working.

JACQUES LATOUR: Well, yeah. But right now it's not working, right, for us? So we need to do something.

UNIDENTIFIED MALE: Oh, yeah.

JACQUES LATOUR: And I see the light at the end of the tunnel for DNSSEC. I can see it [without] the application. Five years ago, we were here talking about validation or signing top-level domains. Now there's real application. We're going to show them what's happening. I'm not ready to support mass domain for the registry. I want to be ready to support a lot of domains for registration.

DAN YORK: Yeah. I'll say too we've seen another reason for this, for folks who are listening here. One of the other reasons why we've been looking at this is because of the large content delivery networks or content distribution networks, the CDNs, who folks like CloudFlare, who were here presenting last time, who would like to sign two million domains but in order to do that they have to be able to communicate with X thousand registrars – okay – and probably 600 registries or whatever to be able to go and do that, and right now the current system doesn't work to do that.

Wes, you have a question?

WES HARDAKER: Yes. I'm very happy that people are diving in this direction because your sacred cow comment is well-placed and that model does not work for some of the bootstrapping that you're trying to do.

But my question was actually related to the ongoing maintenance. You said you're doing CDS. Have you thought long enough into that, whether you're going to do sort of a push or pull kind of mechanism where the user would have to tickle a RESTful API for you to go query, or are you going to query all your subdomains?

JACQUES LATOUR: Yes. The idea is that we're going to go out and pull all of our signed domains on a daily basis or whatever right frequency.

WES HARDAKER: Excellent.

DAN YORK: All right. Let's give a round of thanks for Jacques – oh, nope. Jaap has something here.

JAAP AKKERHUIS: I'm glad people are developing tools to have this program. This is now eleven years old [inaudible]. All the first solutions were, "Well, come to regulate everything, so people need to do this and need to do that. We hand the keys over from the losing part into the winning part."

But this is not going to scale either. So I'm glad the problem is not being ignored anymore.

DAN YORK: All right. Thank you, Jacques. We should note, too, we apologize. Jacques name was left off the brochure. We all did that. That went through multiple different eyes to see that, and somehow we missed that, a bunch of us who were involved with putting that program together. But that was Jacques Latour from CIRA at Canada.

I now remember why I was going to have the order go differently because Danny's going to bring us back to the world of e-mail and follow a bit of what the same topic that Wes was looking at, but coming at it from a different angle. So I will give you over to Danny to talk about that.

DANNY MCPHERSON: Good, good. Thanks for the opportunity. I'm actually standing in for Eric Osterweil and Glen Wiley, who put this presentation together. I think have most of the answers, but if something comes up, we'll definitely get back and hat tip to those guys for putting this together.

Then Eric actually, at the past IETF meeting, in the DANE Working Group Session, did a demo of a Thunderbird plug-in, where this works today. I'll show you a pointer to that in a moment as well.

But fortunately, since I went last, this actually builds really nicely on what everybody else did to his point. Anyway, go ahead to the next slide.

This is all sort of motherhood and apple pie stuff now. We talked about all this. Basically, some of the challenges with DNSSEC were

that it solved a man-in-the-middle problem, but that wasn't enough for encouraging folks to adopt DNSSEC.

One of the points that some folks pointed out earlier is it changes the model from sort of "fire and forget" to "a lot of care and feeding is required." That's why Jacques and others are talking about, "How do I scale and maintain this in a way that doesn't require me to go deal with a lot of complexity and a lot of moving parts?" I think that's one of the things that we're all going to be struggling with, trying to figure out for the next couple of years. But that's a good problem to have now because people are looking at deploying DNSSEC.

If you have DNSSEC, what else can you do with that? That's some of what I'm going to talk about. In this presentation, we can probably skip the next three slides because we sort of beat this to death with Jaap's presentation and Wes's and so forth. But go ahead and step to the next slide if you would.

DNSSEC adoption. People are starting to adopt it. StatDNS.com. There is no shortage of places you can go look at adoption. Some of the stuff that Paul did and the quiz and whatnot were interesting about some of the early adoption. With any luck, we'll start to see a lot more. Go ahead and go to the next slide if you like.

Why DNSSEC adoption? What are some the challenges, of course? One of the key challenges is that it's not easy for people that aren't sort of DNS jockeys or DNS experts to maintain DNSSEC and to make sure it gets updated.

One of the things as well is to avoid downgrade attacks you usually fell hard and you don't resolve them and you give them a failure if something is misconfigured, as opposed to DNS that kind of mostly works. I think that's something that all this work is going to try to move us past.

One of the other things are what are the compelling applications? It was providing integrity checks in the DNS so that people can't lie, so temper-evident wrappers, of course. But one of the nice things if you have that integrity information, as we've seen already as Jaap and Wes and others talked about it, you could help fortify web PKI and you can help sort of secure transactions between mail servers.

But there are other things you can do as well that I'll talk about in just a moment that are interesting in using the exact same infrastructure and capability. So it's pretty much very lightweight stuff. It's kind of front loaded in the DNS since you have integrity protections there now.

