SINGAPORE – DNSSEC Workshop
Wednesday, March 26th 2014 – 08:30 to 14:45
ICANN – Singapore, Singapore

JULIE HEDLUND: Good morning everyone, and hello to everyone remotely. We're going to start the DNSSEC Workshop very soon, probably in about five minutes. People who are in the room, feel free to take seats up on either side of the table. We'd be happy to have you interact with us. We'll start in a few minutes. Thank you.

DAN YORK: Good morning everyone. We're going to get started right about now. For those who are coming into the room, please do feel free to come in and join us at the table. I know it's quite early in the morning for many people who are in here. I want to thank you all for joining us, those who are in the room and those who are remote. I know that typically we wind up having more folks walking in as the day goes on. Good morning Jacques. Hello.

My name is Dan York and we're going to get started with the Workshop that we have. For those who are following along remotely, the slides are also available from the program page that we have. This is being recorded, so we are asking people who have questions to please come to a microphone and raise those questions. We also are going to be… This will be on the Adobe Connect room, YouTube and other places. Do realize that what you're saying is being preserved for posterity or something along those lines.

We are at the DNSSEC Workshop at the 49th Meeting of the ICANN organization on March 26th 2014. If you look at the slide you'll see one important piece to notice, which is that these are the sponsors that have brought this event to you. The major part of what they do is to help pay for lunch, among other things. For those of you who enjoy this session and enjoy having some food as we work through all this, we need to thank the sponsors that are here.

In particular, we have one new sponsor that some of you will not have noticed before and that is in that lower left corner there that is Microsoft. We have here Mehmet Axon who is not here yet but I know he will be here doing the day. He has recently joined Microsoft, about six months ago, coming from ICANN and has all ready done a good bit of work with helping position Microsoft. To get Microsoft a little more involved in the DNS and DNSSEC community.

He's sponsoring this event. He's sponsoring a couple of other events that are going on as well and looking to get much more involved and we're going to talk about that in a minute.

Good morning, Warren. Come on in. Have a seat.

First I want to just thank the program committee whose names are showing up on the board here. These are the folks who work on helping create these programs, these workshops that are here. They are the ones who are out there encouraging people to submit presentations. We're going through reviewing the presentations, putting all that together and making that work and helping create this program.

All of these people, if you see them around and there are several in the room here today, please thank them for the work they've put in to make this happen.

Tonight we have what's called the DNSSEC Implementers Gathering and that's going to be an evening here at the Hog's Breath Restaurant. If you have not RSVP'd we may still have a few places. See Julie if you are interested just to make sure we have a count for you. This is a time for informal social gathering where we can talk about DNSSEC and other topics but it's more a chance for people to meet and interact.

We do have a few people like Ernesto from the .mx Mexico domain sent us a note just the other day that he's looking forward to coming because they're looking to get DNSSEC going further along in .mx looking to talk with others who are doing that to see what we can do.

This is the kind of sharing that we typically would have. Again, it is being sponsored by Afilias, CIRA, Dyn, Microsoft, .se and SIDN. We thank all of those folks for paying for that.

The program today, I am going to be speaking first with some introductory remarks then Xioadong Lee is going to be talking about DNSSEC activities in Asia Pacific region. We've got a number of panelists who are a part of that. We have a presentation in a section we call the operational realities of running DNSSEC but it's actually a case study today from the folks in Estonia who implemented DNSSEC recently for .ee. They're going to be here talking about that.

After our break we're then going to have a panel discussion where Michele Neylon, myself and Jim Galvin and Joe Abley will be up here

talking about the DNSSEC requirements of the 2013 Registrar Accreditation Agreement and how that plays in with what Registrars have as a responsibility for DNSSEC and pieces like that.

I expect we should have a good discussion around that with a couple of different opinions around there. Then we're going to have a piece on Root Key Rollover where we have two presentations. Ron Aitchison is going to talk a little bit about the last mile or last millimeter, last little bit of there and Russ Mundy is going to give a perspective from the SSAC, the Security Stability Advisory Committee around the preparations for Root Key Rollover.

Then we're going to have a presentation from Cristian Hesselman at SIDN about the DNSSEC validation monitor tool that they're working on. At lunch, Warren Kumari who was just here a moment ago. He stepped out. He will be back because he's doing the great DNS quiz and his computer's there so we can steal that. Warren will be here to do the great DNS quiz and if you've never been here for that, it's always a treat of the most esoteric DNS knowledge you could possibly every imagine. Some people actually get most of them right.

After lunch which will be provided to you. You should all have a lunch ticket that is somewhere here and this is your ticket that gets you into the lunch. Julie has very nicely put on the back this very nice little map showing us where we are going because we have to go across the atriums over to this lunch area called Bencoolen to be able to go and do that.

After lunch we're then going to have a presentation where we'll be talking a bit about Dane and DNSSEC applications and some pieces that

are there. At the end we have a little demonstration from Duane Wessels at VeriSign. He's going to demonstrate a couple of the DANE related tools and things that they've been working on in VeriSign labs.

At the end Russ and I will come back up to talk about how we can help and how we can move forward. With that, I want to move a little bit into some of the counts we have about DNSSEC deployment around the world. Many of you who have attended these events in the past know that this is usually a presentation that Steve Crocker has done. Steve was planning to do that until about two days ago when he realized he had some other commitment as the Chair of ICANN that was going to preclude him from being here.

He sends his regrets. He wanted to be here. He enjoys coming here for these events and sessions and has been for as long as they've been around. This is probably the first one he has not been speaking at. We will miss his presence here and appreciate all his help in supporting these sessions and bringing them together. I should note, too, that Steve's group is the one that has been doing much with getting the sponsors together and making this all happen so we really owe a debt to him around that.

To look at our maps and these are ones that are projected forward slightly to April 1 because of a reason that you will see when I walk through the maps. In the mapping project that started originally at Steve Crocker's organization Shinkuro and that now in the last few months has been taken over by the group I work with at the internet society at the Deploy 360 program.

What we do is we track the DNSSEC implementation status of the TLDs that are out there with a focus in these maps on the ccTLDs. We are also entering all the new gTLDs into the database which allows me to have a good deal of fun as I read all of these as they come out and get delegated. We're putting all those in there with the intent that we'll then do some kind of visualization of them.

We have five states that we track. One is experimental where we know that the ccTLD or the TLD in general is experimenting. I'll give you an example of one of these. We just recently learned that Rwanda is doing some experimental work with it for the .rw domain. They hosted a series of DNSSEC workshops recently and are working down the path toward doing that. When we look at the maps you'll see them classified in the experimental.

Announced is when we've learned of a public commitment to deploy DNSSEC. For instance, just this morning…It doesn't show up on the maps because these slides were done a few days ago but we learned that these folks at auDA in Australia have announced publicly that they are going to be signing a domain with DNSSEC so they are in that kind of space on that.

On the partial, the zone has been signed but it's not yet published in the root but we know that is has been done. DS en route is obviously when it's been delegated and we know that from a very obvious way of being able to work with that. On the operational side is a final state when we know that they are accepting domains that are registered, it's all fully operational and working on that.

Here's the counts that we have. You'll note that these are much bigger and projected as of April 1 I should say on this. You'll notice these are much bigger totals than we typically have had on here largely because we have a 100 plus or 100 more of the new gTLDs that have come on which are all publishing their DS en route so we have a very high number in the charts that are there.

This is all for the TLDs that are all either with their DS en route or we note them as operational. The regional ones as it notes here are SU and EU which are ones that are not a single country but are ones that operate as ccTLDs. Looking at the maps you can see we're getting a whole lot of green on here which is a beautiful thing to have. This is where we're seeing throughout the entire area the operational or the DS en route is going through a lot of the world.

As we look at this we'll zoom in on a couple of the areas. This is another map that we have that shows another view of it. It's flattened you'll be able to actually read the ccTLDs that are in the various states that are out there. In Africa, a couple of changes since the last time that we were here, down in the eastern part of Africa we have Kenya has recently published their DS en route that's there and as I mentioned, Rwanda has been set to experimental as well.

You'll also notice in North America, North America has been where it is for a while. It is operational in those regards. In Latin America one of the other changes we've had recently was Peru updated their DS en route in January and so we're moving along with deployment in there.

In Asia Pacific, this is what the view looks like. Australia has announced all ready that was there. The other one, if you look over to the left if you

picture in your mind that you're zooming in on the Middle East, one of the things that we know is that Israel with the .il domain as of April 1 is planning that they will have signed the .il and they will be in the process of moving toward getting it out there. There'll be in the partial state that's there.

Here's a view of Europe. Again, mostly operational as we see through much of Europe, at least through the main parts there. Not so much as we move down to the middle area there. One change that we'll see in here as well is Estonia. They are now published in there as well. If you want to see these maps they are now being made available every Monday morning. There's a link on these slides to where you can go and see the current maps.

There's also a link on this page on the Deploy 360 program where you can subscribe and receive the e-mail every Monday morning of what the latest status is. It comes out with a set of maps which are both the current deployment, the view as of a year ago, the projected view a year in the future. It also comes with a number of CSV files that are dumps out of the database of all the different gTLDs including all the new gTLDs and other generic TLDs as well and their status.

If any of you would like any of that in the data, please do that. We are now as the mapping project has moved over to our group within the internet society, we're looking to do more with that and anyone who's interested, I would like to talk to you a bit more. We'd like to figure out how to visualize the new gTLDs and the generic TLDs so we can see a nice way. They're not actually mapped but some kind of graphic that would visualize what they could look like. Feedback is welcome on that.

Final note before we begin our first panel, we recently saw two interesting documents that were published that I wanted to bring to people's attention. One was a document that came out of .se with a number of partners who published a document around recommendations for DNSSEC deployment. Where this came out of was some work they did with some municipalities in Sweden and that region that were looking at writing down the precise requirements and recommendations that municipalities had to go through to get DNSSEC up and running in that region. It was a really solid set of recommendations.

Patrick, would you like to speak to this? Patrick Fälstrom.

PATRICK FÄLSTROM: First of all let me say that I think this document is absolutely excellent. I was not part of the creation of it but I've been using it myself as a Registrar and working with a couple of citizens. What is important to remember, though, is the way the document is written it needs potentially some profiling. People should beware that you cannot just copy and paste this document last minute before you send in and add it to an RFP. You need to go through the document and see what parts of this you actually need. I think that's the strength of the document. When you see if don't be surprised. It is really, really good so please use it.

DAN YORK: Yes, it's a good list of recommendations, requirements, pieces you can use within an RFP if you wanted to specify that or as a checklist for deployment. To Patrick's point, it is exactly that. It is a list of

recommendations. It's not a tutorial. Here's the things you need to be thinking about. Here's the pieces you need to put together in order to make this all work. That's an excellent document that was just published recently.

The second document that I'll mention is one about DNSSEC in Windows Server 2012. is Mehmet here? No, okay. This is a document Microsoft came out with that really is a very solid document for people who are network administrators who are working with Windows server 2012. It walks through the planning that you need to do with regard to DNSSEC and Windows. It talks about the different steps.

It has series of very detailed checklist of what you need to go through. For people who are working in particularly enterprising environments are looking to use DNSSEC, this is great guidance for people in those spaces who are using Windows server either for their DNS capabilities on the authoritative signing side or on the validation side. It covers both. This is another new document that recently came out and we're very pleased to see that.

With that I will just pause to say are there any initial questions before we begin the rest of today? Is there anything that people would like to raise or additional points that we go on from here?

JULIE HEDLUND: It looks like someone might be in the chat room. David White is noting that the link that was on the previous slide isn't working.

DAN YORK: The link may not work on there. I copied it from where it did work so I will check it out and David, if it does not work I will put another link in the chat room when I get back to my seat. We'll see about that.

I should note again that we do have people in the Adobe Connect room. If you do have questions, please come to a microphone because we do have remote attendees who are listening. Yes, Ron.

RON AITCHISON: You brought up a point on one of the slides which was as I understand it all the new domains have to be DNSSEC they have to publish in the root. Do they have to be operational?

DAN YORK: The question was, "Do the new gTLDs have to be operational?" and the answer is yes. They have to be signed and they have to accept DS records or DNS key records from registrars. We'll talk a little bit later about the registrars and their responsibilities in the panel we have this afternoon.

They are, in theory, supposed to be signed and accepting DNSSEC secured DNS records.

XIAODONG LEE: I thought the map for the deployment for DNSSEC. Is it possible to have a map for the registrars or certain level DN servers and how they support DNSSEC or not. I think this is very important. I assume that all of the TLDs will be deployed at the DNSSEC sooner or later.

DAN YORK: Xiaodong you raise an excellent question. Right now the maps that we're showing and the pieces are just at the TLD level. They show nothing underneath about how much actual deployment is happening in there. That is a visualization of something I'd love to see us figure out a good way to do. One of the challenges we have is how do you get the data in different – out of how many domains are signed at the second level in different places. Some TLDs like the folks in .se and .nl and others, they publish those counts.

The folks at Verasign do it for .com, .net, .edu has it. Some of those are there but there are different domains that do it. Getting information for the individual other ones is a challenge but certainly I think that's the next evolution of where we need to go with this. To show the next level of how much actual activity is happening inside those TLDs. I agree with you.

XIAODONG LEE: I think maybe [inaudible 0:43:13.7] with the gallery so I can have some kind of joint project to do some investigation.

DAN YORK: Excellent, we'd love to work with you on that.

[ED]: One other thing I'd point out too is what those maps don't really show is the IDN ccTLDs being signed or not signed. Same problem – how do you overlap that but it would be good to show.

DAN YORK: That's a really good idea. The point was some of these ccTLDs have IDN variance around there although in some cases there's multiple IDN variance for the same country. I would love to be able to visualize some kind of big grid that shows all the new gTLDs but you could do with IDNs, too and show what are out there as far as the IDNs, which of them are in which states.

Another piece that I want to work on with the new gTLDs especially, we know when the DS is en route. That's easy to find. There are a couple of different sites that are showing that. What I don't know is when we start to see delegations of signed names in those new gTLDs because that's the signal for me to flip the state DS en route to operational.

I know [Oliver Goodmanson] was mentioning that he's got a script he was working to be able to do that but anybody else who has ideas around that. Once upon a time when this database was being maintained it was easy because a lot of people knew each other so you'd contact Nick and say, "Hey, when are you going to do this?" but now as we're adding 10 or more domains a week, we'll go from there. With that I want to wrap up and I want to pass it over to Xiaodong and bring up the panel.

JULIE HEDLUND: I also want to let people know that we do have simultaneous interpretation and that is what these are for. Please avail yourself of that. It will be Chinese/English, English/Chinese and we're very thankful that we can have that. If you're in this panel please step forward. I see most people. I don't see Tran Canh Toan, are you here? Hopefully he'll be joining us.

I want to note also for the program, Geoff Houston is joining us remotely via Skype. He is here. He's just not here physically. He will be giving his presentation remotely. Thank you.

BARRY BRAILEY: It's an honor and a pleasure to be here and talk about DNSSEC and .nz. I'm conscious that quite a few of my colleagues have spoken about progress so I'll skip through some of the background around implementation but try not to spend too much time on it because it's been presented here before. Then I'll talk more about some of the progress last year and where we are with our DNSSEC implementation and deployment going forward.

As many are aware, the DNS for .nz started quite a few years ago. The policy proposal work was finalized around 2010. The implementation was a rolling activity from 2011. Doing each of the second levels zones through 2012 and the New Zealand Registry Service is completely that piece of work toward the end of 2012. All of the information for that is available on that [inaudible 0:47:33.1] website link.

The DNS practice statement is published and if there's anything about the implementation that you'd like to know that you can't find there, you'll see my e-mail address at the end. We're quite happy to share most of that information. The policy piece is something I would touch on. Obviously I work in the domain name commission so we're the regulators. I'm going to focus more on the policy piece than the technical implementation at this point I suppose.

In the early stages and still at the moment we were keen DNSSEC would be voluntary for registrants and registrars. We identified two different roles and it talks to the piece about registrars that was just covered. We identified currently two different statuses for DNSSEC registrars and that is that they either handle DS records or they're DNSSEC friendly.

The DNSSEC friendly registrar guys where it's almost tick box potentially on their website. They have to publish a bit more information about what they do. We publish all of this on our website and we have a commitment to keep that information published on the website. If there was an agreement on how we would categorize that and publish the information then we'd change how we do it probably but that was our decision early on.

The other thing as well, we wanted it to be about registrant choice which was something keen on for .nz and so before we could go live. We were keen that there was an actual transfer policy for signed names because we saw that as a missing piece. Obviously we can only put this policy onto .nz authorized registrars that are also the DNS operator so we set that forward. We'd like to see more practice of it because it hasn't really happened natively with actual registrants wanting to choose.

It's a largely untested procedure and I've all ready been asked if we can provide best practice guidelines how to do that. I had to go back and say there hasn't been enough practice to write best practice about it yet I'm afraid. We've got that out there. It's publicly available in our policies.

That was the work to get us to the end of 2012 and I like to include either a quote from a famous dead general or a movie. I went for a

rather second rate baseball movie, we're at that "If you build it, they will come," phase. Of course the reality of DNSSEC I suppose to this day is that a few will – in fact one of them is here. One of our biggest early registrants was Joe, nearly half of our signed domains at the start of 2000.

We started in 2013. We had two of our local .nz registrars that were really quick out of the blocks to get DNSSEC friendly status. One of them is quite public. I'll flash their name. It's quite literally the tick box on the signing up for the name for I want DNSSEC and they handle everything for you. That was a really promising start. We've got just over 80 registrars and the rest of them weren't quite so forthcoming it has to be said but a good early start, roughly 30 signed domains in .nz at the start of last year – about 12 of them being Joe's.

At the time we had about 520,000 domain names. That's a pretty small percentage. We have seen 200% growth in 2013 but of course if you put the other scale in there that's actual numbers up the side. Towards the end of last year we broke the 100 mark early this year.

In doing our zone scans we've identified currently and growing another 70 domains where we can see the DNS key but the DS record is not in. Some of them are actually with registrars who handle DS records. That's caused a series of discussions with our registrars. A couple of them are with registrars who don't. In fact there's a significant chunk with one registrar who hasn't said that they handle DS records so that's an ongoing discussion which will hopefully will see spikes in the uptake of that graph as we get those people who are clearly trying to do DNSSEC t for whatever reason the relationship with their registrar is not working.

I like to advertise our registrars so the registrar honor roll. The two DNSSEC friendly at the top there, Metaname and Godzone, the other three registrars at the bottom are the ones that have acknowledged to us that they do handle DS records and we mail them on a frequent basis to check where they are at with this. I also monitor any of the other sites, the VeriSign site, if I see one of our registrars appear there it's a cue to follow up with them. If there was a centralized way of tracking them for the registrars, that would make life easier. To keep that up to date and to be able to pass that information on to our registrants.

I reviewed our situation about 12 months ago. Obviously the sources of information for DNSSEC are plentiful when you're thinking about how to promote it in your space. Particularly useful was the [inaudible 0:52:37.3] data illustrates some of the issues where some of the really successful TLDs with the amount of signed names actually have some rather low figures when it comes to their ISPs doing DNSSEC validation.

I was conscious that I want to get the chains of trust out there and actually used or in a position where they could be used. The Deploy 360 tables were also useful when I was talking to our board about the way we should go forward. The obvious thing that dropped out is the ccTLDs that have good growth relied on quite a few things to create the right environment for it.

I sat down with our DNC board and also with the internal group. We identified the obvious things – persuading more registrants to take it up. We're now at the point where we're going out to those significant local websites and online presences .nz presences and having that conversation directly with them. We had one Radio New Zealand was

one success story. They signed their zone. It's not a high online presence but it's a decent one.

There's a little bit of apprehension about doing that because we don't want to upset our registrars by putting them into difficult positions and their customers deciding to move to other registrars because it's a complex set of relationships at the end of the day. Those discussions are happening and at that moment I just want you to go and talk to your registrar about DNSSEC. We keep getting feedback from registrars that there's no registrant demand but they're not talking to their customers about DNSSEC so how do you know if there's registrant demand or not?

We're just trying to generate that kind of discussion at the moment. Our government support and adoption is coming on this year. Thankfully New Zealand government just did a renewal of its DNS services and DNSSEC is very much a part of that. We'll probably do a bit of a communications campaign around that and we'll also see that a significant sites will be signed by default once that comes online someone in the middle part of this year.

We're conscious to keep getting registrars, not just the sheer number of registrars. We also need our bigger registrars to make sure that we've got coverage so that a significant number of registrants could do DNSSEC if they wanted to. I'll touch on DNSSEC validation in a sec is another key area that we realize has to be done.

We haven't started to think about the browser and apps thing. I still want to point people to the cz nick site as the best place to go for browser apps. I'd like to see that adopted further but that's a little bit

outside of our sphere. A lot of time this year as well on improving our knowledge sharing and the COMs message.

That just highlights the stuff in the blue on the right hand side of the screen. It is well within our sphere of influence but we're also doing a bit of time thinking about how we address the stuff on the left hand side of the screen, the slightly outside of the ccTLD zone of influence.

We've got a small internal working group team and we constantly review this. Every change we see if we can capitalize that one in some other way. The DNSSEC for government is going to be useful jump for us. The interesting thing about the Radio NZ one is that they actually moved registrars. They decided they wanted to do DNSSEC. Their current registrar didn't support it so they took their business elsewhere which is a message we're keen to make sure registrars heard before we have the discussion too often.

I also had a bit of luck also this year with engaging the ISPs and the DNSSEC validation. Thanks for the questions on DNSSEC validation for this workshop. I took two of those questions and went to our network operators group meeting back in January and I basically asked the room what it is they needed to turn on validation. Most of them were comfortable with the technical side of it, we can improve some our technical bcop papers for them but they needed a document they could put in front of management that highlighted your customers don't all scream and shout because they can't get to the internet anymore. It's kind of painless.

Our COMs guys interviewing two or three ISPs that have done it quite successfully without major hiccups and we're going to put that out and

share that with the network operating group community as a slightly easier paper that they can put down.

DAN YORK: When you do ask a question as I am doing, please introduce yourself for the record because we are also having the translation going on. That's great. I'm thrilled that you're going to create that paper. As you get it out there, please keep us alerted and we'll blow that all over the place and let people know about it. That's exactly the kind of resources we've seen from other places as a need so thank you.

BARRY BRAILEY: I'm conscious of the time. The more we prolong the approach to create the environment where it can actually grow. It's looking at .se, .nl, .cz. That was a no brainer that we had to spend more time thinking about that. We haven't got dedicated resources to work on DNSSEC. If I was coming at this fresh and had a bit of a checkbook for it I would think about dedicating resources because it is quite a time consuming piece just for the ongoing promotion. It's not the technical aspect. Now this is a program manager and a COMs manager to push that out. If I had a blank slate for it I would think of that.

The other one is that you have to build that demand and persuasion and the sort of arm-twisting that you have to go to. We don't have the learning platform the IPV4 depletion creates around IPV6 discussion and that's hard enough. The thinking through how that's going to work with your local Internet communities is a hard thing. We, at this time, haven't considered financial or policy incentives to force this. That's not to say

that we won't in the future, I don't think we've gone through the robust steps – the likes of .se, .nl and .cz did to create the environment where those sorts of incentives were most effective.

That's where we're at. We're happy to talk about our success stories or get ideas on how to target other bits of this from anyone. My e-mail is there, the manager security policy at MSP@DNC or info@dnc if you're just coming generically. If you've got questions about anything in the slides or you've got thoughts and ideas on things that worked in your area then we're quite happy to exchange that information. Most of what we've done we've borrowed from other people. Thanks to the successful ccTLDs who have done it quite well.

RON AITCHISON: One question, you mentioned earlier on the government. Is there a mandate from government or is it jolly good work chaps, do your best?

BARRY BRAILEY: It would be good if there was a mandate but unfortunately not. The DNS operator services are going to be DNSSEC. For most of the smaller agencies they use that by default because their DNS operator is doing it so they'll be signed by default. Then we'll have to target some of the larger central agencies who do their own DNS and make sure that they take up this offer. It should be relatively painless for them. It's automated key rollover. It was a well thought out process that was put in. It's not a true government mandate. It's just going to happen to them.

XIAODONG LEE: I think we'll have question/answer after the presentations. Next is DNSSEC Deployment.

We started this in 2010 and it's a long journey for us to deploy the DNSSEC. I think it's because doesn't have over domain DNS record so it's a lot so we are very careful to deploy the new technologies into our DNS servers. Also, if you see that in the mail of the journey last year in August there is big DDOS attack put us in. We worry about DNSSEC deployment so it also postponed our deployment for DNSSEC.

Last November, some moved the DS records to new servers. It's stable now. I think this presentation is very technical. I try to give you some details about deployment. Now we support the DNSSEC free to deploy so I think we try to make sure everything is good for DOS and to keep how to security machines to generate [inaudible 1:02:16.1] and also because DNS also run certificate authority in China we try to use similar security level for DNSSEC amendment so that all of the keys would be divided into five segments and three of them can recover their keys. They will be held by five key administrators just similar certificate authority. It's a big room.

We also use our certificate authority machine to manage the keys so it's provided a very high level of security service level. Even that I'm not sure how the situation has never happened very much but in China there's a national standard to provide a security service so if you see Chinese national standard – to build security centers and how to manage the keys.

Also we build backup system so it's about two southern kilometers away from Beijing, it's another city. It's 121 [sim?] as the [inaudible 1:03:49.5]

centers. All DNSSEC is developed by selling itself because it's smart. I think DNSSEC is too complicated for so many people. I hope the next time if we have meeting, maybe next time hundreds of people join this session it will be better so now I think it's too professional for the people. That's why we try to court smart DNSSEC but we use some professional security machines to do the security keys.

We worried a lot about issues about DNSSEC deployment so we do a lot of simulation and test. We try and use the real zones to simulate the operating environment. You can check that. We try to give a lot of updates and how to submit DS record, how to update that and to how do the key rollover. Of course we find a lot of bugs. I think if we try to avoid the similar issues that happened in other TLDs.

Of course as I mentioned to Dan York, we worry about how to deploy the DNSSEC around China. If you only deploy the DNSSEC in cities I don't think it's enough. There are hundreds of southern [inaudible 1:05:42.6] servers and meanings of second level DNS servers and a lot of registrants so it's how to make sure the whole environment can support the DNSSEC into the test.

If you see the test results, there is some of the DNS inquiries failures but if you evaluate the test data the failure is not caused by the DNSSEC itself. It's caused by the network [inaudible 1:06:14.7] loss. I think it's acceptable but it's much better than before and if you continue to go 15 or 20% DNS lost in China Internet because of internet environment is not very good but now it's very good. I think if you have conclusion that an environment could support the DNSSEC but I don't know how to push them to support that. It's very difficult.

Even in China there is three big ISPs run by Chan Telecom, Chan Com and Chan Mobile. I think the users in these three carriers occupy over 90% users so now we are trying to coordinate with the biggest ISPs to deploy the DNSSEC. You also heard that there is a big DNS disaster in January this year. It is also some issues for the DNS carriers. Of course if they supported the DNSSEC totally, I think we can avoid disasters.

It's a big issue for the registry operators so they need to upgrade all of the platforms, the servers, the routers and also extend our bandwidth. We need to extend our [inaudible 1:07:47.7] I don't know how to get [inaudible 1:07:53.3] from DNSSEC in the future but firstly we need to invest a lot.

For example, we double our server memory. Also there is large bandwidth needed. I think now I try to answer questions for .cn, dot China. We support DNSSEC .cn and ccTLD. For the deployment, we do it in two steps. We try to use the real data and carriers to simulate the DNSSEC carriers testing platform. We try to make sure if there is any kind of problems for the DNSSEC we can try to switch off and then back to the traditional one. We can do that within five minutes to make sure that anything embarrassing happens for the DNSSEC, they can provide the stable DNS service for our users in China.

DNS record became effective last November. I think as I mention a lot so we do so many monitoring and monitoring works for DNSSEC deployment to try to find what kind of problem we face with our deployment and when DNS record effective in the new zones and working on inquiries to make that happen for our DNS services. If we see the data, it's not too much because there is not many DNSSEC carriers

but I think it's if the [inaudible 1:10:20.0] server and also the second level domain servers deployed the DNSSEC, I think the advantage would be much larger.

Also in the last slide I want to give a very simple example. Last March, there is a very small DDOS attack for .cn but it's very interesting. This time the DDOS attack is because of DNSSEC. There is a lot of DNSSEC queries so even the similar DDOS attack cost a lot of bandwidth. It's much larger than before. This DDOS attack only hundreds of man hours is not too much, it's very small but if we face this big DDOS attack then it means that our lack of bandwidth.

I think everyone faces a similar problem so I want to emphasize we want to push the curser servers and second level. Most of them are run by the registrars so have a plan this year – actually we dropped the plan. It's not published yet. We would work together with the registrars to provide the DNSSEC registration for the registrar. That's all. I will answer questions after. Next is Geoff Huston.

GEOFF HUSTON: if someone driving the machine will move me to the next slide please. This is pretty clear that you're in this room because you know what DNSSEC does and you know it's a damned fine thing to do and that's all good and wonderful.

So far you've had a couple of presentations talking about how to sign zones in various contexts in New Zealand and China. That's supply but the real question is how does demand work? The fundamental question that I'd like to contemplate here is – if you sign it, will they validate?

What I'd like to do is look at the world of the internet and the world of DNSSEC, not through the point of view of the zones that are signed but from the point of view of users who in theory would validate that. Next slide. The questions that I'd like to answer today are very simple. How many folk will do DNSSEC validation if you offer a signed zone? And B, where are they? Next.

The experiment is actually a perversion of Google's online advertisement system. We noticed some time ago in APNIC that advertisers like to make ads that have lots of flashy, bright, shiny things. The way they do that is by embedding code inside the ad. Interestingly that code could be made to fit URLs.

What we did was launch an ad that had three URLs that were carefully constructed. All of them were non-cachable so every single time a user visited one of these URLs their DNS was caught at our servers. Caching is evil in this case. None of these were cached. Three URLs as you see there, the good which is DNSSEC signed and valid. The bad, which is DNSSEC signed that deliberately with corrupted signature validation chain and a control which had no DNSSEC at all. Of course we enlisted Google and off we went.

Google is pretty prodigious and when you get Google to deliver your ad, they deliver. For a relatively modest expenditure in December we presented 5.6 million people with this ad and most folk, just a little under 5 million completed the ad or in other words let it run for the full 10 seconds just to see what would happen. The results are as you see there and they classify into three buckets.

The first is the folk that we actually saw fetching a URL and doing all of the DNSSEC signature validation work. In other words these folks were obeying DNSSEC and where they saw the invalidly signed object, they did not fetch it. 6.8%, a little under 7%.

The next lot of folk are kind of curious. They fetched all of the DNSSEC credentials and what they got back was basically the DNSSEC validation failure signal which is confusing because it is also called server failure. These folk actually said, “Oh, well. That didn’t work. Let me try another resolver.” A little under 5% didn’t like invalid DNSSEC and then went off and used a resolver that didn’t perform any at all.

The rest of the internet, 88.5%, don’t have a single iota of DNSSEC clue. Next slide. That’s just the summary. 6.5% doing DNSSEC validation and a further 4.7% are a bit confused that when they get an answer that says someone’s mucking with my signatures they go, “Wow, let me use a resolver that doesn’t do it at all.”

The first thing we can do because we actually record the IP addresses of all the clients that fetch the URLs, we can map each individual client or end user to the behavior to the DNS resolver that they are using and the first way of doing this is to sort those end users into a rough geography. Which country do we actually see these users coming from. I’ve got three columns there. From that country that seem to be doing the full DNSSEC validation dance, the percentage of folk that have a bit each way and the percent of folk that are simply not doing DNSSEC at all.

Fascinatingly, and I expect this is one of the few times where the country of Yemen is at the top of the list of countries that are doing something. In this case, 70% of folk inside Yemen we see doing DNSSEC validation

and in December that's a sample of two thousand odd folk. It's a pretty good number. Interestingly, down at number five is Vietnam with 114,000 samples, Thailand 26%, Indonesia 22%, Azerbaijan at 18% beating America at 15%. That's the top 20 and that's amusing in so far as it's not exactly the world's G20. Indeed there are an awful lot of countries there that are entirely in the other area.

Obviously the bottom 20 is also worth noting and after noting China's care in doing signing of .cn, I also note sadly that less than 2% of China actually do DNSSEC validation. Out of the 1.2 million we tested, and that's a pretty significant sample – probably one of the highest, we get one in fifty. The bottom of the graph, we needed more than 1,000 data points so some of the very small countries didn't make it but the Republic of Korea which led the world in broadband deployment some years ago is trailing the world in DNSSEC deployment. Well done.

If you're wondering what's going on in Singapore with DNSSEC, the answer is not much at all. At 1.4%, rank 105 it is hardly a lot of fun. Of course here in Australia the only thing we're really concerned about is whether we beat the eastern islands. Here's the comparison of Australia, at rank 35 with 10% of folk doing DNSSEC validation and the eastern islands at a pretty pathetic 1.57%, Mr. Bailey trailing badly.

We can put this on a map of the world and this actually is the counterpoint to Dan's map of the world of where are these ccTLDs are actually signed. This is where are folk doing the signing. Chile, quite darkly colored. Parts of Africa darkly colored. Then of course Vietnam and Thailand quite evident, as indeed is Finland up in the north, and right there in the middle is Romania.

This is curious. This is completely unexpected. How many folk in the world do V6 after years and years of exhortation? 1.6%, how many folk to DNSSEC validation? Three times that. What's going on? I suspect the real answer is Google because the real big sea change occurred just a little over a year ago on March 19 of last year when Google said, "Look, if you're using our public DNS services they will be doing validation."

We can do that same measurement because we've got a list of all the IP addresses of Google's resolvers that ask the questions. By looking at clients who use Google's public DNS servers, we actually found in December that 10.4% of the entire planet had their DNS questions pass through Google's public DNS servers. Half of them only use Google. That's it. Google says no, it's a no. The other half have a bit each way that if Google says, "No, can't go there," DNS said failure, "That's okay, I'll go and find somewhere else." A bit of a bit each way.

Now we can put the two together and look at those countries who are doing really well in the DNSSC validation stakes by virtue of using Google as distinct from those countries that are doing it by virtue of having their own infrastructure. I've added three more columns, the percent of validating clients who use Google, the percent of validating clients who use a mix of things and the percent of clients who don't use Google service but still validate.

Yemen got there without doing Google. Sweden got there without using Google as did Slovenia and Estonia but Vietnam at number five, of all those folk 42% of Vietnamese users who do DNSSEC validation, they did it by virtue of having their queries pass through Google. Even in the Czech Republic it's 13% using Google and of course in Tanzania, number

15 with 94%, the occupied Palestinian territories at 58% and Azerbaijan. Interestingly the Americans aren't that keen on Google. Only 10% of American users who do validation, only one in the ten validating are actually using Google.

I just pointed out a few where there is clearly a preference for using Google. As well as by country we can do this by network and it's a very similar thing. Which networks are sending their users traffic to Google and which networks are doing DNSSEC validation?

The network that we found doing the most, 98% of all queries to DNSSEC validation is found in Chile. The next one is a mobile provider in Italy, South Africa, Com Hem broadband provider in Sweden and so on and so forth. I'd just like to highlight Lincoln Spa which is down there at number 14 in Italy does so by virtue of handing everything to Google as does the Superlink communications Company in the occupied Palestinian territory where it just hands everything to Google.

We can actually track individual service providers and see how well they're doing. You'll notice there at number 25 Finland where nothing is passed to Google as far as we can see yet there is still 82% of their users do DNSSEC validation. That's sort of the snapshot of the world. There's obviously a lot more detail that I can provide in various resources but that's just an overview of what's working and what's not.

I just wanted to leave you with a few questions you might want to think about. DNSSEC generates much, much larger responses from small queries so it's used as an attack tool is obvious. Are we going to rely on everyone doing source address validation or do we need to rethink about DNS server TCP? If that's the case, is that going to work?

The other thing, I heard a figure from China about 2.5 times the bandwidth. That's not the case. The amount of bandwidth that increases when your authoritative main server and someone does a DNSSEC signed domain on you, it goes up by a factor of about eight. If you have a badly signed signature, the query load can rise as high as 33 times the query load for an unsigned zone. DNSSEC generates a lot of traffic and a lot of queries particularly when the signatures are bad.

The DNS is awfully, awfully, awfully aggregated. Our queries don't come from everywhere. Indeed 1% of the visible resolvers serve almost 60% of the world so this is an area where there's not a lot of resolvers doing a lot of volume. A very small number of resolvers handle a huge amount of the DNS query load. The trailing edge are some awfully weird thinss that still think A6 records are cool and ask all kinds of stuff that appear to be DNS resolvers running bind version 0.001 as far as I can tell.

We had this whole thing about Snowden and surveillance and what's going on. The DNS is a complete and accurate picture of what you're doing. If you can see someone's DNS queries, you know what they're doing – obviously. Google can see at least 8% of the world's users, one in 12 users. A real-time view of what they're doing – are we comfortable with that?

I started looking at this and looking at the percentage of folk who used Google over time. I certainly noticed last year from May through August that the number actually went down slightly as this story gains some national prominence but we're quick to forget and by August it was all over and more and more folk were turning on Google again, oddly enough.

The standards for DNSSEC are weird and I think the one about serve fail is actually horrible because as soon as you get a badly signed domain, clients start behaving extremely abhorrently. As soon as domains go rotten, the authoritative server has the risk of going into meltdown and that's because the signaling coming out of the DNS is actually broken. Serve fail is not DNSSEC is busted. It says the server won't answer you, try another server.

As far as I can see the standards folk aren't finished. We actually need to figure out how to signal DNS validation broken better than just serve fail. This is the weirdest thing. A lot of these resolvers use BIND and BIND has turned on, give me the signatures and credentials almost all the time. 84% of all the queries I see actually generate the huge signed response but only 6% of clients do validation so oddly enough a huge amount of the world is pre-provisioned to do the right thing but then won't. 84% say give me all the stuff and they go, I didn't mean it. I'm not going to do anything with it. I just like getting big answers. Gee, thanks.

That's all I have. I'll see if I can do questions – I think we were going to do that at the end. I'll hand it back to you Mr. Chair and say thank you.

XIAODONG LEE: it was a very wonderful presentation. The next speaker is Tran Canh Toan from Vietnam.

TRAN CANH TOAN: I come from Vietnam and I see under the information and on behalf of my organization I am very honored to present to you about status of

DNS and experience in Vietnam however I'm not the main person who does DNSSEC with us. He is busy and absent so I'm a substitute for him.

Every question you can send to my e-mail and I can ask him to answer for you. Here's my presentation outline. In the first section I will DNS leaders in Vietnam. Then I will talk about our plan to deploy DNSSEC in Vietnam and lastly some of our issues.

Back to history, we do many research to answer the security for the national DNS server operation and in the year 2001 when DNSSEC research so that deployment of DNSSEC looked possible and we started to research around DNSSEC as our main solution to answer the security and national DNS server operation. At the end of the year 2008, we finished research and [inaudible 1:30:44.7] in the lab and in 2010 we finished applying DNSSEC for protocol for .vn domain security in national internet server and now we have a master plan to deploy DNSSEC for .vn domain.

During the research and experience and also deployment we came to the conference to learn a lot from ICANN, APTLD, DNS OARC and here is the modern experience in the lab. In this modem we have my own master and DNS server and also caching server and server of registrar and ISP Vietnam.

In this we do the academic update, inquiry from DNS for ISP [inaudible 1:31:50.9] and ICANN forth to caching and evaluate recent findings. In the experience on the national DNS server we are big on root DNS server and secured the root key signing in operator and also for the .vn and .netvn.

We answered the authorized query between client and DNS server and some impact when deployed DNSSEC on the performance. For example, increase approximately four times. The response time and synchronization time and also CPU and memory increased but no signed. Now we are finished the research and experimental period and we have master plan to deploy DNSSEC for .vn domain and we have three main steps in this plan from 2014 to 2016.

The first step is preparation for infrastructure human resource and we promote the core operator activity and [inaudible 1:33:32.0] for Vietnam ISP and also our HR. We view the policy and process for the deployment. The second step, in 2015, we will officially deploy DNSSEC for .vn domain. That contains key generation, zone signing and public cost and we also continue to promote activity and do training. The third step is deployment. We continue to have ISP registrar and DNS owner in Vietnam to deploy the DNSSEC and now we are at the first step.

Here are some of our interests. In the foremost activity, we want to consider the policy to promote DNSSEC for expansion in government and ecommerce and also get with our registrar and ISP and also domain owner to deploy DNSSEC. In the technical aspect, we care about solution to secure the private key, key rollover and key ceremony and disaster recovery and also we want to integrate DNSSEC with our EVP system and lastly we want to know best current practices and ICANN and answer ccTLD and TLD registry. That's all.

XIOADONG LEE: The next speaker is from IP Mirror, Patrick.

PATRICK VAN HOUT: Thank you. I think I am a bit outside here because most of you will be on the registries. We are a registrar localized in Singapore. I started working with IP Mirror back in 2005. One of the first tasks I was asked to do was to join our CEO to go with her to Argentina. At that time there was a DNS workshop and it overwhelmed us.

Knowing a little bit of DNS, DNSSEC workshop was too much information to get at that time mainly because we are using BIND and BIND was not really automated as it is now. In 2012, we were asked by Malaysia and [inaudible 1:36:46.0] to join them for a workshop which is seven years later and at that time we gathered more interest and got more understanding about DNSSEC. Our team also joined the ICANN Workshop a few days ago here in Singapore.

As G operator, most of our customers are from Singapore. Most domain names are from Singapore and as mentioned just now by Geoff, Singapore is lagging behind in DNSSEC. The .sg master zone, root zone is not signed and as far as we know there are no plans for them to do so. I'm not sure if DNS is present here but it would have been nice if they could have presented their plans for the future. My reason for saying that is because .sg is our largest customer, we see little to no demand at all from the public here in Singapore.

As there's no demand from the public, we are not eager to continue because why should we put in the resources as there's no demand? Furthermore, when putting in the DNSSEC into our system we faced a few implementation challenges.

One of them is the turnover of staff and because DNSSEC is not that easy to understand it takes staff time to learn to know how it works and to make sure that they can follow up with the changes presented by BIND and by DNSSEC itself.

What we would have hoped for is that one way or the other ICANN is able to "force" the registries like SGNIC to become DNSSEC compliant because without the registry, we cannot complete the chain of trust and secondly what we would like to see is what happened with IPV6 two years ago. IPV6 had a world launch day announcing the use of IPV6 through the whole world. It would be nice if ICANN or the DNSSEC community can do something similar to generate demand, to tell the public what DNSSEC is about so that they can start using it.

It's nice that, like Barry said, he goes out himself to Radio .nz to get them DNSSEC compliant but it would be better if those people would come to you because one to many or many to one makes a difference especially to us as a small registrar. We don't have the resources to go out to every single client and ask them, "Will you become DNSSEC compliant?" I'm not sure if you can do something with that. It would be nice. It's quite short but I hope we can do something with it. Thank you.

XIAODONG LEE: Short is good so we can have much more time for question and answers. May I invite the panelists here. Open the floor for questions.

MICHELE NEYLON: The gentleman from IP Mirror, this isn't really a question. It's more of an observation. Please be very, very, very careful about what you wish for

and try not to establish relationships between ICANN and ccTLDs that do not exist because this ccTLD operators will take you out the back and they will shoot you.

You cannot even suggest that ICANN will force a ccTLD operators to do anything. Don't even think about suggesting it. You might wish to consider suggesting to ICANN that they look towards encouraging registries to do something. It will go in the transcript as something else. Bear that in mind so please be very careful.

[MALE SPEAKER]: May I add something? I just want to make sure that one point is covered. This comes back and back in different venues regarding ccTLDs being forced by ICANN. ccTLDs do not have a direct agreement with ICANN so we can talk about new gTLDs but you can't really talk about something that existed before ICANN existed. I don't think DNSSEC should be something that is deployed by enforcement. I keep saying this. It is job security for DNS engineers so the smart ones will go ahead and implement it. Just my thoughts.

DAN YORK: Thank you to all the presenters for the sessions you had. These were quite interesting pieces. To respond to the last gentleman there from IP Mirror, two comments. One is we're seeing a lot of interest from ccTLDs for doing more of this. The advent of the new gTLDs and the requirement that they have to do DNSSEC has raised the level of interest from some ccTLDs have been saying to us, "Well, they don't want to get into a position where all of a sudden the new gTLDs are more secure

than their ccTLDs and so we're starting to see some interesting dynamics around that. People starting to ask questions of maybe we should get in around there and do something about it.

We'll see how that plays out in some of the space around that. The second piece around day around that is we've been talking about for a bit. The challenge we've had is how to create a certain level of momentum or how to measure it and how to address both sides of it. One of the ideas we've had recently is an idea around perhaps having a day that we try to focus on one side of the equation. Like validation and we work with some large names and some large space around that. Part of the thing to do an event like that is you need to collect a good number of names.

World IPV6 launch for instance worked really well because we had Google and Facebook and Yahoo and big names that people knew who were behind that. We are thinking about that. I'd love to talk to people more about that not in this session because that is not the point of this but it is something we are talking about in some way.

RUSS MUNDY: One of the things that has hit some publicity, maybe more in the U.S. than elsewhere in the world. There have been at least two or three attacks that were based on being able to attack DNS, primarily in home routers but elsewhere in some instances.

There was one from Poland where specifically they went after home router configuration changes that resulted in the people in the homes going to the attacker's DNS server which then created themselves man

in the middle situation. Having the ability to do DNSSEC on the end application…I'm not sure, somebody mentioned DNSSEC aware browsers, seizing the plugins and there's the Bloodhound browser.

Some of those are available but attacks such as this really emphasize the need for having DNSSEC in the end application. This is something that I think is going to become more important because the bad guys have really figured it out. Some other things have been plugged off so they're going after building attacks based upon DNS mechanisms.

One other thing that I've noticed in the last…It was really from GoDaddy that brought this to my attention. What they've done, what Comcast has done in terms of packaging DNSSEC. They did not package DNSSEC as an explicit thing. They packaged several capabilities together as an enhanced security service so they have stronger security from several perspectives. This is something that you might also think about and look at whether it's adding a virus protection or adding services that are stronger at the SSL level. Not selling DNSSEC straight out but combining it with other things into a security package.

RON AITCHISON: One observation about China. I don't know if there's a Guinness Book of World Records for the number of KSK rollovers yet but fantastic, really very impressive number. 102 KSKs, 51ZSKs my question is – you mentioned 20 some bugs, with the current discussion about key rollover within ICANN, the root rollover, can you make any observation about the bugs? Were these bugs based on repeat cycles, were they based on new releases of software, do you have any feel for the type of bug you were getting? Can you classify them in any way at all?

XIAODONG LEE: I think that is a good question but I cannot answer you as there were 20 bugs. I will need to bring this message to my engineers so we can respond to what the bug is exactly.

RON ATCHESON: My reason for asking the question is not purely interest. It seems to me that one of the key questions about the ICANN key rollover being proposed is what good does it do? I'm somewhat skeptical about it. The reason being that new software's coming on all the time and a one off hit in time and space is not really what we're after and that's why I'm curious as to where your bugs were coming from, what the characteristics were?

It seems to me that of all of the presentations, yours was the most thorough. Maybe other people have got similar experiences with bug finding and so forth. Maybe one of the things we ought to do is to look at the kind of bugs we are getting and whether they can be classified in any particular way?

XIAODONG LEE: I think in the present years, a lot of TLDs deployed DNSSEC but of course also some charities face some problems. I think if possible, we share the bugs. I think it's not only because of the key rollovers, maybe software bugs and what were they.

DAN YORK: I'd like to just quickly thank Jeff Houston for the excellent measurements you provided and we don't really have time to talk about it here in this session but I do want to chat with you at some point about how we could do more with that or make those results available on a more regular basis. That's great info so thank you for bringing it.

XIAODONG LEE: I think soon to finish this discussion in five minutes so take some questions from chat room.

JULIE HEDLUND: There's a couple of questions in the chat room and I think it might also be helpful for people to take a look at the chat room on Adobe Connect as well. The first was immediately following your presentation Xiaodong was Sebastien Castro had asked, "If you were to switch to the non-DNSSEC system, how would you change the DS record at the root quickly enough?"

XIAODONG LEE: I think it's not necessary to change that. Switch to traditional one is okay because require not necessary to change the DNS root.

JULIE HEDLUND: This was a question from Geoff Houston to you in the chat room. Rather than reading it here, I would suggest since it's not to the panel in general that you go in and type your answer in there so we won't take the time.

RUSS MUNDY: Will do.

XIAODONG LEE: I want to give the last comment. I think that other presenters mentioned there's no demand from any users. From my point of view is no demand from users because the users don't know what DNSSEC is and how they need to deploy the DNSSEC. They just want to make sure that their system is safe and stable but they don't know DNSSEC influences the security for their system. They need more education for the users. Maybe it's the responsibility of the registrars how to tell people what the DNSSEC is and how to deploy the tools for them.

JULIE HEDLUND: Please join me in thanking our panel. That was an extremely interesting discussion. I would ask Timo Vohmar to please come on up. Welcome Timo Vohmar from .ee who will discuss deployment of DNSSEC at .ee to please come on up. Thank you.

TIMO VOHMAR: I'm head of development at Estonia Internet Foundation. In January this year we launched DNSSEC in Estonia. As it comes out, we weren't the last ones so I'm here to share our experience and hopefully help somebody. I'm going to give a brief overview about the foundation and then I'm going to speak about DNSSEC, why we did it, how we did it and where we are right now.

It was founded in 2010 together with domain reform in Estonia. Before that, .ee was managed by government institutions and it was only

available to locally registered businesses. With the domain reform basically freed and registry/registrar model was introduced. We are a team of 11. We have close to 75,000 domains. Currently we have 38 registrars out of which 28 are local and 10 are international foreign registrars.

More than 40% of the domain market belongs to one local registrar so the balance is a bit off. There's good and bad side to it with every new thing change development we have to discuss this with this single registrar but the good side is if they are on the same boat with us, all the other registrars will follow.

Zone updates are done every 10 minutes. There's a good reason for this because it takes about 50 minutes to establish a company in Estonia so we can't be any slower than that. IDNs were launched in 2012. There are more than 1300 IDNs right now in the zone. They are not very popular because of the problems with e-mails and DNSSEC was launched this year with the first two and a half months we have gained 37 signed domains.

When we first sat down about DNSSEC the first question of course was why do it? There's no demand from the market, no business case for registrars nor ISPs. Big international domains weren't using DNSSEC like Google, Facebook, Amazon so if no one's using it and no one wants it - why do it? We found two reasons for it. First was competition, we are competing with gTLDs, namely .eu and .com in Estonia.

As we cannot compete with them on a price level, we have to compensate this with better service and additional services we can provide. As both of them had all ready deployed DNSSEC we really had

no choice. The other reason was prevention. Although we haven't had any publicly known man in the middle or cache poisoning in Estonia, looking at today's IT world, it's evident that if we don't do anything it will eventually happen. It's kind of stupid to just sit and wait for it to happen.

That settled, we started to think for whom we are going to do this, to set a goal for this project. It's a cool idea to target everyone, to make a goal to sign the whole zone but first of all it's unnecessary because for most of the domain owners, they don't care about the DNSSEC and they don't need it either. The other way would be to just do it, do everything right on the registrar's side and let the market decide when, if and how they will deploy it. This also seems like a waste of time and money because market will not pick it up on their own because it's just a business.

We started to think who would benefit the most from DNSSEC? These aer the organizations that deal with money and sensitive personal information. These are banks. These are government institutions. These are internet stores. In addition to that, we also decided that if we launch DNSSEC, we want to do it with working trust chain meaning that there has to be at least one high profile domain all ready signed. It would make communication that much easier because instead of just telling everyone we did it, we can also show that it works and how it works.

It took us almost two years from the first meeting until the launch in January. This is a long time and it can be done a lot quicker but we didn't want to rush it. We took it very slowly. We turned directly to the companies we saw using DNSSEC dealt with opposition and we didn't want to force it on anyone either, namely registrars. The only thing the

registrars had to do regarding DNSSEC is to start forwarding DNS keys from registrants to us. This is to preserve the registry/registrar model.

The alternative would have been that we would have to create our own registrar and this motivated them all very much. Technically the DNSSEC is very simple to implement. There are a lot of very good, well documented software solutions out there. There are even complete DNSSEC appliances so you can take it out of the box, connect it to the network and with a few clicks off you go.

For our system we tested open DNSSEC and BIND and we went for BIND because of its inline signing feature. We didn't want to resign the whole zone every 10 minutes. For HSMs we are using [inaudible 2:01:04.3] cryptic servers. We have three of these. Two are in the live system and one is for testing and acts as a spare in case something happens with the two live. In case something happens we can exchange the faulty one really quickly and then deal with the [inaudible 2:01:27.6] later. This also allowed us to go for cheaper maintenance plan.

Although DNSSEC is technically simple to implement, the testing is very important. We launched our first test system in 2012. For this we registered domain under .net and anyone who was interested to do the tests on their own, they could just register a third level domain with us and test it like that.

That wasn't very popular. There are only two registrars that ever used this system but luckily one of them was the one that manages the domains for the government. They found it very useful and to test the final solution we went for the DLV. We saw it as a very good way of testing our live system because by then of 2013 Google and also the

biggest ISP in Estonia had already enabled the DNSSEC validations in their servers so we could do the tests on the live system without the fear of making our zone unavailable for a big part of the world. Within these tests we actually found few more problems that didn't appear in the test system so now I'm a big fan of DLV.

Below you can see a small and very simple schematic of our system. I guess there's nothing unique there. We have two HSMs, load balancers, BIND 9.9 as a signer. We use [inaudible 2:03:40.3] as the registry system and hidden master is also BIND. In reality, DNSSEC is actually really hard and this is because of the procedural part. There's a lot to think about from Guy and signature overlapping, rollovers, domain transfers. You have to test all of these things like there's no tomorrow.

It's also very important to point this out to all the registrars and registrants because one of the pioneer registrars that we had with us from day one actually stopped their service after a month because during some server maintenance they broke their DNSSEC system and couldn't restore it for a couple of days and this is when they realized that they had missed a lot and underestimated the system so they dropped the service altogether.

There are also a lot of parties to deal with. Registrars, registrants, ISPs and internet users and you should be ready to approach them all. It's a good idea to speak with registrants to create some demand so the registrars would see there's some potential. You should approach internet users or organizations representing internet users so it would create some kind of demand to ISPs and registrants and so on.

We did as much as we could to support anyone interested in DNSSEC. In addition to the test systems and documentations and guides we had a lot of meetings and to break the opposition we created a DNSSEC expert group. In this group we had two of the biggest registrars, two of the biggest ISPs, two of the biggest banks, government was represented and me of course.

All sides were represented. The skeptics and the one who liked the idea and this expert group worked amazingly well because after only two meetings the skeptics were gone. There was a unanimous to go forward with DNSSEC in Estonia.

As we are very small registry we don't have very much funding for big marketing campaigns so we cooperated with Estonia Information Systems Authority. They are also running local cert and together we put together a small budget and bought a small animation for general public to introduce the DNSSEC. Unfortunately it's not ready yet so I cannot present it today. When we launched the DNSSEC on the same day we signed the central government portal and this helped to break the news barrier so we got a lot of free radio coverage, news coverage and it worked better than we expected.

Today we have one local and one foreign registrar offering DNSSEC services. The biggest registrar in Estonia is preparing to come out with their services next month. We are expecting this because they promised to do it free of charge and the third biggest registrar is also considering coming out with their service because there appears to be some small demand from the registrants.

Google made it very easy for us for the ISPs because after they enabled the DNSSEC validation, the biggest ISP in Estonia followed and the rest will follow them. Out of 37 signed domains we can be considered high profile. We are still waiting for the banks and Estonian union of eCommerce to put DNSSEC in the requirements to get the so-called safe place to buy quality tag. That would make DNSSEC necessary for all Estonian internet stores.

We have set the deadline for the project to 30th of June but to be honest I think that we won't get any banks using DNSSEC by then so we are kind of on a road to fail on that one. What did we learn? We learned that it's all about communication. You shouldn't be afraid of opponents and it's a good way to find someone who has the different opinion and put these two sides together. If you are trying to protect the idea of DNSSEC, you will eventually sound like a salesman and no one will take you seriously but if these two sides can talk about his on their own it will go much better. As a project – set realistic targets. Take it easy and test hard. Thank you.

JULIE HEDLUND: Let's take a few questions now. Ed.

ED: It's not so much a question but there was something you said Timo that I think was very important in the middle of your talk. You were describing the use of DLV to test your zone. I remember now when you did that there were a lot of people out there who ran around screaming that DLV is supposed to be dead. I don't know if you were aware of that thread.

Some of the DNS operations manuals were saying, “Why are they using DLV. That was supposed to be gotten rid of before we signed the root zone.” At the time I was defending it saying operators need to have more tools to do some testing but you gave a rationale in your talk. I think that was very subtle but I would like to say as the world of DNSSEC gets larger, it’s hard to have a scope test without something like the DLV out there. I think that’s very significant.

You want to test in a real live environment without bringing down all of the big attention you’re going to get from Google. What if something goes wrong with something that’s a smaller operational tool out there. I think that’s an interesting consideration that some of the operators are not considering that you have to do these steps to get to the final stage. Testing in a limited way with real live data is an essential step to what you’re getting. I think people generally forget about that. I wanted to make sure that got back into the transcript again.

DAN YORK: As one of the people who has been saying, “Die DLV. Die, die, die,” accept that you’re right. There are test situations where it may make sense.

JACQUES LETOUR: Do you have an EPP web interface for your registrar?

TIMO VOHMAR: For the registrars we currently have only the interface.

JACQUES LETOUR: If you want them to do it. It might be an option if they want to do a web interface of to start with to play?

TIMO VOHMAR: Yes, we are working on it currently but it's not ready yet.

MICHELE NEYLON: I'm just going to be awkward because I like doing that. Do you as a ccTLD offer a registry lock?

TIMO VOHMAR: What do you mean by that?

MICHELE NEYLON: That actually is the problem you see. Could someone please explain using terminology that – because Warren is the expert on this. I will let you explain.

WARREN KUMARI: Wow, you're awfully kind. I'm far from expert. Registry lock is an additional level of locking that a number of registries provide. Dot com does it. I can't remember what they call their special option but it's something where actually you have to speak with the registrant in order to unlock the domain or the registrar has a two-factor system that they then send the info for.

That way, even if the registrar tries to initiate a change it doesn't go through unless there's some other band thing. Does that explain it?

MICHELE NEYLON: Sort of. It's a way of mitigating against domain hijacking so the reason I pick on Warren is because he works for a company that is targeted for hijacks. The reason I raise this is because I see a lot of ccTLDs going on and on and evangelizing about something where there's no demand, DNSSEC whereas they don't offer registry lock where there is demand because I have customers coming to us looking for registry lock and a lot of you ccTLD people don't offer it.

Several of the existing gTLDs don't offer it whereas I am yet to feel an overwhelming surge of interest with respect to offering DNSSEC and you registry operators still haven't come together to offer a standardized way of offer us registrars to do it.

TIMO VOHMAR: The answer is we don't currently offer registry lock but we have thought about it and we are probably going to do this sometime, maybe next year.

JULIE HEDLUND: Any more questions? Please join me in thanking Timo for a very interesting and helpful presentation. Now we're going to move on to Michele's panel. Please come forward, Michele is the moderator and we have Joe Abley, Jim Galvin and Dan York.

MICHELE NEYLON: Good morning. As many of you know, under the 2013 RAA which was adopted by ICANN's Board of Directors in June of last year there are now

some light obligations for registrars to support DNSSEC. In the context of ICANN, when I say registrars I mean ICANN accredited registrars for gTLDs, not registrars for ccTLDs or anything else.

This morning we have three panelists. Mr. Dan York you all know, if you don't know him he'll introduce himself at least three times. Dan York from ISOC who evangelizes DNSSEC and IPV6 for a living. Dr. Jim Galvin, I'm not actually sure of his job title. He's that kind of Afilias' super duper DNS tech guy. I'm sure he can explain his job title better, Joe Abley who has a variety of roles in a number of different organizations and has one of the those CVs that goes on for miles and who is currently with Dyn.

The three gentlemen have some slides. If any of them say anything that you think is weird or odd, please do interrupt them because I think it's meant to be a workshop not…We don't fly half way around the globe to look at a bunch of PowerPoint slides unless of course you're just trying to write off your company's profits somehow. I'll hand over to the first speaker who is Dan.

DAN YORK: The point of this discussion was to talk about what our registrar is required to do. This comes to the point that was raised earlier by the gentleman from IP Mirror talking about what ICANN doing, where registrars and registries need to be involved. This is specifically about registrars and what's in the 2013 Registrar's Accreditation Agreement.

As a way of framing this discussion, to begin with what we're talking about here is when you think about DNSSEC there's the signing and the validating side and we're specifically focused on the registrar portion of

that. The Registrar Accreditation Agreement or RAA has a section on DNSSEC. As I state here in the slide, it's the additional registrar operation specification and it has three components, DNSSEC, IPV6 and IDNs.

The key point about this is for registrars to work with, to register domains in any of the new gTLDs they have to sign the 2013 RAA. If they don't want any new gTLDs they can continue on the 2009 or the other ones but.

MICHELE NEYLON: There is no way to renew a 2009 RAA so a lot of registrars will have switched to the 2013 contract all ready in order to offer new gTLDs but as their contracts come up for renewal, they'll switch.

DAN YORK: Eventually we'll see everyone move to this model. The specific thing says that the registrar has to be able to accept keying material – either a DNS key or a DS record and pass that on to the registries. That's the key part of what it is and it says it has to use EPP in order to do that and communicate with the registries. That's the key part of that.

If we think about the way signing works and the path that things go through you have the registrant who interacts with the DNS hosting provider or does that function themselves. They're signing the zones, they're publishing the records, they're providing the DS record to the registrar who is then passing that on it to the TLD and the registry. I say DS here. It could also be DNS key depending on which registry is accepting which. The challenge we have in our terminology is that many times the registrar and DNS hosting provider are the same entity.

If you register your domain with a registrar they are very often doing the DNS hosting for you in which case it's kind of simple. They can sign into domains. They've got the record they need. They can pass it up to the TLD. The challenge we get into and we've talked about this at a couple of things is when these are different functions, when you are providing your own hosting, when you're using another provider for the DNS how do you transfer that up to the registrar and Joe's actually going to talk about that somewhat specifically in his presentation around a couple of proposals that are out there.

Again, the key role that the registrar has is that they are passing this material up to the TLD which creates what we call the global chain of trust, it's intact. We often use slides like this. Many of us have different slides that picture this but the key point is that when the DNS resolver goes out and pulls down its information and comes with an answer to go back it can validate that answer is in fact the one that is there based on this global chain of trust going back up to the root zone with these DS records that are here. Registrars play a very important role with that.

What the RAA requires is the registrar must allow its customers to use DNSSEC and must and to interact with the new gTLDs. They must add, change, remove, they have to have some mechanism to accept it and they must communicate those using EPP extensions that are defined in 59.10.

It does not require, if the registrar, if they also do that hosting side, they don't have to sign domains. It doesn't say you have to. It says you have to accept the keying material and pass it on up to the TLD. It also doesn't

require the registrar to sign their own domains although it would be logical to do that is you're offering DNSSEC as part of that.

MICHELE NEYLON: Could you go back up one slide please? One thing to note here you will see other presentations people talking about different ways to exchange material. We're going to see some more of this on this panel. You'll note here that it references specifically to EPP – specifically which is a little bit of a problem.

DAN YORK: Yes, it specifically mandates in this that EPP is the mechanism for communication with the registries.

The question is why is EPP a problem. You want to expand on that?

MICHELE NEYLON: I'd be happy to. There are multiple issues here. If EPP is the only method which is supported, that means that as the registrar you have to do extra development. If all registries all are supported exactly the same EPP implementation of DNSSEC then one could do the development once. Unfortunately, the registry operators, each one of them, has gone off and done it slightly differently. If I offer one TLD, I have one implementation, for two TLDs I'll probably end up with two implementations and as the number of TLDs expands then the number of different sets of code that my developers have to write and maintain expands almost in line with the number of extensions.

Now, changing name servers, updating contacts, those kinds of functions are things that our clients use. Our registrants use them on a day to day basis but doing anything with DNSSEC is way down the priority list and as I have repeated in the past, I think today we've had four requests for DNSSEC support.

Our customer base is about 60,000 direct customers or something like that. You can ask registrars with a larger customer base and they'll give you similar numbers. The fact that it's uniquely EPP, if it was using a carrier pigeon or whatever method was available to you then that would allow for greater flexibility. Some of the ccTLDs have come up with their own DNSSEC signing service that registrars can use which moves it along a bit faster and reduces the amount of development on our side.

DAN YORK: Just to build on that, this part about EPP specifies there are some very specific extensions for EPP in RFC 59.10 that are around DNSSEC. It says these are the ones that are required and to Michele's point, there is a new group within the ITF called the EPP EXT which is looking to standardize some of these extensions so for registrars there's not a bazillion out there but there are.

ROY AITCHISON: With regards to very slightly different EPP implementation to the registries. As a registrant I have the exact same problem. For a set of registrars that offer me DNSSEC, each individual one does it slightly different. It would be good ifi the registrars would come together and provide a uniform way of registering DS records through their interface.

DAN YORK: I agree with you, Roy.

MICHELE NEYLON: I disagree with you. We 've got potential anti-trust issues. If a group of registrars band together and actually…I'll explain that. If you keep it as a technical thing in terms of coming up with technical standards and trying to encourage people to do it but he said for a group of registrars to come together and do the same thing.

That's not the same thing. I'm not a lawyer and I don't give a damn but any time within the registrars that we've talked about a group of registrars coming together in terms of offering some kind of commercial product, at least one American lawyer will go, "Anti-trust, anti-trust, you can't have this conversation," which I don't full understand but it's something they get very, very testy about. It's both sides, though. The registries aren't helping.

DAN YORK: In general we have seen this comment. To this point Roy, you are absolutely right. Any automation centered on the chain will help things move along so just the comments we can discuss around here, learn more about DNSSEC, identify how you can provide user interface. To Roy's point, what can be done in that regard.

A couple other points to just mention, This is one of your bullets, TLDs have different requirements for EPP extensions. There's also this issue around secure transfer once you have a domain signed with DNSSEC,

how do you transfer that securely to another registrar. There is one way promoted by SIDN. It's a draft that's out there. It's actually in use. They're using it already so that's one way that can potentially solve this particular issue.

Then we have a larger question at the bottom. Some TLD's registries have asked for DS records, others ask for DNS key. The rewording of the RAA is that you need to support whichever one the TLD does. There's a longer discussion we could have beyond that.

For the slides, we've got some resources up here. We have some info on Deploy 360. There's a number of other different pages, Michele's Stakeholder Group is another place to go and talk about this.

That's all I had because I was just supposed to frame this discussion.

JIM GALVIN: I don't have any slides. The shape of this panel has changed a number of times but I really only have two points that I want to make that I want to put a little historical context first. I think I can get through those points relatively easily.

First, picking up on something Dan said earlier in his presentation about EPP extensions and that new working group in the ITF. I'm Chair of that Working Group and I want to clarify one particular point about what it's doing. It's not standardizing on EPP extensions. It's about creating a registry of EPP extensions that are commonly in use.

MICHELE NEYLON: That's all EPP extensions then, not just DNSSEC extensions?

JIM GALVIN: Correct and that is all EPP extension, any being brought to the group. It has a small set of them on its agenda for now and then what happens after those are done is a new work item would require some different chartering just to clarify that point, EPP EXT.

MICHELE NEYLON: Just to explain a little here for those of you who may not be familiar. The way EPP is implemented by registries means that more often than not you have the same functionality offered by three different registries in three different ways. Whether it DNSSEC or registering trademark material, one of the issues is there's no coherent repository of all options.

ROY AITCHISON: Most often, for instance when [inaudible 2:34:32.9] has to provide certain extensions on EPP it is because the established registrars all ready have different ways of doing this and we're just trying to comply with those different implementations. That's why you get this growth.

One other thing, I find the acronym really amusing. It's literally EPP extensions so Extensive Professional Protocol Extension. Good luck there.

RON AITCHISON: Just for clarification, does the current extension set include full support for DNSSEC or not?

JIM GALVIN: RFC 59.10 does. It includes full support for DNSSEC. For historical context so you know where I am coming from. I represent a registry service provider. We are, in fact, the back end for dot org in particular which I bring up here because Afilias signed .org and they were the first gTLD to sign and the largest TLD at the time.

The place that I wanted to get to in that discussion was having signed the TLD zone, the next step was to offer signed delegations. All of this was being done even before the root was signed. We actually did some work with registrars and I'll just pass the kudos to [inaudible 2:36:33.9] and Dyn over here on the end who were the two registrars that we worked with. We worked extensively on being able to offer signed delegations and what it would mean to registrars to make all that happen.

In fact two things came out of that. One was RFC 59.10 because we discovered a bug in RFC 49.10 and the predecessor to 59.10 that needed to be fixed in order to support DNSSEC from registrars. The other thing was we spent a great deal of time talking about the transferring of registrations when DNSSEC is active in the domain.

So far the discussion has focused a great deal on DNS and DNSSEC and worrying about moving DNSSEC services from one hosting provider to another but what's interesting in the context of ICANN is there is a relationship, obviously, between registrations and the DNS services and the ability to transfer a domain from one registrar to another. Transferring a registration from one registrar to another and thus potentially moving the DNS hosting services.

There are some very real issues there and some technical issues that even the proposal that Joe is going to talk about and even the proposal that exists from SIDN don't cover all of the issues. I want to point that out at the moment and highlight some of the issues that are there. Again there's no solved problem here yet.

The two points that I want to make about supporting DNSSEC when you are a registrar so you also have registrations is there are two things one really needs to keep in mind in order to do this effectively. The first thing you really need to do is functionally you have to think about your registration services different from your DNS services and you really have to separate those and be able to work with them differently.

There are reasons why this is essential in order to transfer DNS services at the same time as the registration. One of the things that we had found in doing all the testing that we had done before and some of this has come out over the years and more directly there has been more discussion with people about the right way to do this.

There are a variety of behaviors among resolvers that are out there and it is because of these categories of behaviors, at the time there were four and we're down to three. There are three distinct resolver behaviors that will affect your ability to transition your DNS hosting services from one provider to another when a registration transfer is also active. That's what's critical here and it is those behaviors of the resolvers that put you at risk of your domain being unable to validate so you essentially lose services.

It's something that a domain owner would want to pay attention to or at least some high value domains would care about a great deal. 80% of

the market probably doesn't care if they go dark for three days while their transfer is occurring. If you think about your DNS registration separately…

MICHELE NEYLON: Sorry, back up a little bit. I think you need to say – you're talking specifically about signing and unsigning. I can assure you as a registrar and hosting provider that my clients wouldn't be very happy if their DNS stopped working for three days and by not very happy I think we'd be talking coming after us with pick axes.

JIM GALVIN: Excellent, I'm glad to hear that because that just highlights the fact that we have a real issue here that needs to be handled when registrations are moving. The functional separation of your registration services from DNS services allows you to be able to do things. You need to be able to import new NS sets from new DNS hosting provider when your registration is moving. You have to be able to continue DNS services until you're explicitly told to turn them off.

One of the things we have found amongst gTLD registrars is when a transfer of a registration is initiated that frequently means that the DNS resolution services are automatically turned off and they're disabled. In fact, it is that critical step that from a business point of view makes perfect sense. That crushes your registrant as the losing registrar if you will, you probably don't care very much but as the gaining registrar you care a great deal about that because there's no smooth transition there.

That brings us to the idea that in this category of separating your DNS from your registration services as a gaining registrar, you want to set up new DNS services in advance of actually moving the registration which also puts you in kind of a business model, new requirement which doesn't really exist. Then of course as the losing registrar, any registrar should support the export of the zone file in such a way that you can actually move it from one hosting provider to another in a convenient way. This is another one of those things that needs to exist.

MICHELE NEYLON: This is where on some of the DNS operations mailing list that we have this beautiful schism between those of you from technical operations and those of us who are actually trying to make a living. Being able to export data and everything else is a nice idea but obliging registrars and DNS providers to support that functionality might be a step too far, surely or is that what you're actually trying to say? You're actually trying to oblige us to do it.

JIM GALVIN: Yes, to a first order you've got to output a configuration file with the zone contents in it. You have to have a way to move that. Either someone as a gaining hosting provider, this problem exists anyway. As a gaining DNS hosting provider, I have to be able to get the existing zone file in order to offer new services. Somebody has to recreate it. You have to get it somewhere.

MICHELE NEYLON: Not necessarily because if the services are unique to the service I'm offering then why on earth would I export the data?

JIM GALVIN: The names so you're right. Fair enough.

JOE ABLEY: I have a question. I haven't said much so far – on the microphone anyway. Isn't the basic problem here that registrants have been conditioned to think that registration services are something you pay for and DNS and subsequently by extension DNSSEC is a freebie you get by just clicking a box at the end because if DNS services were something you paid for, particularly if you pay for it separately then you could cancel your registration and continue to pay for your DNS hosting and you wouldn't have this problem.

JIM GALVIN: The problems that I'm highlighting and the reason why we got into this was realizing that if you functionally separate your registration from DNS services and if you actually have a separate DNS service provider as opposed to bundling services, you in fact don't have these issues. You can transfer your registration at will and it's straightforward to do that.

I agree with you, Michele, if I'm only dealing with bundled services and I want to get my bundled services on one side and get essentially a similar services on the other side maybe I don't actually need to move the configuration file because I'm going to be using the same names and you're right, the new bundled services will assign everything that I need

but as a principle you do need to have configuration movement. That movement might be not actual movement because it's part of the bundled services but I don't want to lose the principle of the fact that the DNS zone file is different on both sides.

RUSS MUNDY: When a group of us from the DNSSEC initiative started to look at this challenge, it's a situation where you have on the engineering and specifications side you've got a set of things that are all written down. They're supposed to look a certain way and act a certain way but in the real world it turns out that people didn't actually build them and run them that way. When you look at it from the engineering and specification part where you've got these separate pieces then in reality it is easier to do the movement if the owning activity of the name is actually operating the main service itself.

If the registrar services that they're getting from the registrar are strictly the input to the name system but that's such a small proportion of the cases that we have to think about. How does it work, this cross product of the real world and what the engineers and spec writers came up with to begin with.

JACQUES LETOUR: Is this a problem on paper or is this a best practice problem because right now I don't' think we've had a lot of experience in transferring domains.

JIM GALVIN: I would say that it is in fact a best practice problem, very definitely. Actually there are two issues. There's the technical problem. Some of it Joe is going to talk about here because there is the issue of when you're transferring the DNS hosting, you do have the issue of the key relay. You have to get the key from one registrar to another and in and out of your registrar but the observation that I'm making is there's a lot of focus on transferring DNSSEC services and we're always talking about the DNS hosting.

Since this is the ICANN community the most important thing to keep in mind is there's an interaction with your registration services and moving your registration at the same time you're moving your DNS is fundamentally flawed because they are not coupled. They are not related and it is in fact most definitely going to happen to you without some best practices that if you try to move both at the same time your zone will in fact be invalidated and go dark for a period of time. It's actually pretty much guaranteed if you don't do it right.

RUSS MUNDY: The challenge of what we envisioned originally as separate pieces together in a single bundle of things. If you're not going to take steps that would allow additional DNSSEC keys to get produced and be somehow present in both the present and the gaining name server operator facilities.

You talk about cooperation and when there's not a desire for cooperation because somebody's losing a business that's not a very logical thing to try to use to approach it. The choices seem to come down to being able to functionally think about your name service as a

separate functionality from your registration services and then move them in a way that they are separate from the registration or you can unsign your name for a length of time and just not use DNSSEC for the period of the transfer. It really comes down to those two choices I think at this point.

JIM GALVIN: I'm trying to stay away from the option of unsigning the zone. You're right, if you allow that as an option then you just unsign, do your transfer, get everything set up on the new side, resign and the world comes back together. If your goal is once your signed you want to stay signed then the fact of the matter is that you cannot move them both at the same time because moving registration and DNS at the same time requires cooperation and very tightly coupled cooperation between the losing and gaining in order to make that work and ensure that your zone does not invalidate.

If you're going to say that you don't want to tightly couple them and you don't want the cooperation then you move one or the other first. You move your DNS first and then you move your registration but the problem with moving the DNS first gets to the point that Michele was making earlier which is – if I'm dealing with bundled services, I'm going to have my bundled services at the gaining registrar and bundled services at the losing.

Even in that case if I don't cooperate on the zone configuration I have to bring up DNS services at the new registrar which means I have to point to the old services at the old registrar in order to move the registration

transition and effect all the changes. I'm getting a little too technically into this but trust me, it doesn't work and that's the point.

MICHELE NEYLON: I don't' doubt you at all and what I'm going to do is take one more question and then we have to move to Mr. Abley.

MARK SIDON: May I just point out that stock brokers are instructed by their shareholders to transfer vast amounts of assets every day from sending losing to winning firms and they do this using automated systems with no problem. It's not rocket science. They're just required to do it by the regulators and they do it.

[MALE SPEAKER]: But if they were convinced to use DNSSEC they wouldn't be able to.

JIM GALVIN: I had two points that I wanted to make and we've only covered one. Functionally separate registration from DNS and we've had a long discussion about why that's important. The second point here and we've heard about it a few times is you do need to be able to support the import and export of a key. On the registration side, you have to be able to import keys from other DNS operators. On the DNS side you have to be able to export your key information so that you can take that in as a registrar.

Those are the two minimal functional things that you need to do as a registrar to support DNSSEC, to support the existence of DNSSEC as opposed to actually signing yourself which is a whole different set of issues.

RON AITCHISON: Point of clarification, you're talking about importing a private key?

JIM GALVIN: No, more specifically just the public key information. You need the DS or DNS key record.

JOE ABLEY: I'm not here to describe reasons why any registrar should support DNSSEC. I think we have enough of that going on already. This slide set is really recommendations or some ideas that registrars may not have heard of for how they can make life easier for zone administrators. I haven't said registrants. I've said zone administrators for a reason.

Let's assume we have tool chains that exist and zone administrators have people who know how to run them. Examples are [inaudible 2:52:39.1] not open DNS, to do things like key generation, signing zones, KSK rollovers. I don't think anyone would claim that the quality of these tool sets are perfect but they do exist and they do simplify a lot of this and certainly a lot more practical to use these tool sets than to do any of this stuff by hand unless your really good at base 64 in your head.

When you initially sign the zone or you do a KSK rollover, as a zone administrator related to a registrant in some way there is a need to

publish a DS RR set in the parent zone. There is no standard protocol or mechanism for this. In fact what happens today for name spaces that incorporate registrars, you first figure out whether what your parent wants is a DS RR set or a DNS key RR set. I'm told it's about half and half. You open your terminal window.

You figure out how to run the command to create whichever of those is relevant and then you cut and past the multiline base 64 data with various integers in various orders, sometimes with line breaks, sometimes not, sometimes with spaces in between, sometimes not. You paste it into the form that looks different and every single registrar that supports DNSSEC and then you try again because you did it wrong the first time. You keep trying and eventually you either call the Help Desk or you give up. That's the current user experience.

What I'm going to suggest is that sort of thing there, again with and without line breaks, those are DS records. DNS keys are much bigger generally. This is not a useful thing for a customer who generally struggles to figure out what domain name means. This is nonsense. There is no direct way for the tool the zone administrator is using to get that stuff into the parent zone.

There is this draft in the ITF, if you're not familiar with the ITF and you don't know how to find drafts, you can just Google for that thing in gray. That's the name of the document. The idea is that you publish the information that needs to go in the parent zone in the child zone and you can sign it. Again, doing these things manually doesn't make a lot of sense but imagine for a second, suspend disbelief and imagine that the

tool chains that people currently manage to sign zones with were able to insert these things automatically in the zone.

What we've done at this point is that complicated base 64 nonsense which is effectively binary data is being published as binary data using a protocol which is used handling binary data called the DNS. This gives a means for anybody on the internet to be able to look this stuff up without having anybody cutting and pasting it.

WARREN KUMARI: It's been adopted by the Working Group and I think it's being last called in the next week or two.

JOE ABLEY: If you're interested in the specifics of the document and providing support for it or not or reviewing it and giving comments then Warren will be happy to talk to you afterwards.

There have previously been some suggestions that if your zone is all ready signed and so your interaction with your parent is as a result of a KSK rollover then your parent might be automatically able to retrieve information. I believe it's true to say that this is a little contentious, the idea of automatic changes without a specific request from a client or from a registrant but at the very least and Warren's draft goes into some detail in this.

You could use the data that's in the DNS to at least pre-populate these fields on web pages which otherwise cause problems for cutting and pasting. You could ask the registrant clearly to compare this perhaps or

just confirm that this change has happened rather than having the cut and paste nonsense. There is a related draft written by Wes H and this is called CCYNC and if you like the idea of being to pre-populate forms as a registrar for what the child should be asking for, then this is a way of doing that for NS records and any records for the [inaudible 2:58:08.5] so host objects in some registries.

It's related and if you think the first idea is interesting but this one is not specifically related to DNSSEC. DNSSEC has been taken out of that. The recommendation, if you weren't aware of it, perhaps have a look. If you intend to do DNSSEC anyway and I said this is not DNSSEC advocacy. If you already intend to do DNSSEC for perhaps some of the reasons Dan York came up with, then this might be worth looking at. Show your developers this thing. As I said, you can Google which is a verb the draft if you can't find it otherwise.

JACQUES LETOUR: With the CDNS and the other proposal to pre-publish information in your existing zone, is there a way in there that we could pre-publish information from the gaining registrar, gaining DNS operator, DNS keys and then do without the key relay stuff Mike talked about?

[MALE SPEAKER] I haven't seen any specific proposals. Off the top of my head you're talking about potentially two different zones being published by two different providers. You only get to delegate one of them. It's not obvious exactly how you'd communicate both sets of information but I suppose if you look at it in the sense that you want to be able to publish

two DS RR sets, one for the key that the previous signer used and one for the new one then that would be a way of doing it. That's not specific to this. You can do that in any case.

[MALE SPEAKER] I'll give a partial response, too. What you would do in that case and this gets to one of the issues that I talked about. You have to be able as a losing registrar also DNS hosting provider. You have to be able to import the key information into the old zone so that you can do this mechanism and trigger it up so the registry will come back and get a new key set, create new DNS record.

What you want is to be able to put an on deck DS record into the zone and get it upstairs. The only way to do that would be to get the new provider to export it in such a way that the old registrar. The new DNS provider has to export it and the old registrar can import it into the zone so you can trigger it up.

[MALE SPEAKER]: I think the general answer is it makes things easier in the way that I've described but it doesn't make that problem easier, only the component for publishing DNS records.

JACQUES LETOUR: I guess the point is if we are going to change the process here to do some automation, we might as well do the use case for the entire automation and do it once and get it over with.

WARREN KUMARI: That's purely an administrative thing. There's nothing really technical there. The gaining person just says, "Please publish this as well," and that's an out of band otherwise you're going to have some weird, funky new protocol where gaining operators can speak to registrants and something. I think they just e-mail them a record saying please stick this in your zone as well. There's no way to screw that part up, I think.

[MALE SPEAKER]: The observation that I make is yes, to a first order all of this seems simple but what it highlights is the fact that there's a relationship between registration services and DNS services and it's a pretty deep one. The problem that you have while you're right it's just an administrative step and it seems pretty straightforward to get it into the registrar, one of the things we observe is registrars don't always – and Joe highlighted this, there are various mechanisms for importing that key and pushing it up.

That even presumes that they let you do that. If you're using the registrar as a DNS hosting provider they may not give you the ability to upload arbitrary records and in particular they won't let you put some other key in there because they're already doing the DNS. There's no reason for you to put a key up there. That becomes part of the problem, too.

WARREN KUMARI: Yes but that seems very far removed from the DNS? That's very much an interaction between registrars or providers. That's a different set of protocols, nothing that can fit in here.

[MALE SPEAKER]: You call it far removed and I'm trying to say that it's not far removed. There's a relationship here that the people need to know about. Registrants need to understand that. There's a coupling that's simply not getting traction.

[MALE SPEAKER]: An extreme example of it is if you have DNSSEC being done by your hosting provider which is also your registrar because there was a convenient button to check at some point. It might even have been checked by default so you perhaps as a registrant don't even realize that you're doing it and then you decide to transfer things to another registrar that doesn't even support DNSSEC. Then you end up with DS records in the parent zone. You have no ability to remove them so you can go unsigned.

The whole thing sounds a lot like market confusion about what services people are actually buying. My experience as someone who allegedly knows what he's doing is that you can go to some of the more popular registrars and get so bombarded with marketing that you can't actually find any of the actual DNS to even know what it is that's going to happen when you click Next. That's hard for someone who knows what they're doing. It's extremely hard for an end user who doesn't.

[MALE SPEAKER]: Exactly, which gets us back to the point that Jacques made earlier. At some level, this could just be about best practices for registrars in order to make the right thing work but the best practices that are necessary

really are a change in business model for registrars and they might not like that too much and that creates its own set of issues.

MICHELE NEYLON: That was so easy and such a nice segue. It's not that I totally disagree with you all the time, just a lot of the time. How I ended up coming into these DNSSEC things was because I remember sitting through a presentation several years ago from Dr. Crocker going on about some shiny stuff in DNSSEC and I followed the presentation all the way through. The entire thing was done from a DNS operator's perspective and totally ignored the contractual obligations that registrars have. That was the disjoint.

As an ICANN accredited registrar you are bound by a contract. The contract contains a whole set of provisions and also pulls in a bunch of other policies. These are binding policies. They are not open for debate or discussion unless you want to redo them completely. Domain transfers is one area there. It's as if in the technical community you went off on one track and on the policy side they went off on another track and the two sides weren't really talking to each other which is a little bit of a problem. I'm being told time so I'm going to do something I hate doing which is give Dan York the last word.

DAN YORK: Michele, thank you for moderating this entertaining panel. I guess a question I would have for you but I'm seeing the same note from Julie that we're out of time. You're here with a group from the technical community. One of the things I would like to ask from you is what can

we do to interact with the registrar community to get more registrars involved here or to get more feedback from registrars as we do this? How can we work with you?

MICHELE NEYLON: That's a fantastic question. It's one of these things that I think we've all been struggling with. I think it's an ICANN problem. The silos of interest, it's like the ccTLDs are in one place, the hardcore geeks are somewhere else. The Infosec people are off in a corner and while an exchange of ideas and discussion and cross communication would really help remove a lot of headaches from time to time, it doesn't seem to happen. Unfortunately, I don't have the perfect answer.

I think what is helpful is maybe to get the message out that you guys aren't trying to ram DNSSEC and other things down people's throats because the message we were getting from some quarters was, "Oh my God. You have to do this or the end of the world will come about within the next 30 seconds." It's the end of days.

There is definitely a disjoint between the technical operations area and the non-technical operations. There are very few people who play in both camps and a lot of the registrars who come to ICANN meetings send their sales staff. They send their legal teams. They don't send many of their operations staff. Okay, I will pick on GoDaddy because they have sent more of their technical operations people. I see Ben Butler over there but that's an exception to the rule.

I'm not sure what the solution is but if any of you want to talk to registrars in general, want to buy registrars drinks which I would

encourage. I'm not hard to find. I'm currently the Chair of the Registrar Stakeholder Group and if they choose not to re-elect me I'll probably still know most of the registrars. Thanks for having me.

JULIE HEDLUND: Thank you everyone. Please join me in thanking our panel and Michele. Now we're going to move along to a couple of presentations on root key rollover. I would ask Ron Aitcheson and Russ Mundy to come up please.

RON AITCHESON: This is a discussion. My name is not Al Gore. I don't claim to have invented any of this stuff at all. I'm going to talk about one person's view of what the problems are and going to that last millimeter. Now, one of the points to make here the cultural differences between all of us in this room. The major one is how you spell "metre". Some of us spell it with E-T-R-E. Some of the more ignorant people in the room spell it with E-R at the end.

My name is Ron Aitcheson and I publish the DNSSEC for rocket scientists which is visited about 200,000 times a month on the web. That's my interest in this DNS stuff and specifically DNSSEC. Really the title on this slide which is really meant to be relatively humorous is really asking us all to remind me again why we are doing this DNSSEC stuff.

We tend to focus in on all the techie bits and bytes and all the rest of it and forget about what we're actually trying to do with DNSSEC. It's not really about securing DNS itself. It's about delivering stuff to the people who use the internet, the end users. That's my contention.

If you ask somebody about DNSSEC, it depends who you ask but you get this classic RFC stuff thrown back at you. What we're doing DNSSEC for. It's authenticated, authoritative source integrity PNE all that good stuff. My question for all of us here is so what? No big deal, frankly. Explain that the my grandmother and I'm very happy. You can't explain that stuff to your grandmother, can you and it's your grandmother who will ultimately use this stuff. I don't want to be particularly sexist about this so your grandfather as well.

The reason we're doing this is because applications can use the results. Browsers, mail, LDAP clients, think of any application that runs on your current PC and if there was a secure interface, if there was secure data coming from the DNSSEC they could all do different things. That is my contention. So what do we have to do to make our applications aware of or how do we communicate or how do we signal DNSSEC's ability back to end user applications.

We're really looking first of all at a DNSSEC aware API. There are three issues here. DNSSEC aware API for Posix and Microsoft. DNSSEC aware validating, there's a difference in my view DNSSEC Aware and a validating stub or caching resolver. There are implications for root distribution and rollover and what we can do at an area resolver level is I think very different than the kinds of mechanisms we needed. An area resolver level very different than those to distribute change root keys down to two billion devices.

Just to remind us all about how data gets back to applications – this is one of those reverse numbered things where one odd number stuck in the middle of it just to complicate. When we get data back we're coming

through this route here. If we look at the data that signal back it's a DNS query between four and three down to the error resolver typically the TTL data is passed back at that point. 90%, 95% these days of the cases it goes through a DNS proxy of some sort called the DSL or cable modem.

There's another cache in there so we've gone through at least two cache mechanisms. We pop into the stub resolver. Two here in the PC, mobile device, whatever it may be, another cache involved at that point and then finally we have this weird API. At this level it is classic DNS query stuff and in between 1 and 2 we're getting a different API, get host by name, get address info. At that point we lose TTL data and DNSSEC data. 100% gone, finished, doesn't exist. That cache which is maintained in all browsers is a blank cache in terms of DTL and certainly in terms of DNSSEC.

Here's what we've got from my brief research in all of this. There are three approaches providing DNSSEC aware API. The first one is a draft that expired as far as I can make out 18 months ago, has not been renewed but was implemented by DNSSEC tools. It uses an extended val_getaddressinfo. No bogus capability, no TTL provided. It's configurable, there's a bunch of issues to do with it. It provides the entire interface that DNSSEC offers but maybe too much.

[Inaudible 3:16:45.5] bound is providing a huge fat interface but one of the things I think is interesting about that is that it's conflating, insecure and indeterminate which means that there are four possible solutions that DNSSEC signals back two of which are interesting to the user. I think Lib Bounds has done a good job there. Lib DNS from IFCs provided a solution but does not signal whether or not the results – it validates the

results but does not signal back whether or not they're secure. There's no way the application knows that the data was secure or not. It validates it but if it fails to validate it'll fail but that's it. It fails or succeeds, end of story. There's nothing in between.

I cannot tell at an application level whether the data I'm receiving from DNS is or is not secure and that is the only question that's interesting. That's the only question that's interesting. Frankly, what's even more interesting about it is that's a one bit change on current other get info interface. Secure/insecure byte. It's one bit that we're interested in at the application level. If we had one stinking bit different across that interface we could do all kinds of interesting things with it which I'll maybe talk about it this afternoon.

What do we do here? API outstanding, there's nothing standardized. There's nothing in ITF or Posix. What we're missing here is we need a standardized API either through ITF and/or Posix IEEE. It works with and without DNSSEC so that we know that we get secure or insecure data and it won't and it works whether DNSSEC is implemented or not. It's consistent across the universe. Every application knows whether it's got secure or insecure data no matter how it's obtained.

Primary status okay fail as today. The auxiliary status none secure, it is as I said a one bit change but it would also be useful to solve. I have a thing about missing TTL coming back in that interface. That's just a personal hang-up. Don't take it to heart. If we were to change the interface, if we were to create a new API then I believe it should have TTL data in there as well as DNSSEC data. I'll be happy to talk about that in questions.

The second point is DNSSEC aware or validating stub and/or caching resolver. Sorry for these huge long terms but there are subtle differences between DNSSEC aware and or validating stub resolver most of which today cache so that's why the terminology is as gruesome as it is.

Here are the issues about stub resolvers. Two different architectures in my view – one of them is use AD, interpret the results, pretty simple, needs an API clearly, no trust anchor required. The area resolver does all the work. The disadvantage really is that last point. I have a real problem with validating area resolvers. I believe they're a D-DOS attack waiting to happen and to have all these area resolvers doing all the heavy lifting.

Let's look into the future and hope that one day, one or two or .003% go to 90% validating domains then just think of the work that's being done especially with TTLs these days of two or three or five seconds. We're seeing these lunatic TTLs, we're seeing records. Just think how much work these stupid area resolvers have got to do. It's just a staggering amount of work. Especially when you get idiots – you see them writing on the mail groups on a regular basis. If 204K is good maybe 4084 or 4088 is even better, the theory being that if one glass of wine is good for you, good for your heart then a bottle must be fantastic.

You get people who don't really understand what effort they're putting out there. They just don't' understand DNSSEC even at that trivial level. Secondly there's no work at the local interface. If we look at validations it's fairly complex. We obviously still need the API. There's a lot more stuff to be done there. We can use a full resolver and then BINE, sure.

Use the CD bit, needs a trust anchor but it does distribute the validation load so each individual PC is not really a source of D-DOS directly.

Again just looking at this validation, there are two possible solutions there even in validating stubs full resolver and use CD full resolver the code base exists BIND, Unbound, others, does not use the area resolvers for caching purposes. I think that's a problem personally.

Mobile data volumes, we're getting a lot more data coming down to the end user so if we do any validation at the end user's device we increase the data volumes. We've all talked about that. That's fine. Networks are getting faster and faster and faster. Is it acceptable in the mobile world? Is that data volume increase acceptable there?

Finally if we do full resolver at the desktop, every single device is exposed to all the nasty guys on the web. Is that a smart thing to do? That's the job of the area resolver. If we use the CD bit we can use the area resolver, use its caching functionality and more particularly as defense against the nasty guys. Mobile data volumes are lower, there's less data flying backwards and forwards. We're not doing the whole hierarchical search all the time but mobile volumes are lower but it does need code based changes.

My take on the stubs in terms of desktops, their standing stuff there is DNSSEC API obviously and all methods all possibly exist. There are at least three architectural solutions that I've outlined here. We need some code changes for some of them and we may need to solve mass root key distribution problems. Local validating stubs are orders of magnitude change in terms of distribution of the root key.

Final point, root key handling – let's get down to this one. Here's just a throwaway slide. Sorry it's a very busy slide. Here's my first take. I don't see a difference between getting the root key from DNS and getting the root C sets. I see no logical difference in them at all. I see a lot of people getting uptight about this and I see what the root ca guys get away with and it's frankly terrible. They get away with it because they started it in 1992. You're just more nervous. Getting root keys via HTTPS has got to be someone's idea of a sick joke.

Let's look at key rollover now. My contention and I have changed my view on this. I'll readily admit it. I wrote a book in 2005 for DNS and BIND for where I advocated constant messing around or constant processing and I have changed my mind on that. I don't believe, I think we need a constant test bed is my proposition. It's not unique to me. There are other comments made to this rollover procedure. I think we need a constant test bed, a DLV like approach.

I think not using either/or but within the hierarchy a DLV type system where the .harper that needs to be constantly there so we can test because there is no single point in time when we can make a change. If we do a rollover this year or whenever ICANN has got to do it, in 2027 when half of us in this room are dead, people will be looking back saying, "They did that way back in 2004, 2014 there were only eight people DNSSEC at that point so yeah, it went pretty well. Now that there are two and a half billion people using DNSSEC we're going to have a problem." It's not a realistic proposition. We need a constant test bed in my point of view.

I believe keys ought to get stuck under root.harper. You can have different ones. You can have test ones, emergency ones, next ones, backup ones, a whole host of stuff. Stick them under DNS keys or create new RR type if you want. Rollover, you fail to validate use the emergency key. Maybe it's as simple as that – maybe. I'm throwing this stuff out because problems we all know is not the key change but [inaudible 3:28:09/8] in rollover.

That's the big problem because it implicates every resolver out there will support that new algorithm. The [inaudible 3:28:25.5] approach means all the resolvers have caches which means that we can use the area resolvers as ways to minimize the two and a half, three billion devices that will start sucking new root keys when we rollover hopefully at some point fairly soon. Well, maybe not in my lifetime.

In terms of the key, it's either too late depending on who you believe with all this NSA nonsense. It's either too late to change the key because it's all ready compromised or we have until 2027. Why do it before? I'm constantly shocked. Some of you looked at the expiry date on root ca keys on your browsers. Have you ever looked at them? I was staggered the first time I saw it. 2027, 2028 – I don't believe this stuff. Guess what, that's what it is. Why do we have to roll this stuff over? What's the attack vector on a compromised root key?

What is it? That's a question. What's the attack vector? Do I have to suck onto every instance of every root server, all two and a half, three thousand of them? I have a man in the middle on one little area resolver? Tell me what the attack vector is. Are we being realistic? Do we even need to worry about it? Finally if I look at ICANN's security

process and I compare that with the X509 CA security process it seems to me that ICANN is greatly superior. I think there's an outstanding issue. We need an inbound RFC process for root algorithm changes.

I think we need it. I think it's based on something similar to 5011. I think it made a huge leap forward in terms of regularizing our terminology with keys. I think we need to build on it for the root. That last slide summarizes everything I've said and probably the best thing I could have done was to put that slide up first.

[MALE SPEAKER]: Let's take a couple of questions here. Warren you were raising your hand in the midst of this.

WARREN KUMARI: It sounds like what you're saying is, "I would like a pony," and luckily there is a pony for you. Google sponsored Paul Hoffman to write API specification that largely does everything you've asked for. Then VeriSign and Onet labs have implemented this. It's a DNS API. It's an open source and it's being deployed by the Onet labs and VeriSign and a lot of other people are picking up on it and you can get it today. It provides you Gatehost or something similar, but on steroids.

It gives you DNS signed gives its own validation. It gives you the TTL. It lets you know which trust anchor set you're using. Basically it's all singing and all dancing and it does most of the things you asked for at the beginning. On the root key rollover stuff, I won't go into that too much because I think Russ has a whole long presentation on that. But on that end the CA stuff, there's also DANE which let's you use either the

CA type certificates or if you think that the ICANN system is stronger you can decide to use that instead or you could choose to use both.

RON AITCHISON: Explain that last bit one more time.

WARREN KUMARI: What DANE does is it lets you publish.

RON AITCHISON: I see DANE as for the perennially paranoid.

WARREN KUMARI: Sure, a lot of people are deploying it.

RON AITCHISON: I accept that. There are a lot of perennial paranoids, yes.

WARREN KUMARI: Okay, sure and for key rollover there's also talk about doing basically something like CDS or CDNS key but for the root anchor or for the root trust anchor instead or as well. Then anybody that's using DNS API would presume to be quite happily suck that in.

RON AITCHISON: Two formal questions. Firstly, go through the list of people who are supporting this API?

WARREN KUMARI: The API was released a week ago and so far there's been a bunch of excitement. You're talking about let's build an API. That's been done.

[MALE SPEAKER]: I have some slides I can show. I presented this on Monday at the Tech Day Talk so you can look for those slides there.

RUSS MUNDY: One comment I'd like to put in with respect to the API discussion, the problem has not been lack of API or lack of effort to create an API. The problem has been more likely multiple APIs none of which have been fully and broadly accepted by the applications community. There are a number of applications and application-centric things that have elected to say, "We don't like any of them and we want to do DNSSEC and so we're going to develop our own." I think time will tell whether or not the existing ones are good and will become a singular, common thing.

I'd say it was about eight years ago, the one that's in DNSSEC tools which happens to be a project I'm associated with. We had everyone's agreement they were going to go off and implement that. Everybody started but we got no applications uptake on it other than the applications that we did. We have a group of them including a full browser called Bloodhound that does everything but it's not been community-wide. People haven't picked up the ball and run with it for all types of different reason.

RON AITCHISON: I'd like you to expand on those reasons. It seems to me and this is one of the things that I the Google API might have a problem with I'm going to use the historical analogy here. The drive for standard APIs has come mostly through the Posix industry for DNS interfaces been implemented in C standard libraries pushed out CC++ and then a bunch of folk have put wrappers for Python, Ruby, whatever it be on top of that. That's the driving force. What's coming out of Posix with some support from the ITF. I guess my question is why has that not so far happened with the current proposal and two, back to you are you proposing to go down that route or are you just throwing it out there?

RUSS MUNDY: In terms of the work that we've done and others have done, it wasn't just our group. It really was an ITF related effort that was not actually ever picked up by a Working Group. A lot of it was that the applications folks were more interested in a full replacement for the DNS API rather than just additional API code and specifications that would allow you to do DNSSEC things in addition to the existing DNS things. I think that was one of the impediments to it not going further. Operating system vendors are indeed looking at the DNSSEC API needs at this point in time. We'll have to just observe and see what happens.

WARREN KUMARI: The plan is that this will either be Posix or open Unix standards or the open group, whatever their other set of names are. That's always been the plan.

[MALE SPEAKER]: I just wanted so say that I think when Paul Hoffman started off his project to work on this API specification, he was very smart that he engaged the applications and browser guys very early on and got their feedback. One of the outstanding features of this is that the API is designed to work with any number of event libraries because each browser uses their own event library underneath. That was a design feature from the start. From our talking to them, they are very excited about the release that was made just last week.

WARREN KUMARI: This is a presentation on a report that was issued by the SSAC Security and Stability Advisory Committee with respect to the DNSSEC root key rollover. It has been presented before and I'll go through it fairly quickly and then open up for questions. As much as anything I'd like to give folks a chance to ask questions and interact.

The general content of the advisory is it lays out the topics that are viewed SSAC as important things you need to look at, think about and consider as you go forward with the root key rollover. I won't go into the specifics in depth so we have time for questions but you can see the list is moderately long. It's a fairly technical report for SSAC. It's not something you just want to wade into if you're not all ready familiar with DNSSEC.

The first recommendation is that the root key management partners which are the ICANN, VeriSign and NTIA need to undertake a significant communications effort worldwide to get the word out that this is happening. As Ron mentioned there's not many people using it now and in a few years it might be massive numbers. The presentation by Geoff

Huston earlier today indicates that 6% or so of the Internet is doing validation. People need to know that it's on the way. Communication to the world is a very important effort.

The next recommendations are really pointed at things that are being operated by middle box, by vendor, by home users and when you get into that realm the world grows mighty fast in terms of numbers and counts. Again, this is a suggestion by the SSAC that the ICANN Staff should lead the effort to create a test bed that would provide a place where these could be tested. The third recommendation, we need to have a clear definition of what breakage means. A lot of people use the terminology, "Golly, my DNS just broke." What does that mean? It's really very important to have a definition of it before we start the key rollover things.

Recommendation four is again a recommendation towards ICANN Staff. There might be a need to roll back the root key to the current root key. For some unknown reason nobody can think of why you would want to do that at this point but it is not beyond the realm of possibilities so you should have all ready thought about what the procedures and processes that need to be executed if that did become a reality.

The fifth recommendation was for the ICANN Staff to lead or otherwise coordinate and encourage the collection of as much data as possible and the right type of data with respect to this upcoming root key rollover whenever it might happen so that there would be real data available to examine with respect not only this event but to compare to future similar events.

That is the end of the recommendations. I did want to leave time for questions and we have seven minutes. Do we have questions? We also have Duane from VeriSign who's willing to come up and answer questions in this topic area as one of the folks involved in the root key rollover.

[MALE SPEAKER]: Could you go back to the first recommendation and put up the slide? Just out of curiosity, it says here to talk a lot. Talk about what? I'm being kind of facetious but in a sense what do you think should be communicated besides just communicating?

WARREN KUMARI: One of the challenges involved in doing this is most people who would be using the DNS would likely have absolutely no idea that DNSSEC is there, that DNSSEC is being used by some people and that one of the critical items, the root key itself is going to be changed. We would not expect that it would affect non DNSSEC users but in the wonderful world of uncertainty of DNS, it could. The root key management partners need to get publicity around the fact there is going to be this change that occurs that could cause disruption and problems.

RON AITCHISON: If we look at the current recommendation in terms of key size it's 24K until the year 2030. Now assuming that does not change and something nasty doesn't happen in the intervening 16 years why do we need to change the root – period?

JOE ABLEY: I think there is more than one reason to roll the root zone KSK. The idea of rolling it because the crypto is inadequate is I think last on anybody's list of reasons as to why it should be rolled. The more compelling reasons in my opinion are operational currency. If you've never tried to do it you don't know if you need to do it.

The second part, however much we might hope that the procedures protecting the KSK secure materials remain impenetrable forever you have to prepare for the eventuality that there is a compromise of some kind or some loss of trust in the current key materials. If you believe that then a roll at some point will be necessary in which case you may as well get practice in a controlled environment rather than having to do it in a panic.

WARREN KUMARI: Two additional things, one the HSMs have a limited lifespan on the battery. Eventually this is going to have to happen. Assuming you can restore it to the same HSM and could still get the same HSM and it's still…It's an entertaining and potentially somewhat exciting job to do.

RON AITCHISON: I don't think there's any difference between creating a new key and re-creating a key – none at all.

WARREN KUMARI: Actually there is. If you create a new key you're doing it on new hardware in parallel, you're not monkeying with the existing HSMs which gets fun.

RON AITCHISON: That's not my understanding. If you want to recreate the key because your battery life is exhausted, your HSM is dead then you bring the same group of people together in the same room and do the same fantastic things to create the same key. You must be able to recreate the key – period.

WARREN KUMARI: No, you do not ever want to be able to completely recreate the key or somebody else could.

[MALE SPEAKER]: There's a very, very, very, very big difference between transferring the key between two HSMs and creating what amounts to an additional copy of the original key.

JOE ABLEY: I was somewhat familiar with the processes for doing this because I was involved at the time the root was signed. There is a backup copy encrypted set of key shares that are stored in the same physical protection as the HSMs that can be used to restore exactly the keys that were generated to start with onto the same model of HSM authenticated with these trusted community representatives which are known an RKSH, Recovery Key Share Holders.

There is a procedure and it's documented. You'd fly those people back into the facility. They would make use of their keys and the whole thing could be restored. The last recovery for batteries going bad and HSMs is covered in the existing procedures.

MEHMET AKCIN: I'm quite familiar with the process as well.

WARREN KUMARI: For those that don't know, Mehmet was the person who was striking most of the keys in the original key signing ceremony.

MEHMET AKCIN: I agree with what Joe said and definitely the fact that battery lifetime or HSMs need to be replace is not the real reason. I think one reason that has been discussed is that if you don't change something and keep it as a factor for a long time people are going to embed it in some places and that's going to break things even.

To get back to your question, security-wise it's highly unlikely and to us, the rest of the ICANN Staff it also very highly unlikely but the fact that if someone gets this KSK and embeds into a browser and starts doing something, the next thing we know because this has not changed in the last 10 years and suddenly we change, we are going to experience more problems. Now if we change it more frequently then it's another issue. We need to take this time, maybe four or five years.

[MARY KAY]: I just want to iterate also, I think any of you that have any used any kind of certificate and if you never had a certificate expire and go, “Oops, oh shoot,” then I want to talk to you. This really is a process issue and I will agree with Mehmet. We’ve been very careful trying to figure out how you roll over the root and what do you actually need to do on a step by step basis because you don’t want to screw up. You may, hopefully you won’t, but the more practice you have at it the better. You don’t want to be in the situation where you’re panicked about it to try and do I the first time.

WARREN KUMARI: There was also a proposal that wasn’t ever followed or implemented that when you first signed the root then the week after that you roll it and then a month after that you roll it and then a couple of months after that you roll it. That way you actually get some operational experience with this. It would be early enough that people aren’t relying on this.

Currently if you roll the root key through some manner and it goes poorly there will be some unhappiness. In five years time or ten years time and this is more widely deployed and you screw it up, there’s going to be a lot more unhappiness. There’s also having practiced this a few times but also doing it while there’s less people relying on it as your first roll.

[ED]: I want to say what he just said. The sooner you do it the danger of it going down. If the population is growing, do it now before 10% become 20%. That’s one. The other thing is the current hardware that’s being

used I'm involved with these ceremonies we start losing the HSMs and we are actually able to have a soft crash. We have four of them right now with the keys. If you lose one and are down to three, it's still okay. We can recreate that but we haven't tried it though.

The other reason to roll is that it gives us a change to tech refresh the entire system. Right now it is like satellite years ago it's up in space now, the hardware that's being used right now is technology from at least five years ago. Looking at new laptops, the entire process could be revamped for just generating this. Not changing the procedures and the architecture but the laptops, the hashes we're using, the scripting we're using. This stuff is really old technology that's in the process and coding a new key let's put that aside and just have it over here as a replacement.

RON AITCHISON: First of all, I absolutely agree that we have to do this but my point is this. If we focus on a big bang rollover in 2014, what happens next? Do we have this huge big conversation about the rollover in 2018 and 2020. We need to be able to practice these procedures. We need to have a constant test bed, 100% of the time.

We need best common practices that define how we will recover from root key failures. I don't think there's a standard requirement there but I do think there's a best common practice needs to be documented there. These things need to be permanently available. I think the DNS tree is perfectly adequate to support that. I think it could be done under the DNS tree that exists right now but we need a permanent test bed. If

anybody believes we know what people are going to be doing 2017, good luck with that.

MEHMET AKCIN: A few things, making things more automated and more future ready. This was actually part of the transparency process where we really did not go that route and make everything step by step even if we could not make it automatic.

One thing I would have loved to see in the SSAC recommendation is I have utmost trust in the ICANN Staff but I think there should be a suggestion towards a mechanism that validates and checks externally by some non-ICANN staff. Some subject matter experts, some security experts that the process design internally because some of the process when you are outside you don't really know what the process is. There should be some sort of mechanism that mandates ICANN to be checked by non-ICANN staff.

[MALE SPEAKER]: Thanks everybody. This has been a very invigorating panel. I think it's time to move on to our next one.

JULIE HEDLUND: Thank you everyone and please join me in thanking Russ and Ron and Dwayne. Now we're going to move on to a presentation from SIDN Labs, DNSSEC monitor.

CRISTIAN HESSELMAN: I'm with SIDN, the registry for .nl that's the Netherlands. I'm going to be talking about the DNSSEC validation monitor which is work that has been done by my colleague Marco Davids. SIDN Labs is the R & D team of SIDN. SIDN is a large registry in Europe. We currently have 5.4 million domain names and we're currently the largest DNSSEC zone in the world. 1.7 million domain names have been signed at this point. This is also why DNSSEC validation is an important aspect of our work.

The system I'll be talking about today is the DNSSEC validation monitor. It's basically an experimental service that creates a bridge between the validating side as ISPs and the signing side as registrars. At this point when there's a validation error at an ISP, the registrars usually don't see that. They don't notice and let's say the pain is being felt by ISPs and the place where the errors got created, usually unintentionally. This is where the service comes in. It informs registrars of validation errors that occur at the ISPs and the goal of the service is to reduce validation errors at Dutch ISPs to stimulate adoption of DNSSEC validation.

We started with this work because we noticed that the number of validation errors rose quickly. This was mostly due to transfers of DNSSEC domain names to registrars that did not support DNSSEC. Back in October 2012 we found out that about 10% of the secure domain names that were transferred to registrars that did not support DNSSEC and therefore validation did not work anymore.

[MALE SPEAKER]: Is that because of DS record?

CRISTIAN HESSELMAN: Yes. We talked to ISPs and we also have a tool called the DNSSEC Portfolio Checker that enables registrars or other people to check if their DNSSEC domain names actually validate. We used the logs of that to also check how many domain names did not resolve. We know that low validation error rates are important to them for three reasons.

The first one is validation errors cost money because an error results in a support call to the ISPs support desk. They say usually this costs 50 euros per call. That's roughly $65 U.S. Another reason is that customers of ISPs don't' really understand why a site goes black as a result of a validation error while the same site still works on the ISP of their neighbor so it's difficult to explain this to ISP customers.

This is what the service looks like. It's actually pretty straightforward. On the left of the picture are the validating resolvers at ISPs and they basically send a feed of validation error information to the validation monitor server which is a server than sits at SIDN. We use the Unbound resolver by NLnet labs to check again if the domain name doesn't resolve. Then we do two things with it. We generate an e-mail that we send to the registrar to which the erroneous domain name belongs. We also send an overview of domain names that don't validate to our support desk and they then call the registrars in question.

We currently have four ISPs signed up to this service. It covers a couple of million subscribers. We're using it ourselves of course. We'll soon be connecting three universities to this system. This is the DNS signing uptake in .nl so we started in July 2012. We gave registrars discounts on domain names on registrations if they turned on DNSSEC signing and as

a result you saw it increasing quite steeply. We started with the validation monitor in May of last year. It's been almost a year.

[MALE SPEAKER]: Do you still give a discount?

CRISTIAN HESSELMAN: We still do it. If you look at the statistics, this is what it looks like. There's a clear downward trend. These are the number of errors we receive per day. It's going down. During this period the line was a bit lower. As you can see it increases here again. This was because one of the feeds from one of the ISPs was disconnected for a while. This one is a bit too optimistic. It should have been roughly like this. We're down in errors and that's what matters. We're currently at around 200 errors per day.

The same goes for registrars that had errors. This is the number of registrars with errors per day. You also see it going down from roughly 140, 120 to around 40. These are the types of validation errors that we are seeing. This is what's coming out of Unbound, that's the resolver we use to double check if a domain name doesn't actually resolve. The three most important Unbound specific error types are no DNS key, DNS keys as a result of domain name transfers, which I talked about before. This one is due to domain related errors and the last one is NSEC 3 errors so that's actually quite a few.

What's also interesting is through this mechanism, we get a feed from the ISPs. We also see validation errors at third level. This is an example. This one resolves okay and this one is a domain that also doesn't validate. What did we learn? It seems that this approach works because

we're seeing the number of errors going down and we're seeing the number of registrars with validation errors going down. We also saw validation errors at the third level which is something that we would not have been able to guess ourselves very easily.

We also noticed that sometimes the domain names or sites are broken for weeks because the registrars don't have validating resolvers themselves. They basically need to rely on this type of system to detect these errors. We also discovered that quite a few errors were caused by resellers which means that it's important we stimulate registrars to exercise more control over their resellers.

[MATT]: Matt for .sa, you both send an e-mail to the registrar and call them up. Why do you do both and how much does it cost to have this call center to call?

CRISTIAN HESSELMAN: We didn't check the cost to be honest but we get into contact with registrars quite often and we usually only call the registrars that have quite a few validation errors. If there's one we rely on e-mail but if it increases or if there's something unusual we give them a call.

JULIE HEDLUND: I have a question from the chat room. This is from Sebastien Castro. He said, "Could you ask if they charge for this service?"

CRISTIAN HESSELMAN: No, we don't.

RON AITCHISON: You put up the types of errors, what sort of corrective actions were you seeing at the registrars?

CRISTIAN HESSELMAN: Basically the corrective action is that we call the registrar and we ask them to fix these problems.

RON AITCHISON: What's their corrective action? Have you followed through on that?

CRISTIAN HESSELMAN: We monitor, let's say the number of errors actually go down.

RON AITCHISON: What I'm trying to get at is do you know what's causing the problem? You know what the symptoms of the problem. I understand that. Is there some root cause? Is there a procedural error?

CRISTIAN HESSELMAN: Usually it's people who are not familiar with the technology. We have experts as SIDN and we also often help the registrars to get these errors fixed.

RON AITCHISON: You've not tried to build up a category of corrective action.

CRISTIAN HELLELMAN: No, no, I would need to check with the person at the support desk.

[MALE SPEAKER]: Do you find the registrars reactive when you submit bugs or an error?

CRISTIAN HESSELMAN: Do you mean responsive? Yes, because as you can see the number of errors is going down. Usually they respond quite well.

[MATT]: There are two ways of solving problem. One is to remove DNSSEC and the other one is to fix it. Do you have any picture of what to do?

CRISTIAN HESSELMAN: That's a good point. Again I would need to check that with the guy at the support desk but we know that one problem that causes validation errors is because of the secure transfers. Initially when you register a domain name in our system, the DNSSEC box is set to yes by default. That actually creates problems because people don't look at it. This is what we opted for initially because we discussed this with the registrars and we asked if they wanted to enable it by default.

Yes, let's do it but if a domain name is being transferred to another registrar that doesn't really support DNSSEC but the check box is still enabled you still get all these validation errors. Now we're in the process of really doing this the other way around and disabling it by default so at

least we get of the validation errors caused by transfers. I hope that answers your question.

JULIE HEDLUND: Any other questions? Then join me in thanking Cristian Hesselman for a very interesting presentation. [applause] Now the moment you've all been waiting for, the great DNS quiz.

DAN YORK: You should find a copy of the agenda, because on the back of that you will find a place for you to enter in your answers.

[MALE SPEAKER]: Does everyone who wants one has one? I think we've got extras. There are in fact ten questions. The way this works is you can either play on your own and keep all your answers to yourself, or you can get together in a group and try to collaborate on answers. The top of the form has a spot for you to right your name in it. Please write your name on it. When you've finished answering you're going to be handing your answer sheet to the person next to you and then you'll try and grade each others answers.

Then we'll go over the answers. Sometimes there will be more than one correct answer. This means that you can get multiple points for each one of your questions. If you get a single answer wrong in the set that means that you'll lose the points for that particular question. There are some smart people here that would mark "A, B, C, D" for each of the question. Let's get started.

Question 1: which of these TLDs deployed DNSSEC?

A) .tel B) .ero C) .corp D) .xxx

Number 2: In a response what does AD stand for?

A) Authentication denied B) Ano domini

B) Access denied D) Authenticated

Number 3: Next, the D in a DNS query, is that:

A) DNSSEC off

B) DNSSEC on

C) DNSSEC okay

D) Data out

Remember, multiple answers could be correct. [laughter]

Number 4: Next, the QR bit in a DS message. Does that mean there's a QR code embedded in the message somewhere? Is it a quality response? The DNS message is a response or D) the DNS message is a request?

How many different root server addresses are there?

A) 12 B) 13 C) 22 D) 26?

How many IP addresses are there? [laughter]

Which generic top level domain was the first to deploy DNSSEC?

A) .gov, B) .org; C) .museum D) info.

If you were paying attention earlier during the meeting you might have heard a bit of back and forth on this. Okay, everybody finished with 6?

What does KSK stand for?

A) Key sign in key; B) Kill switch key;

C) Key switch key or D) Kappa Sigma Kappa?

What is the oldest currently registered domain name?

A) rootservice.net; B) symbolicx.com;

C) mita.org or D) glowg.net.

This is the great DNS quiz. This used to be the great DNSSEC quiz, but we had a hard time coming up with questions. So if people have good questions you're more than welcome to contribute them.

Nine, what is a DPS? Is it:

A) DNSSEC Problem; B) Delayed Protection Service;

C) DNSSEC Policy Statement D) Domain Preservation Society?

What top level domain or domains are hosted from the root servers? Is it :

A) dot.com; B) dot.net;

C) dot.arpa or D) root.

I should mention that Roy's the one that came up with these questions. [laughter] Can we have the answers pulled up? Swap your piece of

paper. There are no correct answers in question 1. None of these TLDs deploy DNSSEC currently. [groans] This means that if anybody selected anything for an answer you don't get a point. Sorry. If you left it blank you get a point. If you put "none of the above" you can get a point for this.

Number 2 – the correct answer is authenticated. Number 3 – the correct answer is C, DNSSEC okay. Number 4 is that one. DNS message is a response. Moving on. Number 5 – how many different root server addresses are there? We did clarify that was IPs. The correct answer is actually 22. If you marked off 13 or 12 you probably forgot about V6 answers. If you marked off 26 then you're more optimistic or less cynical than the real world.

Number 6 – which TLD was the first to deploy DNSSEC? The correct answer is .museum. We actually have the dates written down here. .Museum was a couple of months before .org. Number 7 – What does KSK stand for? Correct answer is A. Number 8 – The oldest currently registered domain name is nordu.net. A lot think it's symbolicx.com but unfortunately you're just wrong.

RUSS MUNDY: I can elaborate on that. Symbolicx.com was the very first domain name in the .com zone, but .com was actually an afterthought. .net, .edu and others were first. Nordu.net was the very, very first domain name.

MALE SPEAKER: Number 9 – We believe the correct answer is C but we hear some grumbling from the end of the table.

RUSS MUNDY: It is the DNSSEC Policy and Practice Statement. That is the full term.

MALE SPEAKER: You can get a point if you marked C or nothing. The very last one. Which top level domain is hosted from the root servers? The one and only correct answer is C. D is not a TLD. Let's get a show of hands. Who got more than 12 correct answers? Put up your hand. Who got 12? Anyone? Sure, that doesn't mean that somebody hasn't thought that they've gotten 12. The highest number anyone could have gotten was ten. As a prize we will remember forever who won, and you'll get to go first in the food line. Who won last time? if you happen to be here at the next one of these, you can let us know that you were the winners of this, and that is a great honor. Eight? Seven? Six? Did anybody only get one correct? Less than one? Okay, thank you.

SPEAKER: Thank you everyone. Bravo again. Lunch is in [inaudible 04:38:55]. You need a ticket. There are some more lying around if you don't have one. I'll be standing up there. This is what the ticket looks like. There's a little map on the back. If you go out this way, go to the right and past the registration area. [Coolen? 04:39:29] is the next area on your right and there are ropes across it and people looking for tickets. We'll be back here precisely at 13:30. Take your stuff with you, because you don't want it to wander off without you.

[TAPE CHANGE TO DNSSEC-2-26MAR]

JULIE HEDLUND: Welcome back everyone and this again is the DNSSEC Workshop here at ICANN and here to follow our wonderful lunch is Ron Aitchison.

RON AITCHISON: Listen, even my mother has a problem with my name. Don't worry about it Julie.

JULIE HEDLUND: He's going to be talking to us about some DNSSEC apps. Without further ado I will turn things over to him.

RON AITCHISON: This is really a follow on to some of the things we talked about this morning which is how do we get DNSSEC awareness down to the desktop, to applications specifically. Assuming we can do all that stuff what can we do with the data that we get through that API? In other words, all of the discussion so far and I think Geoff Huston made the point from earlier this morning. We've been talking so far about DNS push coming out from the top, down through the cctTDs, gTLDs, registry operators, registrars but that's not going to be successful, is it?

It's a good thing to do. It gets us started. We had to learn about all this stuff. That part of it has been very successful. We have to go through the painful learning experience. It's not going to get the Bank of Singapore or anyone else excited unless we can deliver value to the end

user. The only way we can do that is to make the end user's applications aware of DNSSEC, not the end user. No one gets excited by this stuff. It's not important. What's important is that the application delivers safe data you can do certain things with.

What can we do if we can deliver secure data through the DNS? What can we do with it? My take is there are no DNSSEC apps – period. None, they don't exist. There are DNSSEC aware apps but there are no DNSSEC apps. That's the basis of this presentation. What can we do with data? What data can we stuff into the DNS or what data can we take out of the DNS and what can we do with that data?

I talked about this stuff this morning and I'm going to spend no time on this. What I'm trying to say is that until we can make applications aware of DNSSEC data then we have nothing. If we have a DNSSEC aware API for Posix, for ms, capable signaling secure/insecure status that's the only two things that we want. We want two stati for secure/insecure, one bit on the interface theoretically. What can we do if it's secure? We know it came from the right place. If it's secure we can trust all DNS data. So what? Here's what.

Look at this diagram. This is what happens to DNS data from the authoritative source, number four in the top right there comes all the way through proxy caches, through resolver caches into browsers. That's the route of DNS data, the same diagram I used this morning. The problem is in the one two interfaces is what we're talking about. Number one happens to be a browser but substitute the word mail client, substitute the word LDAP clients, substitute chat clients, substitute any word you want there. A browser is simply an application.

If I can make that application DNSSEC aware, what can I do as a consequence?

Look at that diagram. This is a standard HTTPS communication. The first thing I do is a DNS lookup. I then get delivered as part of the HTTPS to the DNS dialogue. I then get delivered through to the TLS process, a certificate 509 SSL certificate. Increasingly today I then do an OCSP lookup and guess what I have to do? I have to do a DNS lookup to get the address of the OCSP service and I then communicate with the OCSP service.

Increasingly on the far side, what we're now saying because of mobile devices we're now basically saying the PC can say to the server, "I do not trust your SSL Certificate but I absolutely do trust you to tell me that your certificate is valid or not." Under those conditions, the server is now doing an OCSP check and that check starts with a DNS lookup.

Here's the point. In every case here we've done a DNS lookup before we've manipulated the SSL certificate. What is an SSL certificate? What's an X509 certificate? What does it do? It does only one thing and it supplies a public key. That's all it does. If we're talking about purely public keys DNSSEC it's a new world. We get public keys securely from the DNS implies that we have a DNSSEC aware API. We have three possible things we can do with just getting a public key from the DNS.

One is X509 replacement. Why do we bother? What's the function of X509? Simply, as I said, it provides a public key. If it can get it from someplace else, why do we have SSL Certificates? Opportunistic Encryption OE easier maybe even possible only through DNS. There's a contentious statement. Opportunistic Encryption which is related to

personal digital signatures, we're talking about Egov, all this kind of stuff.

If I can suck a public key then all of a sudden Egov becomes viable and it's possible. We're talking about structures here and a whole bunch of other things. This is only putting a public key in here. We have a DNS key record. We've got two methods at least of getting that stuff in there. There's a resource proliferation. We've all ready got a process for easier RR registration. I don't want to consider anything at all besides public key. I'm simply saying we can stuff other things in there as well. We can put other data in there, too. Let's just focus on what we can do with public keys.

Lets look at X509 replacement. X509, in my view, is just a method to get a public key. That's its entire value. If you look at it purely in terms of TLS, it's one of a number of methods you can use. You can use Diffie-Hellman methods of acquiring that public key. DANE's another method. Why not just say secure DNS? Why is that not just another method for TLS?

A public key obtained from the DNS is EV comparable, Extended Validation X509 comparable. There are four differences as far as we're concerned here. There's a regular SSL certificate that you pay $150 a year for versus an EV certificate that you pay $500 a year for. If you buy an EV certificate, they verify that you own the domain name. Guess what DNS does? If it's your DNS obviously you own it. That's the whole point of the ICANN system, the DNS hierarchy. As far as placing the record in the DNS is concerned, it's an utter waste of time.

Secondly you have to verify as a CA who offers EV certificate you have to certify yourself and undergo a security audit every year. You're paying all this money for this. Now, ICANN has a process. How many CAs do you know of have a public process where the signing ceremony is streamed on the web? I don't know of any. What I'm saying is the audit process is public here with ICANN. It's not with most X509 CAs.

The third difference is you get a special OID, Object Identifier which is part of the LDAP structure that X509 uses. You get a special OID number that verifies you're an EV supplier. The last one is you have to provide an OCSP service. Well you actually have to provide a 24 hour verification service. Most people provide OCSP. OCSP in my view is not needed if you put it in the DNS because what does OCSP do? OCSP says, "Is this certificate revoked or not revoked?" If the RR is there it's not revoked and if the RR is not there, it's revoked. The equivalent in DNS is merely the absence or the presence of a public key. You can replace it as well.

There is one minor wrinkle when it comes to this. That is how the TLS Cipher Suite is negotiated. The issue there relates to the fact that if the DNS of the guy you're talking to is secured, then you can trust the certificate. If you can't then it's not. The client has to do some work. There's a minor wrinkle in terms of the protocol otherwise it's merely an addition to the TLS Cipher Suite. Get it from a secure DNS.

Opportunistic Encryption really relates to the second question. It is essentially saying that you opportunistically encrypt on a session by session basis, mail, web, chat, anything else. E-mail has been incredibly difficult to secure simply because the problem of distributing and managing keys has proven to be very difficult and not really solvable. By

placing public key records in the DNS, we could solve that problem. Opportunistic Encryption, which is the ability to secure all forms of communication between the two end points in a way that cannot be sniffed by third parties like governments.

A lot of discussion is going on independently with Opportunistic Encryption in that context. DNS might be the only way to do that. The issue then becomes where do we place the public keys is easy. DNS, again maybe with a structure like ENUM, use a reverse tree through harper possibly with a country code on that. There's some addressing structure issues in there but I think they can be solved.

Finally, where do we put the private keys? There is an issue to do with that when it relates to Opportunistic Encryption. I can't see any difference between personal digital signature and Opportunistic Encryption except people generally want anonymity for their communication. Personal digital signatures by their definition are not anonymous. They are publicly visible. Then you can open up issues like Egov sensibly. How today does the user participate in Egov other read a website? How do we use the Internet for Egov, genuine Egov? How can I handle transactions on the Internet in any other way?

To summarize, the push is destined to fail. It just won't work. We have to use the pull and I think the pull is not just there. It's screaming out for this stuff. I really do believe that. The missing element currently is the DNSSEC API. If the guys who made the statement are correct. If Google and those folks are not doing evil in this context are promoting some nice interface, maybe my problem goes away. Or maybe it's just a forced element on the list I put up this morning.

If there is no API there are currently no DNSSEC apps. We've got to get the pull side working, not the push side. Just providing the public key in the DNS opens up the entire world. There's no shortage of imagination for this stuff but there are lots of vested interest. If I'm going to do SSL replacement, do you think I might have some opposition from the CAs? That's my presentation. It really is as simple as that. I'm happy to take any questions.

DAN YORK: Thank you for framing some of the issues that are here. I think the get DNS API does perhaps provide some of what you're looking for but the question I really had for you is when you look at this, what are some of the apps that you're interested in seeing that are out there?

RON AITCHISON: Let's just take the simple browser. Why do I have to spend a fortune? There's a move now from EFF putting HTTPS on everything that moves. I think it is a well intentioned but flawed strategy and here's why.

First, you're forcing everyone to buy an SSL certificate. You're forcing them to pay $150 minimum. If I've got some crappy little website that is my own personal one and I want to follow this edict for security purposes, I'm forced to spend $150 a year on something. Once you get over a certain level the law of big numbers starts to play a role here. Big numbers say 1% error rate is going to end up…Essentially it means you're dead. You don't have an effective policy.

If you are forced to click through error messages then the whole thing just falls apart. I'm saying browser. I'm saying e-mail. If I can get your

public key directly from DNS using a lookup strategy. There's a million ways to use that lookup strategy. I can look up your e-mail address, reverse it, do a lookup on it and I've got your public key. As soon as I have your public key I can opportunistically encrypt your e-mail.

DAN YORK: In fact, what you're describing is a number of the drafts that are out right now in the DANE Working Group around specifically how to do this that we're seeing it happen now. You're right, it's a great application for that.

RON AITCHISON: I said this this morning and I'll say it again. I think DANE is for the perennially paranoid. I think it's a waste. It's a complete and utter waste. It's the wrong way to go to put a cert in the DNS. My whole point about this presentation is there is no need for a cert. What does a cert do? A cert delivers a public key. A public key is just a public key. We have records in the DNS which deliver public keys. What does a cert do?

[SPEAKER]: Originally we had key records for DNSSEC and it was also intended for other purposes. Eventually we saw the need to just use it for DNSSEC so we created a record called DNS key. Additionally there's another record that is called the cert record. We can basically put a TLS certificate in. It's literally called the cert records and on the right hand side of the records is nothing else but a bunch of bits. It's basically free form. The problem with that was you can't really assign a policy – what are you going to do

with this? Can I use this for X, for Y, for Z? We have to not only have DNSSEC signed address records but also DNSSEC signed certificates.

We need to be able to express a policy and so DANE is nothing else than a DNSSEC assigned entity. There's an awful lot of free form but it does solve a lot of problems that the original specs had. Really if you want to put anything in a DNS. You could use a text record. I won't recommend it but you could use a text record. What you're saying, you can all ready do that by just using any type of record. There's even a sink record, literally, sink as in the kitchen sink. You can put anything in there you like. There's some good use of DANE. I won't go into the details of the spec but there's a reason for it. There's a lot of enthusiastic behind DANE.

Can I just address another point? You mention Opportunistic Encryption. Opportunistic Encryption is nothing else but encryption without authentication. That actually solicits a man in the middle attack and it's trivial to perform. Yes, I can talk to you via e-mail. I can do opportunistic encryption but I still don't have a guarantee that I'm actually talking to you. I might be talking to someone in [inaudible 0:25:29.4] who is then talking to you and forms the man in the middle.

Opportunistic encryption is actually an off concept in this post-Snowden era. People think opportunistic encryption is lost. You need authentication in there.

RON AITCHISON: It sounds as if I'm fighting SSL certificates and there's a reason for that. That is because I am. I understand your point. I understand where you're coming from. Don't get me wrong. It's a technology that's out there.

Let's look at the history of SSL certificates just for a second because I think this is very important.

We tend to assume that what exists today has always existed. SSL certificates were defined by the X500 Working Group of the ITU when X400, the mail service was being put together. We're now talking about the late 1970s. That's when SSL certificates were defined. They were picked up by Netscape in the early 90s, wrapped around the SSL protocol and became used as a consequence of that.

Point about SSL certificate, it's job was to get a public key across an insecure underlying network. That's all its job was. The key point there was insecure network. What I'm suggesting is that we do not need the SSL certificate if we have a secure underlying network.

Your point is well taken about the key record. It had a whole bunch of different functions, used for a whole bunch of different reasons and when you came to define DNSSEC, you went for the DNSK record as being a specific RR type to only signal that type of information. It seems to me that DNS RR proliferation is not a bad thing. I know some people think it's evil. I know some people think it's a bad thing. I don't happen to be one of those because I think there are limits so maybe I only think it's partly evil whereas some other people think it's inherently evil. I don't see any reason why we shouldn't have a certain amount of proliferation if you want it.

The third thing I would say is that I think you assume that the SSL record itself, the X509 record has a lot more flexibility than it genuinely has. You can stuff all kinds of records in there but the problem is the interpretation of those attributes is not a simple thing. One of the more

amusing things about an EV certificate is it defines how to use the attribute L – locality, sensibly. We've had these certificates with an L attribute and people have used it for all kinds of purposes. What's a locality? Finally these guys, for $350 they tell me what to put in locality. No thank you.

JULIE HEDLUND: We have to wrap up now. We have to move on to last event of the day…Well, second to the last event because I don't want to say the How Can I Help? is not important. Join me in thanking Ron for his presentation.

DAN YORK: For those who are on the audio stream, we will be recording the demonstrations and we will be putting them up on a video link. It will be on the Deploy 360 YouTube channel sometime in the future.

DUANE WESSELS: I'm here to talk about DANE. I'm going to go through a little bit of introductory material. Then towards the middle I'm going to switch out of PowerPoint and give an honest to goodness live demonstration of configuring TLSA record in your DNS zone and showing how to use it.

I'll spend a little bit of time talking about what DANE is. I hope that's new or interesting to some of you. I know some of you know it all ready. We'll talk about the TLSA record which is the record is used to refer to certificates, talk about this browser plugin which was mentioned earlier today. This was a product from CZ NIC. I'll show how to generate the

TLSA record and then assuming there's a little bit of time, I may talk about other uses for DANE besides TLSA records.

DANE is a suite of RFCs that describe how to represent and authenticate named entities using DNSSEC. Examples of named entities are websites, web servers, e-mail servers, e-mail addresses, jabber chat IDs, PGB keys and so on. If you were to start researching this you might start with RFC 6394 which talks about DANE overall, sample use cases and requirements. Today we're going to talk about the TLSA record in particular which is described in RFC 6698.

A lot of the material that follows this is lifted directly from there. There's a number of internet drafts in the works that talk about using DANE for SMIME, for SMTP, IPSEC, PGP and OTR. OTR is a chat protocol, it stands for off the record. Even though these are internet drafts I understand that a lot of these have initial implementations and people are very excited about this.

We've talked a lot about certificates but this is a picture showing the way certificates work in browsers today. At the top you have a number of hard coded CAs in your browser and when you visit a website, there's a chain of certificate authorities going from that server certificate all the way up to some hard coded trust anchor in your browser or whatever application you're using.

The screenshot on the left was taken from Firefox which just shows the hierarchy. You can get to that if you click on the lock icon or whatever icon is on your browser. You can usually bring up this kind of picture. If you're considering how it might look with DANE, it might look something

like this where you have trust established from the root zone on down. In this case we are still talking about the freebiest.org website.

We've got the org zone, the freebiest.org zone then within the freebiest.org zone you have a TLSA record which refers to the certificate. This is just one way of arranging things. It doesn't have to be this way as you'll see the TSLA offers a number of parameters, which can control exactly how this works. For example, the TLSA record doesn't have to refer to the end certificate, it can refer to some intermediate certificate authority or it can provide a new trust anchor that the browser would use to authenticate from then on down.

You can imagine there's a slider here. You can slide up and down where you want to jump from DNS over to the certificate world. By the way, I'm happy to take questions. That's not the only way to use TLSA or DANE. You can match certificates in different ways. You can match certificate authorities instead of certificates. You can match only the key part. You can specify a whole new trust anchor for the application.

One of the first thing to know about TLSA records is their names are different than your typical domain names. They look a lot like SRV records where they have leading labels with underscores. The first one refers to a port number. The next one refers to protocol number. If you were looking for the TLSA number for freebiest.org you would look up this record _443._tcp_www.freebiest.org. You can imagine for other services it would be similar. The port number would change if we were talking about something like SMTP and the rest of the name might change as well.

This is lifted from the RFC. This is the diagram of what the wire data formula looks like. There's four components to the TLSA record. The first is certificate usage, that's an 8 bit value; selector, also 8 bit value; matching type, 8 bits and then a variable length certificate association data blob which we'll talk about.

For certificate usage, there are four values defined. I'll go through those in detail in the upcoming slides. Selector, two values – you can either match on the full certificate or only on the public key component of that certificate. You can choose three values for matching type, exact match means you have to match the certificate exactly, bit for bit. Other options are you can take a hash of the certificate and just match on the hash. The certificate association data can be a number of things as well. It can be the whole certificate depending on what you choose for the other values you might want to put the full certificate there. Only the public key data or the hash value.

Certificate usage zero in the RFC is referred to CA constraint. If this is the usage then it means that the server's certificate is validated by the CA referenced in the TLSA record. Here the TLSA record does not refer to the certificate itself but refers to some certificate authority. Furthermore that authority must all ready be present in the browser or application. That authority must all ready be known to the application. It must validate that part normally.

RON AITCHISON: You made a point a couple slides previously that said you could also replace the CAs root certificate.

DUANE WESSELS: That's a different usage coming up in a different slide. This solves a particular problem where your browser may have 20 or 30 trust anchors known to it and any one of those authorities could be compromised and then issue certificates for servers fraudulently that were not previously known to it but by using this certificate usage zero, you can sort of pin the server certificate to only be valid from a certain authority.

One of the things that's nice about this usage is that if you happen to update your server certificate you don't necessarily have to update your TLSA record as long as you're using the same certificate authority. Certificate usage one is called Service Certificate Constraint. Here the TLSA record refers to the certificate itself, to the server's certificate not the CA. Everything else is much the same. The certificate must validate normally via the applications standard PKX mechanisms. Unlike the previous one, if you use this you have to update your TLSA record every time you change your X509 certificate, perhaps annually.

Certificate usage two is called Trust Anchor Assertion. This is what you were just asking about. This is where you define a new trust anchor for the application. My bullet here says it's similar to usage one but that is incorrect. It's similar to usage zero. The difference here is the trust anchor does not need to be previously known to the application.

JULIE HEDLUND: Excuse me Duane, we have a question from the chat room. It's from Barry – Certificate Usage Zero doesn't solve the problem of an intermediate cert issued by your CA, correct?

DUANE WESSELS: It is my understanding that it does solve that problem but I'm willing to be wrong on this. My reading of it is the TLSA record refers to the certificate of authority which must be in the chain of validation for the server's certificate.

RON AITCHISON: Does that not make it look more like a two than a zero?

DUANE WESSELS: Well, it's not like a two because the trust anchor does not have to be hard coded into the browser.

RON AITCHISON: It's in the chain of the trust anchor.

DAN YORK: The use case people have had for two are people who've wanted to have their own enterprises or wanted to have their own corporate CA essentially not preloaded in the browser. This provides a mechanism for loading that CA essentially into the trust or whatever application is doing the validation. That's the primary use case I've heard for it.

DUANE WESSELS: Yes.

RON AITCHISON: Just one quick question on that. I'm having a problem. I'm trying to envision the trust model where I can replace the root CA certificate. If I get something from somewhere, who do I trust?

DUANE WESSELS: In this case you would be putting your trust in DNSSEC.

RON AITCHISON: DNSSEC or the record in DNSSEC?

DUANE WESSELS: The whole chain of trust from the root.

RON AITCHISON: So what we're saying is that we need a DNSSEC aware API to tell us that we've got a secure TLSA record and then we're prepared to trust it, yes? I can't take a TLSA record from anywhere and be able to trust that, why?

DUANE WESSELS: You don't exactly need an API but you need code to verify, to validate the signatures in DNS and DNSSEC.

RON AITCHISON: Okay, I'll accept tautological difference. The nature is that I have to be able to trust the data. It has to come from a DNSSEC secured domain and under those conditions I can trust anything I get from that. I would also say by the way, if I just got your public key I don't need your SSL crap.

DUANE WESSELS: Okay, certificate usage three is what they call domain issues certificate and here it's one of the simplest cases. The TLSA record refers to the server's certificate and the application doesn't have to do any other validation through any other chains or trust anchors of certificate authorities.

One of the things you start to worry about with DANE and TLSA records is the size of the data. If you're willing to do Shaw 256 hashes then your RR data is on the order of 32 octets, Shaw 512 doubles that but if you're thinking about putting the full key material or even the full certificate into the record, the sizes get big quickly. For example, the worst case you wanted to do a 4K RSA bit key, the whole certificate for that key – you're looking at 1,400 octets response size which is getting quite large. It starts to get worrisome in terms of MTUs and fragmentation and those other problems.

We expect the hashes to be very popular at least initially and maybe like Ron says maybe for the truly paranoid you might go all the way up to these full certificates. For the demo today we're going to keep it simple. We're going to do a certificate usage three, selector will be on the full certificate and we'll use the hash value rather than matching of the full data.

To demo this we're going to use the validator add on, the DNSSEC TLSA Validator Add On from CZ NIC. Here's the url. This is a very nice tool. It claims to work with all these browsers. I've actually only tested it with Firefox and that's what we'll be testing it with today. It seems to be very comprehensive.

At this point I'm going to switch over to a live demo and Julie's going to keep the slides going because they are essentially very similar. I've got to size this right. All right. Here's the validator web page. It's not currently installed in the browser so I'm going to go through that, click on download. I think it's working in the background but it's not showing. It's installed. One great thing about this plug in is previous versions you had to use an external validating name server but now it's all built in thanks to the fact that it's based on Unbound. It's doing all the validation internally. We don't need any external name service to do that for us. Let's test it. Success, okay.

You can see all ready since we've added this there's two new indicators here. This one that has a key tells us that this domain is signed with DNSSEC and this one refers to the TSLA status.

RON AITCHISON: Duane, I'm disappointed in only one thing and that is the huge debate they had over what color to use for EV certificates to put on your address bar and he puts no color there at all.

DUANE WESSELS: Duly noted and entered into the record, thanks. This is the website that I'm going to be using for demoing. You can see that it's all ready signed but there is no TLSA record at the moment. The first thing to do is get the certificate. There's a number of ways to do that. If you're running a website you would have direct access to the certificate but I'm going to cheat a little bit here and get it directly from the browser.

I'm going to click on view certificate, details and then I'm going to export it to the desktop. Let's see if I can bring that up. There it is. Here's the certificate data. It looks like a certificate. The next step is to generate the TLSA record and to do that we'll again start with our good old friend and say, "How do I generate a TLSA record?" I'm going to use this tool here. This is from a gentleman named [Shuman] who actually recently joined us at VeriSign. I have to go here now. This is just very simple web form.

Obviously if you were doing this for real you may not want to use some random guy's web form to generate your TLSA web forms. You might want to do it in a more secure manner than this but for experimenting this is perfectly adequate and we're going to proceed with it here. He's got all the defaults here that happen to be the same as the ones that we're going to use today so all I need to do is fill this in down here, go back to my screen, copy this. Here we have to put in our port numbers. This is obviously TCP.

Here's the record that we're going to put into the zone. I should also mention that there's sort of a back end script that Shuman also makes available. If you didn't want to use the website you could download his…I don't remember what language it's in, Python or something and do this via the command line entirely. There's our record. Now it's time to enter the zone file which is conveniently right here. Here's my zone. Okay, here's the exciting part. Let's see if it works.

This is where I have my little signer script so I'm resigned. Let's see if it's there. Okay, good. The TLSA record is there now. I should also mention that the TLSA record being new you may not find that the particular version of Bind or whatever you're using knows about the TLSA record.

You may have to update your software. If you can't do that, there's a way to enter in records in a sort of binary format. It doesn't have to know about the TLSA record. You would put numbers there.

I don't think I can simply revisit the web page. I'm going to quit Firefox and start it up again. Okay, we're green here showing that it's authenticated or corresponding to the TLSA record. One thing I should also mention to anyone sitting at home, this domain does not have a certificate that would validate in anyone else's browser because I was too cheap to go spend money on a real certificate. This is not exactly a signed cert but it's my own little CA that's loaded into my browser.

If you go through this with this domain you'll get warnings about this certificate is not valid, do you want to trust it? That's basically the enf of the live demo.

[MALE SPEAKER]: Thank you, great demo. One other request if you have a bit of time. Maybe you could do the whole self sign cert thing. The DANE and the TLSA things that you can go through with some validating tools and see that it can be done without spending $150.

DUANE WESSELS: That was my original intention. The only reason I didn't do that is because even with this plugin if you just loaded a self sign cert you're going to get a big warning at least from Firefox that this is not a trusted site. I thought that was a little bit confusing.

[MALE SPEAKER]: Have you experimented with Bloodhound with it?

DUANE WESSELS: I don't know what Bloodhound is.

[MALE SPEAKER]: That's a fully validating DANE aware browser from our DNSSEC tools.

DUANE WESSELS: I'm just a Firefox user. I don't know what other browsers do but I expect that at some point with DANE and maybe you won't have that problem anymore. It won't pop up the warnings when the TLSA matches the certificate.

RON AITCHISON: You're saying that you've got self-sign certs working?

WARREN KUMARI: One of the DANE use cases is for self sign certs that are built into the whole DANE protocol definition and the Bloodhound browser is a modified Firefox, gone through and adjusted the code as needed. It validates all of the regular links that you'll see inside a regular commercial page with 50 to 150 links in it. Those will get validated as well plus we also added the DANE capability in conjunction with any of these that had DANE TLSA certificates.

RON AITCHISON: You have to explain this to me a bit more. How does the self signed trust model work? Who do I trust under these conditions?

DAN YORK: I'll respond by saying you're trusting DNS at that point. DANE without DNSSEC makes no sense. We talk about DANE as a value of DNSSEC. DANE in this context especially in this context, we're only talking about DANE with DNSSEC to provide that trust model. That's where it comes in so if you're using mode three which is the actual cert or mode two where you're winding up with the trust anchors there. You are assuming that is all DNSSEC signed – all the way up to the root so that you have that chain of trust around those.

RON AITCHISON: I understand what you're saying completely but what I'm noting in what you said is that you're constantly falling back – not falling back, don't want to use that because it implies it's something negative and I'm not implying that at all. Your falling back to DNSSEC as the base trust server here.

DAN YORK: Yes, DANE is designed to work with DNSSEC and so it is all about that.

RON AITCHISON: My question, that was what the SSL model set out to do. Why replicate it? Why have two things doing the same thing? Do you understand the point I'm making.

[MALE SPEAKER]: One of the big failures with the SSL model is the fact that you have a huge number of roots. Anybody can issue a certificate for anything. Any of the CAs can issue for somewhere else. With DANE you have a single trust chain, the ICANN run route. Then there's only a single path down to any specific node. Only the person at a specific node can publish that or publish that TLSA record and there's a single chain to a single trust anchor.

RON AITCHISON: I think we're agreeing violently here. I'm buying what you said. There is a problem with the SSL model which is that there are a thousand different solutions.

JULIE HEDLUND: I'm sorry, Duane has a few more slides. We have just only a few more minutes before we have to wrap up.

DUANE WESSELS: I just wanted to mention some of the other uses of DANE that I'm aware of and maybe other people in the audience would have something to add to this. I also used post fix. Post fix looks for TLSA records and can use that when talking to other SMTP servers. SMIME which defines a new record type. One interesting thing about this is the name of the DNS records are hashed, left side of the e-mail address so your zone doesn't give away your e-mail addresses to prevent spamming and things like that.

Paul Waters is very active with DANE and he's got a draft and some code that implements DANE for open PGP keys. He's got this software called open PGP key milter which will attempt to automatically encrypt plain text e-mails. Also mentioned previously is OTR, off the record messaging protocol that Paul Waters is very interested in.

[ROY] I'm just curious. I like all this stuff. Is there all ready a native application interested in offering DANE support by default? I just installed it as an extension in Chrome. It works but it would be nice to have it native in Chrome. I wonder if for instance Warren or Dan or Duane could…

DUANE WESSELS: I don't know about browsers. Post fix does it by default. There's no plugins or anything like that.

DAN YORK: The cool thing is Victor who wrote that worked with Wes [Hardiger]. Not only is it on by default but they also came out with a whole document around operational or guidance for implementers of DANE. It's an operational guideline.

The other place where it's implemented right now is XMPP. The XMPP community has the largest production implementation with DANE right now because with Peter St. Andre's manifesto for ubiquitous encryption across the entire Jabber infrastructure. They've gone ahead DNSSEC and DANE for server certs and the client server certs and using the self sign certs as well. That's a big implementation of DANE right now.

WARREN KUMARI: If people want the browser stuff and push for it, an option would be instead of getting the big red pop up box saying you've got a self signed cert you would get this instead. The browser concern is that is you do a TLSA record lookup for every single site you go to there is twice as much DNS traffic. There's the belief that a number of resolvers will just fall over if all of their clients start doing that. For cases where you don't know the certs, that's possibly an option.

[MALE] And there is also Bloodhound that natively OSX and LINUX.

JULIE HEDLUND: I think we're ready to switch. We've got just a minute or two to do the How Can I Help Presentation by Russ and Dan so you'll have to speak quickly. Please join me in thanking Duane for an interesting demo.

DAN YORK: One of the cool parts of the DANE Working Group is there has been a great amount of actual running code. To Duane's point about people who are bringing presentations there, at our last meeting in London we had four different drafts presented all of which had running code in presentations that were there.

This is the part at the end where we say thank you for coming. We want to just let you know about what we'd like you to look at and what we encourage people to do. For the folks who are operators of TLDs whether they're registries or operators, we'd like you to look at how you

can sign your TLD. I want to see more places on those maps except work with the registrars.

The other piece we'd like to do is help with statistics where you can. Duane pointed out earlier, all the new TLDs have to put their stats into a centralized registry so there may be some good ways we can get some stats around the new gTLDs. We want to get stats to be filling those maps.

RUSS MUNDY: Zone operators – sign yourselves up. That's something that even if you're not doing validation, sign your zone, start doing DNSSEC right now and work with your registrars to ask them if you don't support DNSSEC, when are you going to do it or I'm going to find somebody that does. I know companies that have changed registrars to actually do that and it's becoming a reality that that's happening.

DAN YORK: For the network service providers this is a big one we'd like to push particularly this year. How do we get more DNSSEC validating, DNS resolvers out there. Geoff Huston's stats were great but we want to see them grow even more and to see much more of that happening.

DANE is being used a lot. We mentioned at the last ITF meeting there was a lot of discussion on how to strengthen the security of the internet and DANE kept popping up in many different groups because people started to look and say, "Well, we're all ready doing something with TLD. How do we make that more secure? How do we add additional layers of

trust on top of that?" We encourage network service providers to allow the usage of TLSA, don't block it and help raise awareness around that.

RUSS MUNDY: Website and content providers, look at getting your TLSA records of support out there. Make sure your zones are signed before you start putting the DANE out. This is a great thing to think about. You can put the data into your DNS service and it's going to give you a good learning experience, get integrated into your activity set. Some registrars actually offer an integrated higher level security service. If you're working with some of them they can do that and it's a matter of a little bit more money usually not a great deal. Look at increasing security right now.

DAN YORK: We'd like to encourage you to look at how you can use DNSSEC, share what's there and this is a key thing. We are now done with this final presentation here, this DNSSEC Workshop at ICANN 49 but very soon we're going to start thinking about what's going to be happening at the Workshop at ICANN 50 in June in London. You've heard some great case studies today, you've seen a demo of some tools from Duane and a number of other discussions. If you've got an idea, if you've implemented DNSSEC like the guys in Estonia did. If you'd like to share your story about how you did it, those case studies are very helpful for us. We'd love to have you come and share the lessons learned at the next one.

RUSS MUNDY: If somebody has some new ideas, new applications, new ways that you can do new things because of DNSSEC, because of DANE we're very interested to hear about those also. We're always seeking new ways that DNSSEC is being used in the world.

DAN YORK: With that, we'd like to say thank you. There's a series of resources up here. The DNSSEC Deployment.org site, the Internet site of Deployment 360 program and the DNSSEC tools are all projects and sites that are providing a lot of the information that you've seen here. We'd love your input. We'd love to hear from you about these sessions, about the Workshops, about the pieces that are here. We think they have value and we like to hear that from folks out there. Thank you for your time today.

[END OF TRANSCRIPTION]