DUBLIN – DNSSEC Workshop
Wednesday, October 21, 2015 – 09:00 to 15:15 IST
ICANN54 | Dublin, Ireland

RUSS MUNDY: Welcome everyone. We're going to be starting the DNSSEC Workshop in about five minutes or so. We do encourage people to come and take seats around the U-shaped table, except for the end of the U, where our Panelists will sit. If you're a Panelist in the first Panel this morning, you're welcome to sit at the front of the table. We welcome anyone else to come and sit around the U-shaped table. It's easier to see the teeny-weeny screen that's there. We encourage you to sit around the table, and we'll start in just a few minutes.

DAN YORK: Good morning everyone. Welcome to this DNSSEC Workshop, here at ICANN 54. Are we good to go, Julie? We should say thank you to everyone here. I see some familiar faces and some not-so-familiar faces. We're going to be talking here for the scope of this six hours on a whole range of topics. You're obviously welcome to come and go as you wish.

There's an Agenda that you all should have. I would second the call Russ made earlier, that we'd encourage people to come up and sit around the table. The slides that many people are presenting are going to be up there, on that screen that you see there. If you're in the back there, you can come up here. You're welcome to come up and join us.

There are no special invitations needed. You're welcome here. We will have lunch in here. My name is Dan York, I'm with the Internet Society and part of their Program Committee that puts this together. Let me give you a bit of information.

This session going on here, you can get the slides at the page that's shown up here. The slides are all available there for the different sessions. The audio streams are also available. We're also doing some live video streams on YouTube, just so people could see the shiny faces of all of us here. That's streaming from that webcam right there, so we'll see how that goes. Those are out and available.

This is being recorded on a couple of forums. Yes, it's on YouTube, but it will also be recorded and available from the ICANN program page as well. The Program Committee Members, who's here in the audience? Russ, Jacques, Shiro, who comes into our calls from odd hours in Japan to join us, he gets the award from us.

A number of other folks. This group has been working together for a good number of years to try and put these programs on. They're the ones you should thank for the sessions today as you hear them and listen to them.

We're here for this. We'll be getting going then soon for planning for the next session, at ICANN 55 in Marrakech. As you listen today and hear some of these sessions and think, "I could present on this topic," or, "I have a great idea," then consider it, because we'll be putting out a call for proposals soon, and we'll be looking for people to come and present at the next event.

The luncheon we're going to have, you can see the dishes are out there. We'll be having lunch, and it's brought to us by these five great companies – Afillias, CIRA, DINE, .se and SIDN. We have those to thank. Round of applause for them. They are the folks that bring you food, so that way you're able to continue to be here and have the great conversations and things that we do. I will mention, as it says there, we are looking for one sponsor to join the ranks of those companies.

We need about five of these sponsors to be able to fund this for the course of the year, so if anybody is interested in having their company listed among these names, and helping sponsor the three that are there, and also getting your names on the back of this – as you'll see here – if you'd like to be among those very few companies that help make this, and have the undying gratitude of the DNSSEC community, please talk to me.

We will need somebody for starting in Marrakech and going on from there. Thank you to the other four who are continuing. The one who is changing is .se, who's been sponsoring these for ten years, and they've done a phenomenal amount to help with all this, but Anne-Marie has said they'd like to take a little break and lend that spot to somebody else. Please talk to me. We also want to say thank you to Afillias.

When you see Jim, thank him, because his company sponsored the gathering that we had the other night. It looks dark in those pictures, but it was a good event – in the bottom of the Ferryman pub right across the street here. These are great events that bring together a lot of the community. Cristian has sponsored them in the past, Jacques, some of the other folks who are here.

We're looking for a sponsor for the one in Marrakech, so if anybody's interested in doing that, it's a great way to help the conversations that we have inside of here. Welcome to the DNSSEC Workshop. Come on in, grab a seat. This Workshop, the sessions that we have here are a joint projection of the SSAC here as well as the Internet Society Deply360 Program. The Program on the slide is up there. As you'll see, we have this fine array of folks who are up here in front of us, who are going to talk about the DNSSEC activities in Europe.

Peter Koch is here with a tie and everything, looking very formal! This is great. We have a range of characters up here, who are going to talk to us about what's happening at DNSSEC in Europe. After that, because my eyesight can't read that chart, Jacques is going to be moderating a Panel where we're going to be talking about DNSSEC on the edge, and some of the ways that we're looking at improving these kinds of things. Here we have Roy.

Then we're going to have our lunch break, and then we're going to get into a session where we're going to talk about DNSSEC and applications. We have a number of people who are going to be doing some things. I'm told there might be a demo or two in here, maybe live demos, so we'll see how that goes. Those always add entertainment value.

Then Cristian Hesselman's going to come back up at the end and talk a bit more about mechanisms around stimulating DNSSEC deployment; some of the items he's had in .nl and other questions I think, for the larger community, about how we do that. Then at the very end, Russ and I will be back up to wrap things up and go through this. This is an interactive session. We do ask people to talk to us and engage. If you are going to speak, if you're not willing to come up and sit at the table, you've got to walk to where this mic will be over there.

But if you want to come up to the table, you've got a mic right there that you can just push the button and it turns on and you can speak. It's really good. We do ask you to introduce yourself, just because we do have remote sessions, we do have remote people who are out there.

I'm going to start with a quick tour of what we've been seeing as far as deployment counts and some of the information that's here. This chart shows the latest stats we're getting out of Geoff Huston's APNIC labs that are showing the overall growth of DNSSEC validation.

Right now, his queries are showing it's about 14 per cent of all DNS queries globally being validated. You'll see there's a dip in there. It's partly because the way Geoff measures it is with Google Ads. Google made a change where they dropped Flash and went to HTML-5 and things, and it took Geoff's team a little bit to catch up with how to make their systems work.

He told me yesterday at the implementers gathering that they've got their system back up and going, and they're quite happy with how it's working, so he thinks from this point forward it will be a very solid measurement.

Anyway, it's showing a nice growth overall. If you dive into these numbers, we'll see that in some places, overall we've got really good validation happening, to the degree of about 31 per cent closely in Eastern Africa. I'll dive into that a bit and see a little bit more of what's going on in there. Some of the areas that we're seeing these ranges… One interesting thing about Geoff's graph is he also charts who's using Google's public DNS, because he's seen that that has a lot of people involved with it.

If we look at, for instance, Europe, one of the interesting aspects is you can see where you have DNSSEC validation, and the things I'm always looking for is a high percentage of validation, and quite honestly a low percentage of Google public DNS, which means that more of the ISPs in the region are actually deploying it.

If we look at Sweden, it says it's about 77 per cent of all DNS queries coming out of that area that are validating, and only 7.5 per cent are Google public DNS. That means all of those other queries are either coming from the ISPs in Sweden, or another public DNS. We're seeing some really great uptake on this.

Rick Lamb has his charts that are showing the continued… We love this hockey stick of the TLDs, but of course that's all the new gTLDs coming out, signed from the get go, and so we're seeing this uptick that's happening there. If we're looking for stats, we're now at 84 per cent of TLDs that are all signed in some way. Looking at some of the numbers, Rick added a while ago the ability to look at the number of signed domains versus total domains.

We've got some numbers in here that show, for instance, that the most domains signed in the world belong to .nl. They're coming in about 2.5 millions domains signed inside there, which Rick's stats have at about 44 per cent. Then we go on down from here. We're seeing other ones that are in here. We've got Ondrej with .cz. Other folks around here, .org and others. Rick's data only has the sources that he can get. So he can't get information from everybody, so they're part of that.

Interestingly, we are seeing some uptick in the new gTLDs. One that's interesting is the .ovh. I don't know if anybody's connected to them? It's a TLD that starts out in signing and hosting, and doing all those things. They've had a large percentage of the new gTLDs under there. An interesting other one was .bank.

I've not had much dealing with them, but I know that part of their whole premise was that you'd wind up with secure from the start and all this kind of thing. So all their domains right now, the 2,500 or so in that new gTLD, are all DNSSEC-signed. Interesting thing to do this.

Koch, what are you doing, man? For people who are remote, Peter has just put on sunglasses. Here we go. Okay. I want to look at the implementation status on the maps in the few minutes that I have here. In our maps that we look at, we look at the experimental announced partial, which means the zone is signed but there's no DS in the root. Then we look at what is DS in the root and those pieces. Let's look at our maps, because we like them. Here's how the picture is overall.

We're seeing a lot of nice green all over the place, which is what we want. Africa still needs a bit of work over there, but there's some good news there. One of the good news is

Zambia. Anybody know where Zambia is? Africa, yes! Step one, since the chart is Africa… Anybody know? Which green dot is Zambia? Zambia's here in this area. They just signed in October, so they're our newest ccTLD that's joined the ranks of the secure ccTLDs. Kudos to Zambia on that one.

In Asia Pacific, nothing's really changed since the last time we were standing up here. Europe, nice and green all over the place. We've got a few little spaces to fill in, but overall, pretty good. Latin America, we had two changes since the last time. One was Mexico. It's been working on it for a while, but they signed, and went operational and those kinds of things, and Uruguay joined in as well in August. Where's Uruguay? South America! Good deal. North America hasn't changed.

The deployment maps are out there that we have. You can get to them. You can get these every week if you want to see the new maps, and you can always go and download new copies. I think that's all we have. I've started up an events calendar on the DNSSEC-deployment.org site. If you have an event that's related to DNSSEC, you are welcome to send it to me and I'll be glad to add it to this calendar, so we can have that information up there.

One last thing to mention – we had a hack-a-thon at IETF 93 in Prague, and a number of us were there, participating in this program. I see Sarah's back there, Wes… No, you weren't there. Who else was there? Anyway, we had a good time working on projects that were around DANE, around Deprive, around DNSSEC… it was a good event. We had a bunch of public releases of software coming out of this two-day hack-a-thon. Some new software was released.

I mention this because coming up at IETF 94, how many people are going to Yokohama for IETF 94? A number of folks, okay. If you're able to come in the weekend before, yes, it's Halloween, but if you are you'll be able to participate in the hack-a-thon that's going on there, which is a time when people are just working on code. I know Alison Mankin is looking to organize another group to go and do it. The DNSSEC Team actually won. We were awarded the best in show or whatever for the events that we put together, so it was pretty cool.

Anyway, that brings me to the end of my slides, except to mention that we still do have the DNSSEC history project around out there, if you're interested in helping out with that. I'd love some help. That's all. I'm going to turn it over to Julie.

JULIE HEDLUND: Just a couple of logistic things. So you have a program, and on the back of your program is a ticket, and that's your ticket to lunch. Lunch is in this room, so if you choose to sit in this room until lunch, and don't go anywhere, then you won't need the ticket, but if you leave the room you need your ticket so that you can get back in and have lunch.

Hang onto that, if you do leave, and also, I'm not sure if Dan mentioned but we wil indeed have the DNSSEC quiz, and Roy Arunds is going to be doing that, so the program should say Roy, but we didn't have time to change it. Roy, thank you so much.

DAN YORK: While we're here, I want to say thank you to two other people. One is Julie over here, and also Kathy, who've been helping us with making this program possible. It would not be possible without their systems to make this happen. Thank you both.

RUSS MUNDY: Good morning folks. Really glad to be here. It's great to be in Europe again, especially for a DNSSEC Workshop. One of the things I really enjoy about coming to Europe for these is we very often end up with a competition between the various European countries about who has the most signed zones, and that's always fun for somebody like myself that's been engaged in trying to get this going for a long time. Kudos to everybody who's done so much. In a lot of ways, Europe still leads the world in what's going on with DNSSEC, so I'm really pleased to be able to host our regional Panel.

Welcome to all of our Panelists. You can look at the order on the program. We're doing it in alphabetic order by last name, and that seems to be a nice easy convention. We will start with Ondrej Filip from NIC .cz. We're going to try to do approximately ten minutes per, and as usual I have the little counter here, so people can see how you're doing when you're speaking, and others can wait and wait until it's time to jump up and ask the questions.

We do want to have questions. We'll try to go through all the presentations and then do questions at the end. Ondrej, are you ready?

ONDREJ FILIP: Thank you very much. My name is Ondrej Filip. I'm coming from the Czech Republic. We used to be the leaders of the DNSSEC, not anymore, we are beaten by the Dutch very horribly. I'm sorry to say that, but it's true. The problem is that I think we have 38 per cent of signed domains, and unfortunately it's roughly the same number that I reported two years ago. We had a very fast rise at the beginning, and now we're stagnating a little.

It doesn't mean we're not working on DNSSEC, but it means that we've utilized all possible ways how to quickly make those numbers, because the majority of those domains are domains that are hosted by large registries or DNS providers, and they were quickly able to make it.

The rest of the domains are spread among a lot of multiple DNS servers, which are out of control of the registrars, so it's not so easy for those people to sign. We were able to cooperate this with many important sites in the Czech Republic, mainly newspapers, almost all newspapers, like websites, are signed in the Czech Republic, and it's the same for some major banks. Banks are quite complicated, we still need to work with them, but it's quite okay. Almost all Czech registrars support DNSSEC, and they [unclear 00:25:06], so that's why the number looks as it does.

DNSSEC is quite a good topic in the Czech Republic. We are able to lobby for including this into digital Czech, which is the digital strategy for the Czech Republic. We should start to say Czech here, because that's a new short term for Czech Republic. I don't know how it sounds for native English speakers, but that's a new invention. The digital Czech here, 2.0. Also, in a recent cyber-security strategy, that is mentioning that the government will support DNSSEC and its deployment.

The percentage of validating resolvers is a little better than the number of signed domains, so almost 50 per cent of resolvers, but if you look at the numbers of the [created 00:26:40], it's even better. That's caused by the fact that all major ISPs are validating – all cellphone operators and [unclear 00:26:48] operators. So it's really good. We are still working on it, but again, there's the same problem.

You can easily talk to big guys and bring arguments about issues on validating, but you cannot reach all those thousands of the small ones. We are still trying to reach them, but it of course goes much more smaller than at the beginning. I think really, if you connect to the Internet in the Czech Republic, very probably your resolver of ISPs will validate for you, so that's pretty good.

We are now concerned not exactly on all situations, but we're trying to help the others. As you know, we are more a software house than an Internet registry, so we are developing a lot of stuff, and also we have some small [unclear 00:27:44] company. One of the software we develop is called Knot DNS, the authoritative resolver. Here is some news related to DNSSEC [unclear 00:28:00].

First of all, we switched to GnuTLS instead of OpenSSL, and in version 2.0 we introduced a key signing policy framework, so that means you just define some policy that this domain should be signed, and the key should be rotated in 14 days. Then you just add this policy to the zone, and Knot DNS deals with this procedure completely automatically. It generates keys, makes the rotation, pre-publishes, and so on. So it works very well and helps to deploy DNSSEC for people that are not so technically aware of that.

We are pretty close to releasing version 2.1, which has more features, and that's mainly DNSSEC online signing. We made a special module that helps the ISPs that deploy IPv6 and need to have correct PTR records for all the IP addresses. As you know, the space of IPv6 addresses is vast, so you can't re-generate a zone, but we create a zone online. That was not signed. In this version we'll introduce online signing, so that all the PTR records that wil be syntactically generated will be also signed.

We use a single key, not the pair of keys, like KSK, ZSK, but I think for this purpose it's quite okay. We use the minimally covering NSEC records. If you return the query, it just recalculates the very minimum neighbors that might exist in such an artificial zone. Also to decrease the load, we return NODATA instead of NXDOMAIN, just because there is less computation and it has smaller size in our answers. That is our news on the resolver side. If you're not tested, send us some feedback and we're more than happy.

We also continue on the resolver side. We are really close to release a numbered version of Knot DNS resolver. If you want to play with that, because it's working, I'm using it on my laptop, and Ondrej, who is leading the team, the ugly man there at the back, he's also using that, so it works for us at least. We are trying to [debate 00:30:53] as much as possible. So if you want to test it, please do. We have quite nice documentation. I think that's one of the strengths that we have. Here is the URL. You can read it.

It's really a very modular platform for DNS service. In terms of DNSSEC we support the important RFCs like 5011 and also the Negative Trust Anchors. I think it's pretty modern, written in C +LUA extension, and it's quite fast. As usual, as we start some project, we have a plan, so for this project we plan to make it the fastest resolver in the root, of course. I think we are quite good in that. It's not so bad. That's it internally. We have a network of small routers. It's called the Turris project.

We'd like to deploy a DNS resolver on them, just to have a huge testing bed for Knot DNS resolvers. It's going to happen soon. First it wil be voluntary, and when we're sure that it's working well, we'll switch to [unclear 00:32:13], default option for Turris. That's all from my side. Thank you very much, and if you have any questions I'm happy to answer them.

RUSS MUNDY: Thank you Ondrej. Good to hear what's been going on over there. As always, you guys are fully and heavily engaged in the DNSSEC realm, and we really do appreciate that, and appreciate the support you've given over time. Next up is Cristian Hesselman, and he's going to give us some insight into what's going on from an SIDN perspective, and what are whistles for his later presentation also.

CRISTIAN HESSELMAN: Thank you Russ. The slides are really small, so I'm going to talk a little bit. Don't try to read the slides, because I think it's impossible. I'm with SIDN. We're the registry for .nl, the

Netherlands, which is a country in the western part of Europe. We currently have about 5.6 million domains in our registry, and 2.4 million of those have been signed, as Dan pointed out a few minutes ago.

Ondrej's mentioned that we beat the Czech with numbers of signings, but actually the Czech beat us in terms of actual validation, because that's our major… we need to talk later on, by the way. That's the major challenge that we have right now at SIDN, which is how can we stimulate validation? Because we know that almost none of the ISPs in the Netherlands have validating resolvers in their production environments. This is our major challenge.

Another challenge that we recently ran into is that we heard that a number of ISPs in the Netherlands are actually outsourcing their DNS operations to third-parties, to [oou I 00:34:27], which is a Chinese company, as you know. This makes the ecosystem even more complex, and difficult to find out who to talk to. That's something we've been doing for quite a while; talking to ISPs, and we have not made any progress there, to be honest. What I'd like to do today is at least ask everyone in the audience if they have any radical ideas on how to stimulate validation, because to be quite honest we've ran out of options on our end.

We did take a few actions to stimulate validation ourselves, and I'll be talking about that in the afternoon. We currently think that at least in the Netherlands, ISPs are unlikely to make a move in terms of DNSSEC validation any time soon. Like I said, we're looking for new and radical approaches to stimulate validation, and the things that we can do, they can only contribute so much, because we only control part of the value chain, if you will. That's my main message here today. If you have any ideas on how to do this, I'd be very glad to hear them. I think we're a bunch of smart people in this room.

Money? The thing is that we don't have a business relationship with the ISPs. Our business relationship is with the registrars. We did throw a lot of money at it, in that we gave them a discount over the past few years, if they would sign their domains, which they did. So we achieved these 2.4 million domain names. Getting those signed was a really collaborative effort, together with our registrars.

The signing part is not really the problem. The problem is the ISPs, and we don't have a business relationship with them. Also, we know that it's difficult, as you're probably aware of yourselves, to explain why you would need DNSSEC or DNSSEC validation in the first place, through the common Internet user. Folks usually don't see anything in their browser, unless they install the plugins that the Czech folks developed. Another thing that we thought was we don't really know how often men in the middle attacks occur, that DNSSEC aims to solve.

If we had more numbers on that, we could actually demonstrate, "This occurs 20 per cent of the time," or something like that. Just getting numbers on how often these attacks occur would probably also help, because now ISPs just don't want to do it because they think it will cost them money, instead of bringing them money.

They're simply afraid of – at least in the Netherlands – getting support calls all the time, because of validation breaks, for example; because there's a signing error somewhere, and say in that case a domain name might not validate on their validating resolver, whereas it would work on the network of the competitor who doesn't validate. That's their fear.

RUSS MUNDY: I think Ondrej may want to comment here.

ONDREJ FILIP: Honestly, it’s a really tough job, but we came up with two things that came to help a lot. First of all, the ISPs in the Czech Republic had the same fear that we all have problems with broken signatures, so what we did was we went through every zone every day and checked all the signed domains, and if there’s some bogus domains there are two possible actions – either we delete the DS record if we know it belongs to some registrar or DNS provider that’s not cooperated with us, and just inform us that it was broken.

