SINGAPORE - DNSSEC Workshop
Wednesday, February 11, 2015 – 08:30 to 14:45
ICANN – Singapore, Singapore

JULIE HEDLUND: Welcome everyone to the DNSSEC Workshop on February 11th 2015 at ICANN 52. I'm Julie Hedlund, and I support staff for the SSAC at ICANN. Thank you so much for joining us, especially bright and early this morning. Just a couple of logistic things. There will be lunch today, so that is your incentive to stay all day. There is a lunchroom ticket on the back of your program. Please hang onto that ticket. It's very important. It will get you into lunch. I will be there as the gatekeeper, and if you don't have your ticket… Anyway, I think that's it.

Just a note, the lunch is not in this room, as you might imagine. It's in the Stamford Foyer. There will be ushers and signs to help us all get there. It won't be too hard to find - not like it was in Brussels, as some of you may remember. I'll turn things over to our moderator for the first presenter this morning - Dan York, from the Internet Society. Dan, please go ahead.

DAN YORK: Thank you Julie. Welcome everyone to this DNSSEC Workshop, this tenth year anniversary, as we'll talk about a little bit later. There are a few more seats at the table if you'd like to join us. There's power up here and there's microphones. I want to begin and let you know we are live-streaming this, so it's being streamed through AC. While streaming of the audio and the slides are out there I also have a camera here - I'm

recording this - that we'll put up onto YouTube for people who want to watch these sessions later as well. When you ask questions we'll ask you to speak into the microphones. These are the funky new ones we haven't had before. Then we can have that go out in the stream.

As Julie mentioned, I'm Dan York with the Internet Society Deploy 360 Program. Many of you know me from email and other things. The Program Committee that put this session together and has been involved for quite a while is listed right here. You can see a number of the folks. The Program Committee Members who are here, would you raise your hands? I see Russ, Jacques, okay, Xiodong Lee is on here, another couple of folks. These are the folks who've been helping work on the plan and other things. We have these folks to thank, and also I'd like to thank Julie and Kathy, who we should also mentioned here is a Newcomer - well, she was here last time - but she's a new Member who's also helping us out with running these sessions.

Speakers - you will also mention that Russ has a countdown timer there, so we're trying to keep this on track during the scope of the day, so you'll be able to see that and know what time you have. We don't have it configured to do a gong or anything! I also want to thank these five companies who have graciously sponsored us to provide us a lunch. All of you who have a luncheon ticket, we're able to do that and keep the networking going and such because we have Afillias, CIRA, DINE, .se and SIDN. These are the folks who are doing this. I have to thank them all because they've all signed up for 2015, so the lunches that we have for this entire year are now covered for that.

We actually do have room for one more sponsor; if there's a sixth company who'd like to be a part of this and help this vital part of the DNSSEC community please talk to me - we'd be glad to add a sixth one on here. Last Monday, two days ago, we had our DNSSEC implementers gathering. Here's a picture of us. This was at the Irish pub. As I say, "Where else but Singapore can you go and have a dinner at an Irish pub, eating Hawaiian pizza, drinking Singaporean beer, while a Chinese band sings songs that were popular in the US in the 80s and 90s?" It was just that kind of fusion that is the awesomeness of Singapore - that kind of thing that was going on.

That dinner that we had there, and the beer was not free, somebody has to pay for it, so I'd like to thank as well ComCast, NBC Universal, and the Motion Pictures Association of America, MPA. Now, why are they sponsoring something in Singapore? Partly because they sponsored the one that we had in ICANN and they were gracious enough in their support that they were able to fund the one in ICANN and also this one. We have to thank especially Jason Livinggood who was here in LA, and he's also here in Singapore. He was the one who helped us get this funding here. Also at the meeting, I'd like to thank SIDN and CIRA for volunteering to sponsor the next one of these gatherings in Buenos Aires, so thank you both. Those are always typically the Monday evening, so if you're planning your adventures in Buenos Aires that's the evening. They've always been excellent sessions.

This workshop and the associated activities are organized through the ICANN SSAC as well as the Internet Society's Deploy 360 Program - the two organizations provide the organizational and administrative support to make these things happen, so we need to thank both of those

organizations that are there. The Program, as you've seen on your Agendas, we're starting out right now with this first presentation, and then we'll have our Panel discussion on regional activities. I see a number of the folks who are here, sitting at the head of the table, who'll be talking about what they're doing for DNSSEC in this region. I find that an enjoyable one.

Then we'll have a brief period where we'll talk about the ten years of these workshops, and we've got a few folks who'll be coming in and talking about what's happened over the ten years we've been doing these workshops at ICANN Meetings. We're then going to have a presentation about reverse DNS and DNSSEC in Japan, DNSSEC management from Duane Wessels. He's going to give a talk from [unclear 00:07:30] about DANE and some of the tools we can use with that.

Then we have a larger discussion happening this afternoon around DNS operators and how we solve this challenge of getting DS records from the person operating a DNS zone up to the registry with the challenge of how do we do that in the place where the DNS operators don't have a relationship with registrars. What are some of the tools, what are some of the challenges and ways we can do this? Olafur Gudmundsson is moderating that Panel, and we've got a number of people in this room who'll be part of that. That's something that's come about in Olafur's work directly with Cloud Flare; looking at how do they make DNSSEC available for their two million domains that they have under management.

They're trying to make it so that they can make a little switch that you just click that says "enable DNSSEC", and boom, it just works. In doing that, he's encountering a number of challenges that started being discussed at the IETF meeting in Honolulu. We had a [boff] there and then we'll also continue that discussion today and on mailing lists. That should be a very interesting session. Then we wind up with another session at the end there, and Russ and I will be back to wrap it up at the end of the day. Just to give a little bit of an update of what we're seeing in terms of deployment numbers and counts, et cetera, this is the map or chart that Rick Lamb maintains at his site, which shows the signing of the TLDs.

He's been tracking this back from the early days of things. You'll see it has this very nice chart that's going up here. This is all the new gTLDs. They've all come online and been DNSSEC signed. So if you look at the statistics we're closing in on 80 per cent of TLDs signed, which is a cool number in the sense of being able to see that kind of thing. The reality is the second-level domains are not quite so high in that chart, but it varies according to the TLDs. Some TLDs like .gov have as many as 80 per cent of the second-level domains signed, and others like Brazil have a significant percentage of the TLDs signed, and .nl and .cc, but in other cases as in .com it's a much smaller percentage.

But the good news is this step, at the TLD level, is definitely happening and providing us with very nice charts we can use, like this. the current numbers that we've got coming out of the DNSSEC deployment maps - which you'll remember is the project that was originally started by Steve Crocker and his Shinkuro team and then taken over about a year and a half ago by my organization, by me personally. We're currently tracking

right now a total of 579 classic ASCII domains, which is 579 of the 739 total as of last week; 59 IDNs, out of 80; and a total of 637 of the 819 TLDs that are out there right now - they're signed with DNSSEC and have a DS in the root, or are operational in the way we do that.

If you recall from the charts, we note things in these five stages, where we show some things as being experimental at the TLD level as announced; partial, they've signed the zone but it's not yet linked into the rest, DS in root, and then operational where it's accepting signed delegations and uploading DS records. I will note this stage is very easy for us to find, because we can see there's a DS record in the root. This stage of getting things to operational involves us trying to find out from the TLDs whether or not they're starting to accept records. So this is a bit more subjective and hard for us to find at times. Here's what the overall map looks like, as of last week.

We're looking pretty good. We've got a lot of green happening in a lot of different parts of the space overall, when we look at what's going on as far as DS in root. We need a little bit more down here, we need to fill in a bit of Africa over there, but overall, on the ccTLD side, we're doing pretty well. We'll show you some of these pictures here. This is another high resolution map, and these are available from the site and the URLs in the slide pack, where you can go and get that. You can see here we need to fill this part in a little bit, but I know that ICANN DNS Team is doing a good bit of work with some of the ccTLDs in Africa, and I know that some of our Internet Society folks are working with them as well, and some other folks are working in that space too.

Let's take a dive in and see some of that. There in Africa, this is what we look like right now. We need to fill in a good bit of that space there, but we'll get there. North America hasn't changed. South America, we did add Grenada since the last time we were here. The .gd domain is now signed as well. That's new since the last time we were here. In AP we had Australia. Adam's here to talk a bit about what they've done, but they've been signed for a while, but the DS was put up into the root. We'll find out whether I can update that to operational in a few minutes. It looks like he's nodding, so yes. Indonesia also came in with .id, Vanuatu, and India signed about six of their different IDNs they have, that are out there. Good movement in that space.

Here's what it looked like last time, here's what it looks like now. Awfully nice from a map perspective when Australia signs and Indonesia signs. You get this big bunch of green happening in there in the middle of things. All good. Europe, the big changes were Ireland. .ie came online being signed and operational, and also Norway. Norway had some good number of domains. The .no domains were getting signed at a fairly good clip. I don't know what they're up to now, but they had 20,000, 30,000 fairly shortly after their initial launch. It worked with a number of the different providers to go and do that. The next steps that we continue to want to work on with the DNSSEC maps project is to try to look at how we visualize some of those other areas.

I had a graduate student contact me about how to visualize some of the gTLDs, because we're entering data into the database for all these domains. Every week I'm sitting down entering all these new gTLDs in there, which provides entertainment for me at times, to look at all these new gTLDs we're getting in there. We've got that out there. The maps

are there. You can go and download them. They are Creative Commons, so you're free to use them in whatever form you want. A couple of people contacted me to ask if they could use them on annual reports and things and I said, "Sure. They're freely available that are out there." You can also subscribe and get a new copy of the maps ever Monday morning.

We also have a project that's been ongoing for a while called the DNSSEC history project. It's a project where we're trying to document the history of DNSSEC from its very beginnings on through here, which is helpful for things like our tenth-year celebration here, but this goes back a bit more. We'd love any contributions people have, if you want to take a look at that. If you see there's a spot that's missing you can either set up your own Wiki account and edit it directly, or you can send in a message for me and I'd be glad to take that information. I had a great step here. We had a doctoral student who approached me here saying he was looking to do a project around the history of DNSSEC, and he's interested in curating this and turning into something more meaningful.

So hopefully by the time we stand here in BA I'll be able to give you more of an update about where this may have progressed. I think that pretty much wraps me up. Any questions that we have about the scope of today? All right, with that I'm going to turn it over to Russ to begin our Regional Panel. Again, thank you all for being here. Thank you very much.

RUSS MUNDY: Thank you Dan.

JULIE HEDLUND: Thank you very much Dan for a very helpful presentation.

RUSS MUNDY: As Dan mentioned, I know most of the people here but not necessarily everybody. I'm Russ Mundy. For the Regional Panel we tried to get a group of folks that are engaged in the geographic area that we happen to be having the ICANN Meeting in, to give us some insights as to what's going on relative to DNSSEC from their perspectives. We have a group of five folks here today. I'll introduce them in the order that's on the sheet. We can start with Jay Daley from .nz. Jay, if you want to go ahead and give a few introductory words? That would be fine too.

JAY DALEY: Hello, I'm Jay Daley from .nz, New Zealand, and I run the registry there. We first signed DNSSEC about two and a half years ago, and have been operational since. As a matter of interest, we have another key ceremony coming up very shortly. We put DNSSEC into place using a fairly lengthy DNSSEC practice statement that we consulted very widely about with our community. I've given presentations on this before, hut that's a complete nightmare to do - involve your community in these things. We were going to use a 1152-bit key length, but some people in our community felt that was too short. I believe that's because they killed a chicken and looked at its entrails rather than they have any technical expertize.

We do have one of the world's leading cryptographers who lives and works in New Zealand, who explained patiently to them that 1152-bit

would require a [unclear 00:18:25] to the size of the known universe, but they still, with their chicken entrails, prevailed. So we moved to a 2048-bit key. Anyway, so that's the history of us, and it's all very fun. Recent developments then: we, in .nz, up until recently have only registered domains at the third-level. There are a few hundred domains under govt.nz, which is run by the government. Those domains are moderated, and only government organizations can get them. The government has recently completed the process of operationally putting in place the ability to sign those domains.

They created their own practice statement based on ours. They went out to tender for a registrar who would handle all those elements for them. The registrar put in a great deal of investment and time. The government bought their own signers, specifically to work with that registrar, and they've held their key ceremonies and it's all gone very well. We're very pleased with that. It took quite a community effort. Some people on my team, other people, just taking out government IT staff out for a coffee regularly, drip-feeding the benefits of DNSSEC over about two years, for this to happen, and we're very pleased it's happened and we've got there. We ourselves have got some new signers as well. These are AEP Keepers.

We, like many, use the SUN SEA6000 cards when they came out, because they were cheap, brilliant and they worked. Then Oracle bought SUN and set about destroying SUN entirely, so we can no longer use those because you can't get support from anybody who understands anything. They quadrupled the price and I think they've probably changed the goal contacts out to something cheap and nasty as well. So we've now got AEP Keepers, which are considerably more expensive. I

think we've probably spent in the order of roughly US$120,000 to get these. They are very slow in comparison to the SEA6000s but they're very easy - they just do it and they just work. We are not the largest registry in the world, so they've very suitable for us.

This is the point at which I make the usual plea. If there is anybody out there, business-minded, who understands crypto, there is a huge potential market for making very fast signers, I'm sure. There are lots of chips out there that do this easily. It's almost an assembly, and certification company you need rather than a technical company who ought to be able to do this. Many organizations throughout the world are going to need this type of equipment for their own certificate management processes internally. Anyway, that's my little rant. To finish off in .nz we have 600,000 domain names in total. We just passed that milestone recently. It may be another while before we get 700,000 the way that our growth is going, and the way global growth is going.

We have 210 signed domains, of which 133 have DS records, so that's a lot - that's 72 that are signed but don't have DS records because the registrar doesn't support it. I'm pleased by that number, I must admit, because that means that people aren't waiting for their registrar in order to get DNSSEC, they're doing it themselves anyway. Quite how the chain of trust works there we haven't fully investigated, if they're all in DLV or something. I'm not sure. Sorry for swearing by saying DLV. Anyway, there are five that are signed, but they haven't given the DNS records, so presumably they're in the process of doing that.

Finally, I'm one of those people who is in no way panicking about the update of DNSSEC. Every exponential curve looks like it's absolutely

going nowhere for a very long time and then shoots upwards. We worked with the government because we thought that would improve the security posture of New Zealand to do that, but we're not panicking that we need to somehow [unclear 00:22:50] our registrars into signing domains or doing anything like that. We're happy for it to grown organically over a period of time, as people need it to, when they're convinced that it's the right thing to do.

RUSS MUNDY: Thank you Jay. Let's take a couple of quick questions with each speaker, and then we'll have a few minutes at the end to have general questions. Please say our name and affiliation when you start please.

DANIEL EBANKS: Daniel Ebanks, Cayman Islands, the authority. Wondering what stop gaps, what bad problems, your subdomains are having with getting signed and getting DNSSEC going?

JAY DALEY: We run both the top-level and the second-levels. Gov.nz, the government doesn't own the gov.nz, we do, but the government can set the policies for who can register a domain name underneath that. All I meant was there was a staggered rollout over about three to four months. We did geek.nz first - obviously it's important to do that! - and then we ended up doing one of the larger ones a little bit later, in terms of the DS records going in to .nz. So it took us a little while to do that, staggered, but otherwise there are no issues about those subdomains, because they're fully under our control.

JULIE HAMMER: Julie Hammer from .au. Jay, when you were taking your government colleagues out for cups of coffee and educating them, did you have any problems because there was a constantly changing point of contact, or were you dealing pretty constantly with the same people and therefore it was a pretty smooth education process?

JAY DALEY: As expected with government there was a re-organization every month and people moved around. However, New Zealand and Wellington is small enough that those people ended up in a different job in IT, and there were actually quite a few people from our community who, without being asked, felt that it was their duty to go and persuade government to implement DNSSEC. So it wasn't a coordinated campaign - it was a grassroots campaign of people taking people out to coffee. There must have been about eight or nine people who made it their mission to go and do that. So the coverage they got was pretty large, so even though people did move around we still managed to get everybody spoken to.

RUSS MUNDY: I've got a question for Jay: have you seen any other segment of the country, whether it's a business or other type of interest, that's shown a particular interest in doing DNSSEC?

JAY DALEY: I'm going to answer that in the negative, in that the banks are particularly… For a while the banks were particularly not interested. We have an organization within New Zealand where companies that are interested in security get together to meet and talk about these things, to understand that, and that mainly those are banks or large websites or newspapers, that type of business. Increasingly we see those people recognize the need for DNSSEC-signed sites that they rely on. One of the things we have is we have an RPKI validator, and there are a number of these people who want to start using our RPKI validator and have specifically asked us to sign it so that they can trust it better.

So they're not yet at the stage of considering how much DNSSEC might work for themselves by them signing, but they're now recognizing the value of using a DNSSEC-signed site for some of the things that they do at a security level.

RUSS MUNDY: Thank you Jay. Next on our Regional Panel is Ryan Tan from SGNIC. Please go ahead.

RYAN TAN: Hello. My name's Ryan Tan. I'm the Head of Technical Ops in SGNIC. Okay, so very briefly we started looking at DNSSEC around 2008, around about the time everybody else started looking at it. What happened was we formed a Working Group to study DNSSEC, and this Working Group consists of government officials, obviously us, the registry, and some registrars. As a summary of the findings we found that back then DNSSEC was complicated and was risky for any DNSSEC zone operator to

adopt, if it was not done right. We found that there was no demand from end users or the registrants, and the software tools, policies and best practices are not very much in 2009. Perhaps the best part is that no registrar was willing to participate in the test that we prepared for them.

We put this one back to our management, and this one goes all the way up to the national level. We decided that if we were to deploy at the cc level it's a commitment that cannot be reversed, even though you have no customers and you are subject to all the risks. That was when we decided that we had to adopt, watch and wait the posture while trying ourselves to do DNSSEC, because we knew with the root signed that DNSSEC is here to stay - it's not going to go away. So we just need to prepare ourselves. Between 2009 and 2014 we organized local workshops for our local engineers. Fast forward to today. We found that this study was done last May. It's slightly less complicated and risky for DNS zone operators. There's still no demand. In the five-year period I've had absolutely nobody who asked me, "Do you have DNSSEC?"