One of the things we've been doing at Verisign and I know NLNet – no shortage of folks; Jaap and many others are starting to develop tools and infrastructure for some of these specifications. Let's go onto the next slide there.

DANE puts steam in the DNSSEC engine. I think the entire point of this slide is simply, "Hey, here's an application besides just securing the infrastructure or providing integrity protections that DNSSEC provides." So we've sort of beat this in the ground. Let's go on to the next slide.

How to make some progress? Of course, we have to move the adoption obstacles, and that's very much for example what Jaap was just talking about. If the registrars don't have a compelling reason to provide mechanisms to update stuff or invest in the infrastructure because they have to look at return on investment for things they work on, then how do we in the community around that to allow this infrastructure to scale? That's kind of what we're talking about here.

DANE and DNSSEC is kind of hard to understand. The tools and the infrastructure for this need to be enterprise-level sort of IT administrator levels to help folks get the deployment going. Okay, on to the next slide.

Now here's what I was going to talk about. Okay, good. So we've already similar to other stuff. Anyway, besides securing transport connections between mail servers or any sort of device or fortifying web PKI and taking your [inaudible] servers from sort of all the CAs embedded in the trust or to just the one that you actually use.

It can provide S/MIME protections. It can give us object-level security. S/MIME is not only used for e-mail, but it can be used for any sort of signing or encryption that you want to do on the Internet. It's very popular for that.

There is some current proposals in the IETF DANE Working Group. There were two proposals. I'm not sure how many folk here follow that. There's a Hoffman proposal and a Scott Rose proposal. I think the Hoffman proposal is sort of where things are headed and everybody kind of appears to be in line behind that.

I'll talk in the moment with the implementation that we have that early on implemented the Rose proposal and that model, but it's being modified now to implement what appears to be going forward, which is Paul Hoffman's proposal for S/MIME RR types in DNSSEC for DANE. Anyway, on to the next slide.

One of the things that we developed in collaboration with a number of folks, Eric and Glen in particular, is something called Libsmaug. It's a plug-in library. It's open source. There's working code out there. It implements the Rose proposal today, but again, it's changing to the Hoffman Proposal.

It utilizes full-featured stub resolver if you want to do that. They get DNS API stuff if you're familiar with that or libunbound and so forth and share libraries. It's on GitHub. There's the link. Okay, on to the next slide.

That was the S/MIME one. If you want to see some slides on that working, by the way, you can check out the GitHub site. Then there's also Thunderbird extension there that I mentioned was demoed earlier on.

One of the other things we've done – I have a quick video that probably would have sufficed at three or four slides. But one of the other things the guys put together, Eric and Glen in particular, was a provisioning portal. If you want to sort of muck around with S/MIME [EAE] certificates today or [PMTA] certificates, which [inaudible] payment stuff, then basically you can set up an account on this system we have and you delegate to that effectively, put the DS records in the

zone we'll give you, and then basically use this as the delegation. It'll generate the records and provide a full sort of interface. Let's go on to the next slide. Is that the last slide?

Okay, so basically you want to pull up the video now. Do you have this? It's kind of boring. I was going to do a live one and I was worried that we might have some connection issues. All this is showing you is a minute-and-half, two-minute video and we'll go through it really quickly. Basically all it is showing is that you log in, you create an account, you check some boxes, you throw the DSKEYs in the parent zone. Then you can do a dig or sort of explore what the S/MIME records – you can hit play any time you want while I'm talking here, rambling.

So this is PortalDANE-Provisioning.VerisignLabs.com. It'll be openly available very soon. Basically it's super simple and just allows you to associate resource record types per user or to delegate full zones underneath this if you want, and to play with this. Once you get comfortable with that and the records are generated and so forth, then you can use this to sort of get some feelings and the mood and the production environment for whatever it is that you'd like to do.

Basically, that's sort of the crux of it, and it's sort of an underwhelming video here, but I didn't want to not have access. So this is basically just showing an account creation. It's literally this simple to get the records published and online and reach more of the global DNS. It gives you an opportunity to mess with that.

Eric and Glen – there's actually an e-mail address on the last slide. We'll look at it in a moment I think. You can reach out to those folks and get your account set up here if you'd like to do that.

I know other folks are working out things akin to this as well. It's just meant to help foster adoption and get some deployment going with these resource record types.

Anyway, while that's finishing, I think what I'll go ahead and do now is transition to see if I have any questions about anything I've said so far, or if anyone has any comments. I know I moved fairly quickly, but I wanted to stay on time there.

DAN YORK: Danny, you're not in marketing, are you?

DANNY MCPHERSON: I'm clearly not in marketing. I'm filling in for someone [inaudible]

DAN YORK: Well, no. It was the, "It's boring, uninspiring." I was like, "Wait, wait, wait," you know? I do have a question for you. Could you perhaps explain how S/MIME is different from the other – I know the answer – but what's different from this from the server-to-server encryption that Wes was talking about?

DANNY MCPHERSON: Ah, yes. That's actually a great point. There's sort of two sides that you want to look at. One is at the network and transport layer, which is effectively what Wes was talking about, where you're going to secure the communications between two entities.

But at the same time, what S/MIME provides you is the ability to secure objects or sign and verify the integrity of any kind of object. In this case, the de facto mechanism that people use today is usually PGP. PGP is built out of a web of trust and you know people and you go to key signing parties. It's fairly complicated and it doesn't scale well.

With this global key discovery mechanism that we have with DANE now, we can use S/MIME or PGP or whatever you want to, and discover public keys and do secure e-mail encryption or object level encryption of anything that you want to do. So it provides a nice scaling mechanism to enable that.

Interestingly enough, one of the things was, "Was this a big deal?" At Verisign, with one of my day job hats on, we spend over a million dollars a year on PKI infrastructure. That's for our web certificates. We don't have a lot. We're not huge. We only have about 1200 employees, as many of you know, and that's their S/MIME certificates for their devices for things like network access control and their e-mail encryption certificates.

One of the things we can't do is I can't send Russ an encrypted e-mail today unless I have his PGP key. I can't use our internal S/MIME infrastructure that I buy from a commercial CA to send an encrypted e-

mail externally because Russ has no way of finding my public key or I have no way of discovering his and so forth.

What's nice is that immediately with DANE, I can start using that exact same S/MIME infrastructure where we send secure e-mail internally inside of Verisign and use the exact same infrastructure and start doing that inter-domain on the Internet. It helps you solve the inter-domain e-mail encryption problem. It's really compelling for anyone who wants to do that because it solves the key management issue and it's sort of front loaded into the DNS, which are already captive to, and it already enables the access.

If you can do that, then now I repurpose that system and all of our partners, all of our external communications, can be encrypted as well as internal ones.

So that's a really compelling use case for us from an operational perspective internally that makes this useful. The more people that start to pick this up, the better. That's obviously the "eat your own dogfood thing." Internally it's something that we're definitely working on; integrating our systems to make sure that we publish those records and get those things tied in so we can do inter-domain secured e-mail.

DAN YORK: That's great, and that was a good answer to that regard. Rick?

RICK LAMB: Rick Lamb, ICANN. Great work you guys are doing, particularly with some of the Thunderbird plug-ins and stuff like that.

My question's simple. Do you have any demos on Outlook running under Windows?

DANNY MCPHERSON: The short answer is no, not to my knowledge. However, that's one of the key applications use in our enterprise. So that's exactly the problem that we want to solve. When we solve that problem, then I think a lot more folks are going to adopt this.

We've very, very interested in solving that problem and obviously trying to engage with the right folks to make that happen. Hopefully in short order we'll be demoing that here at some point as well. Anyway.

DAN YORK: Hey, Rick. You left too quickly while I was talking to Julie. I have a separate question in here that I know the answer to, but I'm going to raise it because the person who did these said, "Hi. I need to perform DNSSEC training course with our registrar and registrants in Togo-West Africa. Is it possible to benefit from any support from" – he said DNSSEC Coordination, but it's kind of all of us.

I would say this is exactly what Rick Lamb goes around and does, isn't it? Do you want to speak to that?

RICK LAMB: Yes, absolutely. That is something many of you already know. We have regular training programs. It's free. You just need to ask .We only ask that you have at least 15 people there to make it worth our while. We'll do DNS, DNSSEC trainings pretty much anywhere in the world. It's not just me. We have a team of people that do this actually with us, and with NSRC often.

DAN YORK: So for this person who's in the chat room, how do they contact anybody?

RICK LAMB: Richard.Lamb@ICANN.org.

DAN YORK: Richard.Lamb@ICANN.org. Okay. We had another question that was earlier from [Abdulmonem], who said, "DANE is important. It's a very important topic. Could we have a hands-on workshop?"

I think the answer is this particular workshop format is not necessarily something we can do in a hands-on space, although if somebody wants to propose that for Dublin, we're certainly open to discussions if you've got an idea around that.

But I certainly think that's something that – Rick, do you do DANE stuff in your DNSSEC workshops?

RICK LAMB: Absolutely.

DAN YORK: Absolutely. I thought that you did. So there are certainly options to do that, and I think if anyone would be interested in putting together a DANE module or something somewhere, that would be interesting to do at some workshop tutorial/pre-tutorial. I'm looking at Wes.

WES HARDAKER: Yeah. It'd be fun to put together. Having done some tutorials on how fast can you sign a zone and how fast can you insert new records and then publish them and then have them used and then adding DANE to that mix, it's not a complex problem. It's just you have to do it a couple times. Then all of a sudden, you're like, "Oh, well that was easy." It's that initial step off the cliff to find out that the cliff is only a step down. It's not a jump.

DAN YORK: Yeah, and we've got some good tools now for helping the TLSA records. We mentioned before the one from .BR the folks that have did that. Rick has created a tool for TLSA generation. [inaudible] from VeriSign has had one out there. So there's a number of tools that are there that help create those TLSA records, so we're getting there quicker.

So these are the presentations that we've had. We've talked about securing SMTP e-mail. We've talked about an overview of DANE and different use cases of there. Jacques has talked about the new model for registries/registrars, and Danny talked about securing the S/MIME side of the e-mail equation.

I've got four folks up here. We've got about ten minutes left or so. This is your time. What do you want to ask these folks? Any questions you have about DANE, please come on up here. Oh, Jaap has a question. Jaap?

JAAP AKKERHUIS: Well, I don't really have a question, but there's some work going on at [servenet] for dealing with automating the rollover of certs, especially protocol for that. So if you have a big company with a big PKI [inaudible] it's a pain to update it on a regular basis. This is actually a system which will do that for you, at least help you in a secure way on updating your PKI infrastructure every year when these things expire.

It's also based on similar ideas to DANE. What you see is that DNSSEC is used as an enabling technology for other secure applications. That's actually one of the nice things about DNSSEC.

DAN YORK: We had a comment in the chat room from [Abdulmonem], who said he already signs his zone in an IDN ccTLD, so now he's interested in DANE. It's great to have that and great to see it.

How many folks here are interested in going back and doing more with DANE? Okay. A few people. Good. Excellent. Mark coming to the mic.

JAAP AKEKRHUIS: Especially if you already have DNSSEC [inaudible] TLSA records is a no-brainer. It takes ten minutes.

MARK ELKINS: I'm going to wear a different hat just now. I run a small ISP, and I do hosting. I teach DNS a bit, so I've been playing with DNSSEC for a few years. About a year ago, a light switched on. I have a database and inside that database are the records for generating a zone, signed zone file, and also sometimes some SSL certificates.

Now when I go to my SSL webpage for a domain, I have a button that I can push and it generates the TLSA signatures automatically for Port 25 and Port 43. So it's really kind of cool. It's a single button. It's just a call out to open SSL a couple of times, depending whether it's a 301 or a 311-type signature. It works. Really simple.

One of the conversations that happened was in order to get an S/MIME for mail security signing certificate, you first will have to have a piece of incoming mail with someone signing their own signature.

Is there a quickie way of getting an S/MIME signature for a person into DNS yet?

UNIDENTIFIED MALE: I'll provide one answer. Some of these folks or some in the audience may want to provide another. One of the things that we want to do from a corporate perspective is sort of pre-publish everything and make it available, so when you look up an MX server or other things you can find that information.

It would immediately be available for our employees or people we transact with from that perspective.

So I think at the end of the day you want it there and available, and when you look up an MX record, then you can call it out and find that information so that you don't have to receive something first with a public key associated with it. Does that make sense?

MARK ELKINS: There used to be a person record or something in DNS.

DAN YORK: Rick?

RICK LAMB: That's exactly what the DANE Working Group is trying to do now, to provide functionally a worldwide database in the DNS of S/MIME or PGP certificates that you can not know who you're talking to ahead of time. Go look up their certificate so that you can both authenticate and encrypt them. So if you receive mail, you can authenticate it and if you're encrypting to them, you can pull up their thing and send it to

somebody you've never interacted with before, as long as you have their e-mail address.

There's some tricky elements to it, and it will probably take a few spins in the IETF before it actually comes out, but hopefully we'll have them.

DAN YORK: Yeah. We didn't talk about the OpenPGP record, but there is that effort going on here with Paul Wouters involved. I'm pointing at Paul. [inaudible] Russ?

I'd also like to say, "Uh oh."

RUSS HOUSLEY: I want to correct a misperception there. I chaired the [inaudible] Working Group, so I couldn't let it go by.

You never need a signed e-mail message in order to produce an entry. What's going on there is people are using the signed e-mail message as the way of getting your certificate from one end to the other. If you had another way to get that certificate, you wouldn't need the bootstrapping signed message.

DAN YORK: Rick?

RICK LAMB: And the other way. About a week ago I threw together something on wwco.tt, one of my own websites, that converts between LDAP and DNSSEC S/MIMEA. Now Outlook will just work. You don't have to exchange stuff if you as one of your address books a fake LDAP.

So now when you start in Outlook typing in somebody I don't know from a completely different place who happens to be something who likes DNSSEC – that's going to be a very small set of people – and has an S/MIMEA record in it, it'll automatically convert ASN1 language in LDAP to DNSSEC and pull the certificate, convert it back, give it back, and transparently you'll see Outlook put a little underline. Now you can send an encrypted e-mail that way. So this is great for the terrorist organizations and everyone else.

UNIDENTIFIED MALE: Is it open source?

RICK LAMB: Huh?

UNIDENTIFIED MALE: Is it open source [inaudible]

RICK LAMB: Yeah. Well, it's Rick code and I need [inaudible] Jacob has been on the ground. So yeah, it's a bundle of scripts. Yeah, there's a bunch of C

code. Actually, the ASN1 encoder/decoder is the same stuff I use for the root zone.

DAN YORK: So that was www.co.tt.

RICK LAMB: Yeah. And there's a link underneath that that says S/MIMEA Calculator. If you go there, it'll show you exactly how to set this up in Outlook.

Anyway, it's completely just beta trial stuff here. The long-term goal of course is to have it just a simple app or piece of code running on your windows and device. Then you get the full end-to-end, the thing we want.

DAN YORK: Okay. Cool. Well, thank you, Rick, for that. I also just want to thank Danny. I wanted to mention that on this particular slide still up here that one of the things that I liked when I saw Eric Osterweil present something on this set – maybe it was DANE at the last IETF or something – is there's a language issue here that's interesting. We talk about key learning. One of the struggles we've had when we try to make some of this stuff sound reasonable to people who are not DNSSEC or DNS geeks is trying to help them understand what problem we're trying to solve.

Part of it is we're trying to learn the key we want to get to use to connect to you. We want to find it in some way. I just want to say

talking about key learning was I thought an interesting way to make that perhaps be a little bit more understandable. I don't know. It seems that way to me, anyway.

All right. Any final questions for this group? All right. Well, let's give a round of applause for our panelists and thank everybody for this.

While they're finishing up and leaving here, I just want to mention, too, that this is the kind of thing we'd like to do in Dublin, some more examples of applications, things we've done with this.

We also are open to demos. At our last session in Singapore, we had a couple of different demos that were there. If anybody has some tools, obviously one way to do it is to make a little movie like Danny had there. But another way is we are open to people trying live demos as well. We certainly are open to that. So if you've got ideas, please do that.

I'm going to stand up and move because I just need to move.

I'm going to switch and talk about one of the pieces that was mentioned earlier a little bit, this question of, "What do we do for new DNSSEC algorithms, and what are some of the aspects we have to be thinking about, and what are we doing with this?"

First of all, I just want to take a step back and think about, for DNSSEC, what are algorithms used for? Obviously we use them to generate keys. They're using them in signatures. We use them for DS records. We're also using them in validation. So algorithms go across a lot of this, a lot of this space and what we do, and it is there.

There is this registry – actually, I should back up. This would be a great quiz question. Oh well, it's already in the slides. But we should have said, "How many algorithms are in the IANA registry?" Anybody guess?

UNIDENTIFIED MALE: [inaudible]

DAN YORK: 14 or 15? How many more?

UNIDENTIFIED MALE: [inaudible]

DAN YORK: 14 or 15? Well, probably. Let's see. We've got 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. About 11 or so. A bunch of reserve things in there. As a quizmaster, here's another good question for you to think about. What is the number of the GOST algorithm? Just remember that for next time, next year or Dublin.

But we have this. Now, the reality, though, is that Geoff Huston and George Michaelson, the APNIC folks, went off and did some – actually no, Ed Lewis did these results. I'm thinking the wrong things. Ed did these results at CENTR. He presented something show that if you go down and look through them, almost everything is using RSA algorithms in some flavor and some form.

You can see here the breakdown of the DNSSEC names. There were 682,000 that had DSs, and of those – look – 562,000 were RSA/SHA1 and SEC3. Okay, now you go all the way down to the bottom and you get to, of the one's that Ed did – and this was work that was presented in June and think data was in May – there were a whopping total of 16 with GOST and 38 and 14 in the ECDSA flavors that are out there.

Here was another view of the raw keys that were out there, showing that there were a million that were RSA/SHA1. Down here, the non-RSA ones are quite small.

So the reality is it is a RSA-based world here and there's a number of newer algorithms. One that we've been talking about here is ECDSA, an elliptic curve algorithm that's out there. Another one that is a favorite of the folks over in Asia and Russia and that space is GOST, which is another one that's been defined for a number of years out there.

But there's also work that people are looking at in the future. There's one that's ED25519, which basically is – if I have that right – the EDDSA, if I have the pieces right in there. There's a new RFC out of the cryptographic research group that's encouraging IETF algorithms to use this ChaCha crypto-algorithm and some others that are out there.

So there are other algorithms that are out there, but why do we care? Actually, let me ask you that. Why am I up here? Why do we want new algorithms?

Jacques says, "I don't know."

UNIDENITIFED MALE: Size matters.

DAN YORK: Size matters. Okay. Yes. Why does it matter?

UNIDENTIFIED MALE: [inaudible]

DAN YORK: [inaudible] Law. Okay. All right. Why do we care?

UNIDENTIFIED MALE: Agility if there's a vulnerability.

DAN YORK: Agility if there's a vulnerability. Okay. What's the size? What does that have to do with anything?

UNIDENTIFIED MALE: Do you want your packets?

DAN YORK: Do you want your packets? Do you want them to get there? Yeah. All right. These are all good things.

Let's see what I put up here. Faster. Yes. Well, it can be, although it depends upon the algorithms. Yeah. It can be a little bit in there.

Smaller key size is the big thing. Okay. Packet size, avoiding fragmentation. As we start to get up in larger, especially if you look at doing like 2048-bit RSA keys, you're starting to generate big whopping signatures, etc., which can wind up getting to the larger packet size, which gets into fragmentation, which means you have to go into TCP or you have to deal with other issues that are around with that.

Also, just minimizing DDOS attacks, amplification attacks, which can happen with a lot of different DNS issues, but DNSKEY packets can certainly make them large on that.

And better crypto, just as a general move. There's a lot of movement around moving away from the older key sizes. We look at 1024-bit RSA in particular, and a lot of the web community has moved away from that entirely and is dropping that in some ways.

Why do we even use 1024-bit RSA still? Anyone?

UNIDENTIFIED MALE: Contract.

DAN YORK: What?

UNIDENTIFIED MALE: Contract.

DAN YORK: Contract. Okay. Why?

UNIDENTIFIED MALE: Nice round number.

DAN YORK: Nice round number.

UNIDENTIFIED MALE: Code support.

DAN YORK: Code support. All of that, but also it's because it was smaller. If we look at the structure, the root has a 2048-bit key, but the key-signing key, the zone-signing keys are often 1024-bit because they're smaller and faster to go and generate some of the keys that are there.

So we're going to move away from that. Let's look at the different aspects that we get into when we look at how do we deploy new algorithms. It actually goes across pretty much every aspect of DNSSEC infrastructure, which makes part of it being so hard.

On the validation side, every resolver has to be updated to have this algorithm. If you're going to start to validate on ECDSA or any of these new ones, you've got to update the software. You've got to get it out there and have it deployed.

And there's one little interesting aspect that comes into this. When DNSSEC was defined in RFC 4035, notice this part that's done here. You can read it as well as I can, but I guess for the interpreters and the live stream, I'll say it. It says, "If the resolver does not support any of the algorithms listed in an authenticated DSR set, then the resolver will not be able to verify the authentication path to the child zone. In this case, the resolver should treat the child zone as if it was unsigned."

So it's the classic fail open, fail closed kind of thing, and the designers of DNSSEC chose that it would fail open, fail unsigned. If you choose to only sign your domain name with ECDSA, as I have actually done for one of my own domains, then any resolver that would not be able to validate it by the spec should just ignore it and treat the domain as unsigned.

One of the challenges is, as you go out here, if you're only deploying using new algorithms, then some percentage of the validators out there will treat it as an unsigned zone. So even though you are signing with the newer, better, shinier algorithm, which should make you more secure, you may in fact be less secure until all the validators are up to speed with the new piece like that.

Geoff Huston went off and did some measurements in his team at APNIC that they presented earlier this year, looking at what was the validators. How many of them would not work with ECDSA, as an example? They found that about one in five would not support it. It's actually an improvement because their measurements about six

months earlier had shown it was about one in three. So it was improvement, but still you're looking at about 20% of the measurement of the validators out there would not do anything with an ECDSA signature.

Similarly, this gentleman using a RIPE Atlas probes went out there and did some testing on the DNSSEC validators that those probes were behind and found – again, if I interpreted it correctly – about 12% of so would not recognize the ECDSA signature. So there's this challenge with getting the validation out there.

On the signing side, the same kind of issues exist. The software for the signing mechanisms needs to be updated. The software needs to be deployed. The operators have to offer it. There's a size impact because ideally if you're using both keys for some period of time, you're going to have to generate keys with both algorithms. So interesting pieces that are here.

Registries. This was something that Oliver [Goodmanson] brought to our attention when he was working as CloudFlare. What they're doing is they're looking to sign all the zones with ECDSA. So he went around talking to some of the registries and discovered that some of the registries were only accepting DS records in certain algorithms, the ones that were there, typically mostly RSA.

As he was going to try to give them a DS record, they were just saying, "Sorry. We're not going to take that." They were just not going to do it.

He also mentions that there was no way that he could tell what registries would accept which algorithm, so one general question is, on a certain level, why do registries need to check the algorithm type? At a certain level, should they not just accept the DS record and have this do this?

The comical part about this for people who know, too, is that Oliver was the author of the spec for the DS record. Now as he's going out to people, he's finding out, "Whoops. Little details in this."

On the registrar side, one of the challenges is, because we go back the question Jacques was asking, right now, if I want to sign my domain and have it linked into the chain of trust, I have to use my registrar right now. I might be running my own DNS or having somebody do it for me. I can sign it, but to get that key into my top-level domain, I have to go through my registrar.

This is a screen shot of one of my registrars that I use, where I wanted to go and give them an ECDSA key. But you'll notice if you look at this screen that they have a drop-down menu of the various different algorithm types that they support, and ECDSA is not on there. There's this thing called ECC, but that's an older thing. It's not the newer ECDSA.

So I had no way to give them a key. I have a DS record right here. All I have to do is I have to just go paste it in this field. That's all I need to do. Paste the record here. That's it. But I got to toggle these things, too, and they don't give me anything to choose.

Now, in this particular case, they changed. People asked them to do that, to change, and now there is a choice down here where we can choose this.

Notice something else they did if you look at the slides that are here. Here they just list algorithms. Here they list algorithms and numbers. We have this confusing part when we deal with DS records – and I had this happen, actually – when the DNS hosting operator that I use generated a DS record for me, and it told me the algorithm number. When I went to my registrar to go put that in there on that last slide, they gave me algorithm names and not numbers.

So okay, me being who I am and involved with DNSSEC, I could go figure that out. I knew there was an IANA registry. But the average consumer is not going to know any of this stuff, nor want to deal with any of this stuff. But this was something that was there.

So the challenge we have here, though, is we need to get the registrars to go and do this, which becomes a question that we can ask: "Why do registrars need to check this?" I don't actually know. What's the harm? What is the harm in that? I question I would throw out to people is, "Is this some advice we can start giving to registrars in some way, just to say, "Just accept the DS records? Why do you need to check this?"? I don't know. It may be that they don't want to deal with tech support requests. I don't know.

Yes, Jacques?

JACQUES LATOUR: They don't want to do anything with DNSSEC.

DAN YORK: They don't want to do anything with DNSSEC. Yes. If Michele Neylon was in here, he'd say, "Hey, the registrars don't want to do anything with it because there's no money and no nothing in it for them."

UNIDENTIFIED MALE: [inaudible]

DAN YORK: A registry creating something and taking on a liability. Oh, like if they just allowed that in there or something and then it doesn't work. Then they're afraid somebody could come back and sue them or something like that. Ah, yes. Lawyers. Okay.

So one of the things that's been pointed out – and this comes back into these user interfaces – is, typically if you give developers a list, they'll check something against it. Boundary checking is a kind of fundamental part of what we do in a lot of programming.

But in this case it doesn't necessarily help to go and do this. We need to look at how do developers allow more algorithms.

In my last step, I just want to say I think one of the challenges we all have as a DNSSEC community is that if we want to see more algorithms used, if we want to have better agility and have new

support for this, we do have several different steps that we have to look at that.

One of those is I think we need to start looking at what are the steps to deploy new algorithms, kind of this document, these slides that I've done here, but expanded perhaps a bit. Maybe this is an Internet draft. Maybe it's some other document that resides somewhere. We start to look at what are these steps.

Then I think we really have to look at what are these roadblock here? How do we get through them? How can help the registries accept more algorithm types? How do we work with the registrars to get them in there? Or is just a case that we have to be noisy and go around to every single registrar and ask them to add a new field in there?

So that's what I've got to talk a bit about what there are. I'd love to hear questions and comments.

Julie has one in the chat.

JULIE HEDLUND: I have a question from the Adobe Chat room from [Abdalmonem Galila] of NTRA of Egypt. He asks, "I think the query response size for IDN is greater than ASCII domain names, and you said we have to avoid fragmentation. So how can I select the proper key sizes for signing to avoid fragmentation? Bigger key sizes mean more secure."

DAN YORK: I can give one answer, which is that bigger key sizes – it depends. This is where we talk about the algorithms. The different algorithms, like ECDSA, could generate a smaller but more secure, at least according to our current knowledge, key size, which would then give you smaller packets, which could work with that IDN.

So for an IDN, you may have even a better reason to go and do that. Paul looks like he wants to say something.

Oh, Oliver posted an answer in there.

[PAUL WOUTERS]: That works, too.

DAN YORK: Go for it.

PAUL WOUTERS: What I was going to say is, if you look at the output of a [inaudible] when you do a query for your DNSKEY RR set, you can look at the size of the message and be careful to map it between the size of the message and the size of the packet. But you want to make sure that your packet stays about under 1400 if you're afraid of any fragmentation issues.

You can sort of bump your key up until you roughly hit that size.

JULIE HEDLUND: In the Adobe chat room, Oliver [Goodmanson] answered, "Use ECDSA."

RUSS HOUSLEY: I just wanted to shout about some work that's going on jointly between the IETF Security Area Advisors Group and the Internet Architecture Board. There's a document draft, "IV Crypto-Algorithm Agility." This topic is equivalent to working group [Last Call] right now.

It basically says a lot of what Dan just said. Basically, having that agility is really important as we learn about flaws in particular algorithms. And it helps us make a migration from something like RFC to ECDSA. So this is all really important stuff. The registry is just one important piece of it.

DAN YORK: Excellent. Mark's here.

MARK ELKINS: Does this mean the debate as to whether an EPP-based registry should accept a DNSKEY or a DS record is kind of over, and we should only accept DS records from now on?

DAN YORK: That's a religious war. We're not necessarily solving that one. That's a larger question that's over and above the algorithm piece underneath that.

Any other questions? Comments?

All right. Thank you, Russ, for that reminder. I do remember seeing a note about that document coming through, but I hadn't actually thought about it in this context. But that's ideal. So –

RUSS HOUSLEY: [inaudible]

DAN YORK: Yeah. It is. It is. I was down in the silo of DNSSEC to a certain level, but that's excellent. So we'll take a look at that document.

Anything else? Okay, then let's switch to our last PowerPoint and come up with the last thing here.

UNIDENTIFIED MALE: Well, Dan, one of the things you asked is how we can get rid some of the barricades to deployment issues. One of the interesting things I heard about from some of the ICANN meeting participants is a new technique for such a thing.

Put up barricades in the road, figure out how to set them on fire, and they burn down. That actually happened to some people between the airport and here. they encountered burning barricades and they ended up being a pile of ash on the floor.

DAN YORK: Nice.

UNIDENTIFIED MALE: So if we can figure out how to burn down these barricades, we'll be in maybe good shape, or better shape.

DAN YORK: All right. So we want to just end this by talking a little bit about what you all can do and steps that, if you are an operator of a TLD, we could encourage you, if you're a ccTLD, generic, new gTLD, whatever else – if you're a new gTLD, you had to sign it; if you're one of the ccTLDs, there's folks around here who could certainly help you with it. You also got to work on the accepting the DS records that are there. Work with the registrars.

Also, one piece we'd really love is if ccTLDs and other can help us with statistics. You saw those maps at the beginning. You saw the other pieces. We're looking for ccTLD operators in particular to help us with more statistics.

You want to…

UNIDENTIFIED MALE: One of the things I'd like to mention here is especially the new gTLDs. Though they do have to be signed, the general wisdom at this point is they don't necessarily have to accept signed delegations under them.

So please look at what you might need to do. If you're a new gTLD operator, think about incorporation that in your operations so it's more than just the gTLD itself that's signed.

DAN YORK: If you're a zone operator, please, if you have your own domain name, sign it in some way. You might have to verify that your registrar supports it. We're seeing more registrars, but there's still a lot that don't quite now.

If you're a network service provider, an ISP, please get out there and implement validation. Now you saw that back at the beginning of the day we talked about how it was about 14% of all DNSSEC queries globally are being validated. We'd like to see that continue to grow and grow and grow. And it is growing in some parts of the world, but we'd like to see the overall trend continue to grow up. 14% is already a good number, but we want to keep it going until we go all the way around there.

We also do encourage service providers and others to promote the support of DANE. DANE has a lot of benefits, as we just heard from our last panel about new opportunities and innovations. We'd really like to see that grow.

UNIDENTIFIED MALE: One of the things, especially service providers that are afraid of signing their zones and concerned about the problems that it might cause, Paul Ebersman from Comcast mentioned earlier that, yes, there is

some cost associated, but it's not the terrible, terrible burden that a lot of people think that it is.

One of the other things that's really great about this community is people help each other. That's a huge benefit when you go to try to present information to your upper management. Point out that you can get help, and it's often free. People do a lot of writing and there are a lot of good shared lists around that people ought to look at for help.

DAN YORK: If you're a website provider, a content provider, somewhere, again, work with your registrar or others. Again, one of the things we keep hearing about DANE from some of the folks, like some of the browser vendors, is they say, "Well, nobody uses it, so we don't want to implement it."

So what we're encouraging people to do is if they do sign/create TLSA records like we have, get them out there and publish them because the browser vendors and others who are out there are watching that and seeing how many TLSA records are out there, seeing what kind of pieces are out there. So if you could go ahead and do that, that would be great.

Obviously encourage more validation if they can. For all of you, we'd encourage you to use DNSSEC to a degree. Also, please share the lessons that you've learned. Share the information that you have.

Like we said, we'll have another one of these sessions coming up in Dublin at the next ICANN54. We do these on the Wednesday of every session. We're always looking for new ideas, new case studies, new lessons learned, the pieces that are there.

So please do go ahead and look for that call for papers that are out there. Come up and talk to any one of us – Russ, myself, others who are around here. We'd love to have your involvement with that.

I think that's really it that we have. I guess we'll end with: there are three websites I'll point you to. DNSSEC-Deployment.org is one site that has a good number of information. We got to fix this for next time. [www.InternetSided].org/deploy360 is where we have a good number of tutorials. Thanks. It's not a new gTLD. No. That'd be a big whopping long one. Then also there's DNSSEC-tools.org. We are on all of those sites, looking for more tools for things we can point to and stuff that's out there.

So I think that's really it that we'll mention, except I will put in one little plug. Jaap, who was up here before, too, has a supply of Atlas probes. How many people already have Atlas probes? All right. Everybody else, if you're interested in one of these, they help the RIPE Atlas measuring program. All you have to do is take one of these little things, plug it in into your home network, and it just sits there and helps be a little part of the measurement network that helps in all the measurements that go on, which include now some ways we can measure DNSSEC and stuff like that.

So talk to Jaap right there. He's got a few more, and he'd love to get rid of them before he goes home.

With that, I will say thank you to Julie and also helping her now is Kathy. Putting on an event like this take a lot of work. Julie and Kathy have both been very involved with helping us on the program committee continue to do this. They are a huge help with all this.

So on behalf of our group, thank you.

UNIDENTIFIED MALE: And thanks to all of you for participating and presenting because it truly wouldn't happen without you. You'd get so bored with Dan and I. After about five minutes, you'd be ready to throw us off the stage.

So keep your engagement. Keep coming back. Keep coming up with new ideas. We'll hopefully see you all in Dublin, and even more of you. Thank you.

DAN YORK: Thank you very much.

[END OF TRANSCRIPTION]