Steve Crocker: One of the questions that was asked over and over again in the earlier days of DNSSEC was suppose you get (inaudible). And years ago it was an open question of whether anybody would pay attention, and over the last few years we've seen a welling up of interest and a great deal more involvement, and that…

[break in audio]

Steve Crocker: That turns out to be outside of the rules of the game for what ICANN will pay for so we've gone around hat in hand and solicited to support this and met with remarkable generosity. It's one of the easiest fundraising activities that I've ever been engaged in. So the several sponsors shown on the screen here - .se and the open DNSSEC effort that they and others are supporting, Afilias, GoDaddy, PIR, sponsors .org, operators.org, SIDN the Dutch Registry, Nominet the UK Registry and VeriSign – so I want to thank all of our sponsors. And two more thanks – what happened here.

These sessions take quite a lot of work. In front of you is the Program Committee. Julie Hedlund, sitting on my left, does an enormous amount of work organizing things and putting all the pieces together. Lance Wolick, Russ Mundy, Simon McCalla and I have roughly weekly calls almost continuously during the year; we take a few breaks. And often are not only looking at the

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

upcoming meeting, but sometimes looking at the next one after that and doing a kind of layered planning process. And it operates pretty smoothly; it's a great team. And if anybody thinks that they can help improve, which is how Simon came up one day and said you know this is okay, but you could do some better things and I said and you could help us, and he graciously accepted the invitation; Lance the same thing. So I really appreciate the team and you should appreciate how much work goes into it.

I also want to express thanks for all the folks that put on the DNSSEC for Beginners Monday afternoon. That's an outgrowth of these meetings that we've had. And several months ago, maybe about a year ago, we said it would be good to have a tutorial and then we decided we should schedule it at a different time. That's evolved and matured. I've been caught in the unfortunate position of being double booked at the hours that it's been given, but I've been tracking it as closely as I can and I understand that it's sort of hitting its speed. I heard a comment from somebody who had actually sat through it multiple times and his comment was "oh now I finally get it." So the repetition is helpful.

So with that we'll move on. I hope you all have the agenda. We're six minutes into my time and I actually will keep my remarks quite brief. We have, as we usually do, a very content full set of presentations on key topics that are current in DNSSEC. A panel discussion will follow on the challenges for registrars. We've had very good uptake on the registry side and now time to focus attention on the registrar side. Joe, you had a statistic about

the number of registrars, are you going to share that during…? Then I won't say anything now, but it's a pretty interesting figure.

There's a special topic that has gotten a lot of attention about how do you transfer domain names, operational domain operations from one operator to another or from one registrar to another or both; and particularly in the context of DNSSEC. How do you do that without losing either operational resolution or validity? And can you do that all smoothly while the train is in operation, as it were? So, a variety of meetings and presentations that have taken place on that, some in this forum and some other places, and we'll have a short session on that with Debbie Monahan and Roy Arends.

Last part of the morning will be Experiences, Challenges, Outcomes of DNSSEC Deployment. This is where some of the actual experiences, and that's a code word for some of the problem areas, come up. And we like to be pretty forthcoming about it rather than try to say everything is all rosy and perfect. It's not bad, but there are details and that's part of the learning curve.

And then we'll finish up after lunch with a panel discussion on activities around the world with, as we usually do, a focus on activities that are relevant to this region. So that's the plan for the day here. And in a moment, a short moment – so where Julie is working hard to find the maps that try to produce that show the uptake of DNSSEC in the ccTLD Registries; it's a world map so it's harder to show the gTLDs and it doesn't show anything about the registrars or the validation process and ISPs and so forth. We'll work on that. I'll say, as these maps are being pulled up,

that we started this project some time ago when there wasn't much actual deployment but there was a lot of plans in place and a lot of discussions so I wanted to look at not only what the actual facts were of the moment, but also what the announced plans were scheduled over time.

I've discovered, as I try to keep these maps up to date, two things – there's enough activity that it's getting harder and harder to get all the data. And the other is that there is so much current activity that getting information about the future is much, much harder. So I'm finding that my prognostications are under playing things by quite a bit and the actual facts are catching up faster than I can keep track. So with that here is a map that shows what the actual and planned deployments were as of the end of December last year.

The blue is "fully operational". The green is "partial operation". this could mean that, for example, that the zone is signed but the DS record is not in the root or that the zone is signed and the DS record is in the root but registration has not yet opened for general delegations to subordinate zones; or any other combination. The brownish-orangish color is qualitatively different. That's where the registry has formally announced that it will in fact implement DNSSEC. The yellow is an earlier stage that is not uncommon, which is experimental where there may be a test bed or there may be some things behind the scenes, but no formal commitment to move forward yet. And then the gray is where there's no announcement and we don't know what's happening.

Noteworthy is that even last year, every continent had activity. We are no longer keeping track of who's the first in every continent; we're past that. The thing I mainly regret about the map is that since this is showing in a geographic basis is that the numbers of registries isn't quite evident visually.

So there are a number of geographically small countries that have been quite forward. So that's the end of December last year. This is March this year and I'll toggle back and forth and you can see the transition in the direction of blue. So this is March; this is June of this year. So this is basically now. And this is the projected for the end of this year and this is the projected for the end of next year.

The distinctions from this year and next year are pretty modest. I'll toggle back and forth and you can see just a little bit. There's only, if you look at the statistic in the lower left it goes from 37 to 38. That just shows one more country next year. I am completely sure that that's an underestimate and as I say, represents just a lack of our ability to get that information about what the future plans are. And record will get added to the root and we'll keep track of it, we'll make modifications to the way that we display this in the future and try to bring these more up to date.

Here's the same information presented in sort of tabular form in a bar graph there. And as I said, the numbers for the end of next year, and even probably for the end of this year, are probably underestimates. So it will be interesting to look back a year from now at these versus what we're showing here and I suspect thing

will be better. The top of that, the top line there shows 60 ccTLDs who are in some state of either experimentation or announcement or implementation. And as I said, 37 by the end of this year and 38 by the end of next year as fully operational. Those are substantial numbers.

They're well short of half or 80% of all of the ccTLDs, but they are a very. Very long way from where we were a short time ago where it was hard to imagine that anybody was going to pay attention. So, feeling pretty good, but not too – there's a long, long way to go as we were saying when the root was signed. It's not the end, it's not the beginning of the end, but it is the end of the beginning and we're well launched.

So with that, happy to take any questions, and even happier to turn things over to Matt Serlin who will launch into the first panel.

Matt Serlin: Thanks Steve. So, we're going to get things kicked off talking about a registrar perspective although we have both registrar and registry here represented on this panel. We're missing Jim Galvin so I guess Joe, we'll start with – yep, there's your deck that Julie is running so we've got a presentation from Joe and then we're going to kind of open it up. We've got a list of questions that will guide us through the next 45 minutes or so. So I will turn things over to Joe to run through his deck.

Joe Waldron: Thanks. I'm Joe Waldron from VeriSign and I have responsibility for the product management group that was the implementers of DNSSEC within VeriSign. And I would say that it was a very substantial task for us to implement something like DNSSEC within .com and it took a very large team of people to do that across engineering operations.

There was a tremendous effort to accomplish that task. And as we were undertaking that we realized that it's not just something that a registry can do by itself but it requires significant cooperation and participation across the community. So we spent a significant amount of time looking at what was necessary for the implementation through the registrars; without the registrars a registry implementation isn't as valuable as what I know Steve is hoping. Next slide.

I guess engineers all like statistics and numbers. Steve showed some of these but I'm going to just talk about them a little bit different. I would say that about one-quarter of all of the TLDs are currently signed. And that includes the break down that you see here. I think though if you look at the composition of what those TLDs are right now, we have .com signed, .net, DENIC signed .de recently – if you look across which TLDs are signed it actually represents somewhere between 50% and 60% of the domain names that are currently registered.

So if you are a registrant that gives you the likelihood, I guess it's really binary whether your particular TLD is signed, but that's

tremendous progress on availability of DNSSEC across a large number of TLDs.

The other component for the registrars is that once the TLD is signed that allows you to establish that chain of trust and right now we have about 900 registrars across .com and .net, and we have 26 that have actually registered at least one domain name that has a DS record. It doesn't sound like a lot, but that represents I think either seven or eight of our ten largest. So again, it's a very significant population in terms of the availability of DNSSEC down to the registrant level. Next slide.

As I said, we spend a lot of time working with registrars in trying to understand what the challenges and hurdles were and we wanted to help reduce and eliminate as many of those as possible. So we developed a series of programs and tools to help – and I'll just, for the sake of time, just address a couple of these that are on the slide here. One is the third bullet on the registrar engineering side, which is a DNSSEC Tool Guide.

That was originally intended to be what I referred to as a quick start guide like where you buy some new device and you open the box and it tells you very quickly how to get up and operating. Well that turned into hundreds of pages of documentation on various DNSSEC tools and I think has proved to be a very useful guide and asset for our registrars to be able to reference.

We also have a DNSSEC Transfer white paper and I'll touch on that a little bit at the end. And then over on the other side is what

we refer to as the DNSSEC Analyzer. And that's a tool that was built in house to help conduct analysis of DNSEC errors throughout the chain of trust and I'll show you an example of that. Next slide.

We also wanted to really provide information. The first link on here VeriSign.com/DNSSEC is a DNSEC Resource Center that we provide. And that's open to the public and it's broken into various categories depending on what part of the ecosystem you come from; whether you're an individual registrant, a hardware vendor, an ISP. So you can find information that's relevant to your particular need. But again, a lot of this is focused on what we needed to do for the registrars.

So we created a DNSSEC forum in a web portal that we operate specifically and limited to, access limited just to our registrars. And that DSNSSEC forum was intended as a communication channel for the engineering teams to be able to talk and address various issues and facilitate that discussion. Next.

As we had several discussions we realized that the startup cost for registrars would vary based on their particular business model and their customers' needs. So, one of the things that we wanted to do again was to help reduce some of those obstacles. So we created a cloud based signing service. So if you follow the flow of this service it's a very basic picture of how the delegations work for normal registrations and then if you follow from the registrar when you have a registrant that opts in to sign their .com domain name, the registrar can subscribe that domain name into the cloud signing

service at which point we will pull the zone from the master of the registrar that's hosting. We'll pull it from their master, sign the zone and then push it back. So it's very minimal implementation for a registrar to adopt this service. And then you've essentially established that whole chain of trust. And at the point that the registrar wants to invest in additional infrastructure and have their own HSMs or whatever solution they integrate into their environment, then they're already up to speed and can do that as their business demands.

Okay, so we did this as a pdf so you're not going to get to see the fancy animation, but I'll provide the link to this. But we have the DNSSEC Analyzer or there's a link, Matt will correct me if I get this wrong, but it's DNSSEC-debugger-verisignlabs.com. So if you go to that link, then you can get a web based tool and simply you just put the domain name in and it will validate the chain of trust for that domain name from the root zone all the way down through the domain.

And what you see on the graphic here is a detailed drill down on some of the information. So here you see the .com portion of the results and in this case you see the green checkmarks. But if there was an error in any of those checks that it did it would flag that and then you could mouse over it and it would provide more information about what the error is and offer solutions to correct those problems.

So we think that this is a very useful tool and it's something that our operations team requested because we know that when you

have different types of DNS errors sometimes it can be very difficult to diagnose very quickly. And this is again, a tool that we wanted to put in as many hands as we could so that you can help registrars solve their customer service problems very quickly without having to escalate. Or registrants can use this on their own and be able to diagnose their problems. And I will also say that it's available as an iPhone app and I think maybe some other devices. We've gotten great feedback from people that have used this as a useful tool. Next.

Finally, I had mentioned the Transfer white paper, and there's a link on the bottom of this slide for where you can download that white paper. But we looked at this as discussion was going around about what are the unique requirements once you have a domain name that's signed a registrant wants to transfer that name between registrars. And in reality it's not as much the transfer between registrars, it's really when you're changing hosting. So, even if a registrar within a registrar, you changed hosting providers, or if you're changing registrars.

So we looked at several different sue cases and identified those in the white paper and provided a process. As Steve mentioned in the beginning, when you transfer a name that's signed it's important to ensure that you are able to maintain the signatures and ability to validate those names so you don't have any interruption of service. So most registrars are very familiar with doing that and advising their customers today on how to transfer hosting providers and DNSSEC adds an additional layer of work that needs to be done to

ensure that the incoming and outgoing registrars or hosting providers cooperate to be able to ensure that those names don't have any interruption of service.

So, with that I will…Matt?

Matt Serlin: So, we're missing one of our panelists; I believe Russ, are you going to run through his deck? Is that…

Russ Mundy: Yeah, I'll run through his deck. I'm certainly no Jim Galvin but we have worked fairly closely with Afilias on some of these things so I can at least get his slides up and add a few words to them.

Matt Serlin: He gets credit for being here without even being here. That's nice.

Russ Mundy: Well I am really Russ Mundy but I'm trying to channel Jim Galvin. I'm not Jim Galvin but I do play him on ICANN panels, how's that? So Afilias is one of the active early leaders in deploying DNSSEC and we, as part of our efforts, have worked closely with them on a number of various initiatives. And here's, I think, a list of some of their big registry operations that they support. Let's go on Julie.

The integration aspect of bundling services I think is one of the areas that – maybe I'm not saying this very well, my goodness. Flashing lights here…

Julie Hedlund: Well that was exciting.

Russ Mundy: Lots of excitement here. This has been an aspect of trying to get – boy that is distracting.

Julie Hedlund: Is someone doing something with the lights? I don't know if you in the tech booth can see it, but they are doing some strobe effect here that's a little bit distracting.

Matt Serlin: DNSSEC disco.

Russ Mundy: Maybe it's left over from music night last night perhaps. This is about where they were standing. Anyway. So I will attempt to carry on here. One of the aspects that have been looked at that needs a lot of attention is the operational practices and activities associated with handling of the keying material and the DNS records into and out of the registry. Next Julie. When registrars look at how they interact with the registries, the registrars are often

selling bundled services and they're looking at incorporating or at least, I think the Afilias view is hoping that DNSSEC will be incorporated into the registrar operations and of course from our perspective in the deployment realm oversight of things, we hope that too. And so trying to get the registrar operators to incorporate support I think has been an ongoing effort on the part of Afilias.

And I think the last number that I heard, and it's probably changed, they actually do have a testing and verification program; I don't remember the exact term that they used for it, but you have to go through an operational testing acceptance as a registrar. And I think 10 registrars had completed that the last I heard and they may or may not have increased the number of that, but that's an area that they've been focusing on.

So, 100% of time in service is a real challenge, especially during transfers. And we do have the separate panel, a couple of presentations on that coming up next and you'll see more detail and more of the specifics there. But it's been a problem in terms of keeping continuity of operations and it's particularly difficult when the registrar is also providing the name server operation. So that will get some attention, like I say, later on, but this is an area that Afilias has been working on and trying to get some best practices documented on how to go forward with that. Next.

In the broader area of best practices the handling of keys or handling of DS records I honestly don't know if they've defined that it will only be DS records. I know that that was where earlier they were definitely leaning that they were just going to accept DS

records, but honestly I'm not sure exactly where they are on accepting that because from a theoretic technical point of view the registry can accept either one.

And I guess that's the end. And sorry that Jim wasn't able to be here and I didn't add a great deal, but at least maybe I gave a little bit of insight from what we've worked with Afilias on it.

Matt Serlin: No, thanks. That was good. So, Michele Neylon, who is joining us and is our official registrar representative on the panel – he doesn't have slides, but I want to put him on the spot anyway and just ask that he give us a brief kind of overview from a registrar perspective; kind of at a high level based on what you heard from the registry folks and then we'll have some discussion.

Michele Neylon: Thanks Matt for putting me on the spot; very nice of you. And of course Matt fails to mention that he's also a registrar, though he's pretending to be something else this morning. We're not too sure exactly what. Obviously I cannot speak for all registrars; I can only speak for the one that I'm involved with. And I always find these DNSSEC panels and sessions to be interesting – art entertaining, informative, educational, and I could use lots of other adjectives. But ultimately I'm still not convinced.

This is the key problem. You talk about addressing some of these fine little technical points like key rollovers and signing and

unsigning zones and moving things about as if everybody played nice together. The reality is they don't. And transferring a domain between one registrar and another, between one set of name servers and another, even when both parties are playing nice together and aren't causing headaches for each other more often than not leads to issues; as I was discussing with Roy last night who understand a lot of these DNS points a lot better than I do.

And one of the problems we have at the moment involves one of the large ISPs operating in the Irish market. And no matter what happens any time one of our clients moves name servers that ISP can't see the changes unless you go off and manually remove the DNS records from the old set of name servers TTLs are ignored and nothing ever changes.

I know that's not directly related to DNSSEC, but there's a lot of stuff here that people assume is going to work, and assume that everybody is going to work nicely together; whereas the reality is registrars, hosting providers – we're all competing against each other. And sometimes we don't play nice together. And on the technical side of things, while it's encouraging to see that the registry operators are finally working on making it that little bit easier for us in the registrar side to implement things, it's still not quite there.

Personally I'm not going to invest any of my company's resources in rolling out DNSSEC until such time as my clients ask for it. Of my 40 to 50,000 clients, we have had one request for DNSSEC to date; one. Do you honestly expect me to go off and spend money,

time, resources, and everything else to serve that one customer? Was that Roy? Roy…

Roy Arends: Sorry Michele, were you done? Well you touched on a point that was going to be kind of the first point that I was going to raise and yes, I am a registrar as well. So we in the registrar community hear a lot from the technical community about implementing DNSSEC, implementing DNSSEC and what I hear a lot of from other registrars, including Michele, is that there just isn't the demand for it. So I guess it's, and it's an open question for the room as well, who ultimately is educating end users about the importance of DNSSEC to get that awareness raised so that it does start to become – you're pointing at an individual or…?

Michele Neylon: No, no I'm pointing in back of you.

Russ Mundy: Dan Kaminski.

Michele Neylon: Okay, a part from Dan. The problem is this, from my personal view you talk about registrants being able to do this and being able to do that with DNS, ultimately registrants don't give a damn about DNS; they don't care, they don't know, they don't need to know. Most of us who provide hosting on a large-ish scale, we hide the

DNS; we put shiny control panels and user interfaces in there so clickety-click, magic happens, stuff gets installed, websites appear. The end users don't know what an A record is. They don't know what a Quad A record is. They don't know what a C name is and they don't need to know.

The thing is this, for DNSSEC to be viable, I've said this before and I'll say it again, I mean even for somebody who has actually taken the time to turn up at these things for the last couple of years, I don't even see the value in it at the moment because the tools aren't there to give me that nasty warning. I have to go off and I have to install a third party plug-in into Firefox for example so I can even know whether a site that I'm visiting has a record set.

And I come from a country where the largest ISP, while it did suffer a man in the middle attack about 18 months ago on and off for about a week, users of one of the largest ISPs were being randomly directed all over the internet. But ultimately users don't give a damn about DNS. It's because it's just something that happens in the background.

Now from the registry side, with the gTLDs the situation is kind of interesting because for the most part they don't have a direct relationship with the registrant. With the ccTLDs, and I'm sure Simon and other people up there can talk to this a bit further, there can be that relationship. But I mean how can you possibly incentivize me to actually spend time and energy on this? I don't know.

Male: So, yeah. I guess Joe that brings up a good point. Do you, when you're encouraging registrars to implement DNSSEC what's the sort of marketing spin on – what's the message to registrars?

Joe Waldron: That's a good question. And one of the things that we've done is actually conduct various market research across technology companies, hardware vendors, software providers, individuals to ask them what their level of understanding and level of expectation was from the DNS. And in some cases these were studies that are IT policy makers or decision makers within companies. And there is a lack of understanding – to Michele's point – there is a lack of understanding of the DNS in general.

There's a lack of awareness of the DNSSEC. But what we did find was that as people were aware of DNSSEC they were much more likely to realize that there was a need to implement that. So I think that the education is important. So we've provided some of that research and again you can go to that DNSSEC Resource Center and I think some of those reports are there. Or contact me and we'll get those for you. Patrick I think you were actually involved in one.

The other thing we do is again try to remove some of those barriers. I mentioned the signing service. If you've got one customer Michele that wants to implement DNSSEC and they want to sign their own zone, they're doing their own hosting. So

you've got some smart tech guy and all he needs you to do is to be able to get that record into the registry, one of the things that we did was part of our registrar interface, the web UI that we make available, you can go in and get the DS record from that registrant and you can paste that into the web UI. SO it doesn't require you to do any development, but again, you can choose to implement – that's exactly right, you can choose to invest when the demand is there and as it grows you can invest more.

Michele Neylon: But you're talking about a manual intervention. That doesn't scale for me. Every time one of my staff has to manually do anything for any kind of operation, be it for registering a domain name, updating name servers, or in this case talking about DNSSEC, that costs me money and if we screw it up then there's a liability issue. And this is the other thing as well, if you put humans back into the chain, you leave yourself open to mistakes happening; which is why automation for companies such as ourselves is so important.

Steve Crocker: We have a question from the floor, at least one, but we encourage lots please.

Patrik Fältström: Patrik Fältström from Cisco but it's also the case that I happen to run a registrar in Sweden. Not an ICANN accredited registrar and this is another one of those sort of, when we say how many

registrars support DNSSEC, do you relate it to talk about ICANN accredited registrars or you talking about registrars all across the globe?

So we have to be a bit careful with words when we talk about those kind of things. Anyway, we made the decision of implementing DNSSEC and both registrar and DNS hosting providers, which is two different rules as well but we'll talk about that more later today. And the problem with those kinds of things is of course just like you pointed out, the DNSSEC addition to the DNS hosting is absolutely not visible to the customer.

If they happen to buy DNS from us they get DNSSEC because we discovered really early that it's just not possible to ask the customer whether they want DNSSEC or not. Either you turn it on for your DNS or not and that's where the cost is. You cannot have like DNSSEC only for one of your customers; it doesn't scale. So I just want to emphasize what you said that you either invest or you don't.

The other thing has to do with how the DNSSEC hosting providers actually communicate with the registrar and that must be done in automated fashion. And today every registrar that does handle DNSSEC, including us, develop their own API that the DNS hosting provider can use and unfortunately there is no common API for DNS hosting providers to communicate with the registrars and that is to pass the DS records onto the registries and that's something that I think we, if I say we it's from the IETF, has not really done their homework there. But I do see when the number

of registrars that do handle DNSSEC is going up I actually do see to some degree a common interest of actually coming up with something there. So we'll see what happens.

The third thing I wanted to say is that for the parties that really want to run DNSSEC is normally enterprises. And my experience in that is that in those cases regarding DNS hosting, in that case I encourage these enterprises to actually run the hidden master themselves and take care of the zone signing and then the DNS hosting turns into just an ordinary slave service. Thank you.

Steve Crocker: …full disclosure. We actually – can you hear me? Is it working? We actually supply an appliance that automates a sign in process. So you can understand that we've been out there trying to find out where the interest is etc. We've had this solution for some time. But yesterday I actually stumbled into a session, it was a closed session, but they seemed to have breakfast so I sat in on it.

Matt Serlin: Yeah, that's the ICANN way.

Steve Crocker: It was the Commercial Stakeholders. And a couple of things I learned there, a few people got up and they were discussing the role of ICANN to the consumer, to the registrars, etc. And one of the things that came up was that inherently the customers or the users expectation is that ICANN will provide them with security;

security of resolution, etc. And when you're talking about ICANN resolution can mean many things, but that individual actually meant resolving an IP address.

So if they believe that part of ICANNs responsibility is to create that security in the marketplace I'm saying to myself, and I hear what the registrars are saying because the domain users aren't going to the registrars demanding it, so you're only getting a few requests. And I'm think and I'm saying why would in ICANN, if someone purchases a domain and that zone is signed already within the contract that they have to be DNSSEC. I mean I don't know what the cost is, $1, $2…

Matt Serlin: That's about the biggest can of worms that you could – no, no, no – I mean conceptually…

Male: Why is it a can of worms because when I buy a domain there are certain things, like when I buy a .ca there's a certain…

Michele Neylon: Hold on a second. Don't confuse signing your DNS with creating security. That's like saying that if you buy a packet of condoms nobody is ever going to get pregnant. That's like saying buying an SSL cert is going to automatically secure a website. That's absolute, total and utter rubbish. The thing is this that is an

entirely kind of false sense of security. It's one of those kind of "oh it's got DNSSEC, now it's all nice and shiny and secure."

Male: But we're not in a perfect world.

Michele Neylon: Yeah but you can't realistically expect me, or any other registrar, to suddenly agree to go off and do these things unless I can A-start charging you for it and B-I don't know – there's a B and a C and a D.

Male: Right, but the A is taken care of. If buying a .com domain requires that you be DNSSEC or you be signed and there's an extra dollar or whatever it is, that's looks after your revenue in being able to do it.

Matt Serlin: Yeah but again – settle down – just Michele settle down. I appreciate the sincerity of the sentiment, but I think practically speaking it's not going to happen. The process in the ICANN community to – if everyone even agreed that we wanted to do that, it would be years. To go through the contract amendment process; to change the policies; to make that a requirement. When you talk about requirements in this community it gets very tricky. So while

I understand the sentiment, I don't think it's an attainable goal. And Michele is about to come – go ahead.

Michele Neylon: Well you mentioned an IP address. This is one of the things about, I'm hearing people just talking about DNSSEC yet I'm not hearing people talking about IPv6. You want to resolve to an IP address. If there are no IP addresses and your IP doesn't support Ipv6 it's not going to resolve to anything. And I consider that to be hell of a lot more pressing than building up this false sense of security that signing a zone is going to suddenly give you some super duper power.

The other side of it as well is why would you sign a zone if the domain isn't actually being used or isn't even resolving? What about the companies and individuals who register thousands of domain names for a variety of different reasons and done actually want to do anything with them except just have them? So you want to force them to pay extra dollars just to get a false sense of security?

Matt Serlin: Yeah I think the tendency is because registrars are the link to the consumers and the end users that a lot of the expectation is that it's up to registrars to educate and to make – not just DNSSEC, but IPv6 – and everything to make that apparent to the end user. And I think registrars obviously have a different perspective on it.

Patrik Fältström: Let me just say that in .se we were the first ones started to do DNSSEC. We tried the first couple of months to charge for DNSSEC. Let me tell you it was the biggest mistake ever done in DNSSEC deployment. You cannot charge for it.

Matt Serlin: Right. You can't charge for DNSSEC. I think everyone – unless Michele chooses he wants to.

Michele Neylon: Oh I will quite happily charge for it.

Lars Liman: My name is Lars Liman and I'm with Netnod.se.com, operators of IROOT. I think you have to realize that security always comes at a cost and sometimes it's a necessary cost because we're fighting a battle here against evil forces. And that goes for any part of society. When bad things start to happen, when bad forces gain a new ability to intrude in our lives we have to kind of fight back or invent new ways to protect that. So it's like the question why do you have a lock on your door.

Well you take a cost of putting that lock in to prevent other financial damage that is supposedly or possibly going to be even bigger. So yes it does cost but hopefully it gives us something back. And I'm not saying you have to do it for everything, but I

agree that, I think that it's going to evolve into our default view of how things work. And initially it's going to be high cost because there's always a first implementation that is going to be expensive. But as time goes on we will find ways to automate it, it will be built in and everything and in ten years time all domains will be signed.

Matt Serlin: Yeah. And it's a fair point and I will take my moderator hat off and put my personal opinion hat on…

Michele Neylon: You have opinions?

Matt Serlin: Yeah I have opinions. I'm a firm believer that DNSSEC is absolutely a good step. My issue or my frustration with it is that it does not solve all of the problems in the world. It's a good step, but to Michele's point, I don't want the notion to be that okay checkbox, we've done DNSSEC, the world is a secure place; it's not. And there are many, many different vulnerabilities in the domain name space that still exist with DNSSEC.

Lars Liman: I absolutely agree with that, but I hope that we will reach a situation where people will be surprised – oh the door doesn't have

a lock. The lock isn't perfect. It could break and so on, but you expect there to be a lock on the door.

Matt Serlin: Yeah. That's a fair point. Yes sir?

Richard Lamb: My name is Rick Lamb from ICANN. And this is a question for Joe. First of all I'd like to thank Michele for slapping us around a bit because this is one of the problems I keep seeing is the adoption. But this is a question for Joe and any others might have any feedback on this. How much outreach to the vendors, or discussions have you had with vendors about DNSSEC?

I mean, I've gone to various trade shows, CES meetings and maybe some of the router shows as well and I walked the Expo floor and I talked to these guys and go hey look at this, this is a great thing. Let them market, they're great at marketing. These people will say "look, shiny". And get people to maybe pay for it. Maybe for the wrong reasons, but at least get it out there. But I get kind of a blank stare from most of these guys, so what have you heard?

Joe Waldron: Well we have done some work on that and others have as well. I know there was I think about two or three years ago the SSAC had a report on home router devices and whether they supported DNSSEC. One of the things that we did was go to those trade

shows. We would go to the shows and try to recruit some of those vendors to come into an interoperability lab that we provided, we have I think about 8,000 test cases you can come in and test at no cost, to find out whether the devices or the systems that your building operate within a DNSSEC enabled environment and test IPv6.

So we wanted to give them an opportunity before, and we started this before the root was signed and have been continuing it through today, but we've allowed them to come in. And we have been out there knocking on doors and trying to find some of those and we've had some of the big network providers come into the lab and test some of their equipment.

Richard Lamb: What have you heard for so far as building onto that? Not just DNSSEC, all this future application stuff. That takes about two to five years out for some of these people to get ready for. I mean for chip vendors it's usually two to five years. So, that's the kind of thing I'm just wondering. That should excite some of these people, maybe worry some of them, but that should excite some of them.

Joe Waldron: Right and again I can point back to some of the surveys we did and there is information that these companies are investing in security measures focused around DNS which includes DNSSEC. I think we're going to have the same challenge with preparedness for

IPv6. So I think it's the infrastructure challenge of making sure that the entire ecosystem, because no one component can handle this whole thing, but all of those different components have to be participating.

Matt Serlin: Yes sir.

Bill Manning: Your comment about being unhappy because you didn't have the Swiss Army Knife of security at your disposal kind of makes me chuckle right. DNSSEC is one tool. It's not going to solve the security problems in the DNS. It's going to solve one set of problems as Lars pointed out. I guess the second piece, about regarding cost, is that signing is only half the equation. Validation at the end systems and the ability for applications to take advantage of that has lagged the efforts up front.

So if you sink costs now to sign the zones there won't really be anybody that can use it for some period of time. And then the question is, this is a chicken and egg question and I think Steve Crocker pointed this out maybe a decade ago, which is which do you do first; the end systems or the infrastructure. The infrastructure was cheaper. There are still people working on that validation and application integration; it's not there yet. That doesn't mean you shouldn't provide the infrastructure for that to work because if you wait then it probably never will happen and you'll lost that tool.

Matt Serlin: Yep, that's a fair point. So I guess we've got about what five minutes left, four minutes? I'm being mindful of time Julie. So maybe just real quick, aside from a lot of the educational stuff that we've talked about, if both of you could speak just to what the biggest challenges are for registrar implementation in your viewpoint.

Michele Neylon: Well just going back to what Bill was saying there, I mean that's one of the key problems from my perspective. If there isn't any way for an end user to see something related to DNSSEC then they're not going to A-know about it. If they don't know about it they're not going to ask for it. And if they're not going to ask for it then I'm not going to invest significant resources in developing anything for it. Now you could argue that philosophically I should do it, but I'm sorry I run a commercial organization and I have finite resources. I'm going to put money into other things. For example, IPv6. I mean we enable DNSSEC on our resolvers and that took us 25 minutes to a half an hour so of course we did it.

Bill Manning: The key there was "significant". Don't not do it, but make sure that the value proposition is right.

Michele Neylon: Well my main problem is that I've got a To-Do List that never gets any shorter. I've got IPv6 on one side. I've got integrations of various ccTLDs, gTLDs. I've got SSLs over here. I've got new shiny objects coming from Microsoft. I've got another vendor over here who's decided to rewrite something and make it all lovely and wonderful and new this and new that and new the other.

There's all the other pressures and you have to come back down to something simple in prioritization and that's the key thing. It's fine if you are an uber geek sitting in the corner and you can look at all these wonderful things from a command line and chat with your friends in IRC and just go on about how wonderful the world would be if certain things happened. And I know these people and they talk about it.

It's like when I was talking to one of my techies and I said "Do we have enough bandwidth in the office?" And he goes "Oh, don't worry, its fine. If we need more we'll just get more." And I was like "Hold on a second." So I pulled him out, took him into the office and I said "Alright, choose one of your colleagues." He said "What do you mean?" I said "Well you want more bandwidth; choose one of your colleagues." He said "I don't understand."

I said "Well, if you want more bandwidth I can get it for you but I have to fire one of them because the bandwidth into the office is going to cost so many thousand per month. If I increase it by 20, 30, 40 megabits I'm going to have to pay for it from something." I mean, sure technically it's feasible, but financially it wasn't. And that is the thing. You've got to make it so that it's financially

feasible as well as technically feasible. And that's the kind of gap that I'm seeing.

Matt Serlin: Joe I'm going to give you the last word.

Joe Waldron: So, I guess I'm the glass half full guy. I do think that we'll continue to see adoption. I think we need to continue to educate the community all the way down to end users. Michele will beat me up afterwards I know, but that's okay. And I think the adoption is going to be slow and continuous and then we'll reach some critical mass. And I think, whoever it was said at some point, I think it was Lars, at some point it will just be there for everything; it will just become very routine. And until we get to that point though, we're going to have challenges; things are going to be more brittle.

There are things that break because you have DNSSEC; we have to do things differently. So we need to be aware of the challenges. We have really just begun with the deployments that have happened to date and there are more coming, but this is really the start of the road of a DNSSEC enabled internet and I think we'll all be working together on this for a very long time.

Matt Serlin: Great. Well I'll turn things back over to our hosts. Thank you all for the invitation and for organizing this. Thank you all for participating and we'll see you.

Julie Hedlund: And thank you Matt and Michele and Joe. Please join me in thanking them. And we'll just take a moment to switch to our next panel. Welcome everyone. We're going to transfer to our next panel discussion. It's on the topic of domain name transfers and I'd like to introduce our first panelist, that's Debbie Monahan from .nz and I'll go ahead and turn it over to you Debbie.

Debbie Monahan: Thank you very much. I'm just going to start very briefly by talking about our structure. .nz is set up a little bit differently from a number of others in that we actually split our technical and our regulatory or policy functions. So at .nz the delegation holder is Internet New Zealand, it's an incorporated society owned by its members.

They have set up two subsidiary companies wholly owned by Internet NZ. I'm the CEO and Commissioner of the Domain Name Commission and we're responsible for the oversight of the .nz space. We set the policies, authorize the registrars and ensure compliance against those. The registry, which is actually run by a guy that many of you all know, Jay Daly, is responsible for the technical operations; running the registry and the DNS. Next slide.

So with that structure in mind our DNSSEC development has, if you like, controlled two parallel strings. Both with the same goal of maintaining the chain of trust throughout the entire process. With NZRS responsible for the technical implementation and the Domain Name Commission looking after the policy development. Next slide. So what do we look at when we're doing the policy considerations? This has been mentioned this morning – what is recorded in the registry; who is responsible for what; how do we manage transfers; and how do we manage unsigning a name. Next slide.

So what was decided is that the DS record would be generated and added to the registry to enable the DNS key to be authenticated and that the DS record would be added to the WHOIS output. Next slide. Registrants or the DNS operator will be responsible for managing, generating their own keys; determining how often they perform the key rollovers; and generating the DS records.

So we ourselves won't be actually defining the standards for those, but that could be a point of differentiation between the different services the registrars actually offer. And registrars are responsible for adding the DS records to the registry. And a key part of this is it's only the registrars that have access to the registry to update the records of the domain names. Next slide.

So then how do we manage transfers? Possible approaches are not to allow the transfer of a signed name, or require a name to be unsigned before the transfer. Basically there's no problem if you're happy to sign a name and stay with the same registrar.

However, some registrants might not want to do that. They might want to change whose hosting the name, who's the registrar of the name and unsigning to them, might not be an option. So the possible approach is effectively lock a registrant into a registrar.

And we consider that unacceptable because we've set out to create a competitive environment giving registrants maximum choice and the ability to transfer between different registrars. So our approach was to try and define a process of cooperation in the transfer process. And I think as has been mentioned by Michele, that's not always an easy thing to achieve.

What we do have though, is that registrars are governed by .nz policies. So what we can do, in respect to registrars, is specify that cooperation that's required and our policies to which we govern and control the registrar's actions. The problem is that not all host or DNS operators are registrars. They could be or they could be the registrant or an ISP, any hosting provider. And the problem is that we do not have contracts or cannot control the actions of those DNS operators.

We asked in our various consultations for what possible solutions we might be able to come up with and no suggestions were basically received as to how we could actually get those DNS operators involved. But what we have put in the policy is that the Domain Name Commission will establish a contact repository where DNS operators who aren't registrars can actually log their information with the Domain Commission. And in the case of a

communication issue during a transfer, we can help facilitate contact between the parties.

But what we did do is change our policies and put in what cooperation and participation of the registrars was required. So it only applies in a very limited set of circumstances where both the current and proposed DNS operators are registrars. And as you can see on the screen that prior a name server update the losing DNS operator must provide the zone information from the domain name when requested to do so, and accept and add the new DNS key to the zone for the domain name. Resign it and continue to serve this until they are notified that the change is complete.

The gaining DNS operator then provides the new DS record to the losing DNS operator who provides it to the registry. The name service for the domain name can then be updates with the registry. Following the name server update, the gaining DNS operator must delete the old DS record and DNS key provided by the losing DNS operator. The losing DNS operator must remove the domain name from their name servers when requested, but must not remove it before being requested to do so. So that's actual wording in the policy and the policy does actually say that DNS operators who aren't registrars are also encouraged to follow the process. But as I said before, we have no control over whether they do or not.

And in respect of managing unsigning, again we've actually put in the policy that registrars are required to remove the DS record for an unsigned name as soon as it is practical to do so once the registrant elects to unsign the name. Now, we're not saying that

these policy positions are perfect. We got some great feedback from a number of registrars, including [Glen Ustus] and others who actually helped mold the policies. We don't believe that on Day One that we're going to be faced with a large influx in numbers of people who are going to want to sing names. We expect to have to reform and revise the policy as we go on and potentially as it develops, look at ways we can actually automate it to try and remove any potential issues from the process.

In respect of our timing, the registry is well advanced and they're currently undertaking testing. And if all goes well to plan and there's no fish hooks along the way, they're looking at being fully operational by the end of this year. And more information on the technical side is on the registry site nad on the policy side is on the Domain Name Commission site. So the links that are there are provided. And feel free if you have technical questions to contact Dave Baker who is here from the registry. I myself am on the Domain Name Commission side and so we'll refer to any technical questions asked in this session to… So thank you.

Julie Hedlund: Thank you very much Debbie. And I think what we'll do is we'll just go on to Roy's presentation and then we'll save the Q&A for after the presentations. Let me bring your slides up for a moment Roy.

Roy Arends: Thank you Julie. My name is Roy Arends. I work for Nominet UK. I'm the Head of Research there. At Nominet we do things slightly different than the rest of the registry world. Next slide please. In terms of domain transfers we have a push model. What it means is that if you transfer a domain between registrars, the transfer needs to be initiated from the losing registrar to the gaining registrar. So domain name transfers from A to B, it's A who pushed the domain to B. Now that's different from almost all other registries. Most of the registries that I know have a pull strategy where the domain name transfer is initiated by the gaining registrar.

The gaining registrar at Nominet needs to explicitly accept that change. The alternative is that it has auto accept enabled so that it by default accepts all incoming transfers. Another thing we have now at Nominet, we have a bit basically that says that registrars must indicate that they can handle DS records. It's basically a one pager with a "yes" button on it and when the "yes" button it clicked then the registrar admits or we see the registrar as DNSSEC enabled.

So I'm not going to talk about DNS and DNS domain transfers from the operator's perspective but totally from the registrars' perspective because we deal with registrars and not directly with registrants. So if you look at this in a binary way a domain name might be signed or might not be signed. The losing registrar might be DNSSEC enabled or might not be DNSSEC enabled. And the same goes for the gaining registrar. So that gives us eight possible

different tracks, but let me quickly turn it down to two. If domain is not signed we don't have to talk about domain signing transfer. If the losing registrar is not DNSSEC enabled then the transfers won't be signed. So that leaves us with two states that we have to think about.

One is a signed domain transferred from a DNSSEC enabled to a DNSSEC challenged registrar. Or it transfers to a DNSSEC enabled registrar. So we have two different things that we do. One is if a domain name transfers to an enabled registrar we keep the DS records. We don't touch it; we keep it intact. We see it as just another string just like NS records that transferred with it. If the gaining registrar is not DNSSEC enabled, we simply drop the DS records. And the reason for that is if you keep the DS records intact the registrant can't go through their new registrar to change the DS records. So in a sense the DS record becomes orphaned.

So that has as few consequences, this policy. So if we remove the DS records because of this policy and because the new gaining registrar is unable to work with DS records; that means that the domain is seen as unsigned or as not signed. In fact, DNSSEC records might still be there, but we've simply taken out the link in the chain of trust.

Now, if the registrar, the gaining registrar is DNSSEC enabled, we keep the DS records intact. So we don't do anything. That means that if the operator stays the same, so a single operator just chooses to switch registrars, then in fact there is no problem. But the advice from us is if the operator is changed as well, then it's

unlikely that the gaining operator will keep on using the private keys it has gotten from the former operator. So it has to initiate a DS record change. But it has to do it itself through its registrar through to us. We don't do anything with the DS records if the gaining registrar is DNSSEC enabled.

We don't want to be the exception in the registry world. We want to make it easier for registrars to deal with a single policy. Now of course that's not always possible. Registrars and registries have different policies. But we are discussing this European wide with Belgium, the Dutch and with EurID, with the Germans, we are in talks with Afilias on this to look at each other's policy on this and try to come up with the least set of options if that makes any sense.

That's it for me. Thank you. I'm handing off back to Julie.

Julie Hedlund: Thank you Roy and I think what we'd like to do now is go ahead and open it up for discussion and questions from the audience. So would anyone like to be the first one? No one ever seems to want to. Ah, Bill. Thank you.

Bill Manning: Bill Manning. Co-opting Patrik Fältström. The question that I, every time I look at this the thing that concerns me is the case where the delegation has released the DS record in the form of a secure entry point to its clients and they have put it into their local

validator. What mechanisms are there to help those people update their local key rings when change occurs?

Roy Arends: Bill what we recommend is not to configure any local domains in their validators. So that means that if you configure the root key in your resolver that's fine. We always recommend against configuring the .uk key the co.uk key or any one of the sub domains. What you will see in general and what we have seen in the fields is that folks who do locally store trust anchors for local domains, it's mostly their own domains. We have hardly seen anyone configuring a delegation from Nominet – sorry a delegation assume for instance bbc.co.uk – by someone that's not bbc.co.uk. So my recommendation is against this. What do you do? I don't think we need to have a technical answer for this non-problem.

Bill Manning: Okay, so based on Roy's recommendation everyone on the internet will acknowledge Roy's recommendation as a sound, stable one. It doesn't happen Roy. I know people that in fact do put secure entry points in and continue to do so even after the root is signed because you do not have a consecutive chain. There are good policy reasons to actually put in extra entry points. So recommendation or not it does happen. I appreciate your response that says you have no plans to help people identify and mitigate this particular problem. Thank you.

Roy Arends: Well, let me just rebuttal this a little bit. There is a protocol extension called RFC 5011. We haven't implemented that and I recommend that anyone who configures a key locally, for some domain, makes sure that that domain actually has implemented 5011. That's it. Thanks.

Patrik Fältström: I have a question for you on your slides from what you do in New Zealand and you talked about DNS operator and when you as the registry detect that the DNS operator changes – can you go a little bit more into how you do that detection? And the reason why I ask is because this is something we've been discussing in Sweden since we deployed DNSSEC and we have not found an easy way of doing that.

Debbie Monahan: The policy only covers where the DNS operator is also a registrar and that the transfer is transferring not only the registrar but the DNS operator at the same time. So the policy can only cover that limited seat of time.

Patrik Fältström: So how do you know whether the registrar is also the DNS operator?

Debbie Monahan: They would have it in their systems as well; the name servers and other such things that they're bound by. So basically it's where it's a name server change. The registrar is controlling the name server and the registrar is also controlling the domain name management; the management of their domain name. But prior to that, one of the checks that a registrar on accepting a transfer, if they are not DNSSEC enabled they need to check whether the name is signed before they'll accept a transfer in. So there's a number of other policies stips that we've got in place to try and protect someone who's actually signed a name.

Patrik Fältström: Okay. But I would like to talk more about this later on because if it is the case that you have your zone signed, it's not very often the actual signing that's happening on the name server that you have the delegation made to. So you don't have the NS records at this point into whoever is actually doing the signing which means that you don't really detect, in many case, that the DNS operator that is signing the zone is changing. And the NS record change, it's not really detecting that, but we can talk about that afterwards.

We have some experience with the change there because we need some ideas on how to solve this problem. Because one of the things, let me continue this, we do not want to go down the path of forcing the DNS operators to registrar with the registry because that creates problems with DNS operators that are sort of far away. So we'd like to stay away from that problem, but it's a difficult problem to solve. Thank you.

Julie Hedlund: Thank you very much. More questions from the audience?

Steve Crocker: I've got some from up here. The first one is for Debbie. I'm really pleased to see that you're recognizing in your policy structure that there's at least a potential or a theoretic separation between the registrar function and the name server operator function. Do you have information that gives you any insight as to how frequently they actually are separate entities? 1%, 20%, any idea?

Debbie Monahan: The fact is that we know from looking at the records that a number of .nz names aren't actually hosted by the registrar that's actually managing the name. But to us, it's the issue of actually the DNS operator versus the registrar. And to be honest this is an issue we actually have now with name server changes. And I feel like Michele kind of referred to it before. Some don't honor time to delivers and other such things so there's no standard governing DNS operators doing name server changes now anyway, even without DNSSEC.

So this doesn't try and cover all DNS opportunities and transfers, but DNSSEC adds a complexity to it. And we're hoping that as we work through those issues we actually might learn more to actually give us some solutions to the whole general issues of name server changes on domain names.

Male: One of the things that seems to be inconsistent in various parts of the world is how much transfer actually occurs of names and name servers. And I think that as ccTLD folks, do you have any insight as to some percentage or how when a transfer happens are there some people that have a name that are sort of registrar hoppers or is it sort of randomly...do you have any insight in those kind of activities because that will clearly affect how important or how bad the problem is for DNSSEC is how much it happens later on.

Debbie Monahan: We do monitor the number of domain name transfers between registrars. The thing is in .nz it is actually free to transfer, you just can't transfer during the five day registration grace period. So we do have people who will go to the cheapest registrar to register a domain name and after five days transfer away to someone who might have better services. So there are people who actually do that. We don't believe, there's not so many, the percentages are still relatively low though compared to the number.

And we believe that the percentage that will actually sign a name and then want to transfer will be significantly lower even again. Probably a lot of businesses tend to have relationships with their provider and will stay there and probably at the start, especially the ones that will be most likely to sign will be organizations who want to add that extra degree of security.

Roy Arends: I don't have the exact numbers that you are asking for but our registry is growing close to 10 million data points currently. We see an enormous amount of changes. And with changes I mean address changes for instance or status changes or anything really, or one NS record changed; that kind of changes. So part of those changes of course are tack holder changes; basically when a domain holder changes to another registrar. I'll have to find those numbers out.

We do have them, but I'll have to find those numbers out. The other thing is with regards to registrar transfers we do see a lot is for instance when a large registrar changes one of their name servers where they have a fair amount of domains parked for future use or hold; when they change one of these name servers it's in fact a single change, but we see 10,000 changes in the database. So we have to define before we can talk about those numbers what exactly is measured.

And even in the internal organization we discuss things like what's the unit of change. Do we measure for instance per five minutes, per hour, per day, per month – and do we bucket them and say what the averages are. And that's the research, from my research perspective I want those numbers to be accurate. So I can't give you a ratio, I can't give you a percentage. But if I dig a little bit deeper I'll have an answer for you. Thanks.

Male: Well one of the reasons that I'm asking, and this line of questioning is certainly the gTLD affiliated registrars that are very much in the heavy competition mode with each other. And I know certainly the ccTLD registrars are too, but it varies somewhat by cc. In terms of transfers with DNS once a zone is signed, one of the things that I've not heard mentioned by some of these highly competitive folks is what to me seems like a potential business opportunity for someone operating a separate name server service that would be in place primarily to facilitate transfer between registrars.

Because if the registrar function and name server function for a signed zone are separated, the transfer between registrars is much simpler. And I didn't know if that was anything that either of you had heard anything about or heard any discussions about as a potential opportunity for somebody to set up essentially a transfer-centric name server service?

Roy Arends: Yes, we have thought about that, but it also relates to the fact that we push domains from – or that registrars push domains out of themselves so the transfer is a little bit easier. But we still do have those moments where a losing registrar might not be as cooperative as it needs to be, for instance sharing the private keys and might have a good policy for that. We have a new service that will soon be rolled out and we've talked about this at the last ICANN meeting.

And this is a service called DNSSEC as a service. What it means is that we actually are able to sign other people's domains and just that; just sign them. And become a bump in the wire basically that we receive a transfer from the losing registrar for instance, sign the domain or from the operator, sign the domain and so we basically become the transient man in the middle, the registrar in the middle. So that we can both be the cooperative gaining registrar and subsequently to be the cooperative losing registrar.

Steve Crocker: I like that. I like that cooperative registrar in the middle idea. I haven't heard that before. One of the more subtle details in this process has to do with how long the transfer takes and whether changes to the zone are permitted during the transfer process. Those two things are tied together of course. If you transfer very quickly then it's okay to take an interrupt in your ability to update it, but if it takes a very long time to transfer because it's a very big zone, then that may be a further complication in the operation of that zone. Have you anything to comment about that?

Roy Arends: I was about to say one minute longer and I'll start dancing and I'm not sure that's a good idea. We did consider at one point in time what the delay should be between the transfer between the gaining and the losing registrar when you transfer a domain. The thing is from an operational perspective it's actually an atomic action; moving the tack from one registrar to another. So if you have a

domain name it's either with registrar A or with registrar B so the change is atomic. So introducing a delay means that you have to come up with a threshold that you can introduce. And I think that every threshold that you introduce makes the whole effort much more confusing.

Steve Crocker: So, I apologize. If it's solely transferring the registrar function then I agree with you because that really doesn't have any impact on the resolution process. But if you're moving the zone operation, the name service from one to another then that's a multistage process where there's got to be some overlap between the old and the new.

Roy Arends: Yes. So this is actually independent of registry. If a domain holder transfers between operators and both can sign the domain name, then what we recommend is that the gaining operator will first completely set up the domain so it resolves and the two servers then run in parallel from the old operator to the new operator; run in parallel. Then the registry may switch and then the old operator can stop hosting the zone. There are a fair amount of timers that need to be checked. There's the TTLs from the parent's, the TTLs from the child – what Michele just mentioned that some ISPs will still go to the old name servers. You elaborated on this in your last ICANN meeting. This is a child sticky DNS resolver and you have to take care of that as well. And

then of course when you sign the domain, when you transfer the domain, sorry when you do a zone transfer from a primary to a secondary that's yet another timer that you have to keep in mind. And all these things amplify each other.

Steve Crocker: I have just one final I guess response based on the earlier interchange on the push model question that Bill asked and the trust anchors and so forth. And that is that I would hope as the education and policy documents get put together that there is information as part of that that makes recommendations to people that are using this approach for transfers that, just exactly what you said, they either not use trust anchors or recommend that their secure entry point not be used as a secure entry point. Or if they do that they be sure to use the 5011 mechanism. So get it well documented so people are at least warned that that's the expectations.

Roy Arends: And if I may respond to that – within the IETF there is a process currently going on to get something called a DPS standardized. A DPS is a DNSSEC policy statement and several registries have done this already. We have a fair amount of internal documentation that all put together overlap a DPS, but we don't call it a DPS yet. And as soon as that is standardized we can put our information in the DPS, we can actually already start and we have some internal stuff, and that will explain exactly how we do

it, why we do it, when we do it and also to a certain limit say what we don't do compared to what others do. Timers will be in there. The machines that we use will be in there. The HSMs that we use will be in there. The documentation, it's available, currently only on request. But it will be publicly available once we publish our DPS.

Steve Crocker: Great. Thank you very much, Debbie. Thank you very much Roy. And thank you to your organizations for being so engaged and supportive of the whole DNSSEC deployment activities. We recognize your very valuable contributions to the community. Thanks again.

Julie Hedlund: Please join me in thanking them. Now we have time for a very short break, about 10 minutes. The program will start up at quarter past the hour at exactly 10:15. There should be coffee out in the lobby area and we'll see you back here shortly.

[Break]

Julie Hedlund: …in the vicinity to come on in and join us, bring in a coffee if you want from out there. We will have lunch starting at 11:45 and that will be part of the program for those who are participating here in

the room. So again, welcome to the DNSSEC Workshop and we'll start momentarily.

Welcome everyone again to the DNSSEC Workshop. We're going to get started on our next panel discussion which is Experiences, Challenges, and Outcomes of DNSSEC Deployment. Id' like to take a moment to introduce our moderator and our speakers and then I will turn it over to the moderator. Our moderator for this is Russ Mundy, the co-chair of the DNSSEC Deployment Initiative. Our speakers are Kazunori Fujiwara from JPRS, Vincent Levigneron from NIC.FR, Peter Losher from Internet Systems Consortium and joining us via video is Roland van Rijswijk from SurfNet. So without further ado, I'll turn things over to Russ Mundy.

Russ Mundy: Well this is a great opportunity for us to hear from folks who have actually gone forth to do DNSSEC things in the real world and are willing to share some of their experiences. And we're very pleased to have our set of folks. We encourage questions and interactions. We're going to go through the presentations and then have a question period at the end. So let's go ahead and get started with our first presentation from Japan.

Kazunori Fujiwara: Hell. This is Kazunori Fujiwara from JPRS. I will talk about DNSSEC deployment in .jp. Next slide please. This is today's

contents. Japanese background – what we did – technical evaluation – DNSSEC introduction process.

Japanese background – deploying new technology requires documents written in their own language. But most of DNSSEC materials are in English. There are thousands of ISPs and hundreds of JP registrars in Japan. They offer various DNS services. Their cooperation is requires for successful DNSSEC deployment, but hard to contact and conduct all of them. Next slide please.

What we did – we did enough announcement; technical explanation documents in Japanese; rill out schedule' DNSSEC parameters; JP DPS DNSSEC practice statement. And we did enough technical evaluation with ISPs, vendors, and JP registrars. They did their evaluations for their works. Next slide please.

Technical evaluation – we did two activities: technical evaluation by JPRS and participants conducted by JPRS and DNSSEC Japan, a community initiative. JPRS is a member of DNSSEC Japan. Next. Technical evaluation by JPRS – JPRS did DNSSEC technical evaluation with some participants before implementing DDNSSEC in JP TLD; November 2009 to November 2010. Purpose to collect, share and publish DNSSEC operational practices. And major ISPs, hardware vendors and JP registrars will implement DNSSEC easily.

What we have done – JPRS called for participation in technical evaluation activity to some major ISPs, hardware vendors and JP

registrars. JPRS offered the DNSSEC test bed. JPRS conducted monthly information exchange meetings among participants.

DNSSEC technical evaluation by JPRS. There are six steps, in step from November 2009 to February this year JPRS and JP DNS operators did fundamental functional tests and behavior check of zone transfers. In step three, four, March last year to June last year, ISPs and the hardware vendors joined and we did behavior and load check of full resolver, validator DNS servers and behavior check of network devices. And we listed check items of ISPs and hardware vendors. In step five, July last year to November last year, JP registrars joined. We did behavior check of DS registration and accumulation of operation experiences. And we also tested domain name transfers and then in step six we did joint evaluation with DNSSEC Japan.

This is evaluation environment. JPRS offered pseudo root, pseudo JP-DNS, pseudo registrant DNS and pseudo registry system. And the JP secondary offered pseudo JP-DNS. ISPs and vendors prepared network devices to the pseudo full resolver validator and load generators. The tested name resolution test and performance measurement and that light came, shot through JP DNS, shoot to each of our DNS servers. And the JP registrars prepared pseudo registrar system, pseudo DNS hosting, pseudo validator. The used pseudo registry system. Next.

Results of technical evaluation – participants and JPRS have published four documents: DNSSEC function check instruction; DNSSEC performance check instruction; DNSSEC technical

evaluation report, function and performance check edition' DNSSEC technical evaluation report, operation design edition. Reports are published in the JPRS webpage, but in Japanese language only. English translation is ongoing. Participants and JPRS made DNSSEC presentation at local meetings. Japan network operators group meeting July of last year and Internet week, November last year. Now many stakeholders started or are planning DNSSEC service.

DNSSSEC Japan, a community initiative. DNSSEC Japan was formed at November 24, 2009. DNSSEC Japan is a forum for domain name registries, registrars, registrants and relevant parties such as DNS and network operators with the aim of introducing and deploying DNSSEC. DNSSEC Japan's objectives are to sort out and discuss issues in relation to deployment and operation of DNSSEC; to enhance technical capability of participants and sharing of technical expertise; and to conduct outreach activities such as providing relevant tools and giving technical commentaries.

Results of DNSSEC Japan – DNSSEC Japan published DNSSEC documents in Japanese and DNSSEC Japan held DNSSEC forum meeting twice and members are well learned in DNSSEC. Member organizations are 36 and web page is here but in Japanese language only. This is DNSSEC introduction process in .jp. July 9, 2009 JPRS made first announcement of DNSSEC introduction schedule. Target was by the end of 2010. Then November 24, 2009 DNSSEC Japan was formed. December 1, 2009 technical

evaluation by JPRS started. July 21 last year JPRS made a schedule announcement, the month of signing and DS registration. August 30 last year JPRS published DNSSEC parameters for JP zone. September 6 last year JPRS made an announcement of the date of signing and DS registration.

In September 29 last year JP DNS servers and the JP registry system came to DNSSEC ready. And October 17 last year JPRS started signing of JP zones. November 30 last year technical evaluation was finished. December 10 last year JP DS was registered in root zone. January 14 this year JPRS published a JP DPS. January 16 this year DNSSEC service rolled out. JPRS started DS registration. And May 27 the DNSSEC book was published in the Japanese language and currently 20 registrars registered about 300 DS in JP domain name.

This is a DNS book, [Descend DS]. [Descend DS] means practice DNS. Newly published on this May, authored by JPRS employees, it explains daily DNS operations with DNSSEC. Conclusion – documents written in own language are important. Joint evaluation with stakeholders are important; they become DNSSEC experts in their companies. Thank you.

Russ Mundy: That's great. Thank you and it makes an obvious point of the importance of language because if it's not in language that you can use and you readily grasp it makes it hard to handle. Okay, let's move on to what I'll call the French experience.

Vincent Levigneron: Thank you. My name is Vincent Levigneron and I work for the French NIC registry and some ccTLDs. Next please. Okay, this is the plan of my presentation, not be very interesting, but it will be interesting when you download the full presentation. Next please. Afnic is a registry and it operates six ccTLDs and this is the list of ccTLDs – fr, re, pm, tf, wf, and yt. Each of the zones is signed and DNSSEC was introduced in September 2010. And for each zone we roll over keys, zone signing keys every two months.

And we have chosen to use NSEC3 and opt out options for these zones. Amongst these zones, fr zone is the largest one with more than two million domain names. It's not a very big zone but it's a middle sized zone. And the zone contains about four million resources records. But amongst these resource records we have very few DS records and registration of DS has been launched less than two months for fr and re. So for the moment there are not a lot of customers that want to sign their zones it seems. Next please.

We also use open DNSSEC, but it's only used for key management. We don't use the full capabilities of open DNSSEC. For our key storage we use AEP Keyper HSMs. And all the signature stuff is done by BIND and we use auto-DNSSEC all option. Of course all the NAT is done in the HSM, but BIND controls this.

When we started DNSSEC we used the version 9.7.1, but now we are to change and we deployed the 9.7.3 version after the second outage we had. And we also use a homemade synchronization script to create BIND key files that are understood by BIND and from open DNSSEC data. This is not the same version of key files.

Next please. While there are more than four million records in fr zone, there are less than 100 NSEC3 records and very few signatures. We have at the same time 2 KSKs, one is just published and the other one is active. At the time we have between two or three zone signing keys. One is published and ready to be used and one is active and used to sign records and if we are just after a key rollover, the older active key is still published while inactive.

We dynamically update our zones every hour and once a week there is a complete zone file generation, but it's mainly for administrative purposes. We use dynamic updates only for delegation, not for all records. We use dynamic updates for NS, A, Quad A and DS records. And all key and signature stuff is based on the automatic signing BIND capabilities and we don't use dynamic updates in this case. Next slide please.

We have chosen to use a very large timing when we are under a key deletion process. And when a key becomes inactive it is deleted only one month later. That's why when you create a .fr zone you will often notice that there are more than two zone signing keys at a time during your key rollover. When a key is

deleted we purge the key files three days later. It was just one hour during the first outage we had in last November, but it has been increased after that event. And when a key is about to be deleted we are sure there are no signatures left corresponding to this key.

In fact we had three big problems, not that big because people don't really sue DNSSEC at the moment unfortunately. But the problem is that outages were visible so it's not very good for us. And during key deletion we had a network issue making our HSM unreachable.

The error was not well detected and so the publication process didn't stop, it should stop but it didn't stop as expected. And the zone was not updated as expected and key "delete" state was still present while it was inactive. Our homemade script, which is an open DNSSEC to BIND synchronization process, decided to purge the key files one hour later because it was supposedly deleted. Then, of course, because the key files were missing BIND couldn't process dynamic updates anymore. And that caused a zone file was not signed at this moment. And we also had a BIND private record bug, but we just discovered that two months later because we were so focused on the other problem, the HSM problem, that we just discovered that later. Next slide please.

After that first outage we thought everything was under control, but with DNSSEC you have some surprises. So in February we should have been a boring key deletion operation, but we had an unexpected behavior from a BIND private record usage and this record is called the type 65534 and in fact it is used to give the

state of the sign in process. Perhaps you have never seen this record before if you don't use automatic signing, because it's only used in this specific case, but it's very important record you have to take into account if you use that functionality from BIND.

And what was expected from our point of view, and or course in less than a blink of an eye, after the deletion of the key the DNS resource record corresponding to the deleted key needed to be removed. So the DNS key and resource record set signature needed to be updated. Of course the serial number should be incremented and after this incrementation SOA signature had to be updated. But unfortunately there was a bug in BIND, but of course is has been patched since, very fast indeed.

And that bug led to a bad signature on Apex and NSEC3 record. And at this moment, the fr zone became inaccessible to any validating resolvers. In fact, this was not the first time we had this problem, but it occurred in small zones because we have the fr zone which is very big and the other zones are very small. But it was visible for less than a second, but with a bigger zone it lasts hours so of course it's more visible. Next slide.

The third and perhaps we hope the last DNSSEC outage was in March. Of course after the second problem we had we were working to find the solution but we didn't have time to put this solution in place. And unfortunately we had another problem. And it does happen during where people were in the office so it was not very easy to endure with it. So in the morning in fact there were key states transition on zone fr, it worked. Following

dynamic updates were well processed. Then BIND decided to modify its private records that we had just talked about. But at the same time, unfortunately, again we had an HSM reachability issue and the published zone was not correct.

And a new type 65534 record has been added to the corresponding resource record set. As well the resource record has been modified as expected, but two signatures were missing. The one for this private record and the one for the SOA record. There is already a patch, of course, and it has been applied since. So the slide is not up to date. Is a signature missing for an SOA a big problem? Not really, but it could be worse.

And of course it went worse because we have two NSD name servers amongst our slaves and in this very special case, NSD did something unexpected and the behavior was the same on the two name servers. It also decided to remove all signatures of the Apex, which is in this case very bad. And there is already a patch. And that's what we discovered with DNSSEC, there are bugs everywhere but there is a patch always, very fast. Next slide please.

We would like to thank the community because when we had these problems our monitoring systems failed and now it's better because we have improved our system, but when we launched DNSSEC we didn't check NSEC3 resource records and the first alerts came from people, and perhaps there are some people in this room that sent us email or called us to tell us everything was broken and please do something.

And the problem was those of you who already use validating resolvers were not able to send us emails of course. In this case, we discovered that social networking is a good means to communicate between registry and the community and we received a lot of tweets and direct phone calls.

To help us, ISC provided a patch very fast. And as I told you we also found a bug in Unbound and the patch has been published. In fact, we found the bug in BIND, Unbound, NSD and lot of DNSSEC tools. We also had good feedback on our search for a zone verification tool. For instance, IDNs was really promising but not fast enough. It's not very easy to find a tool able to deal with the a medium sized zone. The last tool we found was validns. While very young and still under development, it was able to deal with millions of entries very, very fast. So it's perhaps the tool that we are going to adopt in the next week. Next slide please.

And what happened after this outage? There will be other issues and unfortunately we are pretty sure there will be other bugs and problems, even if we patch tools. Just after OARC/ICANN meeting, not this one but the last one, we had crisis meeting to decided if we should remove the Afnic ccTLDs DS from the root because it was not a good situation with all of these problems. And some of us wanted to keep the key in the root zone and some of us didn't want, so it was a very difficult discussion.

But it was decided that we would keep DS if we could and finish the implementation of our proxy and deploy it within the next two weeks because we were already working on a solution to avoid the

zone file to be spread and is already a problem in it. It was not deployed when we had the last problem, but it was almost finished.

It was also decided to postpone the implementation of this service for inserting DS records into the Afnic zones, which was the next step of our DNSSEC project. We have also modified our system to have better control of our zone changes and now the zone is validated before it is sent to our hidden name server. And the new notify proxy server controls this. And eventually we launched our DNSSEC-aware version of Zonecheck, which is our technical checking tool, as well as a new version of EPP server.

Our proxy server, I call it our proxy server because it's almost, I know there are lots of people working on such a solution. So first objective of our proxy server is to coordinate all different DNS publication process, which are mainly dynamic updates, key management, complete zone file generation, the proxy itself, zone file transfer between internal name server of hidden primary name server and other things. This prevents for instance, BIND from modifying private records during other DNS processes.

The second objective is to add a validation step in this proxy. In fact, there are, from our point of view, mainly two ways for that. You can do a complete zone DNSSEC validation. It's a long term plan and it's not completely and fully implemented yet, but it should be in the next week. Or you can just check Apex records and some specific ones and we noticed it would have been enough to detect the outages we had; if we had just checked some specific records.

And if there is a problem, the proxy stops the publication system and prevents the transfer from our hidden primary name server. So we tested with this system and if we have new problems the zone file could stay on our private server and should not reach the hidden primary name server. The next steps on these tools are we need to automatized the recovery system because it's not fully documented, it's very concise when people that knows how it works and it's me. And okay, I have to document it and explain to our team how to do if it's broken. And we need to integrate our zone file revision system in the proxy. Next slide please.

Okay, I don't have time for that, but it's mainly our system how it works with lots of the different servers that do publication and the proxy. As you can see on the right of the scheme, it receives notification from our hidden name server, then checks validation (inaudible) and if it's correct it will send notification to the public name server and then the transfer can begin when everything is correct. And if there is a mistake, of course, the transfer is not done. Next slide please.

What we have learned with these problems, the main one is regarding different aspects. DNSSEC is still young and it was still possible to find bugs in the most common DNSSEC tools – Bin, Unbound, NSD, etc. But the good point is that these tools are patched very fast. We also learned that teams training is essential. And when you master DNS it doesn't mean you deal with DNSSEC easily. DNSSEC specialists are still mandatory when problems occur. And we also discovered that there are few field

proven tools available. And zone size is often a problem with the tools.

You should keep all zone file revisions to find the bug, but if you are in the same case as us with a dynamic update and automatic signing, it's not of use to keep all the zone file revisions. But hopefully we have deployed a zone revision system just a few times before the issues and we just missed a version of the zone.

Of course you need to monitor and monitor and monitor again…we didn't monitor enough, but now perhaps it's not enough, but we monitor more than before and we hope that we will find very fast if there is a new problem. And something very important, it's not technical, but we discovered that it's very important to provide as fast as possible completely transparent information to our community. It was much appreciated and all details for each outage is published on our public website and it's still available.

And the good news is that we are not alone. Next slide thank you. And when we had our problems, RIPE also had issues with DNSSEC and we started, not just with RIPE but also with a guy from NLnet Labs, DENIC, etc.; first discussions about the need for a DNSSEC verification tool on OARC mailing list. And with other interested parties in this topic a first meeting was held to gather first requirements during OARC meeting.

And there was a informal meeting during IETF 80. Discussions are still in progress. If you are interested and you can join the mailing

list, it is hosted by NLnet Labs. It's not very active at the moment; there are not a lot of emails. But people are working on tools etc. So if you have some request or if you are interested by some options, please join us and tell us what you are looking for, etc. And it's over.

Russ Mundy: Great. Thank you very much and thank you for sharing those experiences, we really appreciate that. It's very helpful for the community to hear such a forthright description and good details of what happened. Now we'll go onto Peter Losher to tell us about some of the IOC experiences.

Peter Losher: Hi. This will be slightly a more operational and a little bit less technical presentation. This presentation has been given at some of the operational conference like NANOG and as well as the DNS OARC conferences. So some of you may have actually seen this before. This is called DNSSEC in the Glue – an operational tale. Next slide.

The network impact of DNSSEC – it means that now signed DNS responses are big, and we'll show you a little example of that on the next slide. Because they now have DS, NSEC, NSEC 3, DNSKEY and RRSig data. Which means that they dramatically increase query size responses. And because it means that 512 byte UDP packets just don't cut it. So if you thought that DNS was still

just 512 bytes UPD, you're sadly mistaken. And that EDNS0 is no longer just nice to have. Next slide.

So just how much bigger? Basically there are two responses from DiG and without DNSSEC you get just your IP address back. And as you see in the red down at the bottom, the received is 320 bytes. This is the DNS responses that we all know and love. Now with DNSSEC these get just a little bit more complicated. So you get the A record and then you get this lovely RR Signature response. And for the sake of brevity we kind of removed most of it and if you look at the bottom the received size was just over 1600 bytes. So we're talking a non-trivial times figure of response size. Next slide.

So, some of you may know this, some of you may not – we actually operate a secondary name service now. We've run it for both public benefit and we also run a commercial platform. Our commercial platform has three AnyCast clouds with multiple providers, we do IPv6 and we're fully DNSEC capable. Next slide. We host a large multinational internet property on our commercial service. I can't necessarily say who they are, but I can basically hint, hint that it's a small subsidiary of eBay. Their zones were not signed and when they went live with us, some users couldn't successfully resolve records in that domain.

Now, with ISC what we do is we're big DNSSEC proponents so of course we all sign all of our zones from ISC.org to the zones that comprise our SNS service. So the zone of the content provider were not signed. They are planning to do DNSSEC in the future,

some time before the end of the year, but at the time of their migration to SNS they weren't signing their zones. But they also, when they look up name servers for their delegation, of course the NS records for the zone were referencing records that were in a signed zone. So, in our particular case, for an example, we have ISC-SNS.com, .net. and .info and so you'd see the delegation for this particular domain and see DNS records pointing to these sites. So when they do the then look up for the glue, they find that the responses coming back are yes, there's the A record or Quad A record for the DNS server and then oh here is a whole bunch of RRSig's with it to boot. So the resulting responses popped above the 512 byte limit and we're back at the same behavior as the simple case that I showed you earlier. Next slide.

Another issue that cropped up was that periodically the signing keys, the KSK or more often the ZSK, should be changed. So during the period when any server could be passing out the old key, both the old and the new key are included in the responses. So, yet again the responses then just got bigger. This mostly impacts cases where ENDS0 is enabled, but a conservative, often less than 1K limit is chosen. Now, in this particular case the large internet property has lots and lots of customers. And they have lots and lots of customers who depend on the resolution to make their financial transactions.

So suffice to say, if you can't resolve this particular domain people get grumpy and people get grumpy very, very quickly. But it's also the case of with a lot of these customers' it was basically

someone who was designing a website, say three, five years ago they used their provider or they set up DNS and they just stuck it in the corner and completely forgot about it. so maybe it's behind the Cisco pics or set behind a firewall where best common practices five years ago was basically filter anything larger than 512 bytes and don't support ENDS0. So we're running into a lot of cases, and we were working with a company at the time to try to educate their users, was that no, times have changed. There's this thing called DNSEC. There is this support for EDNS0 that you should really support and you should stop dropping packets that are say larger than 512 or 1K.

So there was this one issue when we first started serving the data where people couldn't resolve because of say, the 512K limit. So everybody raised it to one or two K. Then we sort of got double whammied when we did the key rollover since we had double sets of RRSig's that increased it to over 2K. So we were hitting yet another breach and we'd get some of the same people going well you told us and we basically, at least from ISCs perspective were telling them no, just don't filter; allow up to 4K of your responses and then you won't have a problem, don't block fragments, don't block ENDS0 and allow TCP. That was another issue that came up – some of these folks were just dropping TCP responses altogether.

So it's one of the cases, especially as I say, we now offer secondary name service where we actually got front line experience with actual customers as in customers on the ground,

because with ISC normally we deal with vendors and interface with vendors and let the vendors deal with customers. So it gave us a different perspective on sort of the DNSSEC issues on the ground. Next slide.

But really I don't have a problem, really. So the DNS OARC folks have a service where you can give it a DiG query and it will tell you the largest response size that it will allow on your local resolver. So the first example is when it works you basically give it a query against rs.dns-oarc.net and it will run through the iterations and give you an answer back. In this particular case we are able to send the largest EDNS size. When it doesn't, you'll get a response that says the largest response that we were able to give was 512 so we lack EDNS support.

And some of the answers may be in between, may only allow 2K. so this is a quick way to look. A lot of times it's still the case where if you're on a hotel network, if you're not getting captured already a lot of the hotel networks, you can still find many of them that still don't support EDNS0 yet. But it's pretty interesting to see where failures do happen, but more and more you are starting to see EDNS0 support being rolled out. Next.

So, BIND – I'm sure many of you already know this but just a quick recap. We've been doing EDNS0 since a bind date, in particular 8.3.0. We got DNSSEC bis in 9.3.0, but we know that there are known flaws for anything before 9.4-ESV. And it's highly recommended that you run 9.7.3 now and 9.6 is actually close to hitting end of life. Next slide. Note that we also have 9.8

out there as well. So, some of the key takeaways. Make sure all your network elements that touch DNS can do EDNS0 and allow 4K responses. And I would also add to that allow TCP on Port 53. Make sure that any network security elements allow IP fragments. Use the OARC reply size tester to validate your systems and to identify customer problems. And educate your customer base.

I would like to reiterate that, while I can't use their name, they were very, very helpful in sort of dealing with the problem because we could have gone to say, stop signing one of our names in the Glue to allow some of our responses to go back under 512, but actually after talking to them they said no, no, no, no, no. Please continue to do what you're doing. It's basically educating eh customer base to allow us to make it easier for us to rollout DNSSEC later this year.

So you're basically helping us find the dead wood, so to speak, and the people we'd have to interact with anyway. So they might as well learn now. So we were rather take aback by that actually and really appreciated their upfrontness in regards to that. But they had actually, now have an internal document that they give to their customers that basically explains all this in more detail and say these are the things that you need to do to support this because if you're not getting nailed by it now you will be nailed by it later this year when we start signing our zones. Next slide.

So, references for those, you already know what DNSSEC is and there is the URL for the reply size tester. You can also get to it, I

believe, from the DNS OARC main website, main page. As well as obviously the links for BIND. And that should be it.

Russ Mundy: Great. Thank you Peter and let me give all our panelists a round of applause here. We have one more presentation that's actually a video presentation, but since we've actually run a little bit long on the presentations in the room what I think we're going to do is open the floor for questions so we have sufficient time for discussion and questions here, and then while we have the lunch being served we're going to go ahead and play Roland's video since he isn't around for interaction anyway. We can let folks watch it and see it during the meal time. So, time to open the floor for questions and I see a couple of people coming to the mic, who's going to get there first.

Bill Manning: Bill Manning pre-empting Richard Lamb. I'm getting good at this. Peter, I gave a talk similar to that, the one you just gave, a couple of years ago in Bangkok. And one of the things we were seeing is intermittent packet sizes, response sizes that went above 4K. That was two years ago. And that really drives the need to go to TCP. Are you seeing that?

Peter Losher: We haven't seen that yet; at least in the wild – I mean you can obviously pack, and we know some people who do pack their DNS

responses with like four or five keys, which could in theory bump up to above 4K. so if you've got say backup upon backup of ZSKs and KSKs and you're running with two or three or four sets of RRSig's, that could bump it up. I think from our perspective we ran two or three RRSig's and we were getting pretty close to 4K but we didn't go above it. But we haven't seen it in the wild other than ourselves.

Bill Manning: Okay, yeah. The reason we saw them is when people were using multiple algorithms.

Peter Losher: Oh okay.

Richard Lamb: Okay this is a question of comment to the .fr gentleman. First I want to applaud again the transparency with which you described the issues you guys experienced. And my main question is can you tell me what the network problems were with the A and B keepers? Being someone who actually has a number of them in use I would be really interested in hearing anything about that if you could say something.

Russ Mundy: Do I sense a degree of concern?

Richard Lamb: Not really, just interest.

Vincent Levigneron: In terms of transparency I can't tell you everything but don't worry the problem was not [Acheson] problem. It was not the box itself. It was because it was new equipment and we had some problems with our procedures, and a lot of people made mistakes. But it wasn't a problem…

Richard Lamb: I mean it's a relatively old design so I was…

Vincent Levigneron: Yes but we have no real problem with the HSM itself.

Russ Mundy: I'd like to ask a question with respect to complexity of the systems. I'm not sure whether or not we've seen some of the behind the scenes structure of what JPRS did in signing theirs, but in the Afnic case you laid out the structure with the proxies and the HSMs and so forth. Was there a trade off analysis of some sort done for, for instance how many different devices and boxes, whether they're computers or HSMs, and the risk of having the multiples and the connectivity versus a consolidation on a smaller number? Was that part of the considerations of your design?

Vincent Levigneron: To be honest when we started the project we didn't imagine there was so different boxes and we didn't spend enough time on this part and that's why we had this proxy to do the synchronization between these different boxes, different applications, etc. to be sure everything is under control because sometimes you have unexpected behavior from a box or applications and you need to control this. But the study of this part was too small at the beginning of the project. But now we're guessing it's better and it should interact better now with this new architecture.

Russ Mundy: Thank you.

Patrik Fältström: Patrik Fältström with my Cisco hat on. You talk about fragmented packets and fragmented UDP packets etc., large responses and you talked about it in a way which implied that you do not see any problems with the fragmented UPD packets in your deployments for example. Two specific problems I hear people claim is happening in the world, and the reason why I bring it up is that I've been looking for people that really have data on these problems and I cannot find them, people just talk about them being problems.

One of them has to do with denial of service attacks using UDP fragments where the first fragment, constructed attacks with like fragments except the first one. The second one – and that is actually one ISP in Europe has actually blocking UPD fragments in

their network because of rumors that there are a lot D DOS attacks using UDP fragments and I would like to get more data about that if someone has that. So far no one has been able to, no one has contacted me.

The other one has to do with a lot of packagery ordering issues together with UDP fragments. I have one such case, which I thought had to do with Cisco equipment actually, but it was actually bad network design that led to the reordering. So that I actually have one case of, but I would like to see more of those things. So if people actually see issues with fragmenting packets and DNS specifically and UDP, please let me know.

Peter Losher: One thing that, because I come from the system architecture side, in regards to fragmented UDP is that some implementations and some Oss and some firewalls on them to do the IP fragmentation, you have to basically allow all to all frag or fragments. So you have to in theory basically allow anything that has the fragment tag because either the firewall layer happens before packet reassembly and similar actions. So I can see where some people would think that it could perhaps be an attack factor because you could in theory send a fully formed packet and just tack it with frag and then it hits the first rule set, or hits the allow fragment rule set and then you're screwed.

So yeah, we're always definitely interested when it comes to D DOS attack factors, especially for DNS. So along with Patrik, ISC would also be interested in any such data.

Russ Mundy: So, I don't see any in the chat room so I'm going to go tour topics that are on the screen and these are broad topics, but intended to address, from your experiences, what you see as the most important aspects to worry about, to get right and so forth. So the first one's are there any particular things, whether it's documentation, training, software tools, etc. that now in retrospect, after you've gone through what you've gone through, it would have been good to have at the beginning?

Vincent Levigneron: I guess there was nothing important missing. But we had to train our team. It was the most important thing that…that's why when we started the project the first thing we did was to go to ISC and to have a very good training. And that was very good for us to start the project and to understand everything about DNSSEC. Because even if you read RFCs and if you use tools it's not enough. So training is really, from my point of view, the most important thing with DNSSEC. And people who implement solutions in the registry need to be trained, but also the people that do the work every day, and that's an aspect that's not completely finished because everybody in our company is not completely aware of DNSSEC. And I guess it's the most important thing.

Peter Losher: From ISCs perspective, this whole exercise was very instructful for us because as I said before, we're mostly a sort of backend vendor so to speak, so we've never really dealt a lot with the general public to a certain extent. So things like documentation or end user documentation other than to sort of other people and sort of training towards geeks, so to speak.

As I said, this particular internet property has a lot of end users and end users who aren't necessarily say Linux or UNIX literate. They basically write their web pages in the latest technology of the day whether it's a PHP or they do a Drupal website for their ecommerce and DNS is just a backend thing that the ISP or the hosting provider actually manages.

So part of it was sort of educating the end user for this property about our sort of basic DNS to a certain extent. And we actually worked with our customer to basically say here's some of the things you can do, here are some things you can do to instruct them on how to better support these larger DNS responses. The other thing was that we pointed folks to the DNS reply size tester just basically tell them see you do have a problem.

Well, for a lot of these people, they don't even have access to a UNIX shell to actually run DiG. So one of the things that we talked about, and we all actually talked to RIPE about this, is they had a reply size tester in Java that was just Java applet. It was just basically written to sort of prepare people for the root signing so to

make sure that they can see the larger responses from the root. And that's actually something that's probably a little bit more end user friendly for someone to just click on a webpage and run the test rather than have access to a shell to run. And even if they have access to a shell, do they have DiG.

So that was like yeah I guess there is the rest of the world other than sort of the UNIX, the Linux side. So that's why I would say basically documentation, and sort of tools that sort of represent sort of a larger customer base that's sort of outside the geek technical community.

Kazunori Fujiwara: In Japanese case, very important things is native language documentation, native language training. So a country, I think we need document, DNS tool document in Japanese.

Russ Mundy: So the language issue for all aspects was the major thing that would have been helpful to begin with. I'd like to ask a little bit more in the training area for the Afnic, what type of training – is it training in what DNSSEC is? Is it training in how do you operate a signing system? Is it training – what types of training is that you are referring to.

Vincent Levigneron: It's not we don't know what DNSSEC is because of course we operate DNS everyday so we know what DNSSEC is. But its'

completely different from the theoretical aspect particular one and when you operate DNSSEC there are some tricky situations and the training we needed were training about operations. It was not really about DNSSEC.

And that's why I told users… I perhaps also have people doing DNSSEC training but the one provided by ISC was really focused on the tools we used and that's why we'd chosen this one because we use BIND and it was really focused on the professional thing and it was very important to us. Even if we didn't use everything, we don't because we still use Open DSA for instance with (inaudible) France. We have a mixed BIND and open DNSSEC things, but it was really focused on the professional things and it was really important for us.

Russ Mundy: Thank you. So I guess I'd like to jump to question number three – three seemed like a good number to ask for the three most important things that you would recommend for others that are going forth to do DNSSEC; that they think about, examine carefully, and if you will, they need pay the most attention to getting it right to ease their implementation in DNSSEC. Can we start with Fujiwara this time? Question number three – what are the, I picked three, one or two is a okay number to give, but the most important thing that people should think about before they start the process to get right so it will be easier to get it right.

Kazunori Fujiwara: First, people know problems without DNSSEC, for example, [Kaminsky method]. Easy tools, easy signing tools exist – easy troubleshooting tools I think.

Vincent Levigneron: Okay, so the first thing of course is training as I already told you. But if you want something very important to do is perhaps do the things in the correct order because when we rolled the proxy server, perhaps it was too late. We should have started with that part of the system to prevent us from producing unvalidating zone files. And perhaps it's the first thing to do to have a mechanism to validate and to check if DNSSEC stuff is correct on your zone file before you spread it on the internet. And I guess it's one of the most important things we are doing, and perhaps you could try to do something easier than what we do; and perhaps the combination between NSEC 3, [Octout, Dialemic debt] and automatic signing is not the easiest one.

Peter Losher: Well I might actually slightly merge three and four together to a certain extent because I think the three most important things that I could recommend to DNSSEC deployers is educate, educate, educate. Especially if you're handling end users or basically folks who may not be technically, at least with DNS, technically aware of DNS other than it handling in the background. Put up documentation that says we are making this change; what DNSSEC is, I think if you even want to, I am sure at some point

the skit of the DNSSEC for beginners that we did on Monday will be up and link to that to sort of get people an idea of what it's actually all about and what they may see because of it. oh you may not be able to resolve your website because of some intermediate issue resolving because the packets are too big.

I mean, obviously try to keep the document, or try to keep the technical jargon to a slight minimum, but educate that there is a change coming and how they can sort of try to prepare themselves for it and giving them the tools to see if A-they're going to be affected and what they can do to actually remedy the situation.

And barring that you can do all the education, education, education you want, but there are still people who won't notice it until it actually breaks and then have something in there in place to help instruct them, either bulk up your help desk, or train your help desk to be able to take care of these issues. Because what we found in our particular case was that a lot of these providers, if they were running BIND, they were still running like BIND 9.3. So it's really one of those cases with DNS, especially in the enterprise community, you basically set it up and then you stick it in a corner and then you don't think about it till it breaks.

So, it's like jees 9.3, there are like how many security vulnerabilities and how many performance issues and so forth. So if there is one thing I had to take away it would just be educate because, especially if you're dealing with ecommerce where on time reliability is almost a must. The customers will scream and scream loudly back at you if everything is not running smoothly.

Russ Mundy: Okay, well thank you. I think that I'm going to offer one more call for questions from the floor or the chat room. And unless we have some there, please come to the mic if you do have some – ahh, okay good.

Lars Liman: Hello Lars Liman from NetNod again. I support what you said – getting to know the stuff is the most important thing. But I didn't hear any one of you mentioning maintaining a good relationship with your slave operators. Things like DNSSEC timers, because they expire time and all that, may have a large impact on the operations for the slave server system. So make sure that you're in sync with your slave server before you deploy this.

Russ Mundy: One of the things I want to add, one of the things we saw that was documentation for HSMs is very poor. I don't know if you have any other experiences, I'm glad to hear about it. The second thing I wanted to mention is that what we see now when I'm looking into the future is that the speed of signing might be an issue when you have an operational issue and you need to sign your complete zone and it's a large zone. Then it might become unavailable for a longer period of time then what you do when you don't have DNSSEC. And that's something that worries me because I think that signings need to be faster.

Vincent Levigneron: Yes you are right but at the moment we sign very few number of records and we hope that in ten days, ten years when people will need more, will send us more DS there will be more powerful HSMs. But for this moment you are right, if we should sign a large zone it would be an issue.

Russ Mundy: That has to go right, everything signed?

Vincent Levigneron: Yes with NSEC3 and you don't sign a lot of things.

Male: So besides the point raised by Lars Liman there is the concern about mixing transport families. If you have some places that are native IPv6, some places that go through v6 tunneling, you end up with path MTU issues which affect your ability to actually move packets. And the ability to look into the infrastructure to help that debugging, that's part of the educational process, is critical. Particularly since we're transitioning between v4 and v6.

Peter Losher: I agree. I think tunnels should die, die, die, die, die, but I realize that they're also a necessary evil at this point. But we haven't seen that so much for us because most everyone is still using v4. But I believe that will become an issue over time as people enable v6

and they may not be able to make immediately the jump to say native v6 transit, but yeah path MTU, the bain of my existence to a certain extent.

Russ Mundy: Okay, do we have any other questions or comments from the floor or the chat room? Okay, so in that case I think we'll go ahead to Roland's video and we'll ask Julie to go ahead and make the change here.

Julie Hedlund: Yeah I'll switch over. And at some point during the video I think lunch will be ready so we'll probably just, as soon as I see that it's ready, it's not quite yet, we'll let you know that you can head back there. So let me get the video started.

Russ Mundy: And while she's doing that, let me ask everybody to give a nice round of applause to our panelists again to thank them.

[Video starts] *Hello everyone. Good day. Today I would like to talk to you about the DNSSEC research we do at SurfNet and I want to briefly introduce myself and SurfNet. My name is Roland van Rijswijk and I am a technical project manager responsible for our DNS and DNSSEC services. And SurfNet is a national research and educational network in the Netherlands, which means that we*

provide high bandwidth fiber-optic connections to Universities and Research Institutions and that we are a shared ICT innovation center for over 160 connected institutions and about a million end users.

I want to discuss two issues wit you today, one is measuring validation and the other one I will discus later in the presentation. Now measuring validation is starting to become somewhat important because we have a pretty good insight into DNSSEC deployment on the signing side. But what we know very little about is how many people are actually (inaudible) DNS data. Earlier this year Security Week published an article that triggered my curiosity and I read it and it said that well there are very few rewards for enterprises to actually run DNSSEC because nobody is doing validation. And I thought is that really true? Where did they get tat information? So I dove a little deeper into the subject and found that actually there is no data available and nobody knows whose doing validation.

Earlier this year, in March, the Japan Registry Services did a presentation on how to count DNS validators. And what they've been doing is they've been looking at offline data that hey had collected on their authoritative name servers. The link on the slide tells you where you can find the report that they presented at the DNS OARC Workshop. Now we had already started on this very similar effort, but instead of working with offline data like JPRS did, we focused on doing this with like data from our authoritative name servers.

Now our strategy with this research was that we assumed that only validating resolvers will send queries for DS records and DNS key records because if they want to validate our data they will need our DNS key records and if they want to validate sub domains they need the DS records that are available in our domains.

Now what we did was we implemented some simple tools that we based on lipbcap that capture and parse DNS packets. And these tools send this data off to a big server which has a database that aggregates the data and we specifically filter out queries for our signed domains only so that we get representative data on DNSSEC validation.

Now I can show you some early results of the work that we've done and I hope you can all see this on the slide, I hope the video encoder does its job well and shows this in HD quality. And what you can see on the slide here is a map of Europe with some dots in every country that has a color. And the color varies according to the number of validating resolvers that we have detected in this geographical area.

And as an example, you can see a text balloon above the Netherlands that says there are a total number of resolvers that was 24,000 of which we have detected DNSSEC use at 135, which means that about half a percent of all the resolvers that we saw in the Netherlands for both the SurfNet.nl and the Gigaport.nl domains supports DNSSEC validation. And that's actually not a bad score, it was more than I expected. I expected like .1%.

What you can also see is that countries that have been doing DNSSEC a little bit longer than the Netherlands score better on this chart. I hope you can see that the Czech Republic, and let me just see if I can move my mouse cursor, the Czech Republic which is here in the middle of the picture has a purple anchor point in it and that means that over 1% of DNS resolvers does DNSSEC validation. And the same is true for Sweden which is at the top of the map just above the Netherlands text balloon.

Now we also have a different map, which shows you in colors what the amount of validating resolvers is in a country. And the more towards purple the color is, the more validators there are as a percentage of the total number of resolvers that we have detected. So again, you can see that countries like Sweden, Finland and the Czech Republic, which have been doing DNSSEC for quite some time, score better on this chart.

And of course, there are also some anomalies in there. As you can see, Madagascar is also purple and the reason for this is that we see very few resolvers actually sending queries for our domains from Madagascar. So if one of them does DNSSEC validation that will show up as a bit of a bias in the results.

We also have tables that show the results and here you can see highlighted in gray again, the Netherlands with 24,000 resolvers in total; 135 of which are sending out DNS key or DS queries, so we think that they are DNSSEC validators and there is an 0.56% of the total number of resolvers that are out there. What you can also see in the lower table is if you click on the Netherlands for instance

in the table above, you get an overview of all the resolvers that we have detected and we have split them out by ISP block. So what you can see is that there are some resolvers in their for SurfNet and there is one for a technical university and there is also one for a large internet provider, or a large mobile internet provider, which is T-Mobile. And in fact, we know that T-Mobile does DNSSEC validation.

Now what do we plan to do with this tooling? Well what we intend to do is make the information that we gather using this tool available to those who are interested. We are not going to be publishing it on a public site yet because we feel that there may be some privacy sensitive data in there. So we are considering whether or not to publicly make this data available.

But if you're interested you can contact me and I can make it available to you. We're also talking to SIDN, the .nl top level registry, to see if we can run these probes on their .nl infrastructure because of course the data for SurfNet.nl is interesting for us, but it is not very representative because it is logical that universities abroad, or research institutes abroad will be more interested in the SurfNet.nl domain than a regular internet users, which may show up as a bias in the results; whereas .nl is a domain that is queried all over the world and not just from academic institutions.

We're going to release all the tools that we created under a BSD license. In fact, the probe software that runs on the authoritative name server is already available. And if you want to access the

source code please let me know because I can make that available to you from a subversion repository. Also, if you're interested in contributing to this work please let me know. My contact details will be shown on the last slide at the end of this presentation.

Now, a second issue that I would like to discuss with you is UDP fragmentation issues. And the reason I want to discuss this is because we have run into trouble with this since we have signed out domain. Now some of you may know that we signed the SurfNet.nl domain end of last year and published the DS record in the .nl zone. And we started experiences problems with a large ISP in November.

We had just had our DS published in the .nl zone and some of my colleagues came to me and they started complaining that they couldn't access their email from their home DSL connection. And we did some logging and as it turned out one of the firewalls at the ISP was discarding the UDP fragments. Now if you have a large DNSSEC answer that is being sent back that will get fragmented. So if the UDP fragments get discarded, the answer never reaches the original resolver. And even though the ISP was not actually doing DNSSEC validation, they were still sending out DNSSEC queries.

We talked to their engineers and it turned out that they couldn't replace this firewall because it had been there for years, nobody knew who set it up, nobody knew exactly what the configuration was like and they didn't dare touch it just before Christmas. So what they ended up doing was reconfiguring there resolvers which

were actually running Unbound from NLnet Labs. And they reconfigured them to send out smaller EDNS buffer size, which they set to 512 bytes, and that solved the issue because whenever they request something that is larger than 512 bytes then we would get a TCP fallback. So problem solved right?

Well it turned out the problem wasn't solved because early this year, actually in March, we certainly started getting complaints from companies who were trying to send us email. And lo and behold we did some research and it turned out that they were customers of the same ISP that we had had issues with before. And the screenshot that you can see from the email client actually shows you the error that they got, which is basically that the mail they were sending us couldn't be delivered.

As it turned out they firewall strikes back because these customers of the ISP all were using their MS exchange service; they have a managed Microsoft exchange service which they can use to run their corporate email and it turned out that they were all using this. And we called the engineers at the ISP again and said hey, we're experiencing issues again; have you changed something. And they start delving into the problem and as it turned out they had recently upgraded their dedicated resolvers that they were using for this host exchange environment.

And they had upgraded them to Windows 2008, Release Two, which supports EDNS0 and sets the DL bit to one, which means it's sending out DNSSEC queries even though it doesn't do validation. And again, the firewall was stopping UDP fragments

from getting back to their resolvers, which meant that they couldn't resolve our MX records and they couldn't send us email. And the solution to this was to tweak an arcane registry setting somewhere deep in Windows, which disabled EDNS0 and the problem was solved.

Now of course this is a very severe issue because there was very little that we could do about this because we could change the setting for EDNS0 on our authoritative name servers but that would mean we are putting a penalty on 99.9% of the people who are doing it right. So this was a bit of a conundrum. And while we were investigating this issue we actually discovered something interesting.

The resolvers behind the firewall received the first fragment of the UDP packet; we could actually see the first fragment going through the firewall, arriving at the resolver. And we could see that two fragments had been sent from the authoritative name server, so one fragment was being stopped. And actually the protocol stack on the resolver detects this and it sends back and ICMP message, which wasn't being blocked by the firewall, and actually got back to our authoritative name servers.

And this ICMP message tells us that hey I got a first fragment but I didn't receive the rest of the fragment so I couldn't reassemble the packet. So it says, as you can see in this screenshot, ICMP IP reassembly time exceeded. And we could actually see the size of the fragment that they were missing.

So, what we determined from this is we can actually detect resolvers that have this issue. So what we are doing is we are extending our monitoring tools to detect this issue and we're going to log this in the database to see the extent of this problem on the internet.

And we did some initial packet dumpling and that was actually quite scary because we saw these ICMP fragmentary assembly failed messages coming back every once in a while; maybe every one or two seconds, which is actually quite frequent. And another issue is that people seem to think that UDP fragments are some form of attack. Now maybe that was true 10 or 15 years ago when there were all these packets of death methods that you could use to crash Windows 95 computers and Linux computers that had faulty TCP and UDP implementations, but it isn't an issue anymore, we believe.

But still there are people out there who think this is an attack and we actually had abuse complaints sent to our cert team which said hey your NS1, NS2, NS3, SurfNet.nl are trying to flood our severs with UDP fragments so we believe you are attacking us. And it turned out that they were sending DL=1 queries to our server so they were getting back a DNSSEC answer that was larger than the NTU size and it meant that they were getting fragmented packets. So it was perfectly valid internet traffic that they were marking as an attack.

And once we'd explained the problem to them they conceded that this wasn't actually an attack and they fixed it in their firewall.

And this was actually a large university in Canada that was reporting this. So these are people that should have known better.

Now what we are doing is we have a student who is actually creating a lab setup so that we can verify our assumption that these ICMP messages are being returned whenever this issue occurs is valid. And once we have confirmed that this theory is actually sound, we will try to publish a paper about this.

Now the conclusion that I would like to draw is that this is an issue that requires serious attention. It really affected us. People couldn't send us email. My colleagues couldn't contact our server from their home DSL connection because this issue occurred and there is very little that you can do about this if you have a signed domain. Now I have some ideas about how you could make authoritative servers a little more resilient.

You could detect ICMP return packets getting back to your authoritative server and then for the time being mark the server as not supporting larger packets and limit the size of the data that you send to them. But I guess if I were to propose this in an IETF Working Group, I would be severely filleted. But then again, I believe that it would make internet traffic somewhat more resilient so I think that we should start a discussion about whether of not this has merit.

And if you operate a signed zone you may actually want to do some TCP dumping and see if you see this issue; because if it is occurring, you may want to take measures to prevent it. Now that

is all I want to discuss with you today. I think I've managed to stay within my 15 minutes. IF you have any questions about this presentation, please feel free to contact me. My email address is on this slide as well as my Twitter account. Thank you for your attention.

Russ Mundy: Well this was very good. Roland was not able to join us but was willing to contribute this way and I think it's excellent because the video is posted on the Workshop page, as well as all of the slides. And I apologize for not pointing that out earlier. If anyone, especially the folks listening online, want to see the slides a little bit better just go ahead to the workshop page and all the slides are there in pdf and you can go ahead and download them. I believe our lunch is ready and Julie has got our sponsors back up so let me turn it over to her.

Julie Hedlund: Yes, please help yourself to lunch; there should be plenty of it. And we'll give you a little bit of extra time I think since we ran over a little bit. I'll give you a reminder to wrap things up probably at 12:30 and we'll start not too long after that. But please enjoy your lunch. Thank you.

[Break]

Julie Hedlund: At any rate, we're going to go ahead and resume our program and I will monetarily turn things over to Steve Crocker. But our next panel is the discussion on Update on Activities Around the World. So perhaps I'll go ahead and turn things over to Steve.

Steve Crocker: Welcome everybody to the last panel. This is our update on activities around the world with an attempt to shine as bright a light as we can on the region that we're in, which is a quite exciting region. So let's see, is Lee Han…?

Julie Hedlund: Han can't make it.

Steve Crocker: Can't make it right. Krit, and I apologize, but it will be challenging for me to say your name. Please help us practice your name and then plunge right in.

Krit Witwiyaruj: Good afternoon. I'm Krit from .th. Today I'm going to talk about DNSSEC a bit from .th. .th we have been delegated since 1998 and we have more 20 years experience. We are a non-profit organization and we are very strict on the delegation so we are a very small registry. We have less than 100K domains registered. And .th is for Thai people only and some for internet has company located in Thai. .th has started signing our zones since 2009

because the number of threats are rising and we want to be initiative in secure our domain and help people to get started with DNSSEC. Next slide please.

At the beginning we start only two of our zones at the top level, .th and at the second level .in.th on March 30 2009. And we begin signing the biggest zone, .co.th on June 19 2009. We did KSK rollover two times. The first one last year and the second was is May 30th this year. Because we are one of the earliest to adopt the DNSSEC we began the project at 2008. At that time we decided to adopt NSEC to be used because our zone was very small at the time; the biggest zone is less than 20K. And our zone has become bigger about four times, which is about roughly 10 megabytes in size. And the sign time is about 15 second.

And our zone is signed from unsigned zone and we change the RRSigs every time we sign, at the beginning. That is not a good idea for the zone transfer for the secondary zone transfer.

Lessons learned – after the root is signed it's much easier to maintain the trust anchor and we don't have to register our DS key to the third party or to something like ISC, [DLV]. And for the zone transfer, NSEC3 with opt out is better choice for the time being right now because very few people are signing their zones. So there's a lot of NSEC in our zone because we are signing using the NSEC meaning that we are signing every single record in our zone so it takes a really long time to sign our zone. As we tested on using the NSEC3, the time used to sign our zone is greatly reduced from about 15 seconds to less than one second to sign our

zone. So the next move is we will adopt the NSEC3 with our RRSig so we only have NSEC3 for the record that signs.

And that is all for my presentation.

Steve Crocker: Thank you. Any questions?

Julie Hedlund: We can save them for later; which ever.

Steve Crocker: You want to save them for later? Okay, I'm going to try to remember the question that I had. We'll move on. Yong from Malaysia.

Yong Yaw Eng: Right, thank you. I'm Yong Yaw Eng; everybody knows me as Yong. I will share a little bit about our domain experience in terms of how we sign our zones as well as what's after that. SO the next slide is what I'll be sharing about our overview of deployment in Malaysia; some of the issues we had after we deployed, and I'm also sharing some of the findings that we had after we did the public trial, which I think are still relevant. After that will be some of the effort that we are making in promoting DNSSEC in Malaysia as well as the challenges that we see ahead. Next slide please.

Okay this is the milestones that we put in place as our deployment strategy. We had our closed test bed in between March and

October of 2009 that was just signing .my and .net.my. No this on a test bed housing so it's not actual production and we used the IANA, DNSSEC root test bed then. We moved onto the public trial which was the 29th December 2009 to May 2010.

At that time we actually signed all our zones to see how things…so it's a replica of the production system altogether in terms of the interface and how the zones are being handled. So the IANA DNSSEC root test was good for us to use for us to complete the whole chain of trust. And finally in production we sign it on the 9th of October and the DS record was added in December.

Two weeks after we signed the zones, a week or so I think, we rolled out our change of our interface as well to be able to accept DS records from our customers. By the way, .my the registry, we are currently running it as both the registry and the registrar, so we can make the web application to allow our customers to submit in their DS record. So this is actually what we have deployed. We use our RSASHA256 with NSEC3 with opt out and our KSK is a year with 2048. And ZSK is 12 weeks rollover with 1024. Okay, next slide.

So the take up of DNSSEC is low as expected, and the graph that you see is as the 24th of May. There was just about seven domain names. I started collecting the data in March and April; there was only about seven domain names and these are domain names that either we do ourselves or people that is familiar with DNSSEC that we know. Interestingly in May, the one extra DNSSEC signed domain was done by an individual that when I went to his website

he said he did it because he could. So I was pretty glad that was done. Next slide please.

Post deployment issues – these are some of the things that we wanted to share of issues that we discovered. And I really am very appreciative of the community because I must confess that we do not have a very good monitoring system of if things go wrong, but we have been informed of this issue. So that first issue I have not yet found out the solution for it or what is best to do about it.

But what happened is, we've been told that the validating resolver could not actually get the DS response – sorry, NSEC3 response when they request for a DS record to validate. So what happened is, one system using NSEC3 with opt out so the zone is actually only those that has a child DS record is being signed. So a lot of our second level domain names are not signed.

So, for example, JV.mine, we did not actually make any effort to approach the government not signing in the zone yet. So for this particular TLD the whole zone file is almost like a plain zone file except that we have our own signatures. As far as our NSEC3 record file that looks pretty normal, but when the validators try to validate a request for the A record and it got the answer, a request for the DS record to validate, but the answer that was returned was annex domain. So they expected us three to prove that he wasn't signed, that the return was annexed domain and it's considered, they couldn't determine whether he was really signed or not. So he went to become bogus.

So when I was told that this was the issue, I tried to look for a solution. Still yet to be able to find a solution in terms of how the answer can be returned. So what I did was that for all the zones that we do not have a child record, we decided to take away the signature from .my itself so that the validating issue will not be there. So that what I did.

Back to the second point is that this is a simple issue of that timing of the rollover was wrongly set. I'm actually using the [Zackatee] signing tool, so it's all in the configuration. So what happened was that I actually missed the valid configuration for the rollover for the ZSK and I was told also by the community that the key was removed before there was even time for the replacement. So when I looked at my configuration and said okay, I found out that I forgot to change it from the default configuration, so that was the issue that I found. So I hoped that none of this is another recurring issue. Next slide.

Some of the relevant findings we had from the public trial would be that the general public acceptance is quite low. I think it's because of lack of awareness as far as the education on the DNS technology. A lot of domain owners don't actually control their own zone; these are handled by hosting providers. And a lot of people still think it's not urgent so they're very reluctant to do so. ISPs as well, during our public trial there were few of tehm that joined us, but after we went into production – for one thing, we didn't quite able to engage them yet but I think we probably need to persuade them.

But on the other hand as of the issue that I've actually shared just now, it is a blessing in disguise in a sense because none of the registry servers are doing the validating. So when the issue cropped up that it was quite transparent to the general user because they didn't know; this has just got to do with the validating. So when we found out, I mean of course we tried to fix it, but the General public in Malaysia themselves, they did not see the problem. So of course, as much as we want ISPs to do the validating, it is also a good time for us to be able to iron out any issues that we can see.

We also approached the Central Bank to know probably tell them that this is technology that is available so that they know added security. The Central bank was very supportive of the idea. They even hooked us up with some of the banks to share the technology with them. But it is sad to say that it is really at the end of the day up to the bank to adopt the technology if they want to. So as much as we can is just sharing the technology with them. And for us to see in the public trial those who are really able to do something about DNSSEC, they seem to be able to do it without much problem. So I guess those people who are able to really handle their own zone file and able to ride on DNSSEC so much an issue.

Some of our efforts in promoting DNSSEC – we have been doing annual .my training kind of thing, which is DNS training, since 2006 and 2008. 2009 we did the same as well as we did awareness training around in five states in Malaysia. And in 2010 we really prepared to roll out DNSSEC. With met with some of the

resellers. We met with the ISPs and told them about DNNSEC, encouraging them to participate in our public trial. We did some DNSSEC Workshops even during APTLD, I think that is during [Apricot]. And then we met with banks as I said just now.

And this year we are also doing still in the form of training and workshops. We had our DNSSEC Security Talk organized by our regulator, MCMC. We had the ISOC Malaysian Chapter did an awareness series as well on DNSSEC. And we are going to have another DNS training next week too. So these are some of the efforts that we hope to be able to educate the public in general and as well as DNS administrators specifically. Next slide please.

What we can see as challenges ahead is that we probably need to start to talk in earnest with our ISPs to get tehm to enable DNSSEC. Our effort in encouraging authoritative DNS administrators to adopt DNSSEC still needs to be continued. So I guess we need to monitor our signing more and our whole DNSSEC set up more. We probably need to look deeper into this, how we can do this. And there's a lot of improvement in our environment. The more I look into how DNSSEC works the more I think the initial design is not very nicely done; so there's a lot more room for improvement. So that's all I have.

Steve Crocker: Very nice, very nice. Fujiwarasan.

Kazunori Fujiwara: Good afternoon. I'm Kazunori Fujiwara from JPRS. I talk about number of DNSSEC validators seem at .jp. The presentation is similar, but this March at the DNSO meeting and the [IAPG] meeting, but I updated the data. This is today's contents. Basic idea – how to detect DNSSEC validators; JPRS data; results and conclusion.

Basic idea – how to detect validators. JP DS RR has been introduced in root zone. JP DNS key TTL is 1 day. Thus, the DNSSEC validators send JP DNS key query once a day if the validators try to perform JP domain name validation every day. I made assumptions. Validators are IP addresses which sent JP DNS key queries. Resolvers are IP addresses which send JP zone queries. Query ratio from DNSSEC validators equals the number of queries from validators divided by number of queries from all resolvers.

JPRS data set – overview of JP. JP has 1.2 million registered domain names. JP DNS servers serve 1.6 billion queries per day. JPS is collecting packet to captures and query logs. We have seven DNS neighbors – A through G .dns.jp and operated by multiple operators. And there are seven IPv4 addresses, six IPv6 addresses totaling 13 IP addresses. JPRS data set – JPRS sometimes collects two day long full capture DNS packets, once a year, 50 hours, same timing as DITL at the DNS OARC.

When .jp was signed – December 10 last year. When JP DS RR was introduced into the zone – December 10 last year; before six hours and after 48 hours. And JPRS has been collecting DNS

query log from two of the seven JP DNS servers for seven years. Not all JP DNS servers. If number of DNSSEC validators is calculated with the query logs, it outputs continuous information.

Counting method – full packet capture. I excluded obviously different queries and I counted number of IP addresses within each 24 hours. From query log I excluded obviously different queries and I treated an IP address as validator if it sent JP DNS key queries in the past seven days. The data I used to extrapolate the result from packet capture.

Results – results of full packet capture. The data is separated so three times a (inaudible) JP DS introduced in root. Six hours before JP DS introduction; first 24 hours after JP DS introduction; second 24 hours. Four months later two days – the first 24 hours; the second 24 hours. Before JP DS in root there were 280 IP addresses which sent JP DNS key queries. They must be DNSSEC validators. Immediately after JP DS introductions, 2,400 addresses send to JP DNS key query.

And they maybe on the next day 2, 200 IP addresses. Four months later, 3,980, under 3,800 IP addresses found. The number of resolvers are 1.46 million or 1.1 million or 1.5 million each day; not so changing. This shows number of validators are 0.16 and 0.2 in December and 0.25 in April. Validators share of queries are about 5% each day. Next slide please.

This chart shows number of DNSSEC validators. The dotted line shows an adjusted graph from 207 DNS servers created. The

dotted line today is one week. But December 17th the dotted line value is similar with data from packet capture, but April 12 the dotted line value is similar with data from packet captured. So the graph shows interesting phenomenon.

About 900 IP addresses started sending JP DNS key queries immediately after JP was signed. They may be DNSSEC monitors. Immediately after JP DS introduction the number 2,400 incremented to 1,500. There may be 1.500 DNSSEC validators December last year. The number of DNSSEC validators are increasing. May 10 – 4,500 IP addresses send JP DS queries. There may be 3,600 DNSSEC validators. Next slide please.

The chart shows validators share of JP queries. The dotted line shows an adjusted value from 207 DNS servers' query log. Compared with data from packet capture, the adjustment is not good for the analysis. The graph on data from packet capture shows that 5% or 10% queries came from DNSSEC validators. Next slide please.

Results from analysis – we observed 100s of IP addresses started sending periodic JP DNS key queries immediately after JP was signed; it is very interesting. 3,600 DNSSEC validators in this May. The number of validators are still increasing. Validators send 5% or 10% of DNS queries. The result may be larger than the number of real DNSEC validators. If some users of a large scale organization send JP DNS key queries to their resolvers, the resolver sent the JP DNS key query to JP DNS and the resolver is

treated as a DNSSEC validator. I cannot be distinguished from the real DNSSEC validator.

Conclusion – anyone can count number of DNSSEC validators if your zone is signed and you capture you DNS server's query. That's all.

Steve Crocker: That's great. Those are really some very interesting statistics. I'm sure we'll want to ask some questions but we'll move on. Jorg.

Jorg Schweiger: Okay so it's a pleasure to give you an update of the launch of the DNSSEC for .de. To those of you who don't know me, my name is Jorg Schweiger and I'm the CTO with DENIC. Next slide please. Well, we kind of introduced DNSSEC in two stages. First we implemented a test bed that started out almost a year ago and secondly we went live just like 20 days ago. So that was basically on the 21st of May.

Referring to the test bed, what we did over there is we provided our test with a dedicated infrastructure. We wanted to test whether DNSSEC would be really operable, technically operable according to our standards and to our parameters because you might know that .de is probably not the smallest zone. And we wanted to make sure that there is acceptance. Acceptance meaning registrar acceptance and market demand, which by the way, I do have to admit is not the way that we wanted it to be.

After almost a year of running the test bed we kind of seamlessly smooth moved into production. That is, we took the DS records from the test bed and transponded them to the going live, which we did in quite the same way as everybody else seems to have done that. so we rolled out to our 16 locations spread all over the world during the validatable – hard word, I should learn it with DNSSEC now – zone to our different locations and then we unblinded the keys as I said on May 31st and finally zone data got validatable by introducing a DS record on May 7th, into the root.

Well that could be it for this update because reading out the line that is given at the very bottom of the slide you see no unusual traffic, no unexpected traffic patterns, nor any unexpected volumes so we seem to be fine. Next slide please. Well really anything unfamiliar? Probably not. So if you take a look at the chart that is depicted over here, you see DNSSEC related queries. That is a chart from May 31st where we unblinded the key. What you see over here is that there's an instant spike at about 12:15. So as I told you before that the DS record wasn't in the zone in the root yet, interesting feature isn't it? Any ideas what happened?

Well there were first tweets at 12:00 that we were going to unblind the keys in the de zone. So everybody seems to be trying out what is really going on with .de. So even over here it seems to be a Twitter omnipresence. Next slide please. As you can see on that slide, things turned out to be quite normal. So this is a chart from June 7th where the DS record actually appeared in the root zone and that was around 1600 hours. And that is where the queries to

the DS record rose. May I draw your attention, by the way, to the number of queries. That is quite disappointing, I do have to admit, because these are on average let's say 150,000 queries a second where we usually experience non DNSSEC related queries about three magnitudes more. So basically we kind of answered 120 or 150,000 queries a second. Next slide please.

Yeah, that's a marketing slide folks. So heads up. We have a TLD that has the most signed domains. How come? Okay, disclaimer: as to my knowledge…so what happens is quite easy to explain. We're using a feature that's called NS Entries. So we're not delegating domains, but domain data is authorative within our zone. So these zones get signed right away with .de. So basically there is nothing to do for operators, holders, registrars whatsoever. So that's how come. To give you a more let's say fair comparison, let's move to the next slide.

So this is depicting the number of signed secondary level domains. Well, the kind of correspond with what we saw around the world with different numbers of registered or secured domains. So we're currently having about 800 secure second level domains and some of them even stemming from the test bed. That by the way is with about 20 registrars out of 270 and it's just four of them being responsible for more than one of two test DNSSEC domains. So we still do have to work on a uptake of DNSSEC. Next slide please.

Now onwards to some technical parameters and details. What we're doing concerning DS records – we kind of take whatever the

client has meaning we would prefer getting a key instead of a hash so that we can apply hashing algorithms we do want to apply. Let's say in return, we offer our customers syntax checks, validation checks, checks on nothing really specific. Next slide. More of technical details and parameters.

Once again, nothing that is never, ever seen before or spectacular, just one thing or two things I might want to point out. One is that we are very serious about post signature checks. So what we really want to make sure is that the zone we are transferring to our locations is really correct and valid. And another hint that might be interesting for you, and those of you who probably not have deployed DNSSEC so far, what we did do is we used 33 has iterations to calculate the NSEC3 hashes, which was done kind of unintendedly. There doesn't seem to be any best practice and we just want to try out 33 or 32 because we thought we would have to make really sure that no one's going to be able to walk our zone.

And we ended up with, as compared to the test bed, with a query answering performance that was so low we couldn't deploy it. But as I said before, we weren't aware of the fact, so it really took us a hard time to figure out what was going on because the performance was just too low. So if you are up to deploying DNSSEC make sure you choose a reasonable number of hash iterations and we are now operating 16 and we feel quite comfortable with that; on both sides, performance as well as security. Next slide please.

This slide is once again full of information. I just want to give you the impression that there is a well defined, secure procedure being

established with the generation of keys, with rollover of keys so there is a ceremony associate with it so everything, not only on the operational side but on the organizational side is quite secure as well. And we even took care for sure about any disaster recovery concerns that may come up. So we're operating two different data centers and all that. Next slide.

And last one I can promise concerning to provide a change or to be more precisely what we want to call it, operator change, we developed what we think is a very smooth hand over that is based on the RFC that is referred to on this slide. Although we amend the RFC a little bit in the way that we providing our registrars with what we call a drop box where they can just leave their new ZSK so that the old operator is capable of obtaining this new ZSK just to make sure that even though there is an operator change the domain is going to be secured at all times no matter if there is a change or not.

I do have to admit, by the way, this is nothing that comes any close to silver bullet; referring to the problem that still we do have the need that both operators really do need to cooperate. The only thing we do want to make sure with that, that we kind of encourage with that drop box, the operators to work together more directly. And some of you might get annoyed that we're doing something differently. Let me assure you that we are not so different in a way that we surely talk to other TLDs to make sure that we've got the same procedures and we're not providing you with a solution that nobody else got. So we're talking to other TLDs and registries and

there even is an IETF internet draft around. So if you want to dive down to get some more information about that feel free to do so.

I think that's about it.

Steve Crocker: Excellent. Matt Larson.

Matt Larson: Thank you. Good afternoon. So I wanted to give an update on the DNSSEC activities that VeriSign has been involved in the past few months. Here listed are the signs that VeriSign had a hand in signing, of course everybody knows that root zone is signed. VeriSign runs the .edu zone under contract with EDUCAUSE and we're the backend technical provider. That was signed shortly after the root last year. Then .net in early December and then of course the big one that a lot of people were waiting for was .com on March 31st.

So I think this is pretty exciting because when you look at the number of domains registered worldwide, for example, VeriSign does this survey and The Domain Name Industry Brief that we publish quarterly. If you take into account all the large zones that are now signed; .de, .co, .uk, .net. ,com, well over half of the total worldwide domain names can now be reached with a chain of trust starting at the root. So I think that's fantastic for potential for DNSSEC deployment.

Next slide please. I wanted to give just a few details about the actual deployment we performed for .com. Since we started, the team that consisted of ICANN and VeriSign that signed the root, since we developed this unvalidatable zone technique it's kind of becoming a best practice, which is gratifying to see. And we definitely wanted to do that for all the big zones that we deploy DNSSEC in, and .com was no exception.

So we had the zone blinded, if you will, with the keys obscured for about a month. So this means that for that month, starting on February 28th, anybody who had the DO bit set still exercised a path where they were getting large responses. So if they had any issues they wouldn't hear our large responses and of course if they had any issues with middle boxes that didn't like DNSSEC metadata, like DS records appearing in responses or things like that, or I should say NSEC because there wouldn't have been that many DS records, the idea was to ferret all that stuff out.

There was a brief window where we unblinded the zone because we had to have everything out of people's caches by the time the DS record went in. So on March 31st the actual deployment consisted of publishing the DS record in the root. The good news is everything was just silent, both in terms of people contacting us and what we saw on various forums; nobody said anything that there were any problems. So that was very gratifying as well.

I wanted to talk a little bit about what we saw then in terms of traffic afterwards. So about 62% of queries to .com have the DO bit set; this hasn't changed a lot over time, at least not recently.

Interestingly enough, I don't have this on the slide, but .net is at about 50% and that's a discrepancy that I think merits further investigation and we haven't looked into why.

But if you take into account what that means, 62% of queries having the DO bit set, what that means for bandwidth is that if you consider just those 62% of queries, those queries it takes almost four times as much, three and three quarters times much bandwidth to supply the DNSSEC metadata. Because we are using NSEC3 that means more records, more NSEC3 records than there would be with NSEC, and in particular negative responses get larger, substantially larger with NSEC3. When you factor in the non DO bit queries, the 40% that don't need to have any additional information added to them, it rounds out to about a 2X increase. So that's a long way of saying that it's using twice as much bandwidth now for .com responses.

We were quite interested to see what would happen with TCP queries and there was really a negligible increase. When you look at it on a per .com authoritative server basis, so basically per IP, there are 13 IPs for authoritative .com servers and if we look at it on a per IP basis before the signed zone was deployed there were single digit per second TCP queries, and that went to what I categorize as a very few hundreds per second. So when you multiply that by 13 we're talking low numbers of thousands per second which is not, really not an issue. We also calculated this value that we call possible TCP failovers. We look at the query stream and we look for an IP that first send a UDP query and then

sends a TCP query; so the same source and querying for the same query (inaudible). And that's what we classify as this possible TCP failover and we calculated that as well and that's a very low number as well. From basically almost none of those to just dozens per second. Next slide please.

And then finally I just wanted to give some statistics about how DNSSEC is actually being deployed underneath .com. Joe Waldron, my colleague who was up in the morning, mentioned some of these statistics. I think my slide is now slightly out of date, I say 24, he said 26 registrars actually have registered at least one signed delegation in .com and .net as of, well my figure is as of June 1st and his is more recent.

We have one registrar that has almost 1000 signed delegations and then a single enterprise, if you judge by the commonality of strings in the name, just pretty clear it's one organization has signed a bunch of their zones, over 500. And then there's the count of signed names; almost 1500 signed .com names, almost 700 in .net and then .edu thrown in just because it's a number that we track. And note that you can go at any point to scoreboard.verisignlabs.com and get an up to date count. That's updated about once a day so it won't be absolutely instantaneous, but it will certainly be always a reasonably up to date number. Thank you.

Steve Crocker: Excellent. Thank you all. So we have some time for discussion, questions, anybody want to plunge in?

Antin Verschuren: Hi. Antoin Verschuren, SIDN. I have a question for actually all of the members of the panel. You all except DS records or DNS key records for your delegations. Suppose that tomorrow we find a killer app for DNSSEC and suddenly all your domain name holders want to turn on DNSSEC within a month. How many new DS records can you accept with your current infrastructures per hour, per day, per month?

Matt Larson: I'll go. We can accept DS records as fast as we can accept regular registrations and the system is ready to take a DS record from everybody if that's what everybody decided to do. So we could support 100 plus million DS records. I don't know off the top of my head the actual speed number for how fast the shared registration system can go, but it is an Oracle database on the backend so it's, it would be on the order of tens of thousands per second; that's the order of magnitude.

Jorg Schweiger: Almost the same for .de as it's just an enhancement of our interface or just another order, so it can be processed as quickly as any other order could.

Yong Yaw Eng: For .my, essentially we have built into our web application for the user, so it's up to them to load their keys in. So I don't see there is any limitation for us because after they are collected in our database it will be generated again for the signing process.

Krit Witwiyaruj: For .th we still process requests manually. So it will take us some time to process the request. So it makes it a lot slower than the others.

Kazunori Fujiwara: The registration and the DS duration is automatically generated to zone file. So it takes about 15 minutes to 30 minutes in JP case.

Bob Hutchison: Yeah, I filed a comment to the IANA notice of inquiry asking for DNSSEC statistics on adoption globally. This group has produced some of those statistics for their zones and I'm wondering whether if ICANN or the SSAC is considering putting up a place where the zones can report a common set of statistics for the traffic they're getting on their DNS deployments.

Julie Hedlund: Could you say your name please?

Bob Hutchison: Bob Hutchison.

Steve Crocker: So let me make sure I understand. You're interested in the uptake of second level of the registrants within each of the signed zones, how many DS records they have in theirs?

Bob Hutchison: Well I guess there's two global statistics that I think people are interested in. One is what percentage of the names in the zones are signed. Okay, that was a good statistic, if all of the TLDs could report that we could get a good picture of how many, what percentage of things were signed. The other percentage that is of interest I think globally is what percentage of the queries are being made against those signed signatures.

Steve Crocker: Let me just comment on both of those. You started by saying you put in an inquiry or a comment to ICANN, although I have a role with ICANN I want to comment from as if I were completely outside. ICANN could, I suppose, undertake such an initiative to try to gather those statistics, but generally it's not tasked with doing that. it doesn't have a formal obligation to do that. So, these are the early days with respect to DNSSEC and just from the general perspective of how technology gets rolled out and do forth. It's the early adopters and the people working in the field that are typically more active and in a better position to do that.

So you have the work that we do and the work that Russ Mundy and his team does and various other groups around the country who are keeping statistics and providing platforms for reporting those. And I don't think we're quite at the point where forcing a reporting, there isn't any forced reporting actually among the ccTLDs on how many registrations they have, much less… The other thing to say is that, in keeping with the theme that these are very early days, it's pretty easy relatively to track the number of top level domains that are signed. So we know what those numbers are and that we're in roughly a quarter of the total of the top level domains are signed.

The number of registrars that are supporting them, the number of registrations that are signed are now down in the sub 1% levels; so it's very early days. And the number of queries again have sort of two key statistics. One is the number of queries where you're asking for a signed response and that's in a way artificially high because there are a lot of resolvers that just turn on the DO bit even if they're not going to sue the answer. And then the more interesting question is how many of the queries are actually being checked where validation is being performed. And that's down in the super small numbers. Fortunately big enough that we can begin to measure it.

Getting forced accuracy out of everybody is premature, I think, in a way, but there's effort, as you've heard reported in the panels today, to actually begin to measure those things. So I guess the picture I'm trying to paint is that the questions you're asking are

actually being addressed. They're being addressed in a mixture of operational and research and so forth and not yet in terms of organized formal reporting across the industry. That, I think, will emerge gradually, but we're still as much working out what the tools are and what the basis is for measuring things and trying to put things on a comparable basis we are getting accurate numbers. And I don't see anything wrong with that. I mean, that gives an accurate enough picture of where we are.

Bob Hutchison: Thanks Steve. I guess I appreciate that and I believe that the purpose of these statistics really are to make people aware of where we are in the implementation and that CIOs, ISPs and other places can begin to use that rising tide of information.

Steve Crocker: Good. Yeah, I think that I was going to ask where did you want to go with that, what was the purpose and I think that's exactly right; we want to raise awareness and provide a picture that people can begin to choose where they want to place themselves in terms of early adopter or late adopter or – what was the comment that the eighth one was added and the answer was because he could. And then there will be a bunch of people who's reactions will be do I have to yet and at some point they'll find themselves in a position of oh I guess I have to. Good. Thank you.

Russ Mundy: Russ Mundy. I have a question for, about the .de drop box. One of the assertions that I've heard lots of times is that the registries do not have any relationship with the name holders and therefore they really don't want to get in the business of, what's often known as the registrar part of things, and they don't have any way to know if they're really talking to the holder of the name. so I'm curious if the .de structure is slightly different than sort of the open gTLD multi-registrar etc., so where it's slightly different but how do you know, from this drop box perspective, that you're getting the key from the legitimate holder of that name, that goes into the drop box for the transfer.

Jorg Schweiger: It's supposed to be a communication between the registrars and not the holders.

Russ Mundy: Okay. So you know the two registrars involved? Okay, great. Thank you.

Rick Lamb: Hi, Rick Lamb, ICANN. I just wondered if I could ask for the indulgement of the chair. I just wanted to make, give a quick update that the root zone signing deployment at ICANN has gotten the SysTrust Audit Seal. This is an internationally recognized auditing thing. And if you could type something on there, can you pull up something on the web easily – just www.IANA.org/dnssec.

If it works it would be great. Iana.org/dnssec. This is our regular site. And just see how well the net works though. Anyway, the importance is we're the first ones to actually have a SysTrust Certification. If you could click that.

Steve Crocker: Where is that?

Rick Lamb: It's like close to the bottom.

Steve Crocker: Oh the next to the last.

Rick Lamb: I mean the hope here is that others not necessarily will follow something has formal as this, and this is something in fact that I know VeriSign will also be doing as well, but it was something that took us a year, a lot of work, it's a third party audit by PWC, one of the bog four auditing companies. This is a further effort to gain trust in a system, the processes and practices we have and that's all I need to say. Thank you for letting me.

Steve Crocker: Very nice, very, very nice. I made a couple of questions here. So Krit, you mentioned plans to transition to NSEC3, a plan to

transition to NSEC3 – how complicated will that be and do you have it laid out in a nice clear step by step transition plan?

Krit Witwiyaruj: Actually we did some changes in the NSEC3 about last week. I tried to make some changes to some of our second level domains to be used NSEC3. And once I did that some of the guys from the NSEC sent us a mail that complained about our zone that cannot, there is some validation error on our zone. So we decided to move to the NSEC3 for that zone. That is for the second level domain.

We can change whatever we would like to change about the DS record in our zone, but for the top level domain we have to deal with IANA to send in the DS record to the root. So we have to be decided on the plan because the problem we face is we had to double sign our zone with the old zone signing key and the new zone signing key, that will double our zone sign and that would take us around one week to do that, to change to the new key. So maybe we will do that for the TLD, for the top level domain once the key rollovers in the next years' time.

Steve Crocker: Thank you. Also I wanted to ask Matt, I was trying to absorb your numbers and you said, if I recall, .62, 62% of the queries have DNSSEC responses and they're 3.75 times as long as regular responses and that that yields a 2.0, if I understood what you were trying to say, overall average in terms of the…and I was having trouble putting those numbers together because the math that I

would normally do would be to take 3.75 times .62 plus .38 times 1 and that comes out to be a lot more than two, a lot more than 2.0. Not trying to quibble too much, but since you were so precise about all those numbers I was trying to see if I understood the model.

Matt Larson: I think it's making me wish I hadnt so precisely cut and pasted. You know, I'd have – you're right. I'm sitting here doing the same math in my head that you did in your head and realizing that doesn't quite add up. It's not that far, I guess, is what I would say. I would have to go back in more detail. I'm reporting the measurements of one of our obsessive operations engineers and I'd have to go back and look at more detail.

Steve Crocker: Well the good news is that gives you an opportunity to give yet another presentation. Thank you. Questions?

Male: It seems like there has been a lot of difficulty with the tools and organizationally running them, signing your zone and so on and so forth. And I was wondering whether Matt might respond – is there any help that we can get besides these conferences or is there something going on to help people put together more operational excellence around this? It seems like there is going to be a disaster that's going to happen here okay.

Steve Crocker: A bunch of these guys can respond more authoritatively, but let me take a contrary view because we're mixing qualitative and quantitative information here. So where you say it looks like there's a lot of trouble I could take the same data and say it looks like there's hardly any trouble at all. It's only a question of where you put those marks on the scale.

[background conversation]

Steve Crocker: There is a learning curve. There are some, we've been pretty strongly oriented to bringing those incidents to light rather than not for precisely the purpose of trying to get them out of the way early to improve the learning curve, to improve the documentation, to improve tools and so forth. And I'm speaking for myself, I'm pretty comfortable about all this. There is, I don't think we're seeing a lot of repetition of the same problems and I don't think we're seeing, in fact, that many different problems.

So we're still able to count in the single, sort of count each of the incidents one at a time. This is pretty small potatoes I would say. So it's a question of whether one's, how nervous one is about these things and what the consequences are. We're still in quite early days, my view. Other people want to comment? And tools are being built and standalone tools are being built and then

component tools are being built and added into products and this is becoming gradually more automatic.

Russ Mundy: Yeah, Russ Mundy. I'd like to comment on that. We've built a lot of tools as part of our work and it's a well hidden website known as dnssec-tools.org. We're hoping people do a search because it does pop up very high when you do a search on Google for DNSSEC. And all of our tools are out, available, they're BSD, Berkley licensed, they're free. So they are in existence and they're pointed at both operational things as well as end user applications. I've got a bunch on my machine that I can show anybody that's interested in looking at them.

But one of the things that's a very big factor in this space is that nearly every DNS operation, when you actually get down to look at the name server operation itself, is different from the next one. And so each and every operational entity needs to examine, themselves, what they really need. Some of them are highly automated, and especially the ones that are really large and really the business is focused on providing names and name servers, highly technical skilled staff for DNS and automation and so forth. And for DNSSEC things extending that philosophy works marvelously.

And I don't know any of the details about what VeriSign or the others here on this panel have done, I'm sure that that's largely a process they follow. But sort of the other end of the scale, the

small, manual enterprise that loaded up their name server five years ago and stuffed it in the corner – Peter Losher was making reference to operations like that – they are going to be having challenges and there are tools available for this.

Also, Microsoft, in their latest major release, does have some support for DNSSEC. And so shops that are explicitly Microsoft shops are having that available. So yes, folks need to go look for tools, they won't hear about them probably from their vendors because most vendors aren't really pushing them yet, but there are a good deal of tools, tool help, training help available in the world. And thanks for popping up the website, that's our DNSSEC tools website.

Julie Hedlund: It was the first to come, it was at the top of the search.

Russ Mundy: Okay great. That's where we like to be with the Google search.

Steve Crocker: Good. Thank you all very much. Let me thank the panelists here; Jorg, Yong, Fujiwara, Krit and Matt. This continues to be a real pleasure. If any of you have suggestion about how to improve these sessions, we're wide open for improvements. We've evolved these sessions considerably over the few years that we've been doing them. And I think, my point of view is that we've gotten better and more content full as we've gone along and we'd be

delighted to continue that evolution. And if anybody wants, feels even more strongly that they think they can do a better job, boy I'm happy to either invite you in or turn over the entire process. Anyway, thank you all for coming. And Julie, let me thank you very much. This is one of the best organized sessions we've ever had and I think it's all gone very smoothly.

Julie Hedlund: Thanks. And before you leave, be sure to take a plate of food with you.

[End of Transcript]