The only person who came up to me was Rick Lamb, and that was because he was here doing the DNSSEC Workshop. Yes, so according to my study we're looking at the global [unclear 00:29:48] point around five percent. That's the number we're looking at. This is names in the registry - we're not talking about actual usage. Sometimes we look at Rick Lamb's DNSSEC chart. You'll find it's very scary. Some oft eh registries are up and down, that kind of stuff. But we do find that the software, the tools, the policies and best practices are much, much better than five years ago. So I think that on balance this is about the right time to get started on DNSSEC.

So what we will do is we'll need to research and understand the lessons learned from other pioneering registries, which is many of you around this table. Thank you for sharing all the mishaps that you have. We have developed the DNSSEC practice statement. Thanks for all the [DPS 00:30:41] that you've put online. We have also developed the key ceremony procedure. This is modeled after the ICANN procedures. We've got the money. What we'll do next is enhance the software, which is quite a simple task; just a couple of DS validation stuff we need to do, and build a monitoring system around that. We'll develop the policies, the transfer policies, and then seven, this is the hardest part: we're to back some registrars to participate.

Then, eight, we need to establish practice order. We are very worried about the failures, so we'll need to practice our recovery drills to make sure we're absolutely ready before we implement DNSSEC. So our plan right now is to perform a partial deployment, root deployment, around 2016 or 2017, depending on how fast we go. That's the end of my slides. Any questions for me?

SPEAKER: Thank you for coming here and talking about what your plans are. One question for you: your registrars for .sg, are they mostly here in Singapore, or do you have registrars globally as well that register under the .sg?

RYAN TAN: Our registrar mix is about 30 per cent overseas and 70 per cent local.

SPEAKER: Okay. I was just wondering how many of those overseas registrars might be ones who may be able to help you, if they're already doing DNSSEC, or not?

RYAN TAN: Yes, we haven't told them this plan yet. You are the first to know. Hopefully they'll come on board!

SPEAKER: Breaking news! All right. Thank you very much for presenting this.

JAY DALEY: Have you done a scan of your zone to find out how many domains are signed already?

RYAN TAN: No, not yet.

RUSS MUNDY: Thank you Ryan. I have a question: Singapore is a very nice culture and society, but one of the things it does seem to have is a fair bit of oversight and direction and things that should and shouldn't be done, and how they're to be done. Is this something that's being considered for deployment, relative to getting DNSSEC in use? In other words, whether it's some of the government directives, or through some of the business encouragement? Some of the structures that Singapore has in place for other activities, for suggestion that DNSSEC should get used? Even though, as you say, you've had no real raw, unsolicited demand?

RYAN TAN: Okay. I'll take your question in two approaches. Number one, we approached the guys who we thought would need to use DNSSEC, and these are the financial institutions, the banks. The good thing was that the authority here… I'll backtrack. If you want to secure a website there are essentially two major approaches - one is PKI and one is the second-factor authentication. The guys up there decided that the two-factor authentication is the way to go. The banks over here implemented two-factor authentication many, many years ago, so the banks were not eager to adopt DNSSEC. You tell them, "DNSSEC," and they say, "No, I have two-factor, it's good enough for me." So we lost a good number of customers that would come on board. So that's one.

In terms of government, actually it's the subsidiary of the authority, so we do have regular links with the guys that run the government DNS service. We talk to them. We don't really have a coffee - we go into our pantry and we tell them about DNSSEC. So they are quite busy with other things, thanks to [anonymous 00:34:46], over the past two years. So their plan is like ours - to get ready - but they're not very eager to implement it. We, as in they, are also very worried about the potential failures as we see in the us.gov zone. So these are things that worry them a lot. We want to take our time to practice before we implement them.

RUSS MUNDY: Thank you. Jim?

JIM GALVIN: Jim Galvin from Afillias. There was a line on Ryan's slide about begging the registrar to participate, which caused me to think about a general question I'd like to ask all of the panelists, so if Jay could go back and speak to this directly, and the other Panelists might include this in their presentations, I'd appreciate this: have you considered, or would you consider, incenting registrars to participate in some kind of reward mechanism that's possible for them? The obvious choice is a discounted fee, but there are other things that one could do. I'm just curious if folks have considered doing that with registrars, or if they would? Thanks.

RYAN TAN: We look at the Netherlands model. I think it's quite interesting. I think they're the few guys who actually incentivized the registrars. At this stage we do not have specific plans yet, but that's something that we could consider.

RUSS MUNDY: I think .cc did also.

JAY DALEY: We did consider it, but we have a split structure with me running the registry and a separate internal company that runs the regulator and sets the policy about those things. That has some principles that would be violated if we were to do any kind of discount or differential treatment. The other important principle that the regulator has is that it doesn't want anybody to end up with a signed domain unless they specifically choose that. So where .nl has done so well, I believe, has

been registrars signing all of their domains, rather than customers individually asking for their domains to be signed.

RUSS MUNDY: Okay. Any other questions for Ryan? Thank you Ryan. Okay, I believe next on our Agenda is Geoff Huston from APNIC.

GEOFF HUSTON: Thanks Russ. I'm looking at the other side of DNSSEC, so I'm not counting which registrars offer DS records, I'm not counting signed domains, I'm not counting the supply side of any of this. You've seen numbers, that's fine. I'm looking at precisely the opposite question: if you sign a name, which of your users will validate it? In other words, are you signing names into a vacuum, or are you signing names into rampant demand? The question I'm trying to answer here, with as much detail as possible, is that question of who, and how many folk, send their queries through DNS resolvers that perform DNSSEC validation? Let's get this straight: I'm not counting resolvers. If three people send their queries through a resolver, I count three, because that's an easier and better way of counting stuff, oddly enough.

The way I do this is I pass every user, thanks to Google Support, through an online advertising campaign. There's a script behind it and that script causes the recipient to go and fetch the names. No clicks, nothing, it's part of the impression of the ad. To make sure that they're doing the full box and ice I send them a very unique name, so there's no [caching 00:39:17], and that name is signed. It's signed in such a way that I'm not doing wild-card signing; I'm signing it such that every unique part of that

name has its own set of keys, and I'm the authoritative name server - I'm the only authoritative name server for that name. So if they're doing validation I will see not only a fetch for the original A-record, plus the signatures, because that's got to be on - I will see a fetch for the parent DS record, because I own that too, and I will see a fetch for the DNS key record.

Now, to make sure that you're doing real validation and not playing with me, I also send a second test. That test, the DNSSEC signature chain, is busted, so that if you really are doing DNSSEC validation you will never fetch the second object, because the DNS is going to come back going, "serve fail" and no matter what you try, if they all say "serve fail" you're going to give up and not fetch it - there is no answer, because that's what DNSSEC is meant to do. So with Google's assistance here, I do about half a million tests a day across the entire planet, and the ad network is brilliant. They never, ever give me the same address twice. Well, they do, but it takes an awful long time, because there are an awful lot of users and at half a million a day it takes an awful lot of time to recycle because Google constantly want fresh eyeballs, so they deliver me fresh eyeballs.

So that lets me do the opposite of Dan's map. This is where folk validate - the lighter the color, the more folk in that country validate. This is a weird map. It's almost the inverse of GDP per capita, yes? Look at all that stuff in Africa, bits of Malaysia? So the folk who validate aren't necessarily the richest folk on the planet - the UK, France, Spain, Portugal - they don't, neither does Mexico, et cetera. Australia, half-hearted, New Zealand, half-hearted. I actually do this as a table. All these resources are online. There's one observation about this that is

insightful. An awful lot of folk send their queries through Google's public DNS. It's a huge number.

Currently around 20 per cent of the world have their queries passed through Google's public DNS and of those 20 per cent more than half, by default, just let Google do what Google do. By default, unless you say otherwise, Google's public DNS will validate. You've actually got to say, "Don't," to stop it, and most folk don't. So that second column is interesting. That's the percentage of folk in those countries that use Google's public DNS. So the reason why a lot of Africa validates is that a lot of Africa use Google's public DNS and Google's public DNS validates. So Google's public DNS is a major factor in those numbers. But we're talking about Asia, and let's color the map about Asia.

It's kind of interesting, because there's Syria, there's Iraq, there's Yemen, and there's Vietnam, which you'd never expect, would you? You would expect Singapore, Australia and so on. So that's the table, in looking at Asia, and Iraq, Yemen, Brunei, Syria, Occupied Palestinian Territory. Why does the Occupied Palestinian Territory validate? Because all their queries pass through Israel and they don't seem to trust them. No, truly, so the best defense is: validate. So they do. They were one of the very early bit adopters for precisely that kind of reason. Is it Google? Not really. 40 per cent of users in the Occupied Palestinian Territory validate, only 30 per cent use Google.

The rest are using their resolvers that validate anyway, because it's basic defense. It's, "I want the DNS to work, rather than give someone else's twisted version." I'm trying to make this quick, so I'll go straight to what happens. This is the folk that turned it on, but there's some bad news.

TM Net in Malaysia turned it on in mid-December, and when I prepared the slides in early January, 60 per cent of their users were validating. All of this was via Google's public DNS. By mid-January they'd turned it off again and now no one in Malaysia validates. I'm like, "Guys, get it together, what a stupid thing to do - turn it on, turn it off, we don't know what we're doing." Obvoiusly, that's just madness.

Spark NZ, which I think is the remnants of Telecom New Zealand, because that name has long been dead and buried but is a relatively large retailer. 16 per cent of their users validate, so I think that's part of internal segment. I don't think that's users. I think that's actually Spark doing it inside their resolvers. It's not Google. Their Google numbers are quite low. They turned it on mid-December, straight up. And Spark is big - Spark is one of the major providers in New Zealand. The other one I noticed, which is cool, is MCS in Mongolia. Again, they cheated - they pushed it through Google, they're not doing it themselves. So two out of three still have it on. TM Net decided it was all… Whatever.

The folk who turned it off. I think Yemen turned it on by accident, because when you're running BIND it's only one line, you just say "validate" and then they thought, "Whoops, didn't mean it, and then they turned if off again." I don't know why. So their numbers are down from 80 per cent to 40 per cent at the moment. VNPT down from 55 per cent to 35 per cent in Vietnam, because they turned off using Google. They were actually sending a huge amount of their traffic through Google's public DNS - they decided to turn that off. The other one, in Indonesia, Telecom Net PT down from 30 per cent to 7 per cent. Much the same set of explanations - they stopped using Google and they stopped doing validation. Madness.

Singapore - 16 per cent of Singapore users send their queries via Google, and interestingly in November the Netflix app that runs on Android decided to tunnel all of its DNS through to Google, because Netflix don't trust the locals to do DNS, with the local [unclear 00:46:42] all over the planet. The Singapore numbers fell by half, which shows you how many folk in Singapore watch Netflix - about 8 per cent of the population. This is the map of Singapore and as you see, the validation that's happening in Singapore is sitting between 3 and 5 per cent and nothing much has changed, which is a pretty dull picture really.

This is the list of providers in Singapore. The right-hand side is by market size. The biggest providers in Singapore are Magic X, StarHub, StarHub Internet, Mobile One, ERX. If you lived in Singapore these would be very familiar. The amount of DNSSEC validation, nobody does it except Digital Ocean, and fascinatingly the Indonesians run an outpost here in Singapore and they validate here, they just don't do it at home - only for the foreigners. Yes, so globally around 12 per cent of the world validate. I reckon that's brilliant because 3 per cent of the world do v6, so 12 per cent is massively good. In fact, [unclear 00:48:04] goes on is that more than 20 per cent of the world actually do the initial validation, but when they get "server fail" they pick up their second resolver that doesn't do it. So more tried than succeed, and a lot more.

Google, post-Netflix, Google's market-share is up around 20 per cent of the world's users. It's huge, and as long as you do validation you just leave everything to go with Google and the right thing happens. But Google isn't everything. That list of countries don't use Google much at all, and they validate like crazy - Sweden, Slovenia, Estonia, Denmark, Czech Republic - none of these are Asian yet - Luxemburg, Poland,

Iceland, Ireland, Finland, Greece, South Africa, Greenland - you're still not there. Iraq, Yemen and Cyprus though do it themselves. Sorry, Iraq and Yemen are local, the rest aren't. So on the whole Asia, sadly, no.

Everything you've ever wanted to know is there. You either write that down or you bring out your camera and click on that silly QR thing. Either way, you get there, and that's the graph of the world. Up and to the right, not really, but it's not going down all that much. It's kicking there, it's 12 per cent. Folk need to turn it on. That was all. Thank you. Questions?

DAN YORK: First of all, thank you very much for doing these measurements. People will remember a couple of years back this was one of the things we were seeking; a trend chart for validation so we could show people this. So thank you very much for continuing this on an ongoing basis. I had one question, which was you mentioned that the Netflix app is now sent tunneling all its DNS queries to Google's public DNS, and you guys have figured that out?

GEOFF HUSTON: Well, I'm blaming the person on my left here, because I track the use of Google pretty closely through ads, and I noticed a sudden jump in the world's use of Google through November. I was speculating that a sudden jump is weird, because users don't do sudden jumps. So it either had to be a device, a platform or an app that's really common. There's only one thing the Internet does and everything else is irrelevant. The only thing it does these days is stream video. So the obvious candidates

are Apple, Netflix and ChromeCast. I don't think ChromeCast marketshare is that big. They're using Google's public DNS. I don't think it's Apple.

That kind of leaves very little, and then Mr. Kumari over here on my left, when I was speculating about popular reasons, Googled Netflix and Google together and up came a little story from last November that the Android app that runs Netflix, to counter some of these issues across cross-border content control is doing its own DNS via Google's public DNS. It's a new breed of application that doesn't trust its environment. This is an application that says, "I'm doing my own DNS. I don't care what my operating system says, I don't care what the ISP says, I'm doing my own DNS."

DAN YORK: So you can see where I'm going with that, because that's one of the topics certainly we've been talking to application developers about; the need to potentially do their own validation and do those kinds of things. So it's an interesting use-case. Thank you for that pointer. I'm going to certainly dig into that. Thank you Warren for the pointer as well, for Googling that! Thank you Geoff.

RUSS MUNDY: Just to comment, this is an area that we've had several sessions on in this workshop over the years; where and how was the right or best or most appropriate place to do validation, and many people have asserted for a very long time it is the application itself - to not only get the DNS

data in but actually validate it by the application, and then you don't have to trust anything outside your application code.

GEOFF HUSTON: In general you're right, although the case from the Palestinian Occupied Territories is interesting, because they are in a position where some other party has the ability to change their DNS - the ability - and so in terms of a defensive mechanism the infrastructure resolvers in this area of the world are protecting themselves against the [unclear 00:52:45] in another area of the world, where their traffic is going through. So in that case, DNSSEC is really a strategy about infrastructure, not a strategy about application integrity. So I can see both reasons. But certainly, setting the AD bit and sending that to the local DNS is kind of stupid. Anyone can set the AD bit as a man in the middle. Apps shouldn't trust the operating system. Apps shouldn't trust the environment. Apps should validate.

That doesn't mean they have to tunnel. What it actually is - and Netflix was overkill - what it really means is what apps should do is, for themselves, validate what the infrastructure delivers. Netflix went one further and said, "Don't care, queries go all the way through." I think that was a step in a different direction.

SPEAKER: I think it also somewhat depends on what the application is and how much it cares about the answers. For certain things like DANE it specified that the application is supposed to do its own validation, or make sure it's got the data over a way it can be sure is correct. Because

of that, there is the "get DNS API" which provides all this information to applications, and VeriSign is helping build that and get it to where it works really well.

CRISTIAN HESSELMAN: I'm Cristian Hesselman. I'm with SIDN .nl. I was wondering, you used that ad network to generate queries, basically. What was the distribution of traffic across countries? Where did you get the traffic from? Was it equally distributed?

GEOFF HUSTON: No, it's very unequally distributed, but you're not seeing that data. When you go through an advertising network you bid for ads, and typically if the country is rich the folk who do a high bid, "I want to sell you car insurance," tend to get the ad. So I bid really, really, really low. I'm a cheapskate. So I do get excessively large placements in Indonesia, Thailand, Poland - the usual places where no one is bidding high and I'm the lower bidder. So I have to massively re-weight my data, so I do. I actually use the ITU's current estimate of users per country, because what I've noticed is Google seem to be uniform within a country, but they tend to give me different weightings across countries, so I've used country granularity to re-weight this.

So those numbers are what I would call normalized, to the base of this is just a user is a user, no matter where they are, and that's not the raw figures that I get out of the ad system. So yes, there is a real problem in doing this.

SPEAKER: I'd also note to Geoff, you include those numbers or the number of samples in your data, on your site. So you can see in his actual measurements he does show how many samples were there for that given country, so you can get a sense of how accurate that is.

RUSS MUNDY: Okay, thank you Geoff. Next we have Adam King, to my left.

ADAM KING: I've been introduced. I'm Adam King. I'm the CTO at auDA. We manage .au. Before I talk about what we've done to get signed in .au, I'll give you a little background and the structure of .au. auDA's the registry for .au. It's actually a closed space. We only have a finite amount of registrations under .au, and that's for our second-levels; all the registrations that completed the second-level and below. auDA manages those second-level or most of those second-levels. They manage 16 of the 18 that are in there. We approximately have three million registrations currently, and all our registrars interface directly with AusRegistry to submit changes to registrant data.

So where are we now? As we saw, there's a map there, and Australia is light green on that map. We actually can move to the dark green. We are operational, as of the 1st of Feb. On the 20th of November last year we submitted our KSK to IANA. That was dropped in on the 25th of November. We weren't satisfied enough with that, I guess, so we decided to drop another one in on the 1st of December. That must have set off some alarms with IANA because it took them seven days instead of five to process that, but it did get processed and was in on the 8th.

They've put us into a double-sign period and we're double-signed for two months there, effectively, with our KSK, for a rollover. On the 31st of Jan we removed our first KSK that was submitted in November. So we've completed one KSK rollover already.

As for our second-levels, they also went in last year, so we took a cautious approach. Our overall approach with implementing DNSSEC was to take it cautiously. On the 4th of December we added 12 of those TLDs. They're listed there. We did monitoring and waited approximately a week to make sure everything was running okay. The TLDs that were submitted were those with least impact to the .au space, and that is why they were chosen to be done first, so if we did make a mistake or something wasn't quite right, it would be of least impact. So on the 10th of December our big three, which is com.au, net.au and org.au were signed and added into the zone. Again, that also went really smooth.