Now, it has to be bogus for a certain time of course, not immediately. Or, if it’s a registrar that has a very close relationship with us, we just have [unclear 00:39:05] for him, and either they can say, “Yes, we will fix it,” or, “Please delete the DS records for us.” Also, during the transfer, if there’s a change of DNS, by default we’ll delete the DS record. So if you’ve not changed the DNS servers and you want to continue to be signed, you have to explicitly again put the DS records into the system.

So if there’s a change of DNS servers we delete it. So that’s the first thing; just to try to limit the number of bogus domains as slow as possible, and secondly, we created a prestige club of ISPs, which is called Phoenix. It’s associated with our [unclear 00:39:45] exchange point. To be able to join this club and to be able to [unclear] provider, you need to validate and you need to support DNSSEC on your webpages and stuff like that.

We created security as a prestige thing, and those companies are joining the club because they want to be better than the others. So that's how it worked in the Czech Republic.

CRISTIAN HESSELMAN: That's quite a big similarity to how things work in the Netherlands, because we also have this tool that you talked about, and I'll be saying a few words about that this afternoon. We also have the checkmark when you want to transfer a domain name. We also implement secure transfers through EPP key rollover, so that also works. We also have what you called Project Phoenix, and in the Netherlands that's called the Trusted Networks Initiative. So that's very similar, except the Trust Networks Initiative doesn't have the requirement for members to turn on validation, and that might actually be a good idea.

RUSS MUNDY: Thank you Cristian and Ondrej. This is great – having an exchange between the leading country with the most signed zones, and the leading country with the most validations. That's great. Thank you. Next up we have Peter Janssen from .eu, and he's going to let us know what's going on there. Thank you.

PETER JANSSEN: Thank you Russ. Good morning. My name is Peter Janssen. I'm with EURid, EURid being the .eu registry. I used to say we were a young registry. We've only existed for ten years, but of course with the New gTLD Program "young" becomes very relative all of a sudden again. Nevertheless, if you compare us with the existing ccTLDs of most ccTLDs, we're relatively young. As I said, ten years, while your ccTLDs have existed for literally decades.

Obviously we cover the European Union, which is almost the whole of Europe. We piggyback on all these fantastic initiatives and things that have been done by, amongst others, the Czechs, the Dutch, the Swedish registries, because a lot of registrars that are a registrar with the .cz, .nl, or .se registry actually holds their registrars with us and registers a .eu domain name. So by definition we benefit from all these things.

A bit about the timeline. We started accepting DNSKEY material in June 2010. We made it into the root with our DS records in September of that same year. If you look at May 2014, which is a bit more than a year ago, we had 6.9 percent of the .eu domain name space signed, and this year, October 2015, that had risen to nine per cent. What are the vectors that play in this DNSSEC adoption space?

We have registrars. On the right you have all the issues that registrars bring up as being an issue when they are asked to deploy DNS hardware/software, the complexity of the solutions. Procedures need to be in place, because it used to be if you didn't touch a DNS zone for ten years, it would keep on working for ten years. Now in this world where a zone is DNSSEC-signed, if you don't touch it for ten years, most probably it won't be working any more, ten years down the track.

On the other hand, on the far-left, you find the end users, who have mostly no clue about what DNSSEC is, and really they shouldn't be caring anyway. They just want their Internet to work and they want to have a secure environment, if they at least think about it. But no end users are explicitly asking for, "Hey, I want my domain name or I want my resolver to validate," or whatever.

What have we been doing in the past? We've been doing what most of the other registries have been doing. We've been doing DNSSEC workshops to spread the word of what DNSSEC is, why it’s a good thing, e-learning and training. Like Cristian said as well, we’ve been doing a DNSSEC discount, and there is a timeline of signed domains and whereabouts they occur. To the left you see this steep going up.

That’s a bit before we announced we’d be giving a DNSSEC discount, and as with the .nl registry we’ve seen that money talks, in the sense we’ve been giving back money to registrars if they would indeed sign their domain names. On each signed domain name they get a little discount on the yearly renewal fee, and as you can see, it works. The little things going up now and then is a registrar getting it and signing their complete zone, and then you see from one day to another there’s this little jump up, because they’ve signed all their domains.

Who? What is this? This is the percentage of the domains in registrars portfolio that are signed. The label there says zero per cent, and on the y axis you see that 80 per cent of all registrars have exactly zero signed domains. Said differently, the majority of all registrars are not doing anything in the DNSSEC world. On the far left you see 99 per cent to 90 per cent, and then 89 per cent to 80 per cent, and so on.

You see there are quite a few registrars that sign their complete portfolio, but most of them are either doing nothing at all or have done one or two domain names to actually see if it works, and then it's stopped there, presumably because they had either other priorities, no end user demands, no money to be made, or any combination of the above.

This is interesting. As I said, we piggyback on the other registries that have been doing a lot of work. What you see here is taking all the registrars together per country and seeing how many domains they have signed percentage wise. Then you see on the far-left Denmark, I think. I can't read it from here. What you will see is the typical registrars; the Dutch registrar, the Czech registrar, will be there, with the majority of signed domains. Why? Again, because these registries have been doing a lot of effort and we're piggybacking on that result.

If the country is not on this slide, then there is not a single registrar in that country that has done anything in terms of DNSSEC. Lastly I'd say we have about 3,855,000 domains, 348,000 are signed, which is nine per cent. If all registrars who have done something would sign their complete portfolio, that would boil down to some 920,000 domains that would get signed, resulting in roughly one in three .eu domains that would get signed.

But talking to registrars we're asking now, "You've done some of the work. You seem to be getting it. Why aren't you doing the rest?" and we get very mixed answers from, "I don't know," to, "Yes, it's not a priority for us at the moment because we have other things to do." It boils down also to what Cristian has said, which is that if an end user gets an email and he clicks on the link and it looks like eBay, then it must be eBay. DNSSEC is not going to solve that in any which way.

So as far as that is concerned, I think there are a lot of vectors of that that are being used in the world, that make people go to the wrong sides, where DNSSEC is not a solution. So registrars, if they're doing something, they're concentrating on getting other things done, rather than this. That's the last slide. Thank you.

RUSS MUNDY: Thank you very much Peter. Interesting report, and we can have some more questions later on. Now I think we'll move to the next Peter on our Panel, who has, through the gracious generosity of coming, been the best-attired person in the room with his necktie and sunglasses, as appropriate, I'd like to ask Peter Koch from the DENIC to give us an insight as to what's happening here.

PETER KOCH: Thank you Russ. Good morning everyone. My name is Peter Koch. As Russ said, I work for DENIC, the TLD registry for .de. We currently have roughly 16 million second-level domains registered in our portfolio, and I'm going through some of the numbers. I'm going to show you what we've been doing in .de, which is not only the TLD, but also the country. We had a DNSSEC Day end of June that was announced during the previous ICANN Meeting. This is the original announcement. If you look to the right, you'll see I'm cheating. The screenshot was taken later than that, because there are interesting other articles to the right, like the summary of this event.

We got a media partner and some other enthusiasts, which I'll list later. The idea was borne in 2014 and we came together and said, "Let's do something about promoting DNSSEC and DANE a bit. What's the best format?" and with a bit of back and forth we came up with a half-day of video streaming, starting at noon and covering the afternoon so that we could reach people in their offices and also at home. The four hours were like three tracks, with a bit of repetition. We had a frame program that would contain canned video streams that were pre-produced.

Then we had a Panel discussion with four people in an interesting video room, picking out certain topics; addressing the authoritative side, the resolver and validating side, and some technology topics. If it had been a TV program or radio program, we could have had an interesting schedule pre-published. Apparently we had – whatever this means – 500 video impressions. That's maybe 500 people looking in, or 500 consumers with rooms full of another 1,000 people, but I'm just dreaming.

Anyway, this is the original announcement. Then we got some international echo. Dan York was kind enough to mention this on the ISOC website. Of course, this is all in German. Please note the "DNSSEC Day" which is an interesting German word. We started publishing this, or the media partner actually, and then the other partners issued press releases and started publishing that three or four weeks in advance. That was accompanied by a couple of background articles in the print version of the media partners' publications.

They were updated versions of previously issued DNSSEC articles. Again, address beginners, addressing more advanced topics, and then also promoting and explaining DANE, to a certain extent. Then it was a bit interesting, because there are more media magazines that deal with Internet topics in Germany, but they all kept quiet and obviously ignored the press releases, because that was the prime magazine involved. But on the morning of the event we got some additional attention. You can see the headline, and that actually means, "DNSSEC is a total failure."

That was, attention-wise, the best that could happen. If you have better eyes than I do, you will see that above the "DNSSEC is a total failure" there is an "IMHO", which is German for "in my humble opinion". So this is a comment, and it's of course biased, and it was biased to the right direction, I would say. Listing all of the drawbacks, myths and failures and all the criticism that has been voiced against DNSSEC, it was easy to react to that. We were prepared to waive this into the discussions. We were very grateful for all these key words being placed in front of us.

It's not that we didn't have a script, but that was helpful and raised some attention. It was interesting to see that both of the media had web fora with discussions, and much of the discussion happened in this other medium here and was actually telling the author that he was so wrong and everything was fine. I wish the numbers would talk the same language, but let's get there. Who was involved? It was the Heise magazine, that is probably known outside of Germany as well.

It was the Federal Institute for Information Security, the TLD registry, and I've named them DANE practitioners here. Many of you may know [Carson Stultman] from [unclear 00:54:27] and [Patrick Cutter], who is one of the key people behind DANE deployment in Germany. We've been sitting together doing the panel discussion moderated by one of the editors of the online magazine.

So we got questions injected also by people listening to the stream, and as I said, a couple of the myths that were there, like, "DNSSEC is bad, because it's all 24-hours and it's broken…" and so on and so forth. But there were some interesting operational issues that I think we could address. I'll show you who's doing DNSSEC.

We've heard from the previous speakers that mostly registrars are active in doing DNSSEC, like signing their portfolio in part, or completely, and that means that one of the main reasons behind the KZK/ZSK split, that you don't want the interaction with a parent, i.e. the registry, or you want to limit that, is probably not really met by reality as of today. So whenever a registrar is signing their portfolio – and that probably also holds for resellers – they should really consider having a single type signing scheme to avoid double stuff there.

The other one is, going to the same direction, all these fancy rollovers that we did, one of the main reasons behind regular rollovers was actually practice, so that people involved would know how it works. As people are lazy, everybody came up with a software product, and now uses software products to the rollover automated. That's like you buy extremely expensive running shoes, and then when you put them on and decide running in the morning is really boring, so you hire a student to do the exercise for you. That is what's happening with regular key rollovers.

Here are the numbers. In 2015, you see that we got from a remarkable 20,000 to roughly 40,000 in 1.5 days on 30th June, so there was an impact, which is great. Actually, 40,000 out of 16 million is roughly three in one thousands, so I'm not going to compete with anybody who was on the panel here, but actually you can see the impact, just maybe with a looking glass. This is the overall development since we started, which s 2011.

You can see a growth there in 2012, and thanks to our Dutch colleagues and their initiative to convince Dutch registrars to sign everything, we have the first step and then the second far to the right in June is the one you saw on the previous slide. Above the green there is a shady, gray area, and that's another 25 per cent on top of those who are registered that are signed, but not yet registered. So we do have shy registrars and shy resellers.

In part, this is natural, because people sign first and then register after some testing, so it's not always the same 25 per cent not signed, but that's something that needs a bit more investigation. So is this consistent with what the previous speakers said? Mostly registrars doing a full service may not even be involving the customers. Sometimes resellers do this, and the change we noticed was that it was smaller resellers, previously 50 to 100 domains, and now we see registrars in the three to four digit range.

The big step on 30th of June was a single registrar signing all their so many thousand domains. The rest is geeks, some security aware companies, rarely banks – there's one German bank, and PayPal, who are signing stuff – and most importantly in our community, email providers promoting DANE for email confidentiality.

This is my final slide. What else happened, or what did we do as a registry? We added support for elliptic curve crypto, and we're going to hear about that later from Roland and maybe from Ólafur. We do support GOST crypto, and ECDSA, both the [NIS 00:59:20] curves that are defined, which his all current non-deprecated IETF-defined algorithms. Why do we have to support this as a registry? We do cautious pre-delegation checks before accepting stuff for publication as DS records.

We're not believing that this is ready for primetime for ourselves, and we don't recommend using ECC at the moment, given the validation situation, but I guess we can discuss that later. That's basically it. Thank you.

RUSS MUNDY: Thank you Peter.

DAN YORK: Peter, I'd just like to say thank you for talking about that DNSSEC Day. It was an interesting initiative, and I comment you on it. Speaking German, I did tune in and listen for a while, and it was quite good to see, so thank you for doing that, and for reporting back here.

RUSS MUNDY: We were going to wait until the end of the questions. Is this specific for…?

SPEAKER: It's regarding .de. [Mark Street 01:00:31] from Global Village, a registrar based in Germany, and also a DENIC Member. Not to rain on Peter's parade here, but DENIC, you may know, is membership driven, and I tried to start a discussion on whether the German membership would be interested in doing something similar to what the .eu and .nl and .cz does – namely having a discount for DNSSEC domains, and it was turned down.

What also became apparent is that the two dominant registrars in Germany, which have far more than 50 per cent of the market, are not interested in doing DNSSEC. So I'm afraid we're not going to see anything significant in .de any time soon.

PETER KOCH: As [Mark] has rightfully said, this is membership driven, and the financial structure and the governance structure behind that suggests, after thorough deliberation, that doing the discounts would be counter-productive in a way – as in who would be benefiting the most? One thing to keep in mind is to make a discount an incentive, your prices have to be at a certain level. I guess our prices are far below that level.

SPEAKER: What I heard is .de is so cheap it doesn't make sense to do any discount.

PETER KOCH: Yes, that was the bottom line. The ranges where it actually makes a difference, discounting the domain prices – and, in brackets, since we are a not-for-profit, eventually every cent that you don't spend, your fellow registrars have to pay – the range where it would make a difference is probably beyond the 100,000 or 500,000 domain range. But we can talk offline afterwards anyway. Thank you for raising this.

RUSS MUNDY: Thank you very much. Now let's move onto Vincent Levigneron from AFNIC. Thank you.

VINCENT LEVIGNERON: Thank you. My name is Vincent Levigneron. I work for AFNIC, and the proposal in this short presentation is to show you where we started with DNSSEC and where we are now. We started DNSSEC in 2010, like many of you, when the root was signed. We proposed DS registration in 2011. At the beginning we had six ccTLDs that were signed, and we used only three HSMs and AEP Keyper HSMs, which were all in the same facility. We had one for the production system, one for the sandbox, and one only for development purposes.

We used the uncommon configuration with a mix of NSEC3, Opt out and dynamic updates. We also used OpenDNSSEC. We had one instance of OpenDNSSEC for key management, and we used BIND to sign the zones. We had a unique and static Salt. I used BASEBA11, because I am a baseball player, so it was funny for me. We did key ceremonies manually. It took a lot of time, and sometimes we had one key ceremony per year, because we generated keys for one year. We had very few signed records in the zone files.

Today, while we still operate our six historical ccTLDs, we also operate 15 gTLDs, and we have about 20 HSMs, which are distributed in three different locations, and some are just dedicated for our disaster recovery plan. Our HSMs are still AEP Keyper, and we continue with them because it works fine for us. We have 16 independent open DNSSEC instances, and now Salt is no longer a static one. We rollover it once a week, and we have a unique one for all gTLDs and ccTLDs.

We do about 120 ZSK rollovers per year, and we had only six KSK rollovers since 2010, but there will be six new ones in the next month. The key ceremonies are mainly automatized now, and with more than three million domain names, about ten per cent are signed. In fact, it varies from one TLD to another. For some TLDs we have only one zone signed. For some we have more than 250,000 zones signed, and it varies from one per cent to almost 50 per cent.

As some of you perhaps know, AAK and SMK management can be cumbersome. That's why we decided to have the same AAK for all HSMs, which means the same operator and security officer can operate all HSMs. We mainly use two SMKs, because we use a load-balancing tool. We have one for our gTLDs and one for our ccTLDs.   In fact, HSMs are not dedicated. Some can host only one TLD, but others can host eight TLDs. Each TLD uses two load-balanced HSMs, and one other for the disaster recovery plan.

We cannot use HSMs used for gTLDs with those for ccTLDs. It's a choice, because we have different SMKs. We could be, of course, technically it's possible, but with our automatized system it's not possible. For those of you who use AEP Keyper, you know there are only 32 sessions per HSM, and we need to have more than one session for some TLDs, so this resource becomes critical. We still have resources left, but if we need more performance, or if we have more TLDs, it's something we need to take care of; to have enough HSMs left.

HSM batteries should be changed, and we need a plan, because we have many HSMs to maintain. We have automatized many things with DNSSEC, and we have a tailored script that's been written in order to support key ceremony processes, and now the key ceremony only takes 30 minutes. It took hours before, but now it's very fast. It's done in our main facility. We don't need to go into our data centers, because we use a load-balancer, and we don't need access to our HSMs, which are on data centers. We have a HSM that's dedicated only for ceremonies.

Of course, for security reasons, we still need humans to set HSM Onlines and backup keys on Smart Cards. We also implemented a complete rollback, because it's not a future that doesn't exist in OpenDNSSEC and in HSM, so we can do a complete rollback ceremony if something fails. It's happened only once, but with that feature it's not an issue for us.

We do many ceremonies. We need to have a key ceremony per TLD per year, and we have scheduled to have at least one key ceremony per month, with nine operators and nine security officers. These are the same people. They share the [walls 01:09:42] in fact. We have two special operators who operate the scripts. We have also three masters of ceremonies, and they change every month. Everybody is involved at least twice a year.

It's very important to train people, because key ceremonies can be a little stressful, so if you practice them all the time it becomes something very easy to do. We back up Smart Cards, the new keys we just created, and we just need one Smart Card per TLD, because we just back up the new keys, not the whole bunch of keys on the HSM.

Our future plans are of course to improve our scripts, because there are never enough checks in scripts, so we need to add new securities to our scripts, because we use only them, and there are no more manual operations, so we need good scripts. We need to work on a battery maintenance plan, because if you have to maintain the battery on the HSM, you need to send back the HSM to AEP Keyper, so of course when the HSM is not here, you can have a problem.

We need to add a centralized control system for all open DNSSEC and HSMs. It's something that's partly done, but it's not completely finished. We also need to improve our alert system in case of key exhaustion. We also had other actions for DNSSEC. For four years, we have had a DNSSEC training program with a company called HSC, where we provide two days of training. It's successful.

We also have a short session called DNSSEC How To. It's a one-day session where we practice a lot with those that go on the training course. We had one last week with about 15 people, and it was a success. We try to demystify DNSSEC. We just launched our third DNSSEC promotion plan with a discount for signed zones. Last slide? Just in time.

RUSS MUNDY: Excellent Vincent. Thank you. We really appreciate the feedback on the progress you folks have made. It's really been significant, and you have been wiling to come and contribute and tell us what you've been up to several times. I want to also acknowledge the earlier times when you all were here talking about the challenges that you had, and you were very open and willing to share the problems that you've encountered.

So it's very wonderful to see the progress and how so much has moved forward, and it's really smoothed out, especially from an operational perspective now. That's great. Next we have Sara Montiero from .pt, and she's going to tell us what's happening there. Sara?

SARA MONTEIRO: Hello. I'm Sara Monteiro, and I'm here to give you an update on DNSSEC status in the ccTLD of Portugal, .pt. We have considered some questions that the Program Committee has sent us, and we will try to answer them in this presentation. Yes, we are indeed interested to report on DNSSEC validation, but unlike the Netherlands, DNSSEC validation is non-existent. We don't know why. Maybe lack of motivation? How to motivate them is the same question that we have.

Money is always the answer, but we prefer to try probably making friendships, connections, and find something that's not involved with money, that both of us in the community could benefit. What can DNSSEC do for us? I think for .pt we think in the Portuguese community we are trying to provide a more secure DNS service. We are trying to help our community to adopt and use DNSSEC. We have hosted training since 2009 and we are still hosting them.

We think that being ahead on the technology curve will be the best way to be, and we try to do it by best efforts and doing best practice to make the Internet more secure, safer, reliable, and this way our customers can feel more satisfied and secure on the Internet. What doesn't it do? It doesn't make us richer, because it's free. It's not simple, so it doesn't simplify the DNS, and it doesn't make our work easier. But we are tough, and we know that the DNSSEC chain is complete, but it doesn't work properly without our [ESP 01:16:30] support, so we really need to persuade them.

The internal trade-off to implementing DNSSEC in .pt, we felt we were among the first TLDs implementing it, so we feel proud that we are doing that job. I think the cooperation and partnership among peers is essential, because we wouldn't do it without other ccTLDs until this help, and we are trying to give our experience to other ccTLDs as well.

What did we learn in this path? As I said before, the cooperation and partnership is essential, and we value that. I believe that hard work, not giving up, having faith that it will work out eventually are the main goals with DNSSEC, and we believe that the work that we do is for a good purpose. To be persistent and to be patient is our team.

Some .pt data – right now, this chart is not updated to this day, so I can tell you that we have 2,000 domains with DNSSEC, right now, and since we have around 260,000 .pt domains active, we have a percentage of five per cent of .pt domains signed with DNSSEC. So five per cent is good, but it's not the biggest number here. I think it's the smaller of this Panel. We know that we achieved this number because our second-largest TSP registrar implemented DNSSEC by default, so that was good. We hope the first largest one will follow in his steps.

Maybe some time soon, we don't know, we can try to persuade them with also DNSSEC discounts and something like that, but we didn't apply anything besides trying to show them that this is useful and they should adopt it. We believe that new people bring new ideas, so we have submitted a proposal for a Master's thesis related to DNSSEC solutions in one of the main Portuguese universities.

We'll be having a student that is going to collaborate with us, studying a new process, and then analyzing the best solutions to implement DNSSEC. Maybe he wil be original and try and find something that we're not seeing. We hope so. About cooperation and partnership, we are trying to help other ccTLDs by passing onto them our knowledge and experience. We recently created a Portuguese language ccTLD association called LusNIC. You can find more about it on the LusNIC website.

For these three ccTLDs that are mentioned here, they are from Africa, and concerning the .gw, it's the ccTLD for Guinea Bissau. We are helping to manage this ccTLD, so they don't have the infrastructure, the knowledge, the means, so it's being hosted and operated with us. As it's easy for us, we sign this ccTLD, but the DS record is not in the root zone yet, so maybe it will be one more. The only question is when we pass out the operation and management to them is whether they'll be able to sustain it. We are trying to train them to be able to do that.

Considering .cv, Cape Verde, we have been working with them since 2010 and we give them training. We believe that they have all the means to sign with DNSSEC, we are just hoping to have a green light and help them to do it. Considering Angola, .ao, they are not as evolved as the others. So we recently hosted a DNS and DNSSEC Workshop to some local engineers, this September, and we hope they will improve their domain name skills management with this workshop, and maybe further on we'll help them more. That's it. Thank you very much for your time and listening.

RUSS MUNDY: Thank you Sara. That's great to see some of your initiatives there. They indeed are some things that I had not heard about or seen elsewhere, and the grouping together of the Portuguese-language countries is a great idea, and signing and running their zones when you can is wonderful.

Okay, so our final Panelist here is the person whose last name is even more challenging for me than Vincent's, but I know Roland as Roland from SurfNet, and I gave up even trying to pronounce his last name a few years ago. Roland, please proceed and tell us what you're up to there.

ROLAND VANRIJSWIJK: Thank you. My name is Roland Vanrijswijk. My talk is going to be about the use of elliptic curve cryptography in DNSSEC, and I've a couple more slides than some of the other folks, so I hope you'll bear with me. Also, some of you will be more familiar with what I'm discussing than others, and I have to strike a balance. I hope I'm not boring the knowledgeable people, and I hope I have some entry-level information for the people that know less about this topic.

There's been some talk about using elliptic curve cryptography in DNSSEC for a couple of years, and it started gaining some momentum when the nice folk from CloudFlare, who will be presenting later, announced that they were going to do DNSSEC at some point, and that they were going to do this using ECC. What we decided to do, together with the University of Twente, where I'm also a researcher, is to see if, based on some measurements, we could make a case for ECC in DNSSEC, and what that case would look like. So how does it improve the situation compared to what we have now?

So DNSSEC deployment has taken off better in some places than in others. In the Netherlands, for instance, it's taken off quite well. But there are still operational issues, and these are already well known – issues with fragmentation, amplification, and complex key management, as Peter mentioned in his talk. We believe that the root cause of many of these problems is the fact that most of DNSSEC exclusively uses the RSA crypto system. Use of elliptic curve was standardized in an RFC in 2012, but has seen very little use until today.

Just to briefly touch on the existing issues, fragmentation is a well-known problem. Up to ten per cent of resolvers may not be able to received fragmented responses. There are solutions available. You can set your authoritative name server to only send minimal responses. The fallback behavior in DNS resolver software has improved hugely over the years, particularly because of this issue, and the RFC that describes EDNS0, which is the base protocol that DNSSEC is based on, the phrasing in that was made much stricter in the updated version 6891, particularly to address this problem.

To give you an idea of what setting minimal responses does for you, this is a graph from a couple of years ago from one of SurfNet's name servers. If you look at the top graph, the blue line, that drops steeply, and that is the decrease in average response size, achieved by turning on minimal responses. It dropped from somewhere around 800-900 bytes on average, to about 150 bytes on average, which is perfectly acceptable, but fragmentation still occurs.

The bottom graph – and it's a little hard to see on this screen – this is a graph for the past month, most of September. As you can see, there's a steady background noise of answers that are still getting fragmented, and that means that they're over 1,500 bytes in size. Around about

0.1 per cent of v6 responses get fragmented, and around about 0.2 per cent of v4 responses get fragmented.

The other issue with DNSSEC – and this has been pointed out by many, many critics, and I'm sure the people that celebrated DNSSEC Day complained about this – DNSSEC is a potent amplifier. You can use it to achieve D-DOS attacks. In a study we performed last year, we looked around about 70 per cent of signed domains globally and measured the amplification impact that they could have, because this has been discussed for years, but there was very little ground truth. Nobody actually bothered to measure what the effect was.

So we decided to do that. What you can see on this graph on the left-hand side is a representative sample of unsigned domains. These are about two and a half million domains, from which we measured the amplification for the ANY query. As you can see, that's somewhere around a factor of five, so the amplification of that is pretty negligible.

On the other hand, all the DNSSEC-signed domains we measured, where we sent a ANY query, all of them achieve pretty high amplification levels between a factor of 40 and 60, and we set a theoretical upper-limit for amplification in this study, which was what you could achieve if you had a classic DNS answer that was packed to the limit of 512 bytes. As you can see, all the DNSSEC-signed domains exceed that by far.

Now, there's been some discussion about deprecating ANY queries. Ólafur has a draft circulating in the IETF about that. I think it's a good idea, because ANY, we once introduced it for debugging purposes, and it gets abused by some pieces of software, which I shall not mention. In DNSSEC of course we cannot suppress DNSKEY queries, because they're essential to the protocol.

What we found in a measurement study that we performed is about 40 per cent of DNSKEY responses exceed our maximum upper limit that we set for amplification, what you could achieve if you were to use classic DNS. So even if we were to deprecate ANY queries, you could still achieve significant amplification by sending lots of DNSKEY queries, which would be bad.

The root cause of this, we believe, is RSA, because RSA keys are large. A 1024-bit key gives you 128 byte signatures, a 132 byte DNSKEY records, and 2048-bit keys, which are often used for key signing keys are even worse. Also, the cryptographic properties of RSA are such that if you want to strike a balance between signature size and key strength, you end up having a split key scheme, where you have a KSK and a ZSK.

Because your KSK invariably is going to be 2048-bits, because it needs cryptographic strength, because you don't want to roll it all the time, and your ZSK you want to keep small, because you don't want to have huge signatures all over your zone. That means it's going to be very hard to migrate to something like a combined signing key scheme where you have a single key. You could argue that you could go for a key [unclear 01:30:36] in-between the two, but for some bizarre reason people seem to think that RSA keys only come in increments of factors of two.

There's more information about this particular topic in the paper. Next slide please. ECC to the rescue, right? Elliptic curve crypto has much smaller keys, much smaller signatures, and the key strength is better. So good news all over the board. Elliptic curve crypto, with a 256-bit group size is roughly equivalent to a 3072-bit RSA. Two elliptic curves are already standardized for use in DNSSEC. These are the two NIS curves, P-256 and P-384, but they're used very little in practice.

99.999 per cent of .com, .net, and .org domains that are DNSSEC-signed use RSA. Hopefully that's going to change, and Ólafur is probably going to tell us more about that later in the session. There is a lot of buzz around using ECC in DNSSEC. It's getting discussed on the mailing list, it's getting discussed in the IETF, it's getting discussed in this forum. So there's clearly an interest in using this, but how good is it? There are alternative signature schemes that have even more favorable properties.

For instance, there's the Edwards curves-based EdDSA scheme, designed by Dan Bernstein from the University of Chicago, Illinois, and the Technical University in Eindhoven. That signature scheme has even more favorable properties for using DNSSEC. So what we did was we performed a measurement study where we wanted to quantify the impact of switching all of DNSSEC to ECC, and what impact that would have on fragmentation and amplification.

So again, we looked at all the signed domains at .com, .net, and .org, and we studies a couple of scenarios that were from really conservative, where we would use the strongest keys with the most conservative key scheme, where you have the split between KSK and ZSK, all the way to a very innovative scheme where you'd be using EdDSA, based on the Edwards curve, with a combined signing key, to see how this would impact the problems we mentioned before.

If you look at the impact on fragmentation, this graph shows you DNS key response sizes for some of the scenarios that I mentioned before. Now, the original responses that we got by querying all these .com, .net, and .org domains is the solid black line on the right-hand-side of the graph. What you can see is that around about ten per cent of DNSKEY responses, which use RSA at this moment, exceed the minimum MTU for IPv6, and around about two per cent of responses exceed the MTU for Ethernet.

So that means that those responses will get fragmented. If you remember that around about ten per cent of resolvers may have an issue receiving these responses, that is a problem. All of the ECC-based schemes achieve DNSKEY response sizes that are well below these limits. If you go for the more innovative schemes where you have a combined signing key, if you use either ECDSA with curve P-256, so something that you can already use today, or if you were to use the Edwards curves, you could fit your DNSKEY response in a classic DNS message of 512 bytes.

The impact on amplification is also quite significant. First of all, if you look at the ANY query, then still you can achieve quite a bit of amplification, but it is much less than you'd be able to achieve with the RSA-signed domains that are operated today. Then if you look at the one that we cannot remedy in a simple way, which is the amplification of the DNSKEY query, there it's even better. Because there, switching to even the most conservative ECDSA-based scheme, which is to use the big curve, P-384, it would give you an amplification way below what we said is an acceptable upper limit.

We also looked at the A and AAAA responses for these particular .com, .net and .org domains. We queried the apex domain, www, and mail, and if we were to switch to ECDSA P-256, which is available today, then all of the A and AAAA responses that we got back from these domains would fit in a classic DNS response. The conclusion is that switching to ECC is highly beneficial, it tackles major issues in DNSSEC.

It can also give you simpler key management, for which I would refer you to the paper, which I've Tweeted a link to, for the pre-print version of that. If you're interested in that, look on Twitter. There's one thing we need to deal with, which is the impact on DNS resolvers. ECC validation speeds are up to an order of magnitude slower than RSA, and there have been some improvements in this space, but still ECC is slower to validate than RSA.

We were unsure whether that was going to be a problem, so I had a student look at that over the past couple of months, and he's graduating tomorrow. That's why I have to fly back tonight. I'm not going to be presenting his work, but the bottom line is all the modeling and simulations that we did show that even though ECC is slower to validate than RSA, that is not going to be an issue with the current state of DNSSEC deployment, but it wouldn't even be a problem if everybody adopted DNSSEC everywhere. So really there is no reason not to switch to ECC.

I wrote a paper about this for the [ACM] Computer Communication Review. I'm not sure whether this is available free of charge, but there is a pre-print version on my homepage and I Tweeted a link to that, and I'll send a link to the organizers of the session so they can share it with you. Again, I have a student graduating tomorrow, and you can expect another paper pretty soon, which will summarize his results. That was it from me. Thank you for your attention.

RUSS MUNDY: Thank you Roland. As always, doing very progressive and interesting work there. Now, we have a little less than ten minutes for questions. Why don't you go ahead and start the questions?

ROY ARUNDS: Okay. My name is Roy Arunds for ICANN. Great presentations. Thank you. I love this stuff. I would like to ask the audience and any of the folks here who are associated with a TLD if they can comment on plans to deploy using elliptic curve cryptography instead of RSA? Thank you.

PETER KOCH: We don't have firm plans yet, but since we are in the process of purchasing new HSMs, elliptic curve support is mandatory, and we've also claimed interest in EDE-25519 for some of the operational properties that we think might be interesting, like no need for an entropy source and stuff like that. That's probably too technical for this discussion, but the bottom-line is we want to be able to have a system that can sign independently, and we can merge the zones, so we can rely upon the fact that signatures are generated equally everywhere. The crypto that we have there doesn't really provide for that.

Another difficulty is still algorithm rollover. We want that to have settled before we make the move, and while elliptic curve is very interesting, everybody has seen that RSA can be scaled in strength by just changing the key size. Changing the key size with ECC means changing the algorithm, and that again gives you an algorithm rollover, so that's a bit more complicated. In the medium to long-term, we'd really love to go to ECC, but we want to see the validation side clarified, and the operational issues.

We are well aware of the fact that we are pushing the loads to the edges to the validation systems, and that needs to be taken into account.

RUSS MUNDY: Ron, go ahead.

RON: Just to comment on that, because Peter mentioned the EDE-25519 scheme as well, there are already drafts circulating in the IETF. Ondrej from .cz NIC is leading a draft there, and there are also drafts for newer variants based on the same elliptic curve schemes that have bigger group sizes, and they're cryptographically stronger, but of course give you bigger signatures as well.

DAN YORK: I was going to say thank you for bringing this. One of the questions, and I think I see someone at the mic who may talk about some of this, is in the last session I gave a presentation on some of the barriers that we have for deployment of this, one of which is what you identified around the validation side. Is the researcher that you talked about, did they look into more on the validation results?

ROLAND VANRIJSWIJK: Yes. To give you a little bit of an idea of what we had him do, it was that what we wanted to know was how many signature validations you have to do on a validating resolver. Because that basically is going to determine your CPU load, if your CPU load increases because of the cryptographic algorithm you use. So what he did was he created a model that allows you to predict how many signature validations your resolver has to do, and then simply you measure how well the algorithm that you want to change to performs, and then you can calculate where the cut-off point is going to be.

That's actually what he did. We then put different scenarios into that model, which was to take the current deployment scenario and then to grow that to what if all popular domains decide to sign in this algorithm, or what if all domains decide to use this algorithm. What is the impact going to be on the CPU load of your resolver?

DAN YORK: Thank you for that. I'll be curious to see more of that research, because I do believe that we need to move to using these curves, for a number of reasons, so I'm looking forward to more of that. I think we can probably pass it to Geoff to talk about what I think he's going to talk about.

GEOFF HUSTON: Geoff Huston, APNIC. We've actually been measuring validators and their capability to actually validate in RSA and ECDSA. We were testing protocol 13. When we did this about a year ago we found that one in three end users who used validating resolvers that were capable of doing RSA, one in three of those resolvers were incapable of validating in ECDSA. You had about a 30 per cent drop-off. We did the same test again earlier this year, in March, and the number is now a little better, one in five.

What's going on is that there are still a lot of folk sitting behind resolvers, where the open SSL library does not include elliptical curve, and so when it gets presented with the signature, which is elliptical curve, it simply says, "I'm going to treat that as unsigned," and walks away. Now, the numbers are getting better, but it is still disappointing that you're seeing around one in five users, if you went and signed with elliptical curve, they're not going to actually do validation on you.

So realistically, that's another part of this problem about ECDSA. It seems a little bit of a problem to jettison one-fifth of your population by changing protocols. Thanks.

RUSS MUNDY: Thank you Geoff. Any Panelists want to respond? Paul, go ahead.

PAUL WOUTERS: Paul Wouters, RedHat. The biggest problem I think right now for ECC is that most people cannot do an algorithm role, because their software doesn't support it. For instance, a lot of people use OpenDNSSEC, and it doesn't actually support an algorithm rollover. People cannot move from RSA [unclear 01:44:58], just like in fact people cannot move from RSA [shell 1], to RSA [shell] 256, which a lot of people would like to do, because they can, on the fly, decide between NSEC and NSEC3.

So that is one of the bigger problems. With my vendor hat on I can say that people tend to not move to zero versions of various operating systems, so [unclear 01:45:18] 7.0 wasn't very popular, which was the first version where we introduced ECC. So hopefully that will get better soon. Also, the ECC got [unclear] to [rail six], so hopefully we'll see a little more deployment there. The next thing I want to say is the slide that has this title of basically "RSA kills people", I would like to change it a little bit and say, "Adding security to DNS kills people".

ONDREJ SERY: Ondrej Sery, .cz NIC. The draft that Ron mentioned wil be updated in a couple of days, because Simon has updated his draft that we depend upon, but we couldn't make it to the draft cut-off time, but we hope to update it with [unclear 01:46:16] before the Yokohama meeting, and we would appreciate it if you could review the next version that we can move ahead and get it out as soon as possible, so that we're not standing here in another three years and speaking about how feeble the support for EDDSA is in the real world.

RUSS MUNDY: Thanks Ondrej. Let me double Ondrej's request there. People please take a look, review, and send comments in so that we can get progress on this area through the IETF for standardization process. Rick, go ahead.

RICK LAMB: I'm not going to talk any more on that topic because it's clearly very interesting to us, as myself as being part of the design team for some of the KSK root rollover stuff as well, so this is very interesting and very useful information. I'm looking forward to that. I was just going to thank some of the other speakers as well, and ask some specific question.

For .cz, just a clarification question: you described how your Knot resolver responded with NODATA instead of NXDOMAIN and minimized NSEC and stuff like that. Was that just for the IPv6 inverse/reverse lookups? Or was that a general statement?

ONDREJ FILIP: Yes, I think that's just for this purpose.

RICK LAMB: Good. That made me nervous, all right. Then [PKS11 01:47:45], I know you're using the GnuTLS stuff. I've tried to compile some of your stuff before, successfully. Have any of your engineers tried plugging in an HSM or Smart Card and making it worse?

ONDREJ FILIP: Yes, we are working on that right now, so it should be ready by the end of the year.

RICK LAMB: Okay, because I tried, and I didn't get very far. The other question, [.fr], wonderful description of the AP stuff. We're stuck with these guys for a while. You said you pre-generate keys and you do this often. It almost sounded like you had the KSKs offline. Are they on the Smart Cards, or are they in the HSMs? Are you reloading them each time you use the HSMs or…?

VINCENT LEVIGNERON: No. They are online.

RICK LAMB: They're online. They're in there all the time? Okay. With OpenDNSSEC, these pre-generated key blobs, how's that working for you with OpenDNSSEC? Pre-generated DNSKEY RR sets?

VINCENT LEVIGNERON: Yes. We pre-generate the keys for one year, and then OpenDNSSEC do what they have to do. It works fine.

RICK LAMB: All right. I think the only other thing was Sara, from .pt, I'd love to talk to you more about some of the training you're doing for some of these other ccTLDs, and the work you've done there. That's exactly the model I like seeing; to see that kind of train the trainer and expand the expertise scenario. So anyway, thank you.

RUSS MUNDY: Okay, well, thank you everybody. We've actually reached the end of the time on this session, actually very close to on time. If anyone else has any last-minute burning questions, last chance to run to the mic.

DAN YORK: Russ, I would just say I thought it was great. I want to say thank you to Sara for bringing the fact that there's now a Portuguese ccTLD association. I thought that was great information that I didn't have, and I just find it cool about the way that we have the DNSSEC space and the growth in our communities that we have both now, for you with the Portuguese, and we also have the AFTLD folks here as well, we just need to see the continued evolution of the different parts of ccTLD spaces. So thank you.

RUSS MUNDY: Yes, and thank you everybody. This has been such an interesting session. I have heard some really new things, new ideas. It's hard to know how hard it will take to have them reach fruition and success. Dan was pointing to the coalition. I thought the idea of funding a research activity in a university by the cc [unclear 01:50:55] itself, great idea. Get the students educated, and for those that are in the university world, Roland, thank you for encouraging your students to work in this space. That's great.

Thank you to everybody – to the Panel, very interesting, great updates, and thank you. They'll be around for a little bit. Let's give them one more round of applause. Now we have a break until 11:00. We have water in the coolers up here. If people want coffee and tea, I'm sorry, it's not our fault – you have to go down to the first floor and buy it down there. That's just the way the conference center is set up.

[Audio part 2]

DAN YORK: Come on up people. There's plenty of room alongside the tables. We've got more room up here if you'd like to join in. We don't bite, honestly. At least most of us don't anyway. All right folks, I think it's about time that we rejoin here and get started. We have our Panelists ready. Let me go and turn it over to Jacques, who's going to moderate our next Panel.

JACQUES LATOUR: Hello. I think we have five or six spaces still available at the front. Welcome. I'm Jacques Latour, and today we have a Panel of two on DNSSEC on the edge. We're not specifying on the edge of what, but it's on the edge. One of the big reasons we're here today is for.ca we have a lot of issues in getting signed delegations. We have about 100 signed domains for .ca. We spent a lot of work building EPP for

DNSSEC. We did a lot of work with the registrar to get them to do DNSSEC, and there's no traction. The idea is to try something new, to get DNSSEC adopted with .ca, and so we started to talk about that at various panels; at the IETF in Hawaii, and I think this is a result of the work we've done so far. Today we've got Ólafur, and he's going to talk about signing at scale on the edge.

ÓLAFUR GUÐMUNDSSON: Thank you Jacques. I'm Ólafur Guðmundsson. I work for a little content delivery network. We have a few million customer's zones that we operate for them, and we're going to be rolling out DNSSEC to most, if not all of them, in the next few months. We have data centers all over the world. We have thousands of servers. We have lots of DNS traffic. We don't answer most of it, because it's attack. For some reason we're very popular with unpopular people, depending on what time of day it is, but roughly we answer about one in 100 packets we get. The rest is attack traffic that we drop.

This map that you see on the screen shows our current network map, plus/minus one week or two. It will not be valid much longer, because we are adding locations all over the world very fast. All DNS infrastructure is, to a large extent, all built in-house. We have our own authoritative server. We have a proxy DNS service as well, and we distribute our data via a database replication mechanisms to the edges. Things are changed fast. Answers are given out depending on what questions are asked.

Distributing signed answers to the edge for address records is a non-starter. Data changes frequently. We want to move it out. We don't have a zone file. There are no zone files. In our infrastructure we move it out to the edge. The edge servers decide, based on various criteria, what to answer. It is not a traditional "we sign at a central location", blah blah blah. We are different.

We are going to be enabling DNSSEC. Yesterday, Californian time, we announced that we are opening up our beta again for anybody who wants. You can go in, you can send an email to an address that's in our blog, because I had to hand out these slides earlier I didn't get a chance to put the right address in there. Since then we've been getting a flood of people asking to join our beta test. We didn't expect this many. We are getting hundreds of requests to join the program. No matter what people say, there might be a demand for DNSSEC, especially if you don't have to do much yourself.

We are taking the work away from people as much as we can, and we're taking over everything. Real soon, most TLDs wil be enabled. We're going to roll this out slowly, not overnight. Some TLDs may get preferential treatment, if we can inject DS records into them quickly. We're talking to registries and registrars about that. Like Roland mentioned earlier, we are very conscious about the size of our answers, both because of amplification attacks, and also we just want to not send out extra crap.

We selected the electric curve algorithm, and the main reason we selected it was because we get small answers, but more importantly we don't have to do key rollovers, and people whine about it, because of the strength of the algorithm, the only reason we're ever going to do key rollovers is because we think keys are compromised or we're switching algorithms. Everybody we sign gets the same key.

We have a split DS, split zone-signing key, and a KSK for all customers. The main reason for that is we are signing all the DNSKEY records in a central location, sending them out to the edges. Everything else is signed at the edge, so all our servers have a copy of the ZSK. This is an acceptable risk in our system, because we own all the hardware, we control all the connections, and we have our own hardware.

The same thing. Our answers are like one-quarter of what they are if we use the standard RSA setup, like the IETF is using. We think this is a major advantage. Size matters, and also the speed. For us, electric curve is faster. Validation is a little bit more painful for validators, but compared to network delays we theorize it's not going to be a significant factor, and we hope to get an academic validation of our intuitions soon.

In the process we decided to take a look at what is DNSSEC protocol doing, and why is it doing it. if you get a negative answer from DNSSEC offline signed zones, you get two NSEC records most of the time, or you get three NSEC records depending, and each one of these is signed, and that is extra [garbage 00:10:08]. But because we're signing on the fly, we can cost and tail the negative answer to the question being asked.

If somebody asks for a name and type a name that doesn't exist, we will give you a signed answer that the name exists and there are only two different RR types that exist there – the RRSIG and NSEC – and we'll give you a minimalistic answer of what the NXDOMAIN is. If you happen to ask for the NXDOMAIN, we will drop it. We are totally preventing zone walking. We are giving out minimal answers.

We are very interested in the work that's being done on figuring out if we cause NSEC records or NSEC3 records during prefix floods, to help resolvers stop. So we may give out wider ranges, but that is configurable, what we give out. We call this "Black Lies". Some people don't like it, because they don't get a NXDOMAIN, but we tell you the rule of how to translate or answer into a NXDOMAIN locally. This makes the answers really small, and resolvers have to store less, and it works. We've been doing this on a number of zones for eight months, roughly. It works. Nobody has complained.

When somebody asks for a type at a name that exists, but the type doesn't, as we have to calculate this on the fly, we have to enumerate all the types that are there, and we realized we don't really need to do that. So we have the shotgun approach. We list all the types that we think are of interest to you, but we remove the ones you asked for if it doesn't exist. If you ask for some other type, you will get a different NSEC record. This has confused lots of people.

But we're telling you at the time you asked the question, this answer did not exist on that [machine 00:12:27], but then you ask for some other type and suddenly it might theoretically exist. So it's a lie, but it works. Online signing. People have not wanted to do that. We are answering at scale. We are answering tens of thousands of questions from each one of our servers. In our first implementation we had some code in there that said we're only going to generate so many questions per second with answers.

Then we had one of our co-workers who sat down, did a little bit of optimization on the code, and right now we have ripped out all the code that checks on throttling. It is cheaper to sign than it is to compress the names. That might be my next evil idea. By cutting down the NSEC records we send out, that helps us a lot. We re-use the signed SOAs, which we have to put in the negative answers, and so for every question we get, we answer it. We also have done another little hack, so when somebody asks for ANY, we only give them one record.

The key distributions. Like I mentioned before, we control everything. We have a secure boot, we have secure software distributions, we trust our servers. Therefore we have no problem distributing this key to them, and it doesn't make it any less safe that we have only one key for all the DNS server zones, because if somebody steals one of our servers and keeps the power on and reads the key out of the memory, it doesn't matter if there's one key or 1,000 keys. They're all gone.

We needed to address a number of things that normal operations don't necessarily do, or traditional is probably a better word. We have a central signer for all the key records. We sign DNSKEY records centrally. We also publish CDS or CDNSKEY records for every zone that is DNSSEC signed, and we are going to be doing that to allow uptake by registries, registrars and others, of the signed zones. We had to change most of our protection system in one way or the other to support DNSSEC.

This didn't just involve doing the UI. We had to change how we distributed data to the edges. We had to change our databases. We had to create a system of monitoring the health of our clients, because we want to notice if the zones are validatable, if the DS is uploaded correctly, et cetera. We want this to work, and if something goes wrong we'll try to take whatever action is possible to fix things without involving the customer. When the customer is involved, that is a delay, and very likely not going to happen.

We are going to be supporting TLSA for all our zones. Right now we're not able to do that, but that will be coming early next year. Every DNSSEC-signed zone will have TLSA records for them. We really would like to take the customer out of the equation of uploading DS records. Right now, this is the biggest frustration people have. We tell them, “Go to your registrar, upload it,” and A) for us to give information to the customer of what to do, we have to know who the registrar is.

Based on the WHOS information, we may have the accurate information, or we may not be able to get the information because we’ve been blocked by WHOIS servers here and there. My best guess is we have 30 per cent of our customers who we know accurately who their registrar is. Even if we know the registrar, we may not know who the reseller is, which the customer is supposed to go to.

I am a DNS operator. According to the ICANN domain registration model, I don’t exist. The model assumes that zones are operated by the registrant or registrar and reseller. There is no concept of our DNS operator. I have been a DNS operator for my friends for decades – over a decade. Mark, hi! Mark and I – Mark Costers – and I have shared supporting each other’s zones for a long time. Our arrangement has been outside the registration model. I can’t talk to registries, I can’t talk to registrars without having access to the customer account.

I don't want access to the customer account, because the customer is afraid we might steal them, and we don't want to do that. We need an easy way to upload DS records. We saw these presentations from the TLDs earlier today, of the abysmal numbers of DNSSSEC-validatable zones. All of the zones, say 99 per cent of them that are DNSSEC-signed, are parked at registrars. I don't know how much traffic they get, but the inability to upload DSs is a real pain. It's not just having the commercial entity, the registrant needs to go to supporting DNSSEC.

They also need to support the algorithm in use. We get so many reports that these interfaces allow algorithms up to eight. They may allow some algorithms in the 250 range, but they don't allow the algorithm as defined in the last five years, because people assume nothing changes. They run old code, nothing changes. That's why the ICANN network here in this building does not support validation on the elliptic curve.

I've complained about this at every ICANN Meeting I've gone to since I started working at CloudFlare. Every time I'm told it's going to be fixed. It hasn't been fixed, because they use a three-year-old release candidate as a name server validator here. It's not a release – it's a release candidate. If ICANN can't keep their stuff up-to-date, I don't know who can. So it's a long-term project of getting people to run modern stuff. The newer elliptic curve that's being proposed, I don't know how long it will take to get them supported in large numbers.

Going through the exercises with the Canadians and a few other registries of how to do this, we have come up with a simple idea of how to upload it. Jacques will talk about it. The important things that come out of the DNSSEC, we are going to be publishing CDS and CDNSKEY records for the registries and registrars and resellers to pick up, and the customers can look at them. I want to change the dialogue to say, "If a zone publishes these records, it's a signal they want to be validatable."

So it should be perfectly okay to pick it up and start [security 00:21:08] from there. I will call this an opportunistic DNSSEC. What we also discovered is the CDS/CDNSKEY records need a delete mode, because there has to be a way to turn off DNSSEC. Customers may be moving from one operator to another. They don't like what they get, or whatever. So there has to be a way to say, "I don't want this anymore." I have an Internet draft out on that. I got more time than I expected, so thanks to the Panel.

What I want to say is you're going to see lots of signing on the edge by us. I hope other content delivery networks will start coming and doing this. It is hard to build the systems, but once they are built, everything should just run. DNSSEC was designed in an era when everything was static. It supports that very well, so some innovative solutions were required to start supporting online signing on the fly. We tried not to break anything too much, but some things will break always, or there are bugs.

I want to say that we found a bug in one of the testing tools last night. I talked to the maintainer here this morning, and it's already fixed. Things can get fixed. So please keep pushing, keep complaining to your providers to support DNSSEC. There are going to be millions of ECC-signed zones real soon. That's it.

DAN YORK: Thanks. A question. So I think you identified one of the challenges we've certainly seen with the rollout of the EDCDSA and the other algorithms. I think one of the problems that we have as an industry that we have to figure out how to help around is we have a whole generation of software programmers who have learned, through the security vulnerabilities that were out there, that they needed the check bounds on lists. So if you had a list of items, they needed the check bounds, because otherwise there would be unbounded data, and stuff would get in through problems and fields and things like this.

The challenge is – and I think we're seeing this with registrars – those developers are not updating their lists of bounds when new things come along. The ECDSA was finalized as a DNSSEC algorithm back in 2012, so three years ago, but some of the software is not updated to know that there's a new entry in the IANA registry for DNSSEC algorithms. So your point, as we get the new curves that are out there, as those get added as IANA algorithms, we're going to have the same kind of issue that those will be on there and we're going to yet again need to get the software updated to support those algorithms.

I think the larger message to the folks who are doing software out there, that relates to DNS and DNSSEC, is that we need to have people – if they are going to do bounds checking – they need to update the lists of what they're checking on a regular basis, and then get that out in their software updates.

ÓLAFUR GUÐMUNDSSON: This is a good comment. It's a little bit more nuanced than that. The software might be perfectly fine in accepting it, but there's a database behind it that it's driven from, and nobody checks. I basically blame myself for this situation, because I see that they've signed the DS record to have only one field, and then code everything into it and just give it out as a hex field, rather than giving people an opportunity to check bounds.

DAN YORK: For those not aware, Ólafur was the author of the RFC that specifies the DS records, so that's why he's making that statement here.

MARK COSTERS: I have a separate question, and that is what software supports CDS and CDSKEY right now?

JULIE HEDLUND: Can I just remind people to state their names?

MARK COSTERS: I'm Mark Costers.

PAUL WOUTERS: ICANN is a part of it. I know that BIND and Unbound all support it. You might have to have a few compile flags to enable it specifically on older versions, because when there's a draft, usually they add it with a "--enable" option, but the modern ones all support it. Usually they're pretty good at implementing something that's an RFC. When it's a draft they'll have a special option, but when it's an RFC they just enable it.

ÓLAFUR GUÐMUNDSSON: Yes. Knot and PowerDNS also support it. I think [unclear 00:28:15] also support it, but I don't know if Microsoft does.

ROY ARUNDS: Just a clarification question: is it complete online signing, or only the negative stuff? I missed it from the presentation.

ÓLAFUR GUÐMUNDSSON: Everything but DNSKEY and CDNSKEY. Mark wants to speak again.

MARK COSTERS: Can you specify the signing operations per second you can handle?

ÓLAFUR GUÐMUNDSSON: No. A lot. I have a lot of servers. I'm not authorized to answer the question.

ERWIN LANSING: Erwin Lansing, .dk. We're a bit special and we don't follow ICANN, so we don't really have registrars, but we do have DNS operators. We're changing our system a little bit. There are issues you're going to complain about, but from early next year the DNS operators will be able to upload DS records directly to the registries.

JACQUES LATOUR: Cool. That's good. Roy? Last question? I'll do my presentation and then we can have more questions after?

DAN YORK: I was just going to ask, Ólafur, do you have a sense yet of how many of those registrars that you're interacting with will enable you to interact with them? Or is it just Jacques sitting next to you?

ÓLAFUR GUÐMUNDSSON: I'm a registry, not…

DAN YORK: Well, what's your sense? You talked about you have this barrier of being able to interact with all your customers in there. Do you have a sense yet of what the size of that problem is? Or is it just everyone?

ÓLAFUR GUÐMUNDSSON: I will work with anyone. Stay tuned for the official announcement next month.

JACQUES LATOUR: I'm Jacques, I'm with .ca, and what I'll do is I'll go quickly to my presentation, and then we can have a discussion after that. Bootstrapping the DNSSEC chain of trust is the title of this. The idea is that today registrars, for .ca, don't do DNSSEC, although we have EPP, we have everything in place for them to support it. We have a real challenge in getting registrations done. We have about 100 signed delegations. It's pretty sad. It's even in the 0.005 per cent range.

This is an update from the last presentation. The link is there, and you can see the last PowerPoint deck, so it's just an incremental update. The picture here shows the ecosystem that we live in. We have .ca as a registry. We have registrars that have full EPP access to do whatever they want, but none of them support it, like I said. Then we have a registrant in there. Then sometimes a registrant uses a hosting provider that may or may not be the DNS operator.

Sometimes hosting providers outsource to content delivery networks, and they're the DNS operator. In that model, everybody is far removed from the registrar. So today the process is the registrant technically generates a DS or a DNSKEY, and then they push it down to the registrar, down to the registry, and then we put it in the zone, and the chain of trust is established. That doesn't work today.

So what we're working on is building an interface directly at the registry to enable the DNS operator to create the chain of trust, initially, and to do ongoing management. The whole process around creating the chain of trust the first time, it's the process of putting the DS and the TLD, the parent zone, the first time.

For .ca the way we're looking at it is that we need to ensure good hygiene for name servers, so the DNS operator signs the zone, they sign is properly, and then we make sure that over TCP, and for each of the name servers that are in the RR set, that we can actually validate that the CDS, the

DNSKEY, all of the signature, the zone, it's signed across all name servers. So that the work of validating, of doing DNSSEC at the child, is done properly across all name servers.

That's the bootstrap validation process and the idea is that we generate the proper keys in the back to create the bootstrap. If the zone is not signed properly then we're going to give a detailed message to the operator to say this is why it failed, so they can debug their own installation. So the validation process is we, as a parent, poll the child and create the bootstrap from there. The second part of this is once the operator signs the zone and it's properly signed and everything, then we need an intent.

We have an API where the DNS operator goes to us, .ca, and they signal their intent to sign a zone, or to update a zone, or to unsign a zone. We do all of this by reading, interpreting, and managing how the CDS/CDNSKEY records are in place for a zone. Then that's about it. So for DNS operator we have a RESTful API for large volume, and then for individual DNS operator we have a web interface they can log into and initiate that process. The parameters for this process, the validation, is a domain name.

All they need to say is update whatever domain name, and then we go from there in the back and then we do all the instruction from there. When we started this, we quickly discovered that we needed a way to unsecure a delegation – to remove a DS from the parent. We looked at using the CDS record for this. If the child is signed, the chain of trust is established, everything is done property, if they tell us to go and update their domain, we'll read an old CDS, we'll see that everything is good, and then we'll remove the DS and unsign the delegation.

Plus, other registry [staff 00:34:05] will send emails to al the contacts to tell them it's going to happen, and we may add some time delays to execute the transaction, but the idea is if we go from one operator that support DNSSEC to another one that doesn't, we need to unsign a zone. This is the bootstrap. Once the domain is bootstrapped, the next thing we're going to do is maintenance. So automated DNSSEC maintenance. We'll use a CDS/CDNSKEY.

On a daily basis we're going to poll the domain, check if there's changes, we need to do key rollover and all that, and then we'll read the CDS/CDNSKEY and do all the instructions that are in there. Once technically a domain… We talk to BIND, and [unclear 00:35:02] and a couple of other people to automate key rollover with CDNSKEY, so technically a domain should be able to manage from there. There's no need for manual process from a registrant or a DNS operator. The chain of trust should be established, managed, and rolled over when necessary.

We're looking at a policy. The way we do this is we create the DS and we put it in the zone so we're in control of the algorithms, the keys and everything that goes in there. We're looking at a scheme to notify contacts, and how often we need to notify registrants of DNSSEC activities, if we need to notify, if they care, and what we can do about it. Like I said, we control the DS format.

This is the model of the system. We have a DNS operator with low volume that can access our system through a web interface. They need to authenticate and prove that they are whoever they are. Then they go into the interface and all they do is put a domain name, enter, and that's it. No other information. Then our validation engine is going to go and poll the domain, grab the DNSKEY, grab the CDS, everything. We generate a DS, and then we have an EPP module to submit that in our registry automatically.

The maintenance part is ongoing maintenance to update CDS, do key rollover, and all that on behalf of the DNS operator. We have an API RESTful interface with some sort of authentication of an access list to make sure that it's controlled, and then that's about it. The idea is that that piece of code that we're going to make open source should be reusable for registrars. A registrar that wants to use this for their customer base, they can integrate with their own EPP system, and then potentially work back down to the registry.

The idea is to not have the registrant create a DS, copy the DS to a web interface with the registrar, having to deal with issues with algorithms that are not supported and all that, to remove the frustration. It's to automate the process, make it super-easy for a DNS operator to sign, have a good enough trust model to create the chain of trust, and to go from there.

If a registrant or a DNS operator is not comfortable with this model, they can always use the registrar EPP interface to authenticate the account and follow the right process, or a different process. This is an alternative way of bootstrapping, plus a system to keep domains up-to-date.

Right now we're working to write our code. I think we've got a couple of sprints left to go. It's actually going well. We're going to do a pilot project with CloudFlare. They've got about 15,000 .ca domains that we're going to run through this. Then we have an API we can play with, a prototype. There's the URL. We're working on building the framework. It's evolving. I think at the beginning we made it way more complex than it is now. Now it's more simple. There's been a lot of feedback, a lot of criticism, a lot of positive support, negative support. We've tried to integrate everything to make this work.

We talked with BIND and OpenDNSSEC to have the CDS process work. The idea there is that if you want to sign your zone, but not automatically delegate, then you sign it and you just have a DNSKEY record. If you sign and you want to delegate the zone then you sign and you add the CDS record to match the DNSKEY. That's the intent that we're trying to propose here, to create the bootstrap for the first time. Obviously we want to make all of this open source. We want as many registrars and registries to use this framework.

We got a draft done yesterday about this, or the day before. Ólafur is working with others and I on some sort of RDAP extension or framework to find the parental agent for a domain, so the DNS operator knows where to go to initiate this process externally. I guess we'll have more to say about that later on. I think we're… I can come down now. That's it.

DAN YORK: I have a question Jacques. It's Dan York. How are you dealing with the authentication of who gets to make these updates directly into the registry database?

JACQUES LATOUR: The framework is a bit different. It's now who gets to make the update. If you sign your zone and it's property signed and it's got a DNSKEY and a CDS, that means you want it delegated. Instead of us polling 2.5 million domains every day, it tells us, "Go poll this domain," and if it's all done properly, it gets delegated.

DAN YORK: Okay, but I'm just wondering if I'm an attacker and I decide to set up a site, and I want to try to spoof your site, or spoof somebody's site, what's the protection of somebody putting bogus information into the registry through the API? How's it authenticated there?

SPEAKER: The attacker needs to accomplish that they're not going to be picked up by any of Jacque's props, because Jacque's system goes out and asks all the listed name servers, "Do you have the same information? Is it all matching?" He can do that from multiple locations, he can do it from there, so I think worrying about this part has kept us in the place we're in today.

DAN YORK: Okay. I want this to succeed, but that's one of the issues that I've had raised, was, "Could an attacker get in there and do that?" Even if there was more to deny, to cause a problem [unclear 00:42:28] issue. I see Paul and Roland both wanting to say something.

PAUL: One of the reasons, apart from the fact that there was this argument that people can get at your customer if you go outside EPP channel, it's that of course you have a separate channel to establish trust in the key. It's outside the DNS and now it's taken into the DNS also to do the bootstrapping. So in essence it's trust from first use.

Because you have this API to start the polling, have you considered asking the person that requests the poll to include the key in that request? Because again you then bootstrap the trust through a separate channel, where the person says, “Poll me now, and this is the key I want you to poll me for,” have you considered that?

JACQUES LATOUR: Yes.

PAUL: And why did you not do it?

PAUL WOUTERS: I'm Paul Wouters. I helped a bit on the prototype implementation and the considerations for it. If you do anything like the [unclear 00:43:32] did, like adding a token to the zone to prove that you own the zone, you’re not adding more proof than the CDS record.

PAUL: That’s not what I’m arguing. They have a separate system that you tell, “Poll my zone.” That’s a web API or it’s a web portal, or it’s a RESTful API. That’s a separate channel. If you submit the key in that channel and then you have two sources of information, one is the DNS and one is that channel, and you combine the two and they match, then it’s…

PAUL WOUTERS: That channel is not necessarily authenticated.

PAUL: It isn't, but the same is true fro…

PAUL WOUTERS: No, because then you have the additional problem. Now the CA needs to get a million end user credentials on their system to talk directly to… You've just moved the problem. Now you have to prove that you're talking to the registrant or the DNS hoster that is responsible for running the registrant domain zone, and that's exactly the problem we're trying to avoid here, because that's what's not working.

SPEAKER: I run the registry. I've got the authoritative name servers listed for a domain, and if I can't trust those name servers and my registry that these are the guys running the domain, if they're compromised, they're compromised. Most likely, if they're compromised then I'm going to sign the domain. They've got other stuff to do.

SPEAKER: They will also wait a couple of days. They will probe over the course of a number of days. It's not just like a quick take-over you need to do. You need to keep a sustained attack on all name servers going from different views in the world. If you get to that point in an attack, you basically own the domain already, for all practical purposes.

SPEAKER: I have a follow-up question to that, owning the domain. Because one obvious attack vector is now that I find an operator and I want to lock somebody into me, as an operator. I sign the domain and then I refuse to unsign it. Can registrants override the secure delegation through their registrar channel?

SPEAKER: Yes, they could. Yes. [Manuel 00:45:36]?

[MANUEL]: Anything that comes through the registrar interface should override whatever automatic systems have done.

SPEAKER: [unclear 00:45:51], [cc NIC]. We, at Chile, talked a little bit with our operation manager, and actually there is no demand from our DNS operator, surprisingly, however we are developing an open source system thread that's used by seven other countries, so we're thinking about this; maybe not for us but maybe for other countries. We have a slightly different or specific data model in the registry. We have four kinds of objects, like domain, contact, name server set, and key set. The key set is a collection of DNSKEYs.

This key set can be attached to any domain. All of these objects have their specific registrars. We're using this feature specifically for contacts for identity solution. With identify solution there's a registrar that's allowed only registry contacts, so no domains. This is the same for name server set and key set. There can be registrars that can only register and maintain key sets and name server sets, which is something that may be the solution for this case – that technically we could offer the EPP access to our registry, just to maintain the key set and name server set for DNS operators, and there is no problem with authentication.

That registrar, it's just the registrant of the domain that will decide to associate the key set and name server set of his domain to this registrar with this access, and the registrar can do updates in these objects; changing DNSKEYs regularly. So this may be another solution for the same problem, maybe, which you can think about.

SPEAKER: Thanks.

DAN YORK: You're early Jacques, you still have time.

JACQUES LATOUR: Any other questions or issues?

ÓLAFUR GUÐMUNDSSON: Jacques, maybe you want to clarify what to do with the CDNULL record? Or I could mention it? There's also a way where an operator, like a big operator who wants to move away – so for instance we know CloudFlare is running ECC – if they would move their domain to another hoster that doesn't support ECC for DNSSEC, then the domain has to go insecure. Again, to go through the registry in getting this done is not an automated process.

The draft that we wrote actually introduces a NULLCD record that specifically instructs the registry to remove all DS records at the parent. This record is a CDS record that's signed properly, so that you know that the DNS [operator 00:48:47] actually requested this.

JACQUES LATOUR: One of the big challenges with DNSSEC right now is doing a proper DNS operator transfer, and that's something we need to work on. Some domains, I imagine, will not be allowed to go unsecure on a transfer, and we have to find a way of doing this that's more automated, and in this model having the EPP key relay process of transferring the key from the gaining registrar to the losing, it doesn't work in this framework.

I have to do some serious thinking on how to do a secure domain operator transfer. I'm not sure what the solution is. If anybody's got some insight on that, that would be useful. That's it. Thank you.

RUSS MUNDY: Thanks Jacques. Thanks Ólafur. Now I believe… There he is, the star of the great DNS Quiz, Roy Arunds. Please, Roy, over to you.

ROY ARUNDS: This was really a last-minute thing. We have a slacker in our midst. I won't say who. What you're about to see is a bunch of recycled questions that most of you have seen before and hopefully forgotten. This is the great DNSSEC quiz. We've done this before, many times, and the idea now is that we keep on doing them, provided that you provide us with interesting questions that we can turn into a pub quiz. Hopefully in front of you or near you, you have the back of the form with 12 entries that you can fill out. A pub quiz typically is a simple question with a multiple choice answer.

The question is, if this is a pub quiz, where's the beer? That's question number 13. There are 12 questions. Sometimes more than one answer is correct, and you get a point for each correct answer. For instance, if you have a question and A, B and C are correct, you get three points. So the maximum per question you can get is four points, if you have them all correct. Put your name down on the form please. You can work in groups as well. When I'm done with the quiz, please give your form to a neighbor or someone else out of your group who then can check the answers.

After we check the answers we'll put the form back and see who's the winner. Of course, the winner of this quiz has eternal recognition. Who remembers the last winner? Exactly. There we go. Last thing, if you get a wrong answer, you get no points. It's not that you lose points, you simply get no points. Question 1: which TLD has the largest deployment of DNSSEC? Was it A) .de, B) .se, C) nl, D) .br? This is in absolute numbers, so not relative numbers like how many per cent per registration. What I mean is the largest amount of signed delegations.

Question 2: which of these TLDs deploy DNSSEC? A) .ec, B) .tk, C) .tv, or D) .mx? Don't use your laptop to find the answers. Thank you.

Next question: which keys are mandatory in a DNSSEC-signed zone? A) ZSK, B) KSK, C) CSK, D) ESK?

Question 4: what does the AD bit stand for in a response? A) authenticated denial, B) ano domini, C) access denied, D) authenticated?

Question 5: what does the DO bit stand for in a DNS query? A) DNSSEC off, B) DNSSEC on, C) DNSSEC out, D) DNSSEC over? Don't worry if you don't have this one.

Question 6: what does 257, which is an integer, indicated in a DNSKEY record? A) this is a DNS zone key and secure entry point, B) this is a DNSSEC zone-signing key, C) algorithm 257, which stands for RSA NSEC3, D) CCLVII?

Question 7: which of these four are valid DS algorithms? A) [shar] 1, B) [shar] 256, C) [shar] 384, D) [gosh] R3411-94?

Question 8: when was the root KSK rollover? Was it A) July 2010, B) January 2012, C) never, D) the KSK is rolled every three months?

Question 9: what does the CD bit stand for in a DNS query? A) compact disc, B) checking disabled, C) cryptographic device, D) change directory?

Question 10: what does KSK stand for? A) key signing key, B) kill switch key, C) key switch key, D) kappa sigma kappa?

Question 11: how many different root server addresses are there? A) 12, B) 13, C) 24, D) 26?

Question 12: which country, ccTLD, was the first to deploy DNSSEC? A) Puerto Rico, B) Sweden, C) Denmark, D) Germany?

Okay, so again, make sure you've put your name on the form. Hand it outside of your group or to your neighbor, so we can go over the answers.

NEIL: Roy, Neil here. I have a question about the scoring scheme – whether one can score more than one point for a given question?

ROY ARUNDS: Yes. Did I miss that at the beginning?

NEIL: It was a bit like the distinction between any and all.

ROY ARUNDS: I need some help with this. I'm going to go over the first question. Which TLD has the largest deployment of DNSSEC? C. If you have C, you have a point. Question 2: which of these TLDs deploy DNSSEC? A) Ecuador? No, despite the fact that I have DNSS.ec, which spells DNSSEC, I still can't get a signed delegation in .ec. If you need some help, I'm here. B) .tk, C) tv, D) .mx. Is .tk signed? .tv? .mx? Yes, .tv and .mx are signed. C and D are both signed, A and B are not. If you have one right, you have one point. Two correct, two points. New rule! If you have one wrong you default on the question, you don't have any points. Otherwise you could fill out A, B, C, D every time! Question 3: which keys are mandatory in a DNSSEC-signed zone?

SPEAKER: I object to the question. It only requires a key. It doesn't have to be a KSK or a ZSK, because that's a functionality, and a CSK is a combination of the two, and I don't know what an ESK is, but you just need a key. It would be nice if you got a secure entry point set, but even that's not really necessary.

ROY ARUNDS: Okay, so a key with a secure entry point bit set, what do you call that? It's a KSK, yes? Okay, there's a question? That's correct, but that's not actually here. You're right – you need to publish the public key and keep the private key private, but if you have A, you're correct. I'll give you a point if you have B as well, and I give you a point if you have neither, because every time I get into this discussion.

SPEAKER: Roy, the only right answer to this is none. Because CSK and KSK are rules, they're not keys.

ROY ARUNDS: Here's the thing: you need at least a key to sign, is that correct? Here's my somewhat logical thinking behind this:

you need at least a key. If you don't set the secure entry point bit in that key, to me, old-fashioned, long before protocol lawyers got involved, I call that a ZSK. You don't really need to have the flag bit set in order to sign the zone, but it's mandatory to have at least a key, so I call that a ZSK. I thought A was the right answer. Okay, question 4: what does the AD bit stand for in a response? Paul, what do you think?

PAUL WOUTER: I again object to the question, because the right answer isn't there.

ROY ARUNDS: Sorry, why do you object to the question? Lunch is off!

PAUL WOUTER: The answer is authenticated data, which is not listed there.

ROY ARUNDS: Not true. That might be clarified in a later draft, but in the stuff that I wrote it's authenticated.

RUSS MUNDY: There is one other fundamental rule. In the event of a dispute, the narrator is always right.

ROY ARUNDS: The last one was D. Thank you. Question 5: I made a stupid error this morning. In my rush I should have entered “DNSSEC okay” but it’s not on the screen. So silly. The right answer is none. Question 6: what does 257 indicate in a DNSKEY record? A) DNS zone key and secure entry point B) DNSSEC zone signing key, C) algorithm 257, D) CCLVII?

DAN YORK: A, subject to Paul’s objections, I’m sure.

ROY ARUNDS: A is correct. It’s a DNS zone key and secure entry point. That’s the literal meaning of having these two flag bits – I think 15 and 16 and bit one set. It means DNS zone key and secure entry point. Question 7: A, B, C and D, all of them. Four points if you have all of them, subject to Paul’s objection.

PAUL WOUTERS: I’m checking IANA right now.

ROY ARUNDS: What if IANA is wrong?

PAUL WOUTER: IANA, by definition, is never wrong. That's the whole point of IANA.

ROY ARUNDS: Question 8: this is a trick question as well. D is wrong. We roll the ZSK every three months. C) it's never rolled is also not correct. B) January 2012 is not it, so it's A.

DAN YORK: There was a nuance there.

ROY ARUNDS: Sorry guys. I need to get one up for the protocol geeks.

RUSS MUNDY: This is the one I debated with him last time and remembered by own rule for this that the narrator wins. I don't agree that [unclear 01:07:04] was a key that was rolled, but Roy's right.

ROY ARUNDS: Number 9: what does the CD bit stand for in a DNS query? B is correct. It's checking disabled. Number 10: what does KSK stand for? That would be A) key signing key. Number 11: how many different root server addresses are there? C) 24. There are 13 IPv4 and 11 IPv6 addresses. The last one: which ccTLD was the first to deploy DNSSEC? B) Sweden. Please tally up all the points that you have. When you're done, hand back the form to the original owner, and let's see who the winner is.

Before we go into that, if you have interesting questions or curiosities or trick questions, send them to me. I'm roy.arunds@icann.org, and I'll hopefully get them into the next presentation next time. Who has 17 points? Anyone? Okay. Let's do a binary search. Who has 13 points? Okay. Who has 15 points? Here it is. Who has 14 points? No one who had 13 points? Perfect. We have five winners. We hopefully will remember you next time. Thank you.

DAN YORK: That now brings us to our lunch break. For everybody who's still here, you can go over to the lunch area. Julie, anything you want to say to us?

JULIE HEDLUND: They're going to have to move your chairs so that they have space to get the food in back there, because we put in extra chairs because we were getting full. Just give them about five minutes. The people who are in the back row by the food, if you wouldn't mind them moving the chairs and get the food in place? Maybe about five minutes or so? Once you see the food then we're ready to go. Thanks everyone.

DAN YORK: We'll be back here at 13:15 please. We'll start back up for the remainder of the sessions with our DNSSEC and applications. Look forward to talking to you all. See you at 13:15. Hey, I have one more thing. Is Vicky still here? Vicky from ISC has these DNSSEC for BIND quick reference guides that folks there have made up.

She'd love some feedback on them, so if you're a BIND user and you'd like to check out this reference card she has that talks about DNSSEC for BIND, she'd like to give you one of these, and also get any feedback you may have. She's there waving the card up there. Go see her. She has a bunch of these and she'd like to get them out for feedback from folks. Thanks all. See you in a bit.

[Audio part 3]

DAN YORK: I'm going to moderate from over here, purely for the fact that I have my video set up over here, but we'll go with this. Welcome to our afternoon session here at the DNSSEC Workshop at ICANN 54. Thank you for those of you who've been here for the morning sessions, and who are here. Thank you again to our sponsors; Afillias, CIRA, DINE, .se, and SIDN for providing us with that lunch. Pretty decent? That was good stuff. Live demos are starting already with messing up the screen.

I'm Dan York and I'll be the moderator for this session. We have four different demos, discussions, and pieces that are going on. One of them we've already seen, with Wes trying to get his connection working. This is the part where we do the more dangerous aspect of the show. Without further ado, we're going to start up, and we've got until 14:30 that we're going to be going with this, so we have an hour and a bit that we have time for this.

We'll do each of the demos and then we'll have time for questions right after each one. The 15 minutes will include a little time for questions as well, because they are for different topics. I'm told we're having some live demos here too guys, maybe? Sara says no. We might. Without further ado, I'll give you one of the IETF 93 Hack-a-Thon participants, Sara Dickinson, to talk about DNSSEC and legacy applications.

SARA DICKINSON: Thank you very much. What I'm going to talk about in this presentation is a proof of concept implementation; the aim to provide DNSSEC for legacy applications. I'm presenting and I was involved in this project, but unfortunately the people that did the real work behind it weren't able to be here today. So I'm presenting on their behalf. Those people are Alison Mankin and Gary [Visvasvaryan 00:06:50] from Verisign Labs; [Theogen Becuti], who's a student at the University of North Texas and did a summer internship at Verisign Labs, and also [Willem Turrip] from NLnetLabs.

The goal of this work was really to look at how to enable end user applications to benefit from the security that's provided by DNSSEC, but not just to stop there, but to also think about how you can offer access to newer features in the DNS, such as privacy. Some background – the initial scope of the project was to look at Linux and UNIX systems, where there's a default DNS rollover library, and applications typically do name resolution via the getaddrinfo and getnameinfo methods.

The majority of applications on those systems use that default resolver. There are a few – some browsers in particular – who use their own, but that's not that common. One of the big issues though is that the current library implementations don't support DNSSEC, nor some of the other more modern DNS capabilities.

There are ways to work around that. One is you can use a validating recursive, but that last mile issue isn't really solved at the moment. Also, that wouldn't enable access to newer features, such as privacy. There are several libraries available that do support DNSSEC. One I'll mention here is getDNS, which is fully featured, in regards to DNSSEC, and it also has support for TLS. But the downside is if you want to make use of those new libraries, you have to make code changes in the applications.

We looked more at how the default name resolution service is provided, and it's available through the name service switch. This is a pluggable interface, which allows different system services to integrate into the operating system, and administrators can configure specifically which services they want to provide the information to the runtime libraries here.

Very typically it's where you get user information, and also DNS name resolution services. If you've taken a look at this, you'll see that this is configured in the /ect/nsswitch.comf file, and in particularly the DNS service there, very typically the default configuration is that you look up in /files first, normally /etc/hosts, and then do DNS resolution.

The solution that's proposed in this work is to provide a new NSS service that uses getDNS to access the new features that we're looking for. By doing this, it should be transparent to applications, so that any application using the standard API can seamlessly get support for DNSSEC through this mechanism. This is a picture of the architecture that was implemented in the proof of concept. Applications will continue to use the name resolution interface, as they do today.

Underneath that NS switch is managing what's actually offered, and instead of using the default libresolve, a custom module has been implemented that uses getDNS, but implements exactly the same API, and that's a drop-in replacement then for libresolve. GetDNS, in this scenario, works as a fully validating stub. I'll mention in passing that the proof of concept work also experimented with an LD_PRELOAD mechanism, but I won't go into details of that in this presentation.

In terms of configuring this, it's very straightforward. To enable it, it's simply a question of editing the NS switch .comf file and changing the host line, replacing "DNS" with getDNS, and that's all that's involved. The configuration for this is managed in a separate file, and in the proof of concept it was in /etc/getdns.comf, and the default option that's offered is DNSSEC: validate. There is also another stricter mode, which is DNSSEC: secure only, which could be considered for use.

This is a very lightweight configuration, and one of the other aims of the project was that it wanted to be possible to deploy and configure this via automated tools like ansible and puppet. Something else that was investigated in the proof of concept was whether or not it made sense to try and offer end users the ability to do their own configuration, so: are end users smart enough to understand DNSSEC yet? Discuss. What they did look at doing was offering, via a webpage, the ability to make the settings stricter than the system ones. I'm sure this might get some discussion.

One of the bigger issues with this work was the signaling mechanism. The standard library calls, they have an existing interface and standard error messages. What that means is in the case of DNSSEC it's hard to signal to the application that what you've received is an answer, but that it perhaps has an invalid signature. You can signal failure, but that's indistinguishable from many of the other causes of a SERVFAIL. What you would really like is a way to be able to signal to the user, "I did get an answer, it's not that the network's down. I got an answer, but it was insecure."

The initial work done on the proof of concept on this was to look at for those applications that consume HTTP, was to use a redirect page that could inform the user if a site was bogus or insecure. Now, this approach is quite simplistic, and it only works for certain scenarios, but the idea was it was a proof of concept to show that you could provide that information to the user. So what's been looked at in the ongoing work is other mechanisms for doing this signaling – so browser plugins or system try notifications.

That's top of the list on the future work. Other things that are being considered are looking at adding a system cache to the validating stub to improve performance, also offering configuration options related to TLS, and this work is almost working, but not quite. The idea here is you could choose to, for example, disable_tls, prefer_tls, or require_tls. Also, we want to take a look at how you might make that configuration policy more fine grained, because it's quite coarse at the moment.

Another topic is looking at advanced security – so putting this on SELinux, AppArmour, how would it work for containers, et cetera. As I said, this is limited to Linus and UNIX systems, so a slightly different mechanism wil be needed to get support for this on Windows and on MAC OS X.

So the intention of this project is to release this module open source. Currently the wheels are still turning on getting that rubber-stamped, so unfortunately I don't have a repository that I can point you at. But if you're interested in this code, please grab me right after this session and we can talk. Also, to make this viable, there needs to be work done with the various platform communities in order to get this open source module embedded, so that this is available out of the box on all systems.

In summary, what we've proposed here is a solution that enables DNSSEC validation for legacy applications, and that was done through the existing name resolution framework for UNIX and Linux systems and BSD, so it's integrated into the OS via NSS switch. The design here uses the getDNS library under the hood to handle all the DNSSEC-related functions. I don't have a demo to do today, but I do have one on my laptop, so again, if anybody's interested, please approach me after the session and I can show you how it works in practice.

That's all my slides. Thank you for your time. If you do have comments and questions, please direct them at that mailing list, as that's where all the work on this has gone on, and I'd be happy to take any questions now. Thank you.

DAN YORK: Thank you Sara. Are there any questions for Sara about what she did here? Cristian, go ahead.

CRISTIAN HESSELMAN: Thank you. I'm Cristian Hesselman, I'm with .nl. My question is this works for Linux machines and [voodoo 00:17:20] and that sort of thing. How would you be able to get this kind of libraries to more popular operating systems such as Apple and Windows and that sort of thing?

SARA DICKINSON: Yes, so they don’t use that same NSS mechanism, but they have analogues of it, so the hope is that we’ll be able to find a way in to leverage it, but through a similar shared library. That’s the hope.

CRISTIAN HESSELMAN: Because you would somehow need to liaise with Apple or with the folks in [Retmond 00:17:50] to actually get this into their operating system.

SARA DICKINSON: If it were to be embedded, yes, you’re right, but hopefully, if it gets a foothold on the other systems, then that can be a driver for that to happen. But yes, it’s a challenge.

[MARK SULLY]: [Mark Sully] Global Village, registrar. Do you consider also adding privacy considerations into that library? Because the immediate use scenario that comes to mind is using it in our data center on our centralized resolvers – no, on individual servers, so we would also cover the last mile. But what also would be very interesting is if privacy considerations could be taken into account, because that’s the other DNS deficiency that we’re currently thinking about.

SARA DICKINSON: So you're talking about encrypting the channel that the DNS queries go over?

[MARK SULLY]: Yes, and sending [minima 00:18:34] queries, stuff like that.

SARA DICKINSON: So getDNS already supports DNS over TLS, and that's work in progress on the current module, so that can be supported through this, and getDNS will also…

[MARK SULLY]: That is in experimental status?

SARA DICKINSON: In getDNS as a standalone library, TLS is fully functional. All that's left to do is actually implement it in the module via configuration options. So it will be available.

DAN YORK: Any other questions for Sara? I think it's intriguing work. I look forward to seeing what you are able to do this. Please join me in a round of applause in thanking Sara. Next I will turn it to Wes Hardaker from Parsons to show us something here – DANE's secure email demonstration.

WES HARDAKER: We'll talk about the demo part. I'm going to ask later on if you guys actually want to see the demo, because it's going to be very small and everybody ought to walk forward, but we'll get through some slides first and then we'll see what you guys want to do. I'm Wes Hardaker and I'm going to talk about DANE and email in particularly, and how to secure mail – really the only way to really secure mail.

I'm going to talk a little bit about my background, and I'm going to talk about what's in scope, because one of the things I hate about doing demos is I don't get to give you instruction and explanation about stuff – because I'm going to show you more live stuff – and so I'm not going to talk in incredible detail about background. I'm also going to talk about what it takes to secure email and how to implement those requirements.

First off, a little bit about me. I'm part of a network security research group at Parsons, and we are an expert on all things underground-layer security stuff that most people don't have to think about, including DNS and DANE and email and things like that. My DNS history – I've done a lot in the past. There's five DNS RFCs, and I'm pointing the last two out in particular because they came out last week, 7671 and 7672 are DANE operational guidance as well as DANE over SMTP. It's only a week old out of the door. I'm also the founder of the DNSSEC-Tools project, where we have lots of interesting utilities, and DNS-Sentinel, which is our monitoring service that makes sure that your DNS is operating the way you expect it to.

What I am covering today is how to set up secure email with DANE. Operationally, how do you set it up? What I'm not talking about is how it works, because I've done that before – in fact, I did that last time. You can look at the slides from Buenos Aires, where I dive into detail about how it works. I also have a YouTube tutorial that's about an hour long about DANE and SMTP, as well as some other protocols as well. It was recorded in Chile last year.

Also, I'm not talking about securing email clients to their ISP. I'm not talking about POP and IMAP and delivering mail from your email client. I'm talking about the server-to-server work. You don't send mail directly to your destination. You send mail to your ISP, and your ISP figures out where to go next. That is unlike chat protocols and other stuff that may talk directly to the end person. Mail doesn't – it goes to your ISP first. In that diagram it's that middle part between the two boxes – not Alice on the left or Bob on the right.

First off, let's talk about what it takes to receive secure mail. How do you tell the world, "I have a mail server that can do secure TLS as opposed to just accepting anything out in the open"? It takes a few things. First off, you have to be able to be found by the distant server that wants to talk to you, and that involves DNS and DNSSEC – to make sure that they get to the right place, as opposed to spoofed DNS and things like that, that can get you to the wrong place.

You also have to tell them, "Hey, I can accept an authenticated connection and an encrypted connection," and that's where DANE cones in. DANE is what signals that and it's what points to the right [key 00:23:13] material so you know that you got to the right place. The end result is your DNS zone must be DNSSEC signed, and your DNS zone must include a DANE record for your SMTP servers. It gets a little more complex if you dive into outsourcing your DNS, or mail, and things like that, but it all works.

This is where the font starts getting smaller. I wonder if I can read it? Receiving secure mail with Postfix, the first thing you have to do is create a certificate. Every TLS connection requires that you have a certificate, so that's the openssl line to very quickly create a x509 certificate. It does not need to be CA signed. That's one interesting thing about DANE and SMTP - is that actually the CA industry doesn't need to be invoked. You can use it – there are ways of doing that too. I talk, and [Chile] talks all about that; about which method you might want to pick.

This one is a straight TLS certificate without sending it to a CA first. Then the last three lines tell Postfix how to use it. there's only three configuration lines. You have to point it where the key file is, you have to point it where the certificate file is – in this case they're the same, because they're encoded in the same file – and you have to tell it that you want to possibly accept TLS connections. You can say "tls_security_level = may".

In other words, people may talk to you with TLS. You may talk outbound to TLS. It's not required though. It's opportunistic TLS. In other words, opportunistic means you make advantage of it when you can. If you can't, you fall back to none. In my demonstration today I set up a couple of test records. In the dnssec-tools.org zone I created dane.dnssec-tools.org, and in it I put a DANE record that included an MX record pointing to a server, and for that server I put in an TLSA record.

Paul, a little bit later, is going to talk about how to create the TLSA record, so I'm not going to duplicate that here, but he'll talk about how to actually produce that later. Then I signed the zone. Obviously you have to have a signed zone. So the combination of signing the zone and signing the TLSA record means that everything is secure, and that TLSA record points to my certificate that I just created. It's critical when you're managing this system that every time your mail server certificate changes, you must update that TLSA record. If they don't match, you'll stop getting mail.

I'm going to repeat that, because it's important. If you do this, if you set up secure mail, make sure that your DNS infrastructure and your email administrators talk to each other. Every time that certificate changes, you must, must, must update your DNS to go along with it. There's a really cool website, which I can demonstrate again in a minute, if we decide to do the demo, which is dane.sys4.de. It is a fantastic testing utility. You plug in any hosting that you want, and it will test to see if it can securely send you email, and it will tell you what's wrong if you can't.

So the instant you put something out for a TLSA record and for TLS and for DNSSEC, it will walk and make sure that all of those things are operating properly, and it will tell you if it's not. That's how you receive it. You set up those things. You note that I didn't install very special… I'm using Postfix in this example. Later in my slide, if you want to download them, there's a couple of other utilities. [exiam 00:26:55] is another mail server that you can use. I didn't actually have to configure very much.

There was only three lines, and all I had to do was install a certificate. People will find it if they use DANE, and they'll get to you. Now I'm going to talk about how you do it on the outbound side – how you set up your ISP to send mail securely to somebody else. You do that by making sure that your DNS software verifies DNSSEC records. In other words, is it a validating resolver? Every lookup from start to finish, if you're going to do DANE in SMTP, has to be validated, start to finish for that TLS to be authenticated in the long run.

You have to have your MX records and your address records and your DNSSEC signatures, and all that stuff that we've talked about endlessly here at ICANN for years, has to be done. The mail server software has to be able to validate those DANE records. It has to be able to know how to talk to a DNSSEC compliant name server, or do validation itself. In the case of Postfix, it's talking to a DNSSEC compliant name server. The certificates have to match, obviously.

The DANE record has to match the server's TLS certificate that it's offering.

To configure Postfix, it's actually again quite simple. The Postfix team, and [Victor unclear 00:28:11], who's done a lot of the code, did a very good job making it very simple to deploy. But you need a DNSSEC validating resolver. You need Postfix 2.11 or better, or some of the other ones, but Postfix is the first out the door and it's the one I'm familiar with, so that's what you're going to see here today. They have to be running on the same host.

This is the way the Postfix team decided not to do validation in the application. They wanted to make sure that they sent their request somewhere secure so it should only be running on the same host. They expect the local validating resolver to be running on the same host. Then you need some configuration, and there's really only two lines. There are a couple more optional ones, but you set the SMTP TLS security level to DANE. That says basically you want to use TLS, if you can get there via DANE.

It's still a "may". If there is no DANE record, it will not deliver mail. It will still deliver it unencrypted if it cannot find a DANE record. Then you set the DNS support level to DNSSEC, saying you need that AD bit turned onto your local validator. We'll do the demonstration in a second. If you guys want to see it, you may have to crowd around the screen, because the font is smaller. I have a couple of demonstrations. I have one under dane.dnssec-tools.org.

I created a record, and the demo has my local laptop mailing to itself, and my laptop is running a DANE-compliant version of Postfix. It's able to go out and talk to the remote server, do the DNS lookups, and then show that it's getting there successfully. I also created another one that adds the TLSA record, which is actually the same thing.

Then I created a bad one too – so the red marks up there that you can't read from the back, I created a TLSA record with a bad entry, and so I can actually show you that if you send mail to that bad address, it will get queued and it will go through the standard "wait seven days" or whatever you have on your mail agent. It will refuse to deliver it if you've set up DANE and it doesn't match. In this case I messed with the fingerprint so it doesn't match.

The final one is I created another set of records called dane-bad2, where there's one server with a good record and one server with a bad record, and the MX records prioritize the bad ones first. So you can watch it. These are tests that you can do at home, and if you write me I'll be happy to give you the configuration. You can watch it fall back. It will try and talk to the first MX, and because the certificate doesn't match you went to the bad guy, you went to the wrong place, or you went to the operator that failed to configure things properly, and it falls back to the second one.

That's really kind of cool to watch, and it says, "Bad certificate found," and it will fall back to the next one and still deliver the mail. I do recommend you guys come out and play. Remember, the RFC got produced last week. There's 28,000 domains with DANE-active TLSA records. Granted, some of the reasons those numbers are so large is there's a couple of ISPs doing this for every domain that they serve. In Germany in particular there's a whole lot of German domains ending in .de that are signed DANE records.

The ramp is just huge. There's a lot of people turning this on. A lot of them are small domains, but some of them are big – about 10 per cent of them are bigger. First off, any questions? I'd be happy to throw up the demo. I'm running short on time too, but I don't think you guys can read it, so my suggestion was that if you want to see it, I'd be happy to show it to you later, because it's very small text in the log files that say "yes, I did validate". I have some TCP dump files that I can show you to show that it actually turned on encryption and things like that. Any questions at all?

DAN YORK: Questions? Go ahead, Roland.

ROLAND VANRIJSWIJK: Interesting talk. Thank you. I was wondering, do any of the big email providers, like folks like Google or Microsoft or whatever, presumably they support TLS on their mail servers. Have you talked to any of these folks to see if they'd be willing to supply pointers to their customers if you put this record in your DNS zone? Because I have a toy domain that I run on Google stuff, but I operate the DNS for that, obviously. All I'd have to do is stick the right record in my zone and I'd be done, right?

WES HARDAKER: You could do that, but do watch out that if they roll their x509 certificate that you would have to notice it, because otherwise you'll have this period where the DNS record keep the TTL short and notice it as fast as you can. Paul, you want to answer?

PAUL WOUTERS:	Actually, I think you're wrong, because you have to have the MX target signed, which would be the Google domain, so having your own domain signed doesn't actually matter.
WES HARDAKER:	If the target is in Google, that's true, yes, which is the reason, by the way, that DANE and DNSSEC are really the only ways to secure your mail. Because if you have an MX record to evilhacker.com, even though evilhacker.com might be signed, you can redirect people anywhere you want. You have to have secure from the root on down, all the way through the MX chain to you in order to secure your mail. Yes?
[SPEAKER]:	The guys from [cs4.de], I actively work with ISPs in Germany to get this rolled out.
WES HARDAKER:	Yes, so that's [Victor unclear 00:33:55]. He wrote that website that lets you test your zone. It's a fantastic system. He's the one that's reached out to a lot of people to answer your original question – Microsoft and Google – and no,

they don't have DANE records in place yet. There are some other pretty big ones, if you look at the slides from Buenos Aires, which is where that picture was taken.

I do have a list, like [unclear 00:34:19] Foundation and things like that. There are some fairly big names out there that have TLSA records in place. The IETF is DANE-compliant now. ICANN is coming. I talked to somebody about that this week. It's really close.

[MARK SWEIG]: [Mark Sweig 00:34:42] Global Village, newcomer to DANE. I have a question about the certificate. When I have to change the certificate, do I need a rollover process like with the KSK?

WES HARDAKER: Good question. Yes, you would need to put in two TLSA records. You put in the new TLSA record to match your new certificate. Wait for it to be distributed, so wait for the TTL usually twice, and then you can swap your new certificate in, and then another two TTLs later you can pull out the old one.

SPEAKER: So I can have two TLSA records, and it looks for either that matches?

WES HARDAKER: Exactly. Good question. Rick?

RICK LAMB: I'm not going to speak for them, but I had a couple of anti-phishing meetings. I understand that those big players are interested in doing this. It's on their map.

WES HARDAKER: There's a number of secure email technologies that all play well together, that if you have them all, you'll be better off. That includes [dekim 00:35:43] and SPF, and DMARK and DANE. If you do all these, we are beginning to lock down the world into a better place, but it's a step-by-step process.

RICK LAMB: Any other questions for Wes?

[ABDUL]: [unclear 00:36:01], Fellowship Newcomer. It's my first time here. Slide number 14, you said that you must run on the same host. For IDN domain names, or for host names, it is not logical for me to use xn-blah-blah in the host name of the server. So I have made a workaround that I made virtual books for, that have the IDN domain name, and it works as well.

WES HARDAKER: The reason that it needs to run on the same server has nothing to do with the domain name in question. It has to do with Postfix is not doing validation of DNSSEC records. If you had, in your resolve.comf file, if you were sending all your DNS requests to Google's 8.8.8.8, you'd be sending that request out, and you're trusting the AD bit back. You're doing no cryptography to make sure that that DANE record that you're getting back has been verified. You're trusting the network between you and Google in this case, in my example.

By having it on the same host, you know that all of the validation is being performed on the same machine that's using it. it's just a security measure. It has nothing to do with IDN or other related stuff.

[ABDUL]: Okay. There is another question. What is the difference between DANE and PGP?

WES HARDAKER: PDP is designed to secure person-to-person. It is intended to, most of the time, secure somebody's individual email, whereas DANE is designed to secure the transport between two SMTP servers. So very different security models. That's another good email security technology I didn't mention a second ago, which is getting down to the object level; signing the message as opposed to signing just the secure transport between the mail carriers.

DAN YORK: Are you going to talk about that Paul? We may have somebody else who could talk about how DNSSEC and DANE can deal with PGP as part of this, coming up soon. Any other questions for Wes? Yes, gentleman behind?

SPEAKER: Thank you very much. Is this method working with all versions of the SMTP – advance SMTP, secure SMTP, and…?

WES HARDAKER: The SMTP protocol quite a while ago specified how to send SMTP over TLS. It's been around for a very long time, in computer speak, which is not that long. It's old enough that almost every mail server out there supports it, including [sand mail 00:39:05] and other stuff too, which even hasn't been updated that recently. [sand mail] doesn't support DANE yet. So yes, it's a way of securing that to make sure that you're getting to the right place. It's making sure that when you open your TLS connection, you're getting to the right place. If you go and watch my video on YouTube, if you pull the link out of the slides later, I talk about that more specifically, of how that's working.

SPEAKER: Okay. It needs to open the cryptography, because when you're using advanced SMTP it has to open the packet and bring the header, and then [unclear 00:39:43] with [PTR] as I know.

WES HARDAKER: DANE uses the startTLS protocol. When you open a new SMTP connection, the remote server says, "I can handle all these options in SMTP." One of them is startTLS and if both sides support that then they say, "Okay, I'm going to startTLS." What happens after that is on the client SMTP server, it's making sure that the certificate the other side gives you matches what's in the DNS. So that's all that DANE does.

SPEAKER: Another question is does it work [ebac 00:40:30]? In some countries it's the local email. They use some [ebacs] and there are so many servers and they don't use SMTP. There's a special protocol to use only local emails with each other, for all the home towns.

WES HARDAKER: DANE only works with SMTP. That's all it's designed to work with.

SPEAKER: Thank you very much.

DAN YORK: Thank you for your questions, and let's join in with thanking Wes for his work here. I'd also just like to say I think the work that Wes and Victor have been doing has been great, because I find it somewhat ironic that DANE, which is this protocol that we have now for putting TLS certificates into this would find one of its best use cases in dear old email – this underappreciated… Anyway, it's great to see that the work is going on there. I would encourage you to go and look at that site that Wes mentioned, the [cis4.de] site that Victor set up. It's a good test site for email components around that.

We also should be clear – DANE is a mechanism, RFC 6698, for storing TLS certificates or pieces in there, in DNS, and being used in this way. It's the TLSA record and the other pieces. To the gentleman that was just up there at the microphone, asking about that, DANE can be used for lots of different protocols and different things. It happens that Wes, the technology he's working on is focused on using it for SMTP.

Somebody else could choose to use it for another email protocol or anything like that. So the ones you were talking about from those [Friday boxes 00:42:21], they could choose to use it if they wanted to, if somebody wanted to go and implement it.

WES HARDAKER: Yes. I misspoke a few minutes ago, when I said that DANE was only designed to be used with SMTP. DANE is a protocol just for putting out x509 certificates, and again, my YouTube video actually talks about Jabber and all sorts of other stuff.

DAN YORK: Right, yes, and we've seen a lot of uptake in this in the Jabber community and the work they've done, and some of the voiceover IP protocols. It just happens that at this particular session we have most of our Panelists talking about email in some way, which brings me to the next one – giving a different look, which is you, Rick. Paul's going to bat last and clean up all the issues we've slowly been assigning to him. But Rick Lamb is going to talk about a different technology.

RICK LAMB: I'm going to talk about the end-to-end thing – SMIME – being able to encrypt your email end-to-end, and this way, if you're like me and don't trust your cloud provider, or are a terrorist wanting to contact another terrorist, this is perfect for you. I'm going to have some difficulty here probably, in getting everyone to see this. As you see, my slides are going to be really simple. I want to leave as much time for the demo. I'm not going to try and make it look pretty or do anything. That's the name of the talk, that's me. This is stuff that I've done mostly on my own time, if not all on my own time really.

Microsoft Outlook is still a very popular client. Every time I come to these meetings I feel like if I say Microsoft or I say proprietary software, I'm basically shunned from that particular conversation, or even worse, have beer poured on me. It's a popular email client, and I don't care. I just want DNSSEC to get used. It's a platform for everything else, just like Windows is a platform for something. Last program I wrote, I didn't care. I wrote my own memory [unclear 00:44:37], my own [unclear]. I don't care. I ran it onto Windows – who cares? It's like doss.

There's a history of SMIME support, and it's been around for a long time. It's there – it's in Outlook, it's in so many other packages. I'm trying to get some estimate right now – Outlook usage is 80 per cent, something like that, out there, for desktops, mostly because of large corporations. Dan Kaminsky recognizes back in 2009 – I can't take credit for this, though people in the IETF are now working on this very heavily – but Dan demoed this back in 2009 out of Defcon.

He did a real hack – basically a [hackage] that gamers use to cheat games so that they win; basically intercepting DLL calls and stuff. Not really a product, okay? But I haven't seen anything happen since 2009. With my Microsoft hat – I've even attempted to try to fund some efforts to say… We've got enough UNIX geeks here. I want a Windows program. I want something that runs natively on Windows, that fits their model, that hopefully they'd find pretty enough that at some point they'd say, "We'll just make it part of Windows." Bingo! We win. DNSSEC would be everywhere then.

So secure global distribution of SMIME certs has always sounded like the killer app for DNSSEC. It's one of the biggest problems out there. We're seeing a lot of traction in what Wes was talking about between servers, and I think that's wonderful – that's really wonderful. But as far as being able to give true end-to-end encryption of email, where the only way someone was going to get your email was going to be a court order on your laptop, why hasn't anyone done this, done a Windows version?

I've talked about this. We don't like Microsoft. Maybe they don't like me now, but it's an unfamiliar world to us. We've all grown, cut our teeth in the Linux community, in the Linux world. Not many of us – I'm not going to say all, I know there are people that know this stuff; crypto API, outlet plugins, completion port IO – turns out Windows is actually a very fast operating system. It was written by somebody that used to be in the [deck 00:46:58] world, and is patterned somewhat on VMS, if any of you guys are old enough.

That was a wicked, fast transaction and processing system. So if you can get at the base of Windows, you actually have a good platform to develop on. A lot of projects we do are great, on the open source, and they're wonderful. Some of them have a lot of support. But whatever the product is, it's got to be something that's supported. I believe, in order to get DNSSEC widely deployed, there needs to be something there that people can just click, install, and there's support.

With support comes cost. This would not be a free thing. You can guess where I'm heading with this. I want a for-profit company to see this as a killer app and actually spend some time on it. Maybe the problem is there's no motivation. There's one large organization I know in the US. They all have little tags when they walk around Washington D.C., and some of them have maybe little insigne on their lapels.

At least three million users have this and are forced to use SMIME. I have not worked in the military, but I've worked in Washington D.C. before and been part of one of these agencies – and this is many years ago – we were all taught to use SMIME and use this, and we have credentials, we have… Everything is there. But we still can't easily exchange encrypted email or secured email from others, because how do you distribute the certificates?

I'm going to start the demo here. We all know there are a couple of drafts in the IETF. One is exactly on this, SMIME A. It's done by Paul Hoffman and Jakob Schlyter, and it's still in draft state, I think. Us geeks all recognize that this is something we want to do. I'm going to run through a demo here. I have two machines here. I have one Windows machine here. I have another Windows machine here, both running VMs under Linux. You can see what's up there. I'm going to first create an email account and set it up in Outlook.

This is all ugly stuff. I have other businesses and companies that do this sort of thing. I have something that generates an email account. I'm doing this because I'm proving to you that this isn't a rigged demo. Let's create an email account bosh@dnssec.info… fubar2… Let's create that. There we go. Account information comes back, account's been created. I've even created a link to a

PKCS12 package with certificates and everything else. That was the first step. Now set it up in Outlook. That's easy.

I know you guys hate Outlook. I'm going to do manual setup. I need to do this because I need to get a certificate from startssl or something like that. My name is Bosh. Bosh@dnssec.info. IMAP, incoming servers are going to be mail.dnssec.org – that was all on the other page. Other one was outgoing, mail.dnssec.org. Okay. Password is barfu2. I want to encrypt my outgoing stuff. SSL, TLS, 8587 I think is that port number. Hopefully I've typed all that right. Let's see if I can create an email account.

Was it fubar2? Let's try that. Yes, start over. If this gets too weird I'll just go to the movie demo. I have a shortcut version of this. Let's create another email account. Bosh2@dnssec.info. Barfu2. Create. There. Let's kick off Outlook. Let's create another account. Bosh2@dnssec.info…. IMAP…. Mail.dnssec.org… Okay. Password is barfu2. Settings, outgoing encrypted. TLS 587. Cross my fingers. It's testing. Check. Now it's testing to see if it can send. Finished. It worked. Now I have an account there, at bosh2.

I got an account. I've got to now get an SSL certificate for that account. Fine. Go to startssl. Everyone knows these guys will give you free certificates. There you go. Pick one. Everyone's heard of startssl, right? SMIME or for a server. Email address validation. I'm playing ball here. I'm not doing stupid certificate tricks. I'm trusting the CA system here. Bosh2@dnssec.info. Fine. It's going to send me an email. That's why I created the email account first.

Again, to me, if this demo finishes, the goal here s to show that with a very simple, small piece of software that translates between LDAP and DNSSEC, not the other way around – we talk often about trying to put various pieces of data in the DNS and secure it with DNSSEC – this is the reverse, because my interest is in trying to get adoption as quickly as possible. I'm looking for inroads, back doors, connections, whatever, interfaces, APIs, into the large-scale applications like this. I've got my key back in email. I'll paste that there. Fine.

Now I'm going to ask for an SMIME certificate. I know this is excruciatingly boring, but I just want to prove to you I'm not doing anything tricky here. I generate a private key. This is the longest step in the process. There is some work being done in the open source side of this, by Verisign, and my dear friend [Eric Ostarwile 00:57:45] has done an awful lot of work in this are. The barrier I see is that we need to get this out of the experimental stage and into the stage where it's attractive, maybe to some end users.

It's generated a key. I've got the certificate now. Now I need to upload the certificate into my DNS, and my DNSSEC server. I'm going to view the certificate they've given me. If you look at the subject line in here it does say bosh2@dnssec.info. I want to copy this certificate to a file. This is all Windows 10. Export the key, make it look like a [PEM], [base 64] encoded. Fine. I'm going to stick it somewhere. Drive:E/com/documents/certs. Okay. Call it bosh2. Export was successful. Cool.

Now I have a certificate. I want to upload the certificate into my DNS servers for DNSSEC.info. It's controlled with your password. Let's find the file. Bosh2. Open. Fingers crossed. It returns back the SMIME record. I don't think there's an IANA type assigned to it yet, so I'm just using type 53. We're getting there. We've gotten through the most difficult part. I've installed the certificate. When startssl provided the certificate back to me, that installed the certificate into Windows, and therefore Outlook has picked it up.

I have generated this SMIME A DNSSEC record, and it's already been published in the DNSSEC. We need to go to some machine that's outside of this home realm, that has no idea, it's not connected with this at all. Let's go to machine B. Voila. This is my ICANN machine here. We have a strange VPN. I'm going to go out of the VPN, connect back to the VPN. All I'm going to do is try to send the email across, and you'll see it fail. Let's try to send a new email, options encrypt.

I want the email encrypted. I'm an evil guy, hiding from the law. Bosh2@dnssec.info. Test – can you read this… Okay. I'm giving Outlook the benefit of the doubt here. Outlook will sometimes underline the email address once it knows something about it, or if it's able to determine something from its address book. I'll try to send it. Many of you have probably seen this message before. It basically says the underlying certificates don't have any information on this guy.

Do you want to send it unencrypted? No. Here comes the piece that solves all this. I was desperately trying to find someone else to do this, couldn't find anyone to do it, found a friend of mine who is a Windows jock, and I got him to write a full LDAP to DANE converter, full ASN1, DER1, all the ugly crap going on both sides. It's stuff I do too, so I know how to do this stuff. He wrote it multi-threaded, multi-processor, all that stuff. Anyway, I don't care. I'm just an idiot, I just want to send my emails. I click here to download this one little .exe file – lvdt.exe.

Of course, there's a little message down there that says, "Why would you want to do that? It's an executable file." I don't care. There's a [unclear 01:03:16] there as well. Now I'm going to make it really angry. I just want to execute it. "Are you sure?" Yes. This is how most people work. We don't care. It says it's executing. It's down here in the lower-right-hand corner. It's running. Now I'm going to do the magic that has to be done in Outlook. Account settings. This is the magic. The magic is that piece of code that's converting things. I'm going to simply add another address book. The address book is this program that's running on the machine, therefore it is secure.

It has its own validator, written from scratch, that walks up and down the chain to validate, but it's happening on the machine locally. That's the thing to notice here. Finish. Close. It said restart, so I'll close that, restart it. Restarted. Now let's try the same thing. Now that this magical address book is in there. I want to send an encrypted email to bosh2@dnssec.info. Test – can you read this… Okay. I'm going to give it a second to see if it knows anything. I'm going to click send. There, the demo failed. That was going to be the end of the demo…

All right. That's embarrassing, because that was the whole point of this thing. But I'm going to explain to you that, if executed properly, what this does, this little piece here, what it does is it runs as a little background process and converts these LDAP requests in a DNSSEC, and it's an opportunity to convert many other things from LDAP to DANE and to DNSSEC, and to pull things out of there, and by doing that, it's bootstrapping the adoption of DNSSEC. So I will fix this at some point, and you'll see the demo work.

DAN YORK: I want to thank you for doing a live demo in front of all of us here, because that always takes guts to do that. So thank you Rick for doing that.

RUSS MUNDY: Here, here. Thanks for the liveness.

DAN YORK: I do agree with you too that within a lot of the corporate enterprise space, SMIME, this kind of mechanism is highly used, so it's extremely important. The work that you're doing, that the VerisignLabs and the others, it's all good stuff to have in here. We have a limited amount of time left, so I'm going to have to say if you've got questions for Rick, find him after this.

I want to turn it over to Paul Wouters, who is not going to talk about Windows, or if he did, we'd be extremely surprised. You should sometimes, Paul, just to blow our minds. Paul works for RedHat, so that's why I'm saying that.

PAUL WOUTERS: We [unclear 01:06:35] really nicely with Windows.

DAN YORK: Paul is going to come here, and I actually don't know what he's going to talk about, because I just have a thing that says "DNSSEC/DANE" demos. So far we've been told he's going to tell us about TLSA records, and PGP and some other stuff. Here you are Paul. Rock and roll.

PAUL WOUTERS: Actually, I will not talk about TLSA records. I was going to talk about OPENPGPKEY records, and SSHFP records. Here is a very advanced UNIX email client called Alpine. It works in 10x5 or however small this screen is. I asked Dan York to send me an email. This is demo@ [unclear 01:08:00] and he said his signature and deploy DNSSEC. This email came in completely plain text. I asked them to do this because otherwise he'd get gray-listed if I asked him in five minutes to send another email.

Now we want to make all this automatically encrypted. The first thing I have to do is generate a key, which, since it's GPG of course, I forgot to… We'll generate a key. I'll take a small key – demouser… Passphrase… fubar2… Generating key. Not enough random bytes, okay. A trick for advanced users. If you ever want entropy on a machine that doesn't have it… There are also demons, that's right, but I just want to find end/user, and it seems to work very well.

I'm failing faster than Rick did! There we go. We have a key. Gpg/listkey/demo. There we go. There should be a fingerprint somewhere, off screen probably. "--fingerprint". There you go, there is a fingerprint on the screen, so now we're ready to push this key. I wrote a little package called hash-slinger that has a few tools in there, and one fo the tools is called PGPKEY, very originally. I can say "—create", demo@ [unclear].ca. If you can see it there, you can see a little bit that says a hash and then ._openpgpkey.[unclear].nohat.ca. Now the tricky bit. I am going to select it and hope it all works, because I can't see half of it.

Then I will move to my zone file. [buff a] is a separate zone, so it's all on here. Paste. There we go. I'm using OpenDNSSEC so I'm now signing my zone. Just in case, reload it. Now my zones are propagating this new data. The OPENPGPKEY is going to spread to my other name servers. Now we go back to my client here, and I will start my email client again. I will delete Dan's old message, and now we're going back to the mail server.

Here you can already see, on my mail server I have a tool running called OPENPGPKEY [milter 01:12:47]. It's a little bit of Python that plugs into the mail server. You can see that someone else tried to mail, and it gave the message there, "Multi part message type passed unmodified." I'm not handling all MIME types yet. I'm asking them to send me another email. You don't need any PGPKEYs. Dan's going to send an email.

It's going to go plain-test to the MX server, because he doesn't support any of this yet, but he will next time we're at the next ICANN Meeting. Once the email arrives at the MX server, which is not the end machine, it will accept the email and we will see on this screen that it will detect that there's a PGPKEY and automatically encrypt it and send the mail forward to the end machine, and then we'll see an encrypted email. This will all happen really fast and automatic. If not, I have a shortcut.

I'm also going to send an email from the server itself. Just in case the DNS record didn't work, I'm going to send it to another email address. Now you'll see it says there "received DNSSEC secured OPENPGPKEY". It found the PGPKEY for paul@[unclear].nohat.ca. You can see the fingerprint there. It sent an encrypted message to me. This is how you can very easily support email encryption. Let's see if meanwhile I'll put on the…

Here's an email from Dan. It's suspiciously plain text. There's another email here, which also seems suspiciously plain text. Again, Rick, this is how it really works in demos. I will not go to my own personal email folder, because I don't trust everyone, but you can trust me that this line meant that it encrypted this message. So to summarize, the GnuPG now have native support for generating these records.

Even though I use my tool OPENPGPKEY Command, native support is added to GnuPG, and the next version will have it. If you download the GIT version it will already have native support for it. OPENPGPKEY Command encrypts this automatically. Ideally, you'd run this on your machine that you're sending your email from, so then it never actually goes onto the network in plain text. I'll quickly switch to the other part of the demo that I was going to do.

The other thing is everybody uses SSH into remote servers to do administration. Even though SSH is encrypted, if you connect to many servers you don't always know what key that server has, or if the key changes because somebody else maintains the server, how do you know you're still connecting to the right server? I'll try to make this a little smaller. You can see here there's the SSHFP records in my zone.

They're a little unreadable, but note that the bottom one, rogue.nohat.ca has a fingerprint of all zeros, so that's a pretty bogus fingerprint that I put in for testing. The other ones are real. If you now connect to the server, you'll see no message, because I will kill all the… This is the file where it remembers all the previous answers you've given. I've wiped this entire file, so this account knows no SSH keys any more. If I do an SSH again… My default, this is not enabled. This is a four-year battle of me trying to enable this lookup by default.

I cannot get the SSH maintainer in [unclear 01:17:25] to enable this before [upstream] does. If anyone has experience in getting this verified host key DNS option set in [upstream] [unclear] open SSH, it would be really nice.

SPEAKER: Paul? I have a six-year-old ticket on that very topic. They won't do it.

PAUL WOUTERS: That's great. If you give me the ticket number, that would be really useful for me to override [upstream]. Surprisingly, I see it's enabled on this machine. The next check is to see if I'm using a secure resolver. Something happened. Yes, that's pretty secure. I'll jump out of this machine just to do this on another machine. That's better. Interesting. Let's see what happened here. Wow. I guess we open another ticket there.

What happened here is [I SSH 01:18:30], it tells me, "Warning, remote host key has changed," in a big banner. Somebody could be eavesdropping on your connection right now. Then it says, "Or maybe someone just changed the host key like the administrator." It gives me the fingerprint of the ECDSA key, then tells me nothing. There it is. Update the SSHFPRR in DNS. This was a mismatch of the SSHFP record, so it should have not connected, but apparently it connected anyway, because I managed to log in.

That's an interesting bug, and it's not even my software. Now I'm really curious what happens when you go to rogue, because I'm pretty sure when you go to rogue.nohat.ca, it wouldn't let me in. That's better. Now we're getting questioned, except now it doesn't find this record in DNS. This is an even better demo!

RUSS MUNDY: This shows the security aspects working!

PAUL WOUTERS: Not really, because I'm losing my DNSSEC records. Clearly this all worked before. Anyway, there is a slide deck that shows the proper working examples, that have been broadcast during this demo too, so you can grab those from the website and see those working in a little bit better action than I showed here, which of course I made with the exact same laptop two days ago, so I'm a little surprised.

DAN YORK: Thank you Paul for doing a live demo here. Let's give Paul a round of thanks on that one. Any questions for Paul? Go ahead.

MARK [SWEIG]: I don't want to monopolize the microphone. Mark [Sweig], Global Village. We actually discussed using SSHFP records for our network, but discovered that the client support for that is not too great at the moment, so apart from Linux SSH, we couldn't find any, and we have a lot of administrators who are using Windows to connect with the Linux machines. [Putty 01:21:15] doesn't seem to support it. Is there any support on the road for multi-platform support of SSHFP?

PAUL WOUTERS: Not that I'm aware of. I thought [Putty] was going to do something with DNSSEC, but I guess they haven't done that yet.

MARK [SWEIG]: You personally don't know of any developments in that area, or alternative SSH clients for Mac and Windows?

PAUL WOUTERS: No. I don't know that many SSH clients actually. I know OpenSSH and [Putty], which are 99 per cent of the market, and I think there are some FTP clients that support SFTP, but not really SSH. I'm not aware of any other popular clients out there that actually do SSH.

MARK [SWEIG]: Okay, thanks.

PAUL WOUTERS: The one thing I wanted to point out as a known bug in the SSH client was that it actually didn't look at the DNSSEC status, and when you're using an insecure name server it actually also just tells you, "Oh, this SSHFP fingerprint is awesome, you should trust it." So that's three bugs now that we should file.

DAN YORK: All right, well, good that we're getting some bugs filed here. Well, thank you Paul, and Rick, and Wes, and Sara. Please join me in a round of applause for the folks who are here. I'll also point out that if you've got an idea like this, if you want to do something around this, we will be looking soon for proposals for the next session in Marrakech, at the next ICANN Meeting. If you've got an idea, you too could come up here and do that. As Paul noted, he did provide a set of slides that have these on there, and you can go to the main page here for this session on the ICANN website, and we have all of the different presentations that were given today. The slides for them are all there, so if you missed something earlier, if you want to see something that's there, you can go and get the slide decks from there.

We also, on that same page, will have the Adobe meeting room recording of all this. You'll have the audio and slides integrated so you can listen and hear about that, and as you've seen I'm also streaming it through YouTube, so you'll be able to have a recording there as well. Let me get into our last presentation. Rick, you want to say something?

RICK LAMB: Just one thing, because I feel like I screwed that up pretty bad. I'll put a link to a video file, a movie file, for a demo that does work, for those that would care, for some reason.

DAN YORK: Well, Rick, I think it's great that you tried it too. We've had, like this, you get the live demo gods interfering always as far as what happens in that regard. But it's great we keep trying these, we keep doing them. Some of them work, some of them don't, it's all good, and at least it shows we have real running code and pieces like this. I want to reintroduce Cristian, who was talking to us earlier today about what's happening in NL, and he wants to now talk about what we can do to get more ISPs doing validation.

CRISTIAN HESSELMAN: Thank you Dan. My presentation is entitled "Stimulating DNSSEC validation at .nl". It's not only focused on getting ISPs to do some work. As I pointed out this morning, that's difficult. This work was actually done by the three guys that are on that page there, on the slide there, Marco, Jelte and Maarten, and they're in my team. First, a brief introduction. SIDN, the registry for the Netherlands, and SIDN Labs is the R&D team of SIDN.

We currently have 5.6 million domains in our registry, and roughly 2.4 million of those are signed with DNSSEC. We work with around 1,500 registrars, most of which are in the Netherlands, but they're also in the States and also in Germany, for example. In addition to being the registry for .nl, we're also the registry service provider for .amsterdam, which is the Netherland's capital, and we're also the RSP for .aw, which is the country code for Aruba.

As I discussed already this morning, our major challenge at this point is how to get DNSSEC validation going, because signing of course is very important, but the other side of the coin is validation, and without validation, DNSSEC is of no use. What I'm going to talk about here is basically four different initiatives that we took to get this thing going.

The first thing that we did recently was set up DNSSEC resolver servers, which are basically two machines running Unbound that we set up in our infrastructure, thus making DNSSEC validation a service that's being offered by the registry rather than by ISPs.

We did this because we knew that ISPs weren't doing anything themselves, and we didn't want to sit on our hands, so that's why we decided to take the initiative ourselves and set up these two machines. In addition, it will also enable us to get some more experience in running these resolvers, which we haven't really done before. At least, we did it on our own office network before, but not for external clients.

We're currently carrying out a pilot with a high school, which has around 1,000 students in there. Unlike Google Public DNS and Verisign Public DNS, for instance, we opted for a white-listed service, which means it's not an open resolver, but you will need to sign up with SIDN and then we'll give you access to the machines. The reason for doing that is we first ran an open resolver on our lab network, which was spotted as an open resolver within a couple of hours, and it also attracted a lot of abuse traffic, so we decided to take this model instead of the open resolver model.

The second initiative is basically validation on a small device. The working title of that device is ValiBox, as you can see up there. It's a GL.iNET device, which is a very small box that you can hook into your home networks, so this is more for the end users rather than for organizations. The box runs on OpenWrt, the operating system, which we modified the firmware of so that it now acts as a validating resolver.

We configured the device as such so that if you run into a domain name that generates a validation error you get a warning page as a user, and you can either go through – so you can decide to go through to the untrusted page anyway – or you can put in a negative trust anchor, thereby saying to the box not to resolve for this domain name anymore.

We currently have around 20 of these devices configured, and we're handing them out at SIDN to our staff so that they can use them at home. We're hoping that this will take off on a larger scale so that folks will also be able to use it more broadly. The one thing I've forgotten to mention is… You can't really see it, because the version we're doing right now has an antennae on it. It actually uses Wi-Fi, so what you get when you plug this into your home network, it will give you an additional SSID, and you need to then connect to that SSID to make use of the validating resolver.

This is a tool that we also briefly talked about this morning. It's basically to scan the entire .nl zone for validation errors, proactively. About a year and a half ago we developed a tool that would receive validation errors from, say, two or three smaller ISPs that had experimental DNSSEC resolvers in their infrastructure. We would take those validation errors and pass them onto our registrars so that they could fix the error.

What we did a couple of months ago was extent that software so that the validation monitor now scans the entire zone proactively every 24 hours and picks up the validation errors, and sends them as usual through to the registrar. That's something you can see on the figure on the right over there. One other thing that we do is during the previous version of the validation monitor we also learned what typical third-level domains were, and so we're also using those to check validation errors at the third-level.

That's also why we're seeing a sudden spike on this figure on the right. There's a purple line almost all the way on the right, which is when we turned on the DNSSEC validation error, the new one, and as you can see, it resulted in many more validation errors, mostly because of these third-level domains. But fortunately you can already see the line going back down again.

Just to give you an indication of the numbers we're talking about here, all the way on the right, with the new validation monitor turned on, we get around 6,000 validation errors per day, which is around 0.25 per cent of the total number of DNSSEC-signed domains, and previously, before we turned on this new version, it was 205 validation errors, which was 0.01 per cent. The advantage of this system is that it's much more elaborate and it scans the entire zone, enabling registrars to discover validation errors much quicker than previously.

The fourth initiative that we worked on is something that we call the registrar scorecard. This is a broader initiative for a registrar, so that they can get more insight into their domain name portfolio – for instance, in terms of the actual use of the domain names they have registered with us, in terms of data quality, in terms of the level of churn, and that sort of thing, and we provide the registrars with a discount if they perform well here. Part of this registrar scorecard is the number of DNSSEC validation errors.

We previously would give a discount to our registrars whenever they would sign a domain name, but we've now changed that a little and we're now saying if it's signed, that's great, but you only get the discount if it also validates correctly. In addition, we provide the registrar with a couple of statistics on the average number of validation errors, and if that registrar performs below or above that threshold. They can also compare themselves against the other registrars.

This tool makes use of the software, of the validation monitor that I discussed on the previous slide. To sum up, I think that at least what we did in the Netherlands, at .nl, we basically took the lead in trying to stimulate validation ourselves, because we know that ISPs are basically not doing that. We took a multi-track approach. We offered validation functionality – both as a service on the resolver machines, as well as through these tiny iNet devices. We helped to further reduce validation errors through the DNSSEC validation monitor, but also through the registrar scorecard.

We not only go what I call horizontal, trying to convince ISPs to turn on DNSSEC validation, but we also try to target specific application domains, such as for instance in schools, and perhaps even local governments in the future, to also get them to validate DNSSEC signatures. That's what I talked about here. In addition, we spend a lot of effort on things like sponsoring software. We sponsor NLnetLabs for instance, which are the guys behind Unbound.

We sponsored PowerDNS. We previously ran a large-scale pilot with several universities to turn on validation on their networks. We're involved with governments to get DNSSEC signing and validation as part of their procurement procedures, and we basically promote the use of DNSSEC a lot. One initiative that may be interesting is internet.nl, which enables every end user to check if he's using DNSSEC, or if his ISP is using DNSSEC or not, through a webpage.

We're also providing DNSSEC statistics on the site of SIDNLabs, which is stats.sidnlabs.nl. That's the work that we're doing at .nl to get things going, but of course the biggest jump ahead would be that ISPs start to do validation. Please, I encourage you to visit stats.sidnlabs.nl, which contains all kinds of statistics on the .nl zone, including statistics on DNSSEC requests that we process on our name servers.

You can go back 18 months in time, so to speak, because we save all that data on one of our [unclear 01:37:10] platforms. So hopefully that's interesting for you guys to check out. Thank you.

DAN YORK: You also have provided us with very nice little coasters, if anybody wants a coaster that says, "Secure the Internet, do the DNSSEC check." If anyone wants coasters, they're floating around over here. Somebody has done this, and I think Cristian would prefer not to take these back home with him. Questions for Cristian? Comments? Jokes?

ÓLAFUR GUÐMUNDSSON: Cristian, very impressive. Thank you. Have you guys, as you're very polished, thought about suspending domains that state DNSSEC [invalidatable 01:37:56] for a long time?

CRISTIAN HESSELMAN: That's a good point. We haven't done that yet, but we might need to be more strict there, perhaps.

DAN YORK: Other questions? What else are people doing to get people doing validation in their area?

JACQUES LATOUR: One thing we do in Canada is we have an ISP Summit where all the Canadian telcos meet on an annual basis. I've been doing stats from APNIC, and showing the result of Canada doing maybe one per cent validation, and now we're up to nine and ten. One of the main reasons in the recent bump is one large ISP upgraded their recursive name servers, and by default DNSSEC is enabled validation, so that was it. They didn't even know they did DNSSEC until I reported the stats.

CRISTIAN HESSELMAN: I think we've seen that before. We've seen it in the Netherlands with T-Mobile, but at some point they turned it back off. I think we also saw it in Buenos Aires, when I think a person from Chile presented on their work on DNSSEC, and said that one of the largest ISPs in Chile had turned on DNSSEC validation. Perhaps it just takes a smart system administrator and network engineer to get things done.

DAN YORK: Or software vendors who just turn it on by default and don't necessarily make that a highlight of their next announcement.

ERWIN LANSING: I think a year or two ago we tried to get the three largest ISPs together, and two of them said, "We're not even interested in sending anyone to Copenhagen to talk to you," and the third one said, "It's already on our roadmap. We're going to do it in a couple of months." So the largest ISP in Denmark is validating DNSSEC right now. I have no idea about our internal discussions on how that happened, but I do think it was a couple of geeks that got that through.

One thing I would suggest is getting the ISPs to talk to each other; especially having an ISP that does validation talk to the ISPs that do not, and tell them how many more support calls they get. That would be very good, because I think most ISPs are very hesitant to turn on DNSSEC validation when they don't see an incentive of getting more revenue, but do see the fear of getting more support calls, which are expensive.

So having them talk to each other, and for us, making sure that most domains do validate and they don't get support calls, that would be very good.

DAN YORK: How about our Czech friends sitting across the table from me? What have you guys done to get your ISPs validating as much as you have? Or did you all just meet in a bar and decide that this was how to do it?

SPEAKER: Yes basically, and we were cooperating with the national exchange points. They have regular meetings, and on those meetings we were sponsoring some drinks, and while they were drinking we were telling them that DNSSEC is a great thing.

DAN YORK: That's an actually interesting tie-in though to the IXP side of things. You're right, because you do have the ISPs meeting at the IXP, and so that is an interesting way to have some folks there. Good idea. Other comments – what else have people done out there?

ROBERT: I haven't done anything, because I'm not part of the spectrum right now, but I was thinking a registry could do some kind of certification and give a certain level of B+ or B-, A+ whatever, to an ISP, and they can brag about that. I don't know if they would use that for anything, but usually something coming from the Chile administrator might actually carry some weight with the geeks.

CRISTIAN HESSELMAN: In the Netherlands we do have that implicitly through this internet.nl site, where end users can check if their ISP validates or not. But perhaps we need to be more transparent in that way, and also list the ISPs on the site somewhere that do this, or not. A bit more naming and shaming.

ROBERT: Twitter, Facebook.

CRISTIAN HESSELMAN: Yes, that kind of thing!

DAN YORK: Yes. There have been different discussions over time that we should have some kind of name and shame site around encouraging by listing the ISPs that do or don't. Nobody's yet come up and said, "Yes, we're willing to either do that, fund that, maintain that," and whatever else. Because the challenge with any of those sites, such as the list of registrars that support DNSSEC – right, Rick? You and I both have challenges maintaining our separate lists around that.

So it's easy to create that stuff and harder to maintain. Any other comments for Cristian? I really like your different ideas, tracks, that you're doing. I like you provided a DNSSEC validation service right out there, the little appliance things. Then the monitoring service – I think all of those are great ideas. It would be interesting to see what kind of uptake you get on those. When are you putting little boxes out?

CRISTIAN HESSELMAN: Initially we're handing them out to our staff, so that they can try them at home. We recently configured those devices, so we need to simply try them first, and then see if people outside of the company would like them.

DAN YORK: Are they replacing the home Wi-Fi router or whatever that somebody would have?

CRISTIAN HESSELMAN: No, it's in addition to, because it creates an additional SSID, which has the validating resolver on it, because it's a wireless LAN access point, that thing. So in your home you'd need to connect to that particular SSID.

DAN YORK: Interesting. I know you .cz folks have your Turrit project, which is getting CP devices out to people, which do the DNSSEC validation right there. We've had some other good success with DNSmasq now supporting DNSSEC validation, so that will slowly percolate out to the CPE devices to do something around that. Russ, yes?

RUSS MUNDY: One of the things I want to mention is that Comcast, who really went whole-hog into this, the person that really led the charge there was Jason Livingood, and a couple of conversations I've had with him over time, it really, in terms of a major provider – they do signed zones as well as other validation stuff – but essentially, Jason wrapped the DNSSEC part into a larger scale security package.

So if there are ISPs that are focusing on providing a higher level of security than just the generic ISP that people get, they might be a good set of people to approach to say, "Okay, you say you're higher security, here's something else that you ought to look at incorporating as part of your security."

CRISTIAN HESSELMAN: I spoke with Paul in BA and I asked him, "Why are you guys so successful in validating DNSSEC?" His opinion was that the senior management of Comcast was convinced that this was something useful, and they also understood what DNSSEC was about, so that helped a lot.

DAN YORK: Well, yes. Jason Livingood is one of the senior VPs, or…

RUSS MUNDY: He's about three levels up from Paul, and actually, he was the one that sold it. Paul came after it went in. But what Jason has described in the global picture is when he sold it to the people, basically he convinced them, because they were, as a corporation, trying to be the most secure home ISP provider around, and they offered several other security things. So he was able to say, "And you must include DNSSEC as part of it, because it's a critical part of the overall security picture."

JACQUES LATOUR: I guess we need to write some sort of document, DNSSEC for ISP Execs.

DAN YORK: Yes, we need to have that for execs. In fairness, I've talked to Jason too about how he can network in with some of his peers to help do that too. Robert?

ROBERT: Just one last thing. I think there's still some stigma from many years ago when somebody made a presentation that recursive servers would need way more CPU power, way more memory, way more bandwidth to process, to do

DNSSEC validation, and that's not true. We need to dispel that myth somehow.

DAN YORK: Who wants to make that presentation in Marrakech? Anyone want to work on a presentation like that?

RUSS MUNDY: Hopefully we can get the results from Roland's students that will help in that space. Perhaps he'd be able to participate at the next meeting, or following meeting.

DAN YORK: All right, that sounds good, but also maybe I'll throw that out as a topic for the community. If that's one thing we could work on, it would be good to find anybody who could do a little bit of research into what does it take to go and do that. Right, well, thank you Cristian for bringing this to the group here. The final little bit is the Russ and Dan show talking a bit about thanking people and going on from there. Julie is going to bring up our slides.

I would just start by thanking, once again, before we leave, the five sponsors who brought this here – CIRA, Jacques; SIDN, Cristian; I don't know if we have anyone from .se here, but Annemarie is always around, and has been a great person with us here; Afillias, Jim Galvin, if you see him any time tomorrow thank him, because it's through his support and others that we've been able to do this; and DINE. How many of you went to their party last night? A number of folks.

RUSS MUNDY: Also, DINE and Afillias both have booths, so folks can stop by down there and thank them for lunch.

DAN YORK: Yes, thank them for helping provide this lunch. Again, I'll put a plug in. If anybody's interested, it's a very inexpensive sponsorship, but it helps keep us all happier. With the scope of 2016 we've got one spot open. Anyway, let's go on. We want to wrap this up by saying how can you help? One of the things we like to say is that for TLD operators we would encourage you to sign your TLD, accept your DS records, work with the registrars, and also help with statistics.

One of the things we've been trying to do is to gather good statistics around what's the range of validation? Geoff Huston has the APNIC stats that he uses, that we use now to show the overall state of validation, but we're looking for more ways to do it, and we're looking for more mechanisms. So to the degree if anybody can help plug in with this, it would be excellent.

RUSS MUNDY: Just a broad generic – any zone operator, anybody that operates an authoritative server, ought to look at signing your zones, because especially on the zone-signing site, that's really straightforward now. There's lots of tools, lots of automation as part of the whole key change process and update process, and most of the software has it where you just have to watch to make sure there's not a software. So signing zones is something that's a really good, really interesting first step.

A lot of you have taken that first step. That's wonderful. Working with your registrars to generate support. If you're a registry that's signing, that's what we've spent a lot of time talking about today. There's been this challenge in the registrar space, but as registry operators working with your registrars and… Like I mentioned earlier in the interchange, one of the biggest success stories we have was Comcast, and they sold it as a package. So if you have some registrars that are pushing their high security capability, go to them and encourage them to sign it.

Again, work with statistics and use the DNSSEC tools that are out there in your day-to-day work so that you can have real world end user experience in your own environments.

DAN YORK: For network service providers, ISPs, we really encourage, as we've just talked about, encouraging ISPs, if you know if your ISP, to deploy validation – get this out there, get this working on that. If you're not directly with an ISP, we do ask people to go and ask their ISPs, because we have so many network service providers who come to us and say, "Nobody ever asks me for DNSSEC." So raise the support tickets. Send an email in and say, "Will you support DNSSEC validation?"

As Robert said over there, contact them on Twitter. Tweet them and say, "When are you guys going to give us DNSSEC validation?" Those things actually do matter, and start to make sense inside that somebody says, "Hey, maybe we should investigate this." So one big thing you can do to help move that forward is just to raise those kinds of issues. We also ask service providers, ISPs, to look at DANE. We've talked about this here, and encouraging the use of DANE is something that again can be done to help raise the awareness around this.

Websites, we just encourage anyone with a website, sign your zones, sign your domains. In this case, contact your DNS hosting operator, which may or may not be your registrar, and see if they'll do it for you, if they're the ones doing your DNS for you. If you're operating your own DNS, then obviously you can go and do that there. Contact your registrars, because sometimes they don't support it.

We've heard yet from registrars in this meeting and other places, "Yeah, but nobody ever asks me for DNSSEC." So ask for DNSSEC. It will help those registrars and to certain registrar advocates we can say, "Well, somebody has asked for it." So go ahead and do that. Also, ask anybody in your environment, in your network, to get the validation out there.

RUSS MUNDY: One other thing that we probably need to add to this slide, Dan, is instead of just websites, it's also SMTP and email providers, because there's a big and emerging area and a lot of capability, and there may in fact be a number of providers out there that have the capability, especially with Postfix, shipping with it by default, it's not turned on but it's there and it's a very easy configuration to set up, and EMXI I think, also.

DAN YORK: Yes. There are email companies in Germany who are advertising that they support DNSSEC and DANE, which is cool. We should see more of that. Use DNSSEC. Share your lessons learned. Participate in this community and in the Workshops. There are a number of mailing lists that a number of us subscribe to. There are some LinkedIn groups, there are some other different places that a number of us are connected to in some way, and please, you can go and join that. I think on the next page we have some of the links throughout there.

DNSSEC-deployment.org is a site we still have out there, and it's also a site which, if you're interested, we can post content and information to. "We" being myself in this case, as far as the one who's maintaining that. If you've got ideas or things you'd like to write about with regard to DNSSEC, we're always looking to post more information and content. The Deploy360 Program, it's internetsociety.org/deploy360. We have a number of resources out there.

Also, we're looking for people to help write some more resources and things to help explain more; the tutorials and things like "DNSSEC for Executives" and things like that. Part of our mission with Deploy360 is to help make this easier to understand. We're looking to do that. If anybody would like to contribute some time and write some of those types of documents, or if you've written one that's really good, that you think we should help spread the word about, we're always glad to do that and help spread the word and do that.

Finally, DNSSEC-tools.org, which you heard Wes talk about earlier when he was here, and Russ is involved with that as well, has a set of software that's always there and growing in terms of what it's about. I think that is all. Thank you very much for participating.

RUSS MUNDY: One more quick comment. We have a number of people that are maybe first-time attenders here, or haven't been here very often. I think everybody's heard that there's a lot of interchange. There's a great deal of willingness to help throughout this community, so if any of you need help with anything related to DNSSEC, just start finding people asking questions, going to the website, joining mail lists.

There's an extremely high likelihood you're going to get a fairly fast response from some of the most knowledgeable people in the field, because the folks involved in this are very passionate about making it happen, and are willing to help pretty much anybody get going. So thanks for joining us, and please continue to work this way and ask questions if you have them.

DAN YORK: If you're from the Ecuador ccTLD, Roy Arunds really wants to talk to you. He wants that DNSSEC.ec to be signed. With that I want to say thank you to Julie and Kathy again for all of their work to make this happen. The Program Committee could not do it without these two over there, who keep us going, and all of that. So thank you Julie and Kathy.

JULIE HEDLUND: Thanks everyone. I just want to say too, I think we equally need to thank Dan and Russ, who also keep this thing running really well.

DAN YORK: Thank you Julie. With that, we'll see you all in Marrakech. Thank you.

[END OF TRANSCRIPTION]