As I just noted, on the 1st of Feb we then enabled registrars to accept DS records from their registrants. We took a bit of a break over Christmas and waited for the 1st of Feb for that to go out. How do we get there? Well, back in 2010 we decided, "Yes, we'll go ahead with DNSSEC." So we came up with a five-phase process, as you can see there. We didn't really do much else in 2010. It was mid- to late-2010 when we decided to do that. So in 2011 we started testing on a lot of manual signing. We looked at key sizes, played around with different algorithms, but mainly during 2011 we just kept a watch of those who signed. There was 20, I believe, signed in 2011. One of those was .com, and there were four outages reported in 2011, as far as I could find.

So we really just monitored the environment and were looking for uptake and things like that. We also added a sub-phase to our initial five-phase rollout, and that was to engage our stakeholders. 2012 rolled around and we decided we needed to set a set of goals for deploying DNSSEC - the main one being that DNSSEC should be as easy as DNS. We have quite a small zone. As I said, it only has a second-level pointers in it, and glue records, so we manually edit our zone; we don't use dynamic updates. DNSSEC was around at the time, but you needed to be using dynamic updates for that to work. So that wasn't a fit for us at that time. Our overall statement was that we wanted to sign our zones with as little complication as possible, using processes that are the least time-consuming but are balanced with the appropriate level of security.

Luckily for us, in February ISC brought out BIND99 and that had inline signing, so we were able to maintain our manual editing of the zone, and 99 signing with auto-DNSSEC. Then we moved onto playing around with encrypted data stores for storing our keys or our private keys. We were using locks on RAM discs, that comes with its own security concerns - you keep your key online, take it offline, if it's online and the store is always online, if your server gets popped then your private key gets taken. So there was a lot of playing around with that sort of stuff and looking at what the impacts were there.

In April of 2012 we formed our Working Group, which was that sub-phase that I mentioned. Basically that was to help us with pushing out and bringing together our practice statement, bouncing that off our stakeholders to see if there were any real issues there. They were also there to help us with non-registry aspects; so educating their areas, providing awareness to their customers, and things like that. June and

July we got introduced to AEP and started looking at HSM providers. We got into greater talks with AEP and they gave us a test HSM in September, which we've started playing with. 2013 was more about developing policy, monitoring, and making sure we had the right verification stuff in place.

HSM was the better fit for us. As Jay mentioned earlier, it's quite easy to use, at the end of the day. We also have only a small zone, so we're not signing a lot of records at once, and HSM does the job. We can keep our key online, and it was protected in the hardware itself. We spent quite a bit of time writing policy, and I believe that's probably where the most work is for DNSSEC - your policy and your documentation for processes. You can make it as easy or complicated as you like, but the key there is getting all your processes written so that they can be easily followed, and that also includes disaster, recovery and what to do in emergencies, because the last thing you want to be doing is scratching your head and guessing when you are going dark.

We worked on a lot of monitoring to make sure that we're always aware if anything does change, of if there's an issue. So we do [RIC 01:03:11] monitoring, we grab some tools from places like measurement factoring and things like that. We use an [agi os 01:03:19] so we looked at different plugins to put into there. Then we also do validation on all our responses, so we query all our slaves for every record that we have in our zone and do validation on that. We've written a whole bunch of verification checks and scripts, so we've set it up that our zone will not pass to any of our slaves that does not pass any of our verification checks. We do sometimes get false positives, but it keeps us on our toes. So we spend a fair bit of time working on that.

Again, the last thing you want to do is push out a half-signed or broken zone to your slaves, and then have it out there in the wild. Moving onto 2014, basically it was finalizing everything, bringing it all together and signing the zone and putting it into production. Again, really finalizing those processes, tweaking them, going over them, trying to make them as easy as possible. Ceremonies - walking through some of our signing ceremonies just to make sure that all those that will be involved understand the process and why things are in place; documentation again. So in April we moved into an experimental phase. We added our KSK and ZSKs into the production zone. We were rolling ZSKs one a month for the first three months.

We were using double-sign at that time, so after the first month we re-looked at that and went, "We probably don't need to do double-signing, it's pushing a whole lot of data back into the network that probably doesn't have to be there," so we tweaked and played around with the pre-publish method, and by the fourth ZSK we switched over and are now using pre-publish on our ZSK. To make sure we got that right we rolled another one in September and then in October we moved our experimental KSK and added the KSK that we were going to submit to IANA. The rest is history. Next slide please.

What did we learn? Technically, signing is not difficult. It's running a bunch of commands, hugging the keys, putting it to your zone, and it's done - particularly with later versions of BIND and other name software, it is mainly straightforward. So most of your time, as I mentioned earlier, is spent on policy and documentation - who has access to the keys, who generates the keys, where you store the keys, your processes, all those sorts of things. With that in authentication you add a new

layer, and it's important to get all that information written down and well documented. We realize it's probably okay to wait, as Ryan at .sg was saying earlier.

Now is probably the right time to be getting onto DNSSEC. A lot of things are starting to catch up technology wise, so it hasn't been a huge push other than from this community, IETF and things. But from users out there, there hasn't been a huge push to get DNSSEC out there. So it has been okay for us to wait. It allowed us to make design changes. We moved from using software signing to hardware signing, changed our processes, as I mentioned, the double-signing and ZSKs. We've played around with different key validity periods, trying to get the ones that fit right for us - everyone's are different, so it's no one-size-fits-all.

It gives us an opportunity to look at the interactions with the zone. We wanted to really limit the amount of time we manually went into the zone - the more human touch, the more errors seem to occur, and it gave us a chance to look at what personnel needed to be involved. Document approval, as I said, re-writes, improving on validation checks, and of course the technology improves as time goes on. So between 2010 and 2014 there were some pretty good jumps with the tools that you can use to do validation, to do signing, and that sort of stuff. That certainly improved.

Again, manual versus automatic management. Removing the human touch. From what I understand, most of the outages that have occurred have been because of human error - so people copying and pasting wrong, or running the wrong command or missing out a command. We try and learn from that and we thank all the early adopters for going

ahead and documenting the power outages are and reasons why. I'm not saying all are from manual but there are some out there that are because of manual stuff. So automation is a good thing, where you limit the amount of manual work that has to go in and then let your application handle all the key signings and rollovers and those sorts of things.

Really, the key thing is processes and verifications. So ensuring that you have your processes really dialed-in and that you perform verification over and over again before you push your zone. So what's next for .au? From the five phases you can see there the first two we ticked off. We actually skipped over the trial for registrants. Again, because we waited there were people enquiring and we didn't feel that there was a need to have a test-bed and a trial for registrants to submit their DSs. People I'd spoken to were already using the DLV and had signed their own zones, and were really waiting on us to get to that point.

Skip past that and we've also ticked off production DS for registrants. At a check this morning, we have over three million names, and we have just under 60 that are DNSSEC signed. Our next step is to encourage validation, so for that we'll keep monitoring the take-up. We'll work with our registrars as needed, if we find… I'll touch on Jim's question before. We haven't really given too much thought about what we are going to do there in terms of incentives or if we need to do incentives. We are a bit like .nz. As Jay said, we want to let this run organically; not force registrants to sign their names if they don't want to. We'll keep an eye on this.

We are aware that there may be some issues that we will have to address with registrars on transfers, where you've got some registrars that provide DNSSEC services and then others that don't, so that may be a challenge for us at some point. So Geoff just presented a whole bunch of stats, so I ripped one of his graphs there. I noticed the comment of his that in 2013… Sorry to pick on you here, Geoff, but the statement is there that, "Two per cent of Australian users appear to be using DNS and 70 per cent of them were doing it via Google." So that's substantial using Google there, and that goes to what Geoff was just saying.

In 2014 the graph shows that this actually has increased in the terms of Australians that are using DNSSEC. It's jumped to about 15, 16 per cent, and it's dropped down to about half doing that through Google. I think that's about 50 or 60 per cent. It's on the up, and I would expect that now that .au is signed that we'll see an increase in this, but again, not drastically. That's it.

RUSS MUNDY: Thank you. We're a little behind on time so I think we'll skip the questions and just head right to Xiaodong.

XIAODONG LEE: This is my first time to update the DNSSEC Department, so I'll try and give a brief introduction. I'll give a very quick review of what we've done in the past few years and then an update about the last year, and our consideration for future plans. We're similar to .sg in that we started DNSSEC testing around 2009, so after four years we've done a lot of tests with partners in China, including the carriers in China and the

registrars. We submitted the DNS record to IANA, and then it was enabled in 2013, almost at the end of this year it was introduced to the new servers. It's up to a lot of testing.

We have big concerns about the zone file and the packet size, that it increases the traffic, but actually there's not too many worries, because we measured that the zone file increasing is almost not too big. It's about seven per cent increasing for the zone file. The packet size [unclear 01:13:06] with DNSSEC, so the packet size is almost two sizes bigger than before. Next slide. I think you mentioned that there is an automated management, because we developed the system ourselves we used DNSSEC, and all of the department would be automated. We use HSM for the encryption. But now the registry is run very well, but we still have concerns if it will be stable for the next couple of years.

We have almost 11 million domains under .cn, so it's a big zone for us. The security and stability is very important for us, so we try to upgrade our Internet standard to make sure that all the operations will be stable and secure, and understand that [in a 01:14:42] document. Next slide. Last year we had the ASCII rollover [unclear] and finished the [unclear 01:15:00]the first time. Based on RFC1511 we used an automated update for DNS [anchors]. Up until now, everything's been smooth. We haven't seen big problems. Now there's not many DNSSEC queries. [unclear 01:15:28] 2005, our operating system, but it was no more applications for DNSSEC.

So if we compare the zone file and the packet size, at the end of 2013 our registrations for .cn is about nine million, but last year we increased it almost two million. Even the zone file increased; less than 2013, about

five per cent, because the [unclear 01:16:10] technology is okay, and the packet size is also lower. But why? We want to know why the zone file and the zone file size and packet size is lower than before. We didn't find the reason, but we just guessed it was because we upgraded the software, and also some of the [unclear 01:16:33] upgraded. We don't know. We didn't do more tests. Maybe Geoff has some data for that. How many servers have you upgraded in China?

So in 2013 we tested that almost 70 per cent of the servers were in the DNSSEC queries, but in 2014 there was only 50 per cent. Maybe some work on the software assume that DNSSEC queries are by default, but even in the newest version maybe you [extend 01:17:09] the DNSSEC queries by [unclear]. So we didn't know the reasons. We will test it in the future. At least it's better for the software to adjust to the queries; to send the DNSSEC queries based on user requirement, not based on the DNSSEC software. I think now that's an issue. Next slide. I've almost finished, but I'll give you some update about [CINIC 01:17:41], because we host the new [gTLD]. [CINIC] is the .cn .china ccTLD registry, but now we have [unclear 01:17:49] and .network in Chinese, and there are also another two gTLDs. There is [unclear] for a Chinese city name and the province name.

Now we use this [unclear 01:18:01] DNSSEC and also [unclear] itself, to manage the DNSSEC, because we trust the machine, instead of trusting people. Also, [CINIC] supports the data escrow and EBERO. We have one of the three EBEROs accredited by ICANN. Next slide. I'll show you some other concerns. We're worried about D-DOS attacks. We're also worried that if we deployed the DNSSEC the D-DOS attack would be disastrous for us, because the queries and packet size would be bigger

than before, and there'd be more traffic. If you use the same [panelist 01:18:48], if we have a larger packet size, it would be disastrous for us. So we upgrade our D-DOS device, because this device is designed by [CINIC] itself, so not it's ready. Maybe in the next year we'll support the [40 giga 01:19:11] [unclear], so it will be better for the DNS system and the future, maybe stop traffic.

Also, because this device is based on [IPG 01:19:25] the cost is higher. So we tried to lower the cost. We used a software solution, and also, based on our software, and we can also stop some traffic. For the zone DNS it's developed by [CINIC]. We use [BAN], and we also use other software, but some of our servers use our own software. It's almost five or six times compared to others' open-source software. Next slide. I think now we have tested the DNSSEC in the network. Maybe next time I'll update that for the next DNSSEC Workshop. But my concern is that in China [unclear 01:20:22] report. I'm not sure how many [servers] supported DNSSEC.

I mentioned that there are some queries about almost 50 per cent of the [unclear] in China that [send] the DNSSEC queries by default. But I know that so many [requests 01:20:39] in China would never enable the DNSSEC, but they'll send the DNSSEC query. It's very ridiculous. I don't know why. Maybe some of you can give answers. But the next step, seeing it now, there's only the ccTLD registries support DNSSEC, but there are so many registrars, and there's many DSs and because servers in China would never support DNSSEC, seeing them now it's trying to send some collaboration message to the carriers and the registrars to deploy DNSSEC. Up to now there's almost no DNSSEC registration, because no hackers hack the domain name.

It maybe happens five or ten times every year, so we don't need the DNSSEC, but up until now there's no cases of it. Maybe someone can bring more cases into the next DNSSEC Workshop. How many hackers use this method to stop the website, or change the website? So it would be better if DNSSEC to be deployed. My opinion. That's it. One minute.

RUSS MUNDY: Thank you Xiaodong. We have time for just a couple of quick questions. We're a little bit over schedule and we do have someone with us who has a very tight schedule. I'll make sure we give him time to get up here too. Questions for Xiaodong or the other Panelists? Yes, Geoff?

GEOFF HUSTON: I have a comment in response what you're seeing inside China, because everybody is seeing this. The use of BIND for recursive resolvers is not quite complete, but there is a lot of BIND, and for many years now BIND has been turning on, by default, the "[ED-NEX 0]" option, and the "DNSSEC okay" option, even though it does not validate. So as soon as you field a signed zone, BIND recursive resolvers will ask for the signatures all the time, even though they're not validating. So what you find is as soon as you sign a zone, the queries coming in from these recursive resolvers get the signature data back. So whether they're validating or not, 87 per cent of the world do this already. That's why you're not seeing much change.

What I am seeing inside china - and it's difficult in China because of the way I measure - there are a very small number of providers who have a fair deal of validation going on, but predominantly that's because they

seem to be sending their DNS to Google's public DNS. There is very little in China of native mode validation, of resolvers that do it themselves, that I can see. China is one of those places where it's difficult for me to look from the outside-in. I think you might find a subtly different picture from the outside looking in.

XIAODONG LEE: Yes. If we look at the [unclear 01:23:50] query logs, about 50 per cent is from the Google DNS.

RUSS MUNDY: Okay, I'd like to thank all of our Panelists and ask if we could have a change of our Panelists for the ten-year anniversary panel.

DAN YORK: Whilst those Panelists are getting set up, I'll mention too that we'll also be looking for Panelists to participate in this Regional Panel in BA, so if you're in that region of the world we'd be looking forward to having you participate in this, and we'd encourage you to start thinking about what you might be able to say in that session coming up there.

RUSS MUNDY: Since we're slightly behind on our schedule, we have with us today for this Panel our celebration of ten years of DNSSEC Workshops, and the people up here as part of this Panel participated in the first Workshop. I'll have a few remarks. I'll introduce the folks here with us. [unclear 01:25:48] was the first official DNSSEC Workshop, from what we can see. There were DNSSEC meetings before, but that was really where we

acquired the tag of DNSSEC Workshop. DNSSEC Deployment Initiative was the primary driver; the organizer, that tied to the ICANN organization as it's always been - is the Security, Stability and Advisory Committee. You can see the counts; there've been quite a few Workshops in quite a few countries.

A few years ago we started the DNSSEC for Everybody Session, which was oriented towards folks who have very little background and knowledge about what DNSSEC was, because this was certainly one of the feedbacks we were getting from our Workshops on Wednesdays. People would wander in the door and their eyes would glaze over if they didn't already know everything there was to know about DNSSEC. So that was the reason for the creation of the DNSSEC for Everybody Session, that's not normally held on Monday afternoon. We can see the list of organizations that have participated. It's quite long. I have to give due credit to Julie Hedlund for collecting and organizing this material, because it's amazing.

In addition to really keeping us on the Organizing Committee organized, Julie was very effective at pulling all this material together so we can see just how broad it's been. The Program from that first Workshop is what's up there. You can see that there are a pretty fair turnout of those that were at the first one, that we managed to get here today. We'll be asking the folks on the Panel to give their thoughts and recollections of not just the first one but other Workshops over the years. Of this list, Bill Manning was not able to joint us; he had a last-minute problem where he wasn't able to come, but the rest of the folks are here. Next.

The topics have expanded also very substantially over the years. The first Workshop was much shorter than what we have now, and obviously the topics were much more constrained. I won't read them all, but the slides are available on today's Workshop Meeting entry, so everybody can see all the slides from today's presentations. You can see, as we go through the expansion of the topics, in some ways you can see some of the maturing of the technology that's been talked about today - how it's gone from many software-based signing to now much more a heavier reliance on the hardware-based signing and the creation of DANE. DANE has been created in the time frame after the DNSSEC Workshop started.

It didn't even exist at the time we started the DNSSEC Workshop, so it has been brought in, brought to fruition, and is now gaining even more wide use throughout the community. The set of topics is spreading. The sponsors and implementers Dan recognized earlier, and I also want to include them here. In addition to the current ones we've had several other sponsors over the years, and the implementer gatherings have also been very broadly sponsored by the various activities. How will they go forward in the future and what needs to change? We've taken some surveys. We'll probably try to do some more. We want to encourage more demonstrations of DNSSEC-related things. The third bullet; I think many people here in the room are aware that there's challenges of various sorts with respect to DNSSEC and registrars.

I see we have some new participants from the registrar world here today; that although the people may not be new, their organizations they're with may be. Greater emphasis on DANE and then the enterprise - lots of work and focus over time on the enterprise, but honestly, very limited progress there, so lots to do. More regional

participation. So we want to also expand beyond the traditional folks we've had. I want to open this up to the other Panelists, since I've had a chance to talk first. To my far left is Steve Crocker, who along with myself was really the key organizer at the [unclear 01:31:29] Workshop, along with Alison Minken, who was not able to make join us today.

STEVE CROCKER: Thank you Russ. It's an incredible pleasure to be here. Russ and I have been working together for quite a long time. Behind the scenes we've had the benefit of some directed funding from the US Government, specifically to foster the development of DNSSEC, and so we've been able to put a lot of energy into this. I think that's been helpful. Russ covered almost everything. There are one or two things I can fill in around the edges. As most of you know, I Chaired SSAC from its inception until several years ago, and in the early days - and SSAC started in 2002 - one of the persisting questions was on what we should focus on attention. DNSSEC was one of the topics we put energy into.

There were DNSSEC presentations and discussions prior to this series of Workshops, and in Tunisia in 2003, I think, Bruce Tonkin took me aside. Bruce was Chair of the gNSO Council at the time, a Member of SSAC, and he works for one of the large registrars, Melbourne IT, and is a great technical guy. He took me aside towards the end of the week, after we'd had meetings, and said, "This is a weak effort, and in order to really make DNSSEC go it needs to be split off and pushed as a separate thing." I took his advice to heart and fortunately a number of things came together. The funding that I talked about became available, which was very helpful on the one hand. He said, "We should start a separate track

outside of the regular SSAC Meetings and create a parallel track, under the egis of SSAC but get it launched on its own."

That's what kicked off these series of meetings, and the results have been spectacular - absolutely amazing. We've had the benefit of the extraordinary hand of Julie keeping everything on schedule and organized. We formed a Program Committee that works harder than you might realize, putting each of these sessions together. Another fortunate thing that happened along the way is that the Program Committee, working each session after another, actually started to get a little bit stale, a little bit tired. Somebody came up to us and said, "You should do the following," and so we said, "You're right, and you are hereby on the Program Committee." That was Simon?

Yes, and he jumped right in. We also realized the larger lesson from that, which is that it was important to refresh and revitalize the Program Committee. So over a period of time we've had increase in participation, and we've made a point also on focusing on each region to the best that we can. It was mentioned we're going to be in BA and we should have participation. We've tried to do the same thing at the Program Committee level, of bringing someone onto the Program Committee from the region so that we could reach out. That's the behind the scenes stuff that's helped make this go. None of that would make any difference if it wasn't for the enormous participation and enthusiasm, and intellectual contributions, and just honest, hard labor on everybody's part to move this forward.

The work here has been in conjunction with the work in other forms around the world. The IETF has put a lot of work into DNSSEC, from the

original specifications to evolution, to the creation of DANE and so forth. Also, as Russ mentioned, for all the progress that we've made, which is very substantial, there is still quite some distance to go. It's hard to describe where you are when you're in the middle of a long effort. It's easy to describe the beginning and it's easy to describe the end - it's all black and white - and in the grey areas where we are you can have whatever description you like - it's terrible, it's wonderful, we've made terrible progress or wonderful progress, and so forth.

I take some encouragement, but also find it sobering that it continues to be a long march. In any case, I've blabbered on long enough. It's truly heart-warming to see the amount of energy and enthusiasm, and the raw talent that's represented here. This is a very, very smart group of people.

RUSS MUNDY: Thank you Steve.

RAM MOHAN: Thank you Russ. Thanks for bringing me back on, ten years out. This is one of those classic takes-ten-years-for-an-overnight-success type of stories, right? When we first came on, I was also a Member of the SSAC, and so was deeply involved in the effort to root DNSSEC and to first define the technology well, and then work on implementation of the technology. That time, the biggest issues that I recall were about what, in hindsight, you could quite easily characterize as FUD, right? "If you deploy DNSSEC the CPU utilization on your networks will be

tremendously high, the memory footprint will increase dramatically, you will create a new vector for attacks," and things like that.

There was really a lack of practical implementation and examples to prove or disprove these points. So we had a bunch of opinionated experts come in and make their points of view, and be absolutely convinced that that was the right point of view. For me it was refreshing to be able to come in and start to get some reference implementations going, and be able to present data on what it takes to actually start implementing DNSSEC. So that's one interesting thing that's changed over time, in the sense that there are many more implementations. I must say that I still hear echoes of the original concerns. I no longer would call them FUD but it's now converted from FUD into just pure apathy. Nobody cares, nobody needs it, why do you really want to do this?

Therefore it's really a terrific move that the DNSSEC Workshops have gone from simply disseminating "What is DNSSEC?" to "Why DNSSEC?" and how can you actually do something good with it?" I also recall in the early workshops a bit part of what I was doing, and many of the other Panelists was doing was to clearly distinguish what DNSSEC woudn't do. It didn't guarantee that you would suddenly have a more secure Internet. It didn't guarantee that there was validation; things like that. So there was quite a bit more focus on that, and over the years it's been very good to watch the evolution from focusing on clarifying the technical underpinnings of this technology to moving quite a bit more to the business value or the practical value of implementing DNSSEC.

So that's been very good. In 2008 Afillias began a significant program to sign .org and in many ways that was a seminal event. it was the largest TLD, at the time, to be signed. I just wanted to share a bit of data on a few trends. I'm going to just look at from January 2014 to February 2015. Let me just share the percentage of signed delegations, across a few TLDs, that we are responsible for and manage. If you look at .org, which is far and away the largest zone, in January 2014 about 0.3 per cent of the zone had signed delegations. We're at about 0.44 per cent, so it's inching up in a steady way.

.info was at 0.0 in January of 2014, and it's about 0.2 per cent right now. .in, India, the country code, was at 0.01 per cent in 2014 and 0.02 per cent in 2015. 100 per cent growth! Interestingly, .me, Montenegro, was at 0.25 per cent in January of 2015, and it's about 0.43 per cent now. It's almost the same in percentage size as .org, which is interesting. To underline, be careful, about percentages, .post has gone from 90 per cent in January of 2014 to 95 per cent in February - 38 domain names in .post. [laughter]

RUSS MUNDY: Okay, thank you very much Ram.

KAZUNORI FUJIWARA: I'm Kazunori Fujiwara from JPRS. Thanks for inviting me here. I was in the first Workshop, but I didn't attend India. I did the DNSSEC at the DNSSEC Summit in February 2005, and some people are interested. My processes [unclear 01:43:10] attended the first Workshop [unclear], and in [Birimani] a type of experiment. I'm happy [unclear] contributed

[unclear] DNSSEC. After then, .jp TLD implemented DNSSEC and now I'm [unclear 01:43:33] the effect of DNSSEC and considering how to improve the DNS on DNSSEC.

RUSS MUNDY: Thank you. We have, on our Panel, a couple of our distinguished Members on the Panel are also Members of the Board, and they have other commitments, so I think they have to slip out here shortly. Let's thank them for giving us their time. [applause]

STEVE CROCKER: I apologize - we're double-booked here. It's a pleasure to see you. The classical thing to say is "carry on" and I mean that not just in respect of this meeting of course, but carry on with the great work that's going on here. This is one of the efforts that has the most substance and the least politics of all the things going on around here, and it helps keep us grounded. Thank you.

RUSS MUNDY: Thank you Steve. [applause]

DAN YORK: I think we also want to just say again a thanks to Steve in particular for the support you've given us to continue this; both at your level within ICANN, but also through Shinkuro and all the efforts you've done over the years to help provide the back-end to make all this happen. So thank you very much for all you've done over this time.

RUSS MUNDY: Frederico?

FREDERICO NEVES: I'm Frederico Neves. I work for the Brazilian registry, and I was at this first Workshop in [unclear 01:45:12] in 2005, after being a while at the SIC. It was quite a journey, definitely. I'd like to make a comment regarding Steve saying that it was not that political in this arena. That's not true. We had quite large political fights in the IETF arena. Jim definitely knows here that we had a fight in 2001 because of [opting in 01:45:47] and then in the end we had to put this kind of [cover] as DNSSEC [3] with opt-out, and then we finally got to sign large zones in 2009. Definitely the Workshops helped a lot, keeping the subject still in the spot - especially in the ICANN Meetings, and for the people that normally approve budgets and letters continue to improve technology.

As I said, it was quite a journey, and we learn a lot of things. I remember Steve and Russ in the ICANN San Paulo 2006 kind of hijacking the event network. You remember that, Russ?

RUSS MUNDY: Actually, yes I do. That was the story I was going to relate at the end if no one else had raised it, and I wasn't actually going to say which Meeting it was at.

FREDERICO NEVES: I think that was November 2006. So that's it.

RUSS MUNDY: Thank you Frederico. Let me just add a little bit more to that particular episode. At the very first Workshop there was a hijacked demo provided by Bill Manning, and that really helped get the attention of people. So afterwards we would do, at each of the Workshops for several years, a demonstration of DNS hijack. But it was carefully orchestrated so that it stayed within the DNSSEC Workshop room itself. But that particular meeting we had actually a miscommunications in terms of the setup practice between myself and the ICANN person, and the support folks in San Paulo. It was Steve Contain we were coordinating with at that point, so we said, "We can do it, we're fine." But we got to the meeting room the next day and the folks that were providing the local support said, "You're all set, everything's fine."

So in fact, we just went on and did the normal hijack, thinking that it was just in the room, and it did. We did hijack DNS within the room, but as Frederico said, we also hijacked the entirety of the rest of the meeting for about five minutes, so everything was going to my laptop for every DNS query. That's actually my most memorable event of the humorous nature of these. But I'd very much like to extend what Steve said: thank you everybody for all of your hard work in helping bring these together for all the presentations, all the sponsorship. There's still a lot of work to do, so let's keep working on it, because we've got more meetings coming and more Workshops on the way.

Does anybody else want to make a comment or recollection to some of the other Workshops? Okay, well, thank you. We now have a coffee break for ten minutes. Thank you. See you back shortly.

JULIE HEDLUND: Thanks everyone. We are starting. Please do take a seat at the table, where we want everyone to be. We'll ask our next speaker to come forward - Akinori Maemura. He will be doing a presentation on DNSSEC for reverse DNS. He is from JPNIC. Please take a seat and we'll be starting shortly.

AKINORI MAEMURA: Thank you very much everyone. My name is Akinori Maemura. I'm working for JPNIC, Japan Network Information Centre. In the ICANN arena the acronym NIC usually means a ccTLD manager, but in the case of JPNIC it's a bit different. JPNIC is doing the IP address management at the national level under the APNIC, which covers the Asia Pacific region in terms of the IP address management. This time I'll make some brief presentation regarding the DNSSEC for the reverse DNS. I hope it's informative enough for you.

Today's Agenda looks like that: the current status of reverse DNS, DNS cache poisoning in the case of the reverse DNS. That will be my major point of this presentation, breaking the trust chain. Next slide please. JPNIC has its own program to deploy the DNSSEC in the service of the reverse DNS. As you know, all RIRs have already deployed DNSSEC in their reverse DNSSEC service. It's mandatory, because if the RIRs can't do the service of the reverse DNS no one can enjoy the DNSSEC for the reverse DNS. So regional Internet RIR are quote obvious. They must deploy the DNSSEC. On the other end, at the ISP level, they are really reluctant to deploy the DNSSEC for the reverse DNS, because it costs. It's a huge cost.

So I've been in discussion with ISPs in Japan about there being a huge [unclear 02:08:44] of being reluctant on the ISP level to deploy the DNSSEC for the reverse DNS. So the JPNIC, between APNIC and the ISP, it's located in the middle. So we're not in the situation where we must deploy the DNSSEC, but we should, maybe, deploy the DNSSEC. So it's really hard for us to justify the investment to the DNSSEC deployment in our reverse DNSSEC service. Then we did a survey for the service providers in Japan. This slide shows that. The survey target is the service [unclear 02:07:45] for the network, email, and IP address reputation service features the [unclear 02:07:52] the safety and the [cleanness 02:07:58] of the IP addresses in case of the trade/transfer kind of thing.

The cloud service, data center service, and the security service operators, we try to reach out to 14 respondents, and out of that we had response from 11. We asked about several points; the use case of the reverse DNS and the importance of the usage of the reverse DNS, and the demand for the reverse DNS service, and the degree of dependence of the service on reverse DNS and other comments. Next slide please. We found a very good response from our respondent; that's showed us they actually quite depend on the reverse DNS service. Why we put so much importance on the reverse DNS is quite [natural 02:09:18] because sometimes they doubt they need the reverse DNS. "You don't use that reverse DNS? Why are you using that?"

In that situation, the same situation applied to the reverse DNS in the IPV6. "Why do we need to use the reverse zone in case of the IPv6?" It's too [volatile 02:09:46], for example, and then the same applied to the DNSSEC, so we made a start point to know how important the DNS

service is itself, and then if we can identify that then we can argue the importance of the DNSSEC in the reverse DNS. Actually, the use case of the reverse DNS reaches out in several fields. The most significant thing is the validation of sending the email. The JP server usually validates the recipient by reverse DNS. If the reverse DNS response was not consistent with the name resolution, it's not to be validated. So that's the most significant thing.

We found that in many operators, they refer the reverse DNS resolution for their analysis on the [unclear 02:11:11] of the services. For example, there are some malicious operations in the service, and they need to identify who it is. In that case, it's not really an automatic process, but still the operators need and rely on the information of each [unclear 02:11:37] by the reverse DNS. Almost all respondents recognized the degree of dependence is high, that they cannot do their services without the reverse DNS. So we found that very helpful for us; to argue the importance of the DNSSEC in the reverse DNS.

Next slide please. They are the most visible cases where the reverse DNS is used and important. So in case of the Google and [unclear 02:12:27] apps, they divided the recipients by the reverse DNS, of course. If the DNS resolution failed they can send or receive the messages. Amazon supports the [PTL 02:12:39] record [restoration] and so do the Microsoft and [Azul] cloud. Many operators depend on the reverse DNS for the service provision and they need a stable and continuous provision of the reverse DNS. Next please. This is a summary for your information. I think we are fortunate. This is a totally different topic from the DNSSEC, but it just shows that there's some activity on the [unclear 02:13:19] delegation.

Now that JPNIC is doing the notification of the [unclear] delegation to the registrant, if the notified registrant doesn't take action then the delegation [unclear 02:!3:43] is to be taken down. So it's actually benefitting significant improvement in [land 02:13:49] delegation. Then the operator needs to be mindful that there's no [land] delegation for the normal service. I think that benefits in a consciousness; it keeps the operators' consciousness high in the reverse DNS services. This is not only for the reverse DNS, but DNS itself - explaining cache poisoning. This is well shared with a lot of people, so I'll skip this bit.

The cache poisoning and sending the false data to a cached DNS server, and then it's possible for the offender to be malicious on the cached server and then override and pollute the DNS data. Those users who reserve the DNS by that cached server will be informed with counterfeit data, that it will introduce some wrong behavior of the network. We have some quite epic results of the cache poisoning. In 2008 we had quite an efficient method to attack. If it's known as the Kaminsky attack then it's a huge problem and we needed to take action on that. In 2014 we had the more efficient attack method, which is really similar to the Kaminsky's method, which is attacking on the [unclear 02:16:14] record in the same manner.

Then the misinformation in this record is directing people to the wrong zone file, and the zone file is a lot of fakes - so that's a big problem. The risk of cache poisoning has been significantly increased these days. The risk of the cache poisoning is as I said increased, but especially in the case of the reverse DNS. As I said, if the reverse DNS is utilized for SMTP and sending email then it will introduce the wrong behavior in email services. In cooperation with the names and numbers resolution the

reverse DNS has the bigger zone file than the name to number resolutions. If the zone file at the cache poisons, the impact is huge. Moreover, reverse DNS serves as well for the IPv6, and then the reverse zone is huge, then it will result in a huge problem if it's poisoned.

A benefit of DNSSEC is quite apparent. DNSSEC will benefit to enable the validation of the zone file content, so the poisoned data will be failed in the validation by DNSSEC. From now on, I will explain some problems and the solutions at the [unclear 02:18:423] level. It is of the view of IP address distribution that IANA administer the entire IP address as well as the name space and the protocol parameter. So IANA holds the root registry of IP addresses. But IP addresses are distributed by the five Internet registries and those five are measured and the main responsibility is to manage, administer and distribute IP addresses. Then usually the [LIR 02:19:31] featuring ISPs are the members of the RIRs. That's the usual thing.

Then JPNIC has some statistics on DNSSEC records in the reverse DNS. APNIC, RIPE NCC and ARIN, they're the registries of the Asia Pacific region, European region and the North American region, respectively. They have the stats on the FTP side and they are updated daily. You can find in [unclear 02:20:20] record there are the stats out of that zone to say, for example, in the 203 [unclear] zone consists of 74 DS records out of that zone. So that's really convenient for us to know; the overview of the deployment of DNSSEC. Then LACNIC and AFRINIC there's no such data, but we ask them for that data in cooperation with APNIC. So this is the kind of situation of the deployment of the DNSSEC in the reverse DNS.

In the case of APNIC the number of zones that are DNSSEC enabled - that means that zone itself has a DS record - counts up to 405,000. So it represents that in the APNIC region the DNSSEC is quite ready for the ISPs and end users. Out of the 400 zones that are DNSSEC-enabled, the number of the DS record is counted at 184. It can be interpreted as a very small number - maybe it's a usual interpretation - but for the APNIC engineer it's a huge number, they say. That means several years ago, when APNIC enabled DNSSEC, there were really few DS records in their zones. Finally, the DS records on our zones finally exceeded 100 and now we have 184.

RIPE region is quite deployed - over 1,000 DS records. The ARIN has 457, so it's a situation in the reverse DNS in terms of the DNSSEC deployment. As I said at the beginning, the National Internet Registry, like JPNIC, which serves the IP address distribution and management at country level, has its own program. So APNIC has already enabled DNSSEC in their reverse DNSSEC services, but the NIRs under APNIC, including the JPNIC for Japan, CINIC for China, are not able to provide a DNSSEC service to their own NIRs and end users. The NIR needs to equip the DNSSEC function for their own registry. There are two things we need to do. One is to enable their registry database system to allow the DNS register in their database. Then that database is near to the APNIC database and they can provide a DNSSEC service on the reverse DNS.

That is one point. Another point is that in the case of JPNIC we have our own delegation from the APNIC, so we have our own [unclear 02:24:42] block, so in that case we need to deploy the DNSSEC functionality to our own DNS service. That's another problem. IPv6 has a quite similar nature, by the way, [laughter] and the DNS costs. So we actually take a

hard time to justify that. This illustrates what I mentioned. IANA and APNIC have the trust chain between them, but there is no trust chain between APNIC and JPNIC. It breaks the trust chain from IANA to end user. That's a problem. Then we finally determined, as an organization, to deploy the DNSSEC in our reverse DNS service. In the near future, in the APNIC area, we will construct the new trust chain between APNIC and JPNIC when JPNIC will emable the restoration of the DS record to our ISPs and end users. Then the ISPs and end user under JPNIC IP address management will enjoy the restoration of the DS record.

So our deployment plan is we'll be ready in 2015 and we will start that DS record restoration in October this year. APNIC started that DS record restoration several years ago, so we are later than that, but I hope it's not too late for our customers, ISPs and end users. Maybe that's all for my presentation. I'm not a guy who developed this topic, but I have my author online to help me, so please ask me questions.

JULIE HEDLUND: Thank you very much. Let's please open it up for questions.

MARK: Actually, this is more [unclear 02:27:31]. If we go back a few slides, where you talked about the various regional registries in terms of their DNSSEC capability, there's a number of DS records and that sort of thing. AFRINIC currently, I believe, does support DNSSEC. LACNIC does not. I notice on the project plan that their zones are publicly available and they all follow the same format, but you're more than welcome to take a look at that, and if so I'll show you the URLs a little bit later. So four of

the five regions do have DNSSEC on the reverse trees right now, so it's really good news.

AKINORI MAEMURA: Thank you very much Mark.

DAN YORK: Mark, while you're there, looking at what's been presented here, any thoughts that you guys have had in ARIN as far as around issues with signing the zones, or anything there?

MARK: That's a good question. One of the things that we've done most recently is we've tried to make our updates in real-time, in the preparation of DANE, and if there's anything that we can use to quickly fix things if necessary. We've implemented some middle-ware between to actually solidify the way that we were dealing with zone signing, and it's worked out really well. It was a really hard project to put together; making sure it was right all the time, but it's been in use now for about five months. We've been having DNSSEC going now for about six years. It's very important in ARIN. It's one of the most important things we do.

JULIE HEDLUND: Thanks Mark. Other questions? Russ?

RUSS MUNDY: Yes. Early on in the presentation you mentioned there was a very substantial cost. Could you describe a little bit what is driving that cost

and what some of the relationships to other things, such as your ongoing normal upgrade cycle of some of your computing environment and so forth? Just to give a little more detail, feel, as to what the cost is and what the drivers are?

AKINORI MAEMURA: Right. The cost involved is mainly in the upgrade of the DNS server facility, and then equipping the new process to make sure the key rolls over normally, because we know that there was a quite serious problem before in the name to number resolution, at the country level for example. Our pre-requisite to start the DNSSEC on the reverse DNS service was to secure the operations; the stable and normal operations without any risk or with little risk. That's the cost.

RUSS MUNDY: One quick follow-up - and you expect your customers to have similar cost impacts then, as far as further delegation down?

AKINORI MAEMURA: It depends on the size of the ISPs. The big ISP needs to reinforce their operation and the facility to provide DNSSEC, and the small ISP is not really serious, but still, largely, DNSSEC costs in operation have very skillful engineers for the DNSSEC. That's cost. So we don't expect a very fantastic huge number of the DS records registered under our restoration - but still, if we have a very small number of people who need the DS record restoration, that is a sufficient reason for us to deploy the DNSSEC. That's our position.

RUSS MUNDY: As you're dealing with the ISPs in the reverse zone space and DNSSEC, do you see that there might be an opportunity to also encourage the ISPs that decide to sign the reverse zones to sign their forward zones also, at the same time?

AKINORI MAEMURA: At the same time, yes. We fortunately have Mark here and he can share the situation now. Do you have any idea, Mark?

MARK: That's a good question. I've never looked to see whether or not the forwards have been signed for the ISPs as well. That's a good thing to actually look at and see what they're doing. We signed our forward, but admittedly it went in after we signed our reverse, so it's just one of the things you have to be very careful of; making sure you don't make a mistake, right? You don't want to go off-air. So we wanted to make sure we didn't go off-air on our forward at all, so that's why we took a little bit more time and care, to make sure that didn't happen.

JULIE HEDLUND: We're getting short on time. Did you have a short…

MARK: Yes, I just wanted to say thank you for presenting this. It's interesting, as I looked at your presentation, I liked the fact that you presented why we should care about the reverse zones in the cloud providers. That's

something I think we, as a community, don't talk enough about, as far as what the role is of the reverse zone that people are using for this validation. So thank you for highlighting that. I think we, as a community, need to talk about that more, because it is a way, especially when you think about how it's being used to authenticate and connect into those cloud services. So thank you.

AKINORI MAEMURA: Thank you very much. Actually, JPNIC has had one or two years discussing this; and that's my big pleasure, to share this. Thank you very much for the opportunity.

JULIE HEDLUND: Thank you too. [applause] I want to move onto the next Item. We have a presentation from Wes Hardaker at Parsons on DNS and DNSSEC management and monitoring changes required during a transition to DNSSEC. So I'm going to go ahead and turn things over to you, Wes.

WES HARDAKER: I'm going to do a bit of a departure from some of my normal presentaiotns I've done the past year, because my goal for today is not to give you all the answers and all the tools that you need, but rather to make you start thinking. This is more brainstorming, and please feel free to jump in with things you think about as I progress, with your own comments. If we don't finish the slides because we get a good discussion that's actually better. Feel free to jump in when you have thoughts. What I'm going to talk about in my first presentation today is what's required for managing and monitoring your zone, as you switch

from DNS to DNSSEC - of if you're already there, what things you may be missing that you might want to go out and look at.

I'm going to go over a few things. First off we'll discuss what business model changes you might need to think about and make, and with that comes relationship requirements. You probably have relationships with your parents, regardless of who you are - unless you're the root - and you certainly have relationships with any children you might have, and what does that take in order to transition to DNSSEC - what additional things you have to think about. Then finally there's timeline changes of what has to change as you progress over the years, and how many additional steps you have to add over the course of that time period.

First off, the business model changes. I think most people have a good sense of what needs to be done in normal DNS when you're trying to converse with your parent. With normal DNS you purchase your domain, you win an auction, you register under some parent somehow - whether you're a TLD or somebody inside a .com, it doesn't matter. Upon doing that you have to use recent DNS software, you stand things up, you attach to your parent, and there's some relationship there. With a TLD you're attaching to ICANN/IANA. With an enterprise you're probably going through a registrar and registry. Then you have to use that interface to update your NS&A glue records, for example.

So what does DNSSEC add? That's all known. Most people know how to do that right now, otherwise you wouldn't be in this room. DNSSEC adds a few things. You need to add one more thing in order to update to your parent. Not only do you have to update your NS&A and quadi 02:37:41] records when you're signing up, but you have to add a DS record to your

key. On the diagram on the right you'll see there's now a little green bubble that shows that the DS record has to be pushed up as well. The parent and their interface must be DNSSEC-compliant, which actually limits your relationship status. You have to get to a relationship with a parent that actually can do DNSSEC, because if they can't, that's where the business model change comes in - you're reducing slightly the number of people that you can possibly consider as your parent.

So as you're going forward and you're thinking about future zones, you have to make sure you're picking a registrar that will allow you to publish that data. It'll affect your buying decision. With DNS, the relationship you end up building with your parent, you have to constantly synchronize, over the course of years, your name server records and the glue records for those name servers. You have to add NS&A glue, and if anything changes over the course of a long period of time, you have to go back and update it. So normally, we think, "Okay, I have to go and add a new machine," and any time you think about changing hardware the human brain is pretty good at knowing, "I probably ought to go and update other stuff too."

So we're very good about that, because it's a one-time change and our human brains are very good at trying to brainstorm all the things we have to think during a one-time change. That's the advantage of DNS, because you're only doing it occasionally. You're adding NS records and A records just every once in a while, and you're probably fairly sufficient. Unfortunately it turns out, if you go and look, there's a whole lot of people who do not synchronize their NS and glue records quite consistently. We're going to talk about testing here in a second. The IETF's [ceasing 02:39:34] draft is one that's just coming out and helps

you automate this. Adoption of it is yet to be determined, and all [the fur is 02:39:41] around and is looking for other ways to push data up as well.

So, what does DNSSEC add to this equation? What do you have to do with your parent on an ongoing basis when you are coordinating with that? Again, you have to maintain your DS records - so any time you are needing to change your keys, your parent has to know about it. Before, when you had NS&A records that were possibly slightly out of synch, it might be okay as long as one at least synched up, because as long as the parent had one correct record, everything was okay. With DNSSEC you have to make sure that there's at least one DS record that points down, and if one of them doesn't you'll break. So if you roll your key and you forget to talk to your parent you will become invalid, and that obviously is a much worse case than having one out of two of your NS records be usable.

So when you roll your keys, make sure you tell your parent. Here's the thing before; what I was saying is that as humans we are very used to knowing when we have to deploy a new box. We think about those changes that we have to make. When we get to periodic things and we're doing things on a regular basis it becomes very easy to forget stats. So I strongly suggest you write things down as the order of things that you have to do every time you're going to make a major change, like rolling a key. In my next talk we'll talk a lot more about writing things down. Make sure that you have a to-do list, because people do forget things. The IETF's recent RFC7344 CDS again might help automate this, if you want to read that and find some software that implements it.

Let's talk some more about relationship tests. How are you going to test that everything's going correctly? It's nice to know that you need to do something, but how are you going to notice if you fail to do something or if your parent fails in some process? So what tools are you going to use to make sure that you and your parent are properly synchronized? This is true not just for DNSSEC but it's true for DNS. How do you know that your parent and your zones all align? Are you using tools? Are you using software? Are you using self-written scripts? Are you using a monitoring service? We happen to run one called DNS Sentinel that allows you to detect these kinds of problems. How often are you going to monitor it? Are you going to notice within five minutes?

Are you only going to run this once a quarter? And will you test your infrastructure to make sure everything aligns? With DNSSEC, as I said, it becomes more important because you have to monitor that DS record too. You have to know that the cryptographic pointers are working out as well. So does your DNS monitoring service or tool support it? If it doesn't, you may need to find additional services or buy some additional software to make sure that you can test that infrastructure. Here's an example. This is an example DS record checking tool. It's a free tool called "getdns", and it's in the DNSSEC tools package. If you look, the first set of records says, "These are DS records generated by querying example.com for keys and then generating DS records, and the bottom set of records are the records that were pulled from the parent of example.com, in this case .com. Now, clearly you can see that there's four and two, so something doesn't line up. What's happened here?

If we paste in the entire outputs of the "getdns" script you'll find that it actually lists the errors for you, and it shows you that two of the records

are not published in the parent - so the child has keys that there are no pointers to, and that green circle at the top shows those two keys. Here's the other interesting thing: if you were coming and looking at this data fresh, regardless of whether it's your zone or someone else's, there actually no way to tell if those two DS records at the top, generated from keys, are from new keys or old keys. Are those DS records from a key that's going away, or from a key that's just gotten certed and hasn't been synchronized with the parent? There's actually no way to know.

So timeline thinking becomes very important, and if you just generated keys and you put them off on a box and you were signing with them for a while and forgot which was the old one and which one was the new one, you're going to be in a world of trouble later, trying to figure out, "Which one should I be using in the future?" So make sure you have some sort of history notion and that your testing infrastructure has an audit log, like our DNSSEC product that allows you to determine over time you can know exactly when your key rolled, when new DS records got certed, when an old one was removed and when the old key was removed after that. So time becomes very important in DNSSEC, when it was slightly less so in DNS.

Again, testing. Does your parent near your real data in DNS? How often do you check? What about DNSSEC? Is your parent's published DS record for you correct, and how often do you check that? You have to have at least one that matches. Then are you testing end-to-end validation? Are you actually testing all the way from the root, all the way down to your www record or your mail record or whatever, end-to-end? Are you verifying that the validation succeeds from top to bottom? Because you don't care just about your parent - in a lot of cases you

probably care about the root. What if the root messes up? This can happen on the DNS side and the DNSSEC side. Olafur, go ahead.

OLAFUR GUDMUNDSSON: The question is: DNSViz is doing a wonderful job of doing this graphically. Is there anything they're not doing?

WES HARDAKER: DNSViz does some wonderful things if you want to go and type it in manually and do it occasionally. DNSViz also now has a command line tool that lets you also do that as well. I have not checked the complete list myself. I wonder if you have personally? Are they checking for everything? They are a fantastic diagnosis tool that shows great circles and lines in terms of are things validating correctly? There's other software that does it. DNSViz is one you can run perfectly. As I mentioned, we have a tool that does stuff. You could run a web browser with a validation plugin to see if you're validating all the way from the top to the bottom. There are a lot of timing related stuff that's a lot harder. DNSViz doesn't do that timeline over a month, it does, "Here's a single snapshot when you push the button."

There's another one. [Accelerance] has one that they allow occasional free monitoring, called DNS Sherlock that actually does additional stuff too, but I haven't compared the feature set. Have you done any comparison of that?

OLAFUR GUDMUNDSSON: I found that I was looking at some failure mode and DNSViz was not telling me exactly what the error was that was happening on that site, but having that as a call-out, once your script fails validation, is what I've taught my support people now to use.

WES HARDAKER: Yes, and a lot of times, knowing that there's an error and determining what the error is are two very different questions. There are a lot of things that will tell you "it's broken" but not how to fix it or what's broken. Did you have a question too?

DAVID LIMES: Yes. David [Limes 02:47:13] from [unclear]. I just wanted to mention that some operators, such as [unclear], but I believe others are doing it too, continually monitor their customer zones and look for any errors including all of a sudden DNSSEC validation is failing.

WES HARDAKER: That is an excellent point; that a lot of parents offer monitoring as a service. There's a whole lot of registrars that will do some level of monitoring as well. There are different feature sets there. A good comparison chart with checks and boxes would be a wonderful thing for somebody to put together. Personally, I haven't done it. Any more questions on where we are today? All right, I'll go on then.

What about with your children? What if you are a parent? What if you are a TLD? What if you're a university with sub-departments? Being a parent is clearly the inverse of being a child, but there are a couple of

extra points I want to make sure you consider. First off, with DNS you're likely to have some sort of API, whether it's over a webpage or email, you have some mechanism for you and your children to communicate so they can distribute new data to you - new NS&A records, perform possible transfers and then again [unclear 02:48:29] is something you could implement and offer to your children as a new tool. What about DNSSEC? DNSSEC, you again have to have some new elements to your API to allow your children to submit the right data to you.

They have to be able to add a DS record to your zone. How are you going to get that in there? How are you going to check it? How are you going to maintain it? How are you going to ensure that you're using the parameters that you like? There's a lot of debate within some parents about what they should accept. Should you let the children generate the DS record and paste into some form on a webpage? Should you get their key and generate the DS record yourself because you want to control the algorithms that are used? That's all stuff that you have to think about. I'm not going to give you the answers because there are enough opinions out there to know whatever answer I give you, half the people will disagree with me. That's okay.

And then, are you going to use CDS to offer synchronization to your children? The one really critical thing, especially if you're concerned about the business aspects of running DNSSEC, is if you do have an API and you're a registrar that children can choose from - be it whether you're a TLD; and people pick different TLDs based on their needs - if you have an API that allows your children to use DNSSEC underneath you, make sure you advertise it. It's pretty amazing how sometimes you see TLD owners that don't really advertise the fact that they're

compliant. How are you going to get that list of people out looking for registrars and TLDs that can do something? You're never going to get those customers unless you make sure the customers are aware that you're up to speed with this stuff.

Moving onto timeline changes. This is where it gets more interesting. One interesting thing about what we've learnt with DNSSEC is that there are an awful lot of people that didn't really have an interface before, especially if your children didn't change very much. They would very often just call you on the phone and say, "Could I get another address record for another name server? Please add 122.0.5," and hang up the phone and you're done. That doesn't work with DNSSEC. There's actually been a lot of parents and registrars that have added service because of DNSSEC in, to automate stuff. I think that's a fantastic end result that we probably didn't originally expect.

Some of that comes from timeline changes, So with DNS data, it's frequently static. There are addresses and mail records, and you add an A record to your zone and you add a change in MX record occasionally over time, but the integrals of time between these two bars there are often far. They're often years between adding an A record to adding an MX record later. They're not something you do very frequently. Sometimes it's automated. Sometimes you're adding A records every five minutes because you're doing round robin support, or load based record changes and things like that, but it's a system that's automated in place, and frequently you don't need to do much other than make sure it's working.

So there's a lot of generated records. DNSSEC black lists are an example of something where records are added and removed based on mail and spam checks and things like that. But again, it's automated, and people fire and forget these. Once the service is running there's often very little maintenance that needs to be done. What changes with DNSSEC? Signature records suddenly have a lifetime, whereas before there was no lifetime - TTLs are not a lifetime; that's just a refresh time. DNSSEC keys suddenly require possible periodic rotation based on your policy. So it's no longer fire and forget. You now have operational procedures that you probably need to change.

You need to make sure that if you're going to be rolling keys and if you're signing, that you do so on a periodic basis. Some people that have ben testing DNSSEC infrastructure for a long time have certainly noticed that during the winter break between the end of December and the 1st of January, there are more DNSSEC invalid zones then because operators go on vacation and they don't push the button anymore. That's not good. So there's every x period of time you have to resign, and for every y period of time, based on your policies, you need to roll your keys. I'm not going to define where x and y are. Typically, rolling keys, the process itself, takes months.

Pictorially, this is a graphical representation of what I just said. Let's take the previous things of you have A records that change and MX records that change. What do we add for DNSSEC? First off, we have to sign and republish. Every so often - and it's a periodic thing; maybe it's every two weeks, maybe it's every month, it's frequently half of your signature lifetime would be a good minimum if not more frequently than that. You have to sign in and republish. Here are a couple of interesting

points. When I edit an A record, I happened to have done it right at the time I was going to resign anyway. Note that over here when I change the MX record, any time you change data you can't just add the data, you now have to edit and resign the zone, or at least that record.

You can see there's an additional green line in here where I've resigned one extra time based on the fact that I actually changed data itself. What about rekeying events? When you go into rekeying events there are three phases, at minimum. You add a new key, you wait a while, you swap the keys, and you do these during the signing periods usually. Then at the third iteration you delete the old key. That's the minimum. A lot of times it's longer than that. So you have to think about these and plan these into your rollouts and your infrastructure. How often should you resign? As I mentioned, a good rule of thumb is you should resign at least every signature length. If your signature length for your data is a month long, you might want to resign every two weeks. If your signature length is only a week, you want to resign every couple of days.

That rule of thumb is based on the fact that people forget to push the button over winter break. You want to resign it more than that in case you do slip or in case your infrastructure fails. Then again, test and monitor your infrastructure. How do you know your restructure actually worked? If you're not validating top to bottom, if you're not checking all of those signatures, how do you know that your data hasn't gone invalid? How do you know that your infrastructure actually succeeded in resigning on the time it was? A lot of people run software and then they leave it and they expect it to always work. If it doesn't, you won't know until it breaks. That's a little late. So good software, and the DNSSEC tools project actually has some software to help you check.

There's a command line utility called Donuts that you mail yourself to make sure you don't suddenly get warnings saying your zone is about to expire. DNS Sherlock I think will do the same thing, and DNS Sentinel. What are the reasons for rolling keys in the first place? Really quickly, there's key strength. Some people like to roll keys because they believe the keys aren't strong enough, won't go into the cryptographic side, and there's a lot of disagreement there. It's good operational practice if you roll your keys every once in a while. It's more likely you're going to do it correctly when you have to do it, so rolling it every once in a while proves to yourself and reminds yourself how to go through that process.

And you get to test that parent/child relationship. If you're rolling a key, you want to make sure your parent doesn't blow it too - and they need the exercise and the practice just as much as you do. You're going to be the one to make them exercise that practice - they can't do it for you. How often you should roll your keys is very situation dependent, and there's a lot of disagreement there. Some do it once a year for their key signing key. .com I think does zone signing changes every three months. VeriSign that is - picking one at random. Rolling the key signing key annually is a good middle ground that a lot of people fall to, especially from the operational practice point of view.

But do you have a plan in place? Are you thinking about this, or did you fire and forget and your keys have been there for years? It's not that that's bad, it's just that you've got to make that decision as opposed to not making the decision. One more thing - DANE TLS records. One of the interesting things about mail in particular is you cannot really secure mail without DNSSEC. DNSSEC and DANE and SMTP marry well together because that's the only path forward for securing mail. There's already

been known instances of people that have published TLS records with certificates in DNSSEC and then upgraded their TLS record and forgot to change the DANE record in DNS and DNSSEC. That's common. Again, what are you doing to test for that?

Do you have in your documentation for when you go buy a new certificate from some certificate provider, that you also need to roll your DANE record for your mail server? Or else you'll stop getting mail the way you want, which is probably not a good thing. That's it. Again, this is brainstorming. You can tell me what I left out. That was hardly an exhaustive list. That was about the list that I could fit into the time window I had. I know there are a lot of experts in the room, besides myself. Any last comments or questions, or things you think I forgot that are important?

DANIEL EBANKS: Daniel Ebanks from the Cayman Islands. We obviously have not implemented DNSSEC for the .ky domain, so we are at ground zero. It all seems very daunting. Are there any parts of what you just talked about that we, simply from the ccTLD point of view, can ignore for now and promote the more important things, on the daunting list of stuff that we have to work on?

WES HARDAKER: That's a very good question. My advice would be in your planning stage, one of my goals for today was not to make you do everything today. One of my goals was to allow you to have a list of stuff that you can go and pick and choose from, as a menu of what has to be done early on

versus stuff that I can push off for a year - key rolling for example. You probably don't need to make those decisions today. You can put that off, as long as you make the decision. Don't let yourself go five years and then go, "That's right, I was supposed to decide on some key rolling mechanism." The things that you have to do right away: you have to make sure that you're periodically resigning your zone. You can't get away from not making that decision really fast, because you have to determine how long your signature are going to be and things like that.

I can't go through the entire list, but I can tell you the big one, the one that most people really worry about, and that is key rolling. That's something you can put off for a little bit, but don't put it off forever. Any other questions?

NAVEED: My name is Naveed. I'm from Pakistan. Just a one-liner. I want to have your opinion about how do you view the complexities that this transition has from DNS to DNSSEC? How do you see the counterpart? Would DNSSEC threaten that DNS kind of thing, when things get more dynamic in future, that we foresee? That would be even more complex, or what?

WES HARDAKER: That's an excellent question. Dynamic DNS and the ability to add and remove records quickly, there's a lot of material out there that you can go and look for. I didn't have time to put it into my slides. There are a couple of ways to go there. There's software that can help you manage that already. If you look at the TLDs that are signed, they are simply resigning very frequently. .com is resigning its SOA every few minutes - I

know, because my monitoring software, when I put in .com, it's telling me, "You've resigned! You've resigned!" It happens frequently. That's one option. The other thing is that some people, in order to get up and running, they put their dynamic stuff in a subzone that's not signed, so that it's a secure subzone in order to get their static data signed first. It gives you a step kind of approach.

In one of my early tests, I was putting stuff under .dyn under my main zone for dynamic records that I allowed to be unsigned for a while. That's a really good question. I can't answer it in full, but do go and look online for what other people have done in that regard. I think we're about out of time.

JULIE HEDLUND: For dynamic DNS you can talk to the AFNIC people. They have their own - .fr is all true dynamic DNS with inline DNSSEC signing, and they have a lot of experience on how to make it work well.

WES HARDAKER: Do monitor and test though - I reiterate that point. Thank you.

JULIE HEDLUND: Thank you very much, Wes. Please join me in thanking Wes. I just want to remind everybody, before we move ahead, there will be lunch at noon. If you haven't kept your program or you need a program, there are some programs lying around. They have a luncheon ticket on the back. You'll need that ticket. There will be an usher waiting there. I'm going to go up and be with the usher as well. The lunch is in the

Stamford Foyer, which is, if you go out into the main hall and go straight down off to the right to the end, you'll end up at lunch. We are going to try to stop on time. With that I'll move ahead to the next presentation. We have Duane Wessels from VeriSign, who is giving a presentation for Shumon Huque, and that is on DANE and application uses of DNSSEC.

DUANE WESSELS: My name is Duane. I'm here presenting on behalf of Shumon, who couldn't make it. He gave me something like 40 slides to get through in 20 minutes, so I'll be skipping through some of them. The theme of this talk is the way that applications can make use of DNSSEC. Some of the possible applications are listed here. You're probably familiar with all of these. SSH, TLS, HTTPS, PGP, SMTP and so on. We'll talk a bit about some of the currently existing ways that applications can use DNSSEC, DANE, and we'll talk about some newer things that are coming on the pipeline. Diving right in, this is what an SSH FP record looks like. This is a fingerprint for connecting to an SSH server, and so this record type exists already. Interestingly, this predates DANE so it doesn't really fit into the DANE system, although it's very similar.

If you're an SSH user there's a directive you can define in the configuration file that will instruct it to verify the fingerprint via the DNS. I believe this works normally by just looking for the AD bit, although when you compile SSH there's an option where you can tell it to link with LDNS and in that case it will do all the validation itself directly in the application and not rely on just the AD bit. There's an older record type called IPSEC key, which stores IPSEC keys in the DNS. This hasn't seen a lot of uptake, and it's likely to be superseded by a very similar effort

within the DANE umbrella called IPSEC A, but this is what that looks like, should you be interested.

I suspect a lot of us are already familiar with DANE and TLSA, so I'm going to skip through these quickly, but just to note that there are a lot of applications that use TLS and a lot that can take advantage of DANE and a TLSA record. Those are listed here. We probably also know a lot of the reasons that the certificate authorities are a little problematic - the most obvious way being that when you have a bundle of CAs in your browser, it only takes any one of those to validate a TLSA certificate. So what DANE brings to the table is, in a sense, some certificate pinning, where you can say, "This certificate must have been signed by a particular certificate authority, which is referenced in the TLSA record." Here is some research that's done an analysis of those threats. You can refer to those in the slides later.

Again, this is all the justifications for considering use of DANE and TLSA. Here's a nice cartoon by someone who calls himself Kloot. The idea here is that you can see that DANE or TLSA doesn't really replace the PKI system, but it augments it and allows you to constrain it a little bit. The TLSA record is defined in this RFC. It's quite a complicated record. Here's what it looks like in the zone file, but it has these different fields; usage field, selector field and matching type field. So it gives you a lot of choices and flexibility in how you would specify your DNSSEC signed TLS records should match your TLS certificate. I know Wes just talked about this.

One thing I wanted to point out is in one of these usage fields, where you can specify usage two, your TLSA record can reference not the

certificate itself but the authority that signs your certificate - in which case you can change your TLS certificate without having to go in and update your TLSA record in your zone. Again, there's lots of flexibility there. This talks more about those different ways of constraining. A couple of these allow you to bypass the built-in browser or whatever the application's certificate authorities, you can bypass them entirely. But others allow you to just augment and constrain the way that those CAs are matched against. Here are some examples of some websites that are already using TLSA. There's quite a few high profile ones that are very good to see.

I don't know if Shumon chose this specifically because he knew you'd be in the audience, [laughter] but this is for the project, obviously. Okay, well, that's not in the slides so that's off the record! There are a few tools out there that would help you deploy a TLSA record. One of those is written by a [Paul Haslinger 03:09:53]. There's one here called [Swede], which I'm not actually familiar with. Shumon has listed a web-based tool that he's got on his website where you can type in your server name or maybe your certificate data and it will spill out a TLSA record for you. There's a very well-known web-browser plugin called DNSSEC validator from the cc.nic folks, which displays very nicely when TLSA validation is successful or not, and Shumon has a blog up there about it.

I also want to mention there's a fork of Mozilla called Bloodhound, which does a lot of this without the use of a plugin. It's built directly into the browser.

SHUMON HUQUE: Duane, if I could just also add that recently too - and Wes may know of this too - Victor Dukhovni has been very involved in the DANE implementation for us, and TP has put up a site for testing DANE SMTP records, and the URL you can redirect is tlsa.info, which will get there, and is a new tool that we have for that specific usage.

DUANE WESSELS: It's very interesting that SMTP is a place where, as Wes said, it's almost a perfect storm for TLSA and DNSSEC, so we see a lot of deployment there. As this diagram shows, you can secure the submission channel and you can also secure the server to server channel with TLSA records. One thing that's interesting to note is that even without TLSA a lot of the SMTP servers opportunistically encrypt their communications when they can, but this is a little bit vulnerable to attack because it's vulnerable to a downgrade attack - if one side can spoof the fact that the other side doesn't sport TLS and so on. So the DANE effort can help here because you can use the presence of the TLSA record to prove that the server supports it and that the downgrade attack should not be possible.

SPEAKER: My question is: you say attackers can strip away the TLS capability, so how can one see this when you are say downloading your email, for example? How do you see life? In Wireshark or those kinds of things? How do you see that part of it?

DUANE WESSELS: I think you're asking how you'd know if it happened? The server itself for the client probably wouldn't log that level of detail for the

connection, so you'd probably have to use a Wireshark or some kind of packet capture to actually see that… I don't know if wire shark is going to display… You may have to do some work, but…

PAUL [MARTIS]: Hello? I'm Paul [Martis], [unclear 03:14:00]. Actually, Victor made it so that it is logged in the logs. It will say "TLS failure and you can actually configure to hard fail or soft fail based on the verification failure.

DUANE WESSELS: That's for Postfix? Yes. Here's a TLSA record for SMTP. Notably, [Free bs 03:14:29] has this enabled, which is very nice. Is this the one you were referencing, Dan? Yes, so this is the same site, and here is a survey of lots of mail servers that are already supporting TLSA records. It's much more extensive than this. This is just a few of the notable ones. Paul mentioned Postfix, which was the first adopter of TLSA records. Exim apparently has some work underway, but as you can see it's not really all that difficult to enable this for Postfix. It's something like three lines in the config file. Of course, you need a validator to go behind it also, but that's pretty nice.

Jabber, AKA SMTP servers are also adopting DANE TLSA records. I've deployed this myself on a couple of Jabber servers that I use. That's what they look like there. All right, so exiting the world of TLSA for a minute there's a new record type called open PGP key, which encodes a PGP public key into the DNS. Although the specification is still under development the research code type has been assigned already and I know there's a few of us that have experimented with this and actually

deployed some open PGP key records. I believe Paul's [hash slinger 03:16:06] code can generate the record for you. It will fetch the key and spit out a record suitable for stuffing right into your zone file.

One thing that I wasn't prepared for when I did this was the size of this record. Since it's just a hash of your PGP key it can be quite large. I guess proceed with caution there. You may not want 10K records in your zone file. Or I guess you could strip out some of the signatures from your key before you put it into the DNS.

PAUL [MARTIS]: So the tool actually tries to create a minimum expert of the key, using in this case the GPG options for expert minimum. However, that still drags in a lot of data. In effect, when for the [unclear 03:17:02] project.org I imported all known keys of all the developers that they have; they have an internal database of PGP keys. So we're running this on [unclear] project.org and it's about 1,500 PGP keys in that zone, and there were about 20 that failed because there were actually more bids than could fit in a single record. There's still something not very minimum about GPG expert minimum key.

So that's one issue. Other than that, it works fine. The draft actually tells you the resolve issue should only answer with this record when the source address has been verified - the source address of the query [unclear 03:17:41] which means either it should have come in on TCP or on another draft called DNS [unclear] cookies. So you shouldn't just spit this out. Unfortunately, because most resolvers don't properly implement open PGP keys, as they're not aware of it - they know how to serve type 61 records but they're not aware that this is specifically

meant to not be spit out on UDP packet that you haven't verified, we actually need to talk to the implementers to make sure that they don't allow that, because otherwise the D-DOS amplification attacks we've seen, this one will be to about a factor 100 worse.

DUANE WESSELS: Another DANE record type is S [unclear 03:18:26]. This is in the Internet draft stage. It's a key for an S/MIME encryption certificate, and VeriSign has an early prototype that uses S/MIME in the Thunderbird mail client, I believe, and that was presented at the last workshop. But if anyone's interested in knowing more about that, please let me know. Want to spend a little bit of time talking about "getdns". We've already heard some about it today, but it's a new API for getting DNS and DNSSEC data in your application. The idea is that this replaces "getadderinfo" and "getnameinfo" and allows you to request all kinds of record types and to receive all of the signature information that you would need to do validation.

This diagram shows the problem of securing the last hop. In general you have a host or a client using a resolver that's on another machine. That last hop is a little bit vulnerable to attack and spoofing, so you may want to move your validation directly into the application and illuminate that threat as a possibility. "Getdns" has a couple of modes. It can run as a stub resolver, whereby it sends all its queries to somebody else, and it can also run as its own recursive resolver where it does all of the iterating and fetching and validating on its own. There are other options to securing that last hop, such as DNS scripts and TSIG keys, but

especially in the case of TSIG it's pretty rare to find that, I believe, used to secure the last hop.

If you're interested in "getdns" there's the webpage for it. one thing to keep in mind is that "getdns" means two things. It means the specification, which was written by Paul Hoffman in cooperation with others, and it also means the implementation of that specification. You can find both of those at this website. The code itself, the implementation, is written in C, but there's a number of bindings for other languages, such as those listed here. A few of them are in progress and coming up soon. If you're a fan of [Jason 03:21:27] or that kind of thing, you'd be very comfortable in working with "getdns". It uses these data structures that look very much like [Jason]. I think we have some examples at the end here.

Another important features of "getdns" is that it can do asynchronous lookups, so unlike our other friends "getadderinfo" and "getinfo" it doesn't block the process waiting for the response, so that's very important. Here are the basic functions you might use to make queries in "getdns". You can ask for an address, either IPv4 or IPv6. You can ask for a host name. You can obtain SRV records, and then everything else falls into this general category where you can request any record type data. This is how the data is delivered back to you in this data structure. You can see it's actually quite rich and complicated. You get for example the raw packets. I think the reply is full there, and shows a very raw format, and then it also parses out the records, IPv4 or IPv6.

If you set this flag called something like "full replies" you can get the whole reply tree. You can get the c-name record and the other side of

the c-name record. You can get all of the DNSSEC data. I don't think we included any of that because it would be messy here, but here's a very short example of what it looks like in your program, looking up a host name. In this case we set this flag that says "give me both IPv4 and IPv6" in one function call, and the output there shows that we indeed got both of those for this example. Here's another code snippet that shows how to get a TLSA lookup. I do believe that in the case of looking up this record, the library will enforce the fact that it must be signed with DNSSEC and validated. Sorry I had to rush through that. [applause]

JULIE HEDLUND: Let's have a couple of questions.

DAN YORK: I'll just say it's great to have this catalogue of DANE apps. This is good, so thank you and Shumon for doing that. Xiaodong?

XIAODONG LEE: Very quick question. I think there's a lot of discussion, but my concern is from your experience, how many years until we can adopt the application? I just wondered how many years for the application to support DANE by default? Just like the IDN came in 2003, but it took many years to support that, and even now there are some that can't support it.

DUANE WESSELS: It feels to me like we're still 2-3 years away from that, because before the applications can really support DANE they need a tighter integration with a validating resolver.

XIAODONG LEE: 2-3 years? Because we assume so many people need to work together.

SHUMON HUQUE: I would just say too, to your point on the browser side, I think we've had questions with the browser vendors or discussions, as Warren can attest, at different times, and they're focused around speed right now and so for them they're not entirely excited about things such as DANE and other pieces, so I liked what I saw on here. One of the interesting things we've seen with DANE is though we talk about web browsers as one of the use cases, because it's easy to explain, the reality is that DANE is finding a home in a lot of other applications and places, especially SMTP but also Jabber and some other places that need the kind of mechanism to help ensure TLS is right.

I think it would be interesting to see where it takes off in these other applications and other uses, and that's probably the better place to focus on, from making things happen. One of the points we've heard back from some of the browser vendors is, "Show me the proof that people really want this with TLSA records." I think what we're starting to see now is more and more people are putting TLSA records out there because of these use cases, and I think that will help impress upon the browser vendors that this is real. I know that Peter Caulk at DNIC has been running some workshops for his registrars around DANE, because

interestingly, in Germany, the mail providers are advertising support for DANE.

So there are a lot of domain registrants who are going to the registrar saying, "I want to use DANE with my email." So Peter at DNIC is in the situation where he's having to help educate the registrars about this so they can add the fields so people can put TLSA records in. That's driving it in Germany anyway.

XIAODONG LEE: You're right, but my concern is our discussion is not limited to the DNS community, because even for browsers, even for Microsoft, not only for them, but if DANE can be supported, that means all of the products need to support that. DANE is a very fundamental function for the authentications. That means you need to meet the product timeline for the software vendors. So I'd suggest if we discuss DNS in the future, then we need to collect software vendors to join us, not only for the DNS community. That would be better. I've had very bad experience with IDN support.

JULIE HEDLUND: It sounds like we maybe have some more things to talk about over lunch. Please thank me in thanking Duane and Shumon. [applause] Again, if you don't have your program that has a ticket there are a few up here. I'm going to go ahead and make sure you all can get in there. Again, it's the Stamford Foyer. Go out into the main area and go all the way down as far as you can go, to the right, where there are windows and a roped-off area and a sign that says it's your lunch.

RUSS MUNDY: Let me remind folks that this room is not secured, so please take your stuff with you.

[LUNCH BREAK]

JULIE HEDLUND: Welcome everyone. I'm ready to start. People are coming back from lunch. Our next Item on the Agenda is a Panel discussion of DNSSEC and DNS operators, and our moderator for that Panel is Olafur Gudmundsson from Cloud Flare. I'm going to turn things over to you Olafur.

OLAFUR GUDMUNDSSON: I'm Olafur Gudmundsson from Cloud Flare. This is a Panel that's going to be talking about some of the operational issues we see with DNS and DNSSEC. It's not going to be the same old, same old. This is going to be something new, hopefully, from most of you. We are going to be talking more about problems today rather than solutions. We'll be talking about what is needed because this is a problem that spans multiple ICANN areas and how to fix or address this is not necessarily going to have a simple fix or a one fix - there may be multiple things. Those of you who can see my beautiful picture on my first slide, this is the view that you get when you come to ICANN of the state of the domain industry; it's beautiful, everything is working fine, everything is so good.

But we go to the reality now. There are some rough edges. It's a cold place and it could be dangerous. When you start figuring out how the DNS delegation system works you run into certain edges. The registration systems we're dealing with were designed about 20 years ago. They were based on technologies and operations that were at that time. The registrant buys a domain from a registrar. He enters this information through some kind of an interface and then it gets pushed out to the registry. But this is a reasonable model, and there were reasons why this was picked, but it has certain edges. In the good old

days when we started selling and trading domain names, almost every registrant happened to be its own DNS operator.

But then because domains became available, people started buying them, and suddenly we had people that didn't operate their own DNS or had access to them necessarily, so the registrar became a DNS provider or [unclear 04:22:24] resort. Then the registrars got really smart and realized this was a way to upsell. So they started providing hosting services and other things, so they became the most common DNS operators. Then over the years there has been an evolution towards third-party operators. Those are any commercial entities or friends that you have that operate the DNS on your behalf. In the typical registration model this third-party is a non-entity. We don't exist. When I try to explain this to some who are long-term participants in ICANN they have no clue what I'm talking about.

They think, "We operate DNS for 90 per cent of our registrars." Okay, "But do you operate it for the one per cent who really care what's on their website?" "I don't know." Okay. We are important as an operator. I'm one of the largest third-party operators on DNS at Cloud Flare. We operate about two million domains. That's close to one per cent of all domains in the world or something like that. People who care about various things go to third parties because we offer various important features that your mom and pop hosting provider may not provide, whether it's digital footprints, security, capacity, or access to other resources.

Cloud Flare, as an operator, we are a very important player for people who are unpopular, .i.e. they get attacked a lot. So we're dealing with

constant D-DOS attacks, and we're not the only one. David here works for the largest outsourced DNS operator, because ICANN operates many sites that give you all the videos you spend all your time watching. What DNS operators want to be able to do, in a perfect world, would be, after a customer has signed a contract with us and given us authority to run DNS for them, it's to be able to modify the delegation information on the fly when it's needed. Whether it's because we want to move a customer away from an attack, whether it's to move a customer to a no-route address space, whether it's to change their keys, whatever - for convenience.

Or if the customer is leaving us we want to make it happen in as smooth a way as possible. So DNS operators may have a problem, so we need to renumber some address space or something. So there are a number of reasons why we want to be able to change things. As a non-entity in the ICANN process, when my support staff calls a registrar and says, "This customer of the registrars is having a problem and they need an emergency fix on NS records or DS records," a good registrar will hang up on us, because this is a social engineering attack. There is no record. We are the operator. The only way a reseller can determine we are who we say we are is by looking at the names of the name servers or the addresses that are being used to operate the DNS servers.

But the standard technical support of the registrar is not at that level yet, and they don't have any way to actually assess what the address ranges are that Akamai uses, DINE, or any other third-party operator easily. If we look up the WHOIS for contact information we get only non-actionable things. We get phone numbers and email, which is last century's way of communicating. What we'd like, in the perfect world, is

to either know how to contact them or have an interface, URIs or something like that, that we can create a connection and express what the desires are, and have it acted upon. Right now there's no model for anything - communications or authentications or parties, or what could be done.

Right now if we have to change anything the only way possible is to talk to our registrant and say, "By the way, you need to go and log into your user interface and do this." How many of you, when I call the UK right now and ask them to do it, it's the middle of the night for them? Because of this DNS operators are being forced into a role they don't really want to be in. To gain access to the registration systems we are becoming registrars. We don't want to be in the business necessarily of selling domain names. We're not necessarily able to go into the domains that we need to be in, so it's not a good solution. We'd like a more [unclear 04:28:06]. In the perfect world we'd like to have something developed that we can automate the process in relatively legit ways. I will turn over now to Duane Wessels from VeriSign who's going to talk to us a little bit about some of the [unclear 04:28:34]. Thank you.

DUANE WESSELS: Thank you Olafer. I'll try not to be too redundant here, but we'll see how it goes. Similar to what Olafer was saying, for some domain owners or for some parties the registry/registrar/registrant model is really an impediment to scalable deployment of DNSSEC. I've got a few examples of what that is true. I would argue that a lot of this hinges on this thing we call the DS record. This is the glue between zones. This ties parents

to children and so on. It's a cryptographic hash of the key signing key, and I would put to you that it's really not understandable by humans. If you look at these examples here, these are all DS records in various formats. One of them is valid, one of them is not, and by looking at it we can't tell which one is correct.

This is what you get when you go to a registrar and you try to enter your DS record. It's a relatively complicated page with lots of forms and various things required or grayed out, and it's not exactly clear how you'd actually do this. Another reason is that key rollovers are hard. To be honest that's where a lot of the problems come up. When we see bogus names or validation failures it's because a key rollover has gone bad. Today it requires interaction with the registrar. I suspect a number of people, like myself, for my personal domains I've never rolled my key. I've set it and I've just left it there and I'm living with that. I fear going there and doing this for all of my zones and in fact it's a hassle because there are so many.

Say I have 20 domains that I own, I wouldn't want to go and do this 20 times and fill a form in 20 different times. As Olafer said, for third-party DNS operators, they're significant and the fact they're not party to this model is a big problems. The point of all this is to say that in order to increase DNSSEC deployment, we should really explore solutions to make this easier - especially with respect to the crypto data. Next: what if? What if registrars weren't required to submit their crypto data through the registrars? We might imagine something that's a little more simpler to understand - perhaps something like a pointer that changes infrequently, it's more stable, but which in other ways is treated like a

DS record - that is to say it's authoritative data in the parent, it's signed with the DNSSEC.

Something like this could enable a not-strictly hierarchical chain of trust. What if registries could take data directly from registrants? We've already heard, earlier today, a couple of ways that you could do this. There's an RFC that defines the CDS and CDS key, which Olafer knows all about. There's another one that's child synchronization, which I believe Wes knows all about. These are good, but they still have bootstrapping problems. You can only do this after the zone has been initially signed. What if registries could accept data directly from DNS operators? So again, back to what Olafer was saying. This is beneficial for more things than just DNSSEC. This is very good for registrants who happen to use these third-party operators, but I'd say it still omits a certain class of users.

If you don't happen to use a third-party DNS operator or a large third-party DNS operator, this may not be something you could take advantage of. So it's not the total solution. So we've talked about a few different problems and hinted at a few different solutions. I'd say that these were not necessarily in conflict with each other. These are complementary. They have different trade-offs and benefits. All of them are a little bit painful. They're going to require changes to the protocol or changes to the process or to the model. Myself and others would really like your feedback on these ideas. Thanks.

DAVID LAWRENCE: Thank you Duane. David Lawrence from Akamai Technologies. Many of you know us as an extremely large content delivery network. We

provide a number of other services, among which are DNS hosting. Let me plow right into the slides. There's a little bit of redundancy here. On the first slide I want to show you what it looks like inside our operation at the screen that the customer would be looking at when they're trying to add DNSSEC to one of their own domains. This slide highlights exactly the problem. That line down there says one of these records should be provided here: parent zone to establish a DNSSEC chain of trust. That big block of gobbledygook is what a customer has to look at, wonder what it's about.

One of the other things that's bad about the user experience for people in general is being presented with the internal workings of our protocol that you really don't care about - it just adds confusion to what you're looking at and what the meaningful parts are. So we'd like to not have customers worry about providing the DS key to their registrar in order to get it into the registry. The three blue blobs show the current model as it is within ICANN. There's the registry, the registrar and the registrant. There's actually a fourth R that's not included in this particular diagram because it actually confuses the situation even more and that comes to resellers. Resellers interpose themselves between the registrar and the registrant.

Whenever we're talking about a solution for this particular problem we also have to consider how resellers fit into the entire picture. One R that was never considered was the [ridgoperator 04:37:09], maybe because it didn't fit the pattern really well, and so that offended some people aesthetically or something. But what it basically means now is that third-party operators were second-class citizens because we're not formally acknowledged by the process that we're constituents in the

entire process. This has a lot of history though. Before ICANN established the three, sometimes four R model, the registry and registrar function was combined, back in the day when .com was just VeriSign and VeriSign was acting as both registrar and registry.

But the same problem existed back then, even before there was DNSSEC, even before there was the triple R model. But it mattered a whole lot less in the past because we were a really small community, most of the people involved with the DNS were very technical, and we learnt to make it so that once you establish DNS records you very rarely had to touch them. This changes a lot now with DNSSEC, because it requires more frequent updates to your parent that are really hard to get around while maintaining the security guarantees you're trying to get from DNSSEC. So now it becomes another obstacle, the DNSSEC adoption, this longstanding problem that's been around almost since the DNS began.

This demonstrates the original problem with NS records, that that red box that highlights the same set of instructions: "Here are a list of records that we need you to put in your registrar in order to get up to the registry so that your DNS all works. We can't do this for you so you're going to have to cut and paste this data and hopefully you're going to get it all right and establish the records we need to have established in order to be successfully hosting your domain." So there are a lot of consequences of this particular problem. Perhaps the smallest of them is just that it creates unnecessary [unclear 04:39:06]. You're relying on manual intervention from registrants in order to make the proper updates to get the service done that you need done.

But one of the other problems with customers is that they often don't do what you've requested of them. So sometimes - it might be days, it might be weeks - we have had some requests that just seem to go into a black hole. They just never, ever get acted upon. One of the other problems with manual intervention though is that human error can enter at several different points, and not to say computers can't make mistakes, but when you have humans adding their own steps in there you're much more likely to make a mistake. So there are all sorts of problems that lead to problems with domain resolution, and they get even worse in the DNSSEC sphere.

The DNS, before DNSSEC, was pretty tolerant of mistakes. You could have five name servers, originally defined for your domain. If four of them went away your DNS would still work. It might not work as highly performing as you would like, but it would still keep working. You break your DNSSEC, you're breaking it for everybody. This also leads to diminished resilience. It means that we can't maintain the set of authorities the way that we want them to be maintained for the customer in order to provide the performance guarantees. For example, at Akamai we have many, many customers, but they each get an independent set of name servers so that if any one of them were to come under attack, and somehow we were to be so overwhelmed that somehow their complete set of name servers all went away.

The rest of the customers would still be able to continue because they had some name servers that were not affected by the attack. But that security design gets compromised when you have a customer that only decided that they were only going to upload two of your names out of the six that you gave them. It also constraints operators to the changes

they can make after the fact, even if they did have all six but they are not willing to change your name as we come up with some additional security enhancements that should be reflected through their set of name servers. It's really hard to accomplish that. finally, this makes additional workload for everybody - not just for the customer, not just for the operator, but then for the other organizations like recursive resolvers that have to handle customer complaints.

The classic example is when NASA screwed up their DNSSEC it affected Comcast very heavily. Comcast took a lot of heat for it and their customer support people ended up having to deal with the problem that they had really no original cause in generating. So there are a few different options. We can tell operators to become registrars. A couple of operators have chosen that path, but as noted in a previous talk, there are a number of reasons why an operator does not want to become a registrar. Even in our case, Akamai is becoming an ICANN-accredited registrar, but only for our own internal domain purposes. We don't have any interests currently in productizing it as a service.

But even to the extent that you become a registrar, you only do that with a certain set of domains, and so becoming a registrar you then find additional barriers with trying to become a registrar for different ccTLDs, for example. We get operators to interface directly with registrars. The one thing I wanted to mention about this also, the operators becoming registrars, is that I did a quick, casual survey, on the Alexa top 500 domains, and probably a fifth of them are running on four operators who are not registrars and don't have an interest in becoming registrars. Another quarter of those domains appear to be hosted by the registrant

themselves, so less than half the domains appear to be hosted by a registrar operator.

Operators could directly interface with the registrars, as will be mentioned in another talk. This has a little bit of a problem in that the registrars typically have not had much of an appetite in order to tackle problems like this, and we've tried to take steps in ICANN, like the recently updated RAA to make sure they're doing DNSSEC, but it turns out there are some giant, gaping loopholes in there, that perhaps Dan would like to tell his story about during the discussion for example.

Even if an operator is interfacing with the registrar, you have a really hard time identifying how you're supposed to go about doing that - identifying the correct registrar and their process for interfacing that. Another choice is that operators can interface with the registries. I believe for both Olafer and I, this is our preferred approach, although it's not without its own landmines that have to be dodged. It does mean fewer entities to deal with. Several registries have indicated a desire to also help move DNSSEC along on this path. It is complicated by the existing registry/registrant barrier, and what that would mean by being able to authorize people.

It would also involve, so far, most of the approaches that have been taken to look at this problem within the IETF. As we'll see on the next slide, they focus on the DNS protocol. However, registries don't tend to maintain their data through the DNS. They use a separate protocol called EPP, the extensible provisioning protocol, and so there would be some work that has to occur on both sides in order to enable it through that channel. Then last but not least, ICANN could just ignore this

problem and say, "Hey, well, status quo seems to be working well enough at least, so let's just plow ahead this way." So there is relevant work going on, as previously mentioned.

Wes Hardaker put out the [CCINC 04:44:52] draft, which is really helpful for maintaining the NS records, the name server delegation records and the addresses that are associated with them. It could be pretty cumbersome for large registries, as is mentioned in the draft, and it's also explicitly not intended to help bootstrap the process. Then Olafer and Warren's draft on CDS and CDNS key, that became an RFC, is much the same idea as [CCINC], in that it has a lot of the same limitations with regard to bootstrapping, polling and scaling.

Mark Andrews has posed a draft that basically proposes you use the existing DNS update protocol mechanism. It hasn't been that warmly received, but he's right about, "Well, this already exists in the protocol." But it has its own complications. One of the only interesting thing about this particular draft is that at least it does attempt to even bring up the problem about how you find the right registrar to work with. The key thing about all these, these are all just strictly the DNS protocol. None of them attempt to address business relationships and how you establish that a given operator is actually acting on behalf and with all the due consent of the registrant, the reseller or the registrar that they are actually operating for.

So this is really ICANN's purview; to look at acceptable business processes and how that can all work. Once we get over that ICANN hurdle about "how can the business side of it work?" the protocol side will follow it much more easily. One other bit of relevant work I want to

mention, and I think Dan will provide information for this later, and that's that we've started a list at ISOC for discussing how to handle this particular problem. It's called the DNSSEC auto DS list, and on that list Jacques Latour and Stuart Olmstead-Wilcox from CIRA wrote a pretty good introduction. They got a good start at a whitepaper on what the problem is and different ways to address it. It needs a lot of retuning and refinement in order to really be a document that we can pass around, but it's excellent and we should end up using that.

Operators need a way to maintain data at the registry and there is a little bit more protocol work that's needed, but it does have its limitations, so why we're here talking about this now is because it's up to ICANN really to look at the policy changes that would be necessary to make this all succeed.

OLAFUR GUDMUNDSSON: Thank you David for a very good talk. Jim Galvin is now going to talk to us and approach the problem from a slightly different angle.

JIM GALVIN: Thank you Olafer. The slide that's going to come up here is just a little bit of a look at Afillias and who we are and how long we've been doing DNSSEC. The most important thing I want you to take away from this is the fact that we're a registry service provider, and we deal with a lot of TLDs. Now we host three dozen of them. By the time this new round of new gTLDs are there, we'll have over 200 TLDs. The particular issue I'm going to get to here that I want to focus on, we have a unique visibility and experience in that. I want to start from the point of view of just

reminding us that on the provisioning side DNS generally works. It really does work for most people. We're focusing a lot here on some of the problems, but there's a limited community of people who have to deal with that problem.

For the largest part of the DNS industry, people get their bundled services from a registrar or reseller and everything is handled for them. That's when the situation works - when everything is tied together, when your registration services are combined with your DNS services. Then the set of problems that you have are much more contained and much more addressable. What we've been hearing a lot about here so far - and a lot of attention goes to this particular problem - is the fact that you do have this air gap between your DNS provider and getting that key information up. The DNS provider is the one whose doing the signing. Again, in the largest portion of the cases in the industry, the registration services and the DNS are tightly couples, and so this problem doesn't really exist.

I'm not going to get too focused on this. Most people have been talking about this from a couple of different perspectives, but this is the problem space - that they're outside of the loop. We've been exploring a variety of different options for that. I want to move in and talk about a particular scenario that actually has some other interesting problems, and in fact it touches on the need for some particular policy changes, and in the ICANN community that would be useful. I'm going to use the registration transfer as the example of how to highlight this problem. A domain owner wants to move their registration from one registrar to another, and their assumption is their DNS services are obviously tied to this.

This scenario actually applies in the case of DNS operators who are registrars. They may in some circumstances, when the DNS services are moved, this problem also still highlights in that scenario too. I'll tell you more about that when we get there. The usual protocol - the thing you have to understand about transfers - is that the domain owner goes to their new registrar, they ask for the transfer, and then there is a back channel during which the new registrar passes a message up to the registry saying, "We want to move this." There are some authentication mechanisms that go along with this. The registry then tells the old registrar that this domain owner wants to move, that the registrant wants to move between the two registrars.

The losing registrar may or may not ask on the request. Then there's a five-day period during which this transfer is subject to review, and the old registrar could wait for that five-day period, in which case the registry will automatically approve the transfer, and it will then allow all of the credentials and the authority to make changes to the DNS for that domain owner. It will then delegate that to the new registrar, or the old registrar could of course acknowledge the transfer and let it all happen immediately. I should probably have prefaced this by saying this is the situation in the gTLD community. Let's be clear about that, because obviously ccTLDs can have their own sets of rules, and many don't have this specific problem because they're able to do things to make all of this work.

Focusing on that question of "does the registrar act on the transfer requests?" the old registrar has been notified that they're losing a customer. So what do they typically do in that situation? It turns out it's uniformly very common for them to go, "Oh, I'm losing this customer,

let's take him out of the DNS." So they immediately remove them from DNS services, and they will no longer serve their zone. Then of course they simply wait, and they also do not acknowledge the fact that the transfer was requested, so that you wait for TTLs to expire and then when the transfer request happens the new registrar can then push up a new [NSEC 04:52:51] and whatever else they want to do for the domain name. But over a period of 2-4 days the TTLs will expire for whatever was there, and then the domain name goes dark and they're not available.

Now, this problem has not been terrible up to this point because you've got a situation with a relatively benign "site not found" but suddenly, when DNSSEC is in place, you've now made the error become a scary "do not go there!" because it's known that it's supposed to be a signed domain. Next slide. The important thing here is that solution that's really needed in this. What you really want is for the registrar record, the old DNS provider, to maintain DNS services while this transfer is in progress and is occurring. Further, you really need them to be able to import, which brings us back to the problem we've been talking about anyway. They need to be able to put the new key information also in the zone for pre-publication purposes, so that you can deal with caching and so it's available. I comment here on the requirements of what's necessary in making all that work.

The situation even exists if you're transferring your DNS services away from the registrar. You still have this problem of the old registrar maintaining services and continuing to maintain those services while you transition to a third-party service provider. These requirements still exist, that you still want them to pre-publish the key and of course

maintain services until the transition is complete. What I've referenced here in the end of this is the observation that this five-day period - and I want to be very careful to say that it is not a grace period, for those of you who pay attention to registration and EPP. This five-day period is officially not a grace period, because "grace period" is a term of art associated with EPP in the life cycle of a domain name.

It is simply a five-day transfer period during which the transfer request can be disputed by the losing registrar. It's the opportunity for them to deal with any fraud circumstances or situations that might come up during that. But that particular policy that I reference there, what's interesting about it is it has no DNS requirements. That's what's missing from that policy that defines the rules, procedures and rights associated with the transfer of registrations. That's it. Thank you.

SPEAKER: Olafer, could I ask a quick question? Jim, you mentioned the bad registrar who doesn't respond and the domain ages out and then the registry, after five days, gives it to the new one. Do you have any sense from your own date or others' of how common that is?

JIM GALVIN: As I said, uniformly it's what they do. All the time. It's common business practice.

SPEAKER: Really? Huh. Thank you.

OLAFUR GUDMUNDSSON: Thank you Jim. Last but not least is Jacques Latour from Canadian Registry.

JACQUES LATOUR: I'm Jacques Latour with CIRA. I think we've covered all the problems here from end-to-end. The key point here is that the DNS operator has multiple faces. It can be the registrant, it can be the registrar, it can be a web hosting on behalf of a registrant or registrar. It's fairly complicated what the DNS operator is in this model. I made a picture. [laughter] on the left we've got the standard registrant/registrar/registry model. This is all a straight line down that works well. But then we've got the hosting companies too that can be part of the registrar, and sometimes it's not, and these hosting companies can use the DNS operator on a contract and there's no relationship to the registrar at that point. There's no optimal solution there to address this problem. There are multiple use cases.

The one constant thing is that the large DNS operator, in my view, from a registry point of view we only accept changes to EPP. The only way we can change the zone file on the registry is through EPP or a web interface. Us going out and getting data and updating the zone file, we can't do that. It's not part of our framework. So we need the mechanism to bring the changes in the registry to EPP, and that's what the line is between DNS operator and the registry. The idea is for this to work somehow the DNS operator needs to be authorized by the registrar for certain domains to do transactions; work on a domain. Anybody that touches the registry has to be accredited to do EPP commands, and it's got to be secure. The idea is that DNS operators can

modify the name servers and the DNSSEC keys and material on behalf of a registrant, authorized by a registrar, and somehow it should work.

OLAFUR GUDMUNDSSON: On that hopeful statement I think I'll open up the floor for questions and discussions. Dan?

DAN YORK: Since David asked me to say a couple of things there let me just say, David's right. There is a mailing list for this. It's called DNSSEC-auto-ds. If you use your favorite search engine you can bring up the info page where you can subscribe to it. It's a standard thing. If you're interested in working on this, join that mailing list. Jim, thank you for highlighting the problem of why people so seldom change registrars, because it's such a pain to do that. Since David mentioned the challenge, the challenge I had was a good number of domains with a certain registrars out there. Back when I joined the Internet Society in 2011 I raised a ticket in their help system because I wanted the full registrar hosted thing. When I knew they weren't going to do that I said, "Can you give me a box to fill in my DS record?" like the one Duane showed.

Maybe a dozen people like me also piled onto the ticket saying, "We want this too, why aren't you doing this?" and this and that. When the 2013 RAA came out I was excited. I said, "Hey, this is going to be a way to go and do this." I posted that in there. This is a consumer-facing side of a registrar hosting operator that has a wholesale component. Anyway, they should have been bound by this. They were saying, "Yes, it's still on our list, it'll get there some day." Eventually numbers of us

kept saying this, and I filed a compliance request with ICANN saying, "These guys signed the 2013 RAA, they're there for not in compliance." Well, so this particular reseller would do it, they told me, if I wanted to pay them $500 as a customer consulting engagement to go and do that. I was like, "Seriously, you're going to charge m e $500 to just go and take my DS record from me and upload it?"

Well, the reality was that this was enough that by the letter of the RAA they had provided a mechanism for me to provide the DS records and to do that, so from the ICANN compliance side they came back and said, "The registrar has provided a mechanism for you to do that. You just may choose not to do that." My response was that I went through and moved my domains to another registrar, but that's the situation out there with some of the registrars that are there. The 2013 RAA only gets us so far in regard to that. Jim?

JIM GALVIN: Just to add a little more context to all of that, the new rules and the 2013 RAA, when you take these two sets of things in combination you have a clause for registries that requires them to sign their TLD but there's also a little hole that doesn't require them to offer signed delegations. There's a way to escape that too, which is interesting in this spirit of trying to enforce or promote the deployment of DNSSEC. What happens in the RAA 2013 is the clause is also written in such a way that the registrar does not have to provide DNSSEC services unless the registry requires it. You've got this interesting disconnect; those two contracts are not quite synchronized in the way in which you would

expect and like them to be. This is something ICANN is now aware of, and it's been brought up in various forums.

The solution to it is obviously not trivial from a policy point of view, because as hard as things are from a technical point of view they're even worse on the policy side. But it's something that we'd all like to fix. Thank you.

WARREN KUMARI: I just wanted to point out that it's exactly things like what Dan described that make people hate their registrars. In case we haven't noticed…

OLAFER GUDMUNDSSON: Warren, can we not turn this into a registrar-bashing session?

WARREN KUMARI: Sure. Okay. Sure enough.

DAN YORK: Olafer though, just another point - Daune mentioned this whole thing about he hasn't changed his keys on his domains. I have a couple of my personal domains hosted with somebody who takes care of all of this for me. I went through the form, did a couple of things, good. It was at one of these DNSSEC Workshops a year or so ago where, unbeknownst to me my provider, a DNS operator, had rolled my KSK. I had completely ignored the email warnings they'd sent me a couple of weeks in advance telling me there was going to be a key roll, I had to be prepared, blah blah, and I completely ignored those. My key and the old DS expired, so

somebody contacted me while we were in this workshop and said, "Do you realize your personal domain doesn't validate? Come on!" But it was that exact example.

As an individual I'd love to have this automated service because it's too prone. The question I have is how do we get the registrars - as you mentioned, they're doing 90 per cent of the hosting themselves; the ones who are registrars and operators - what's the motivation for them? Because the challenge I've run into, I've talked to them and they'll say, "Look, the DNS hosting and the web hosting on the pieces are what I make my money off of. I don't make my money off of selling domains, I make it off these hosting services. Why should I make it easy for one of my customers to use somebody else for DNS hosting?" What do I tell them?

JIM GALVIN: It doesn't have an easy answer. You have to look at the legacy system and where things came for legacy reasons. Even before registrars would get into hosting services, as part of buying a domain name they just gave you email and DNS kind of thing. So by default, because that's how the system evolved, they started providing services that essentially were free, and they had no direct revenue from. That's the situation that you're in today. If you look for where DNSSEC is deployed, where it's deployed in the largest population, a lot of it is it's all because it was either mandated or there was some other incentive to the registrar to make this happen.

Absent that, if you look at it from a purely business point of view, there really is very little incentive for the registrar to go down this path and do

it, so there has to be an incentive that comes from somewhere; either from the registry or from a regulation that simply starts to require it. That's fundamentally what you're up against, and it does not have a trivial solution, as I'm sure you can expect.

DAN YORK: One incentive they have is that if they actually force operators into the corner of becoming registrars themselves, so registrars of these customers, then they lose the business anyway. The operators are reluctant to do it, but it doesn't mean we won't do it if we're compelled to. We're already setting up the processes to be able to do it, but we'd like to coexist peacefully. The other assumption based in that question is that the necessary path that we pursue, and it does look like this from Jacques' slide, is that somehow this authorization to interact with the registry would come through the registrar somehow. But we might be able to develop a business process that just sidesteps the whole issue. Like for registrars to do their things, but to the extent that an operator is the legitimate authority to act on behalf of the registrant, there might be some other way to interface with the registry and to indicate that.

JIM GALVIN: I've wondered if we could sell this to registrars as a way to help make things easier for them in some ways, or to help automate some of their process, but…

SPEAKER: I just want to find out from you what happens if the DNSSEC key is stolen during the process of a transfer?

OLAFUR GUDMUNDSSON: The standard operating practice is that each operator has his own unique set of keys, so the private key material should never be transferred between two identities. But if someone wants to move the key over, yes, bad things can happen.

SPEAKER: Yes, so in that case have you come across a scenario to resolve the situation?

OLAFUR GUDMUNDSSON: Revoke the key.

DUANE WESSELS: To expand on Olafur's answer, somebody who might not be as familiar with the entire DNSSEC protocol, there is a process in place by which you can mark a key in the DNS as no longer being valid, and so what you would do simultaneous with doing that would be to have the proper operator in the zone install the proper key, at the same time as saying that that old compromised key was no longer valid.

SPEAKER: The reason that I asked - and I won't go into detail of the case - but a registrar tried to do a criminal act and pretend that key was lost, so that the guy cannot do the transfer, blah blah. You understand the scenario. So the subscriber becomes a victim of the situation. I'd like to hear your enlightenment. Thank you.

JIM GALVIN: I can only observe for an answer that, sure, we've now just defined another way for a bad actor to make things worse. I'm not sure what else to say about it. People will always find a way to do bad things that they shouldn't be doing in the first place. We're focused here on reasonably well behaved circumstances, and the kinds of things that go wrong, even when you're trying to be well behaved. You're identifying a circumstance - well, what if you're not well behaved? Sure. There's lots of ways to not be well behaved and make the situation a whole lot worse, so there's no easy answer there either.

JULIE HEDLUND: This is a question in the Adobe Connect chat room. It's from Rob Golding, astutium-1471, and he asks: "From analyzing our registrations in - limiting it to domains which resolve - 91 per cent of domains use either the registrar or host's name servers, so "DNS operator" is not separate from those, therefore is this really a big issue that "third parties" aren't generally provided a mechanism to update DNSSEC?"

JIM GALVIN: This gets back to the comment I was making when I was first starting. In many ways you're dealing with an 80/20 situation, or it might be 90/10, so in terms of percentages it might not look like that big a problem. For 90 per cent of the market there really is no issue here. The average person goes to the registrar, they buy their services, stuff is signed, it's all bundled, it all works, and it always will. The problem there is getting the registrar to support DNSSEC in the first place. If they're willing to do

that then they're fine. So in many ways you're dealing with 10 per cent of the market or 20 per cent - whatever your favorite of the 80/10 kind of thing is, and now you get into discussions about absolute numbers.

How big is that market? The important thing here is that there are a number of significant players in the DNS operator market. There are a number of large enterprises in the world. For some absolute number, these people care about this problem. This is a serious issue, and from a business point of view there's a lot of money involved here in this kind of problem. So would it only take a small set of registrars to do the right thing, as it were, and maybe everything works? Then you have to get to those registrars, you've got to get to those DNS operators. DNS operators are not the only part of the problem. We keep talking about DNS operators here, but enterprises themselves - people do this for themselves, or you do it for your friends.

You'd really like for DNSSEC to work all the time. I'll go back to the presentations we had this morning. We often talk in this Workshop about DANE, and DANE depends on DNSSEC, and even DANE is growing in the applications to take advantage of it too. This problem is going to be very serious; not just for the DNS but for everything and all the things that depend on the DNS.

SPEAKER: I just wanted to follow up on the 90/10 rule. I think it's naïve to do a count of domains. Look at it this way, not all domains are created equal. 10 per cent of the market in one measure is not 10 per cent of the market in all measures, right?

RUSS MUNDY: In fact, that was the exact point that I was going to make - that it's extremely hard to measure the value of a name, but it's my personal opinion that the highest valued names are the ones that tend to be operated by some of the folks that you see, the companies they work for, sitting at the table, because of various services and offerings that are provided. So percentage wise it might be small, but if you will, value and importance-wise it's probably quite large. But that's hard to measure.

SPEAKER: I think David started that right with his comment about the Alexa top sites. Maybe that's an avenue we need to go to, to do a survey to help with this point; is to be able to state that for certain areas, a percentage of Alexa sites are doing this. That might be a way to help us.

JULIE HEDLUND: Could I remind people - even those who have been speaking, like Russ and Dan, to state your names? Because there will be a transcription and I think the transcribers probably aren't going to know.

SPEAKER: [Elo Lance 05:19:40], .dk. I want to go back to Jacques' slide over there, and with one of those crazy registries that don't follow the model directly to the big annoyance of the registrars, one of the things we do have is the dotted line. There is a possibility for the registrants to go to us and assign a role of DNSSEC key holder and assign a third party - it could be the DNS operator, it could be whoever - to hold the keys, and

only the keys, and change the keys directly with the registry through whatever mechanism we have for that - in .dk, Denmark.

SPEAKER: Is that done via EPP, or some other…? Can you say? Not yet? Okay.

JAAP AKKERHUIS: Jaap Akkerhuis, .nl. The problem is actually very old, and it's already signaled by [unclear 05:20:48] in 2001, and basically he, by that time, took polls indeed in something similar like .dk, but has an extra function, which is the DNS operator authority. It's actually not due. I'm always surprised that everybody ignored it at that time. We spent quite some time trying to push this out, and only now it pops up. But I'm getting old.

GODWIN: My name is Godwin, .ky registry. I'm also an ICANN Fellow. I wanted to ask some of the registries that are here if they've implemented outer DS using the EPP protocol? Because we're working on something to automate our registrars, and if we can integrate that with the EPP protocol I think it might solve some of the outer DS records that we're looking at. I don't know if there's someone who's implemented it, without looking at the hosting? Because I've seen we've separated the hosting and the registrars, and in Kenya most of the registrars also have hosting services. That's why we are creating an API for the registrars, because it will point directly to the registry system. Thank you.

SPEAKER: Was the question: what registries have implemented some type of EPP system for registrars?

JIM GALVIN: I know that VeriSign has something similar. I haven't actually looked I your toolkit for the details, but I assume it's all there. We've provided a toolkit that registrars can take and use if they want, for implemented EPP, which includes modules to support all the DNSSEC transactions that go with it. As well as us for on our side, on Afillias' side, when we have a registrar and they become accredited and they're on-boarded with a particular registry operator, they get access to a web interface so that in fact the registrar does not actually have to do an implementation of the DNSSEC EPP transactions - they could do it manually because they're automatically given access to a web interface that they could use to deal with their customers for low volume operators.

So there are solutions that are out there that would… Let me just leave it at that. Thanks.

NAVEED: My name is Naveed. I'm from Pakistan. As DNS operators, when you talk about all this, are you guys suggesting that ICANN should start the process of considering DNS operators as part of a multistakeholder model? Or do you have a working plan that it can be done in a month or so? Do you see what I mean? I mean whether this process should start to happen or it can happen right away?

OLAFUR GUDMUNDSSON: I'm so glad that you stole my closing question to the Panelists. Those are exactly the questions we need to ask. In the current ICANN model I think it's an omission that DNS operators are not included in it, and we don't have a seat at the table. To solve the problems we've heard people talk about it here, so I was going to ask the question of my Panelists and others of A) how long will it take to devise a technical solution? And B) how long will it take to devise an ICANN policy solution? But yes, DNS operators need an access and we want to be able to do it within this framework, because even if we can make all of this technically happen, like in .ca and .in and other ccTLDs that are not under the ICANN umbrella, having a common solution everywhere would be good.

Some of these things we are talking about are also applied in other situations, like enterprises where there is geographical distributions and others.

SPEAKER: To a technical solution, we do have one that's out there - RFC 7344 CDNS key. A question would be… I saw the note on here that maybe it doesn't scale on all the cases, et cetera, but one thing would be that is a solution. A question I would ask is for registries or people out there, who's implementing it, or thinking who has implemented or thinking about implementing it? Can we maybe start building a list of those registries that are doing that?

OLAFUR GUDMUNDSSON: For .ca we're not doing any of that yet. The lines in the registry are there. We have data registry with DPP [unclear 05:26:27], so like I said, we're not going to scan the .ca zone and figure out what domain needs to change keys and update our registry with that. It's not really scalable. But the control we have is there with TTPN. So far that's the position.

SPEAKER: As a third of the editor on that document we admitted it would more likely be registrars that would be doing the checks, and whether they were doing it on schedule or open request is left for each entity to decide.

SPEAKER: Maybe the answer is that we don't have a technical solution with 7344 in the sense that it's not something that would solve this particular challenge.

OLAFUR GUDMUNDSSON: It's not the complete solution, and in Cloud Flare we are rolling out DNSSEC for our customers and every zone we will have a CDS/CDNS key in when they are signed, and they'll be in there until the parent replaces them, however long the transfer takes.

DAVID LAWRENCE: David Lawrence, Akamai. Just to address that issue too - on the IETF DNS op list there was recently a message that came up with the idea that this has the potential of fracturing between the big operators, the big registries, who might form some type of agreement to have big, fat

communication spikes between them - not in a physical, literal sense, but just in their business process. And to the extent that then CDS and CDNS keys still provide an additional way for somebody who's not a big player to continue on it, it's not necessarily that it's one or the other, we don't have a technical solution, it's just maybe this is a technical solution in one sphere that is not ultimately what it is for other people, because of some of those other scaling, polling issues and so forth.

JULIE HEDLUND: I'll read this comment out. There are two from the same person. These are both from Rob Golding and they're related. He says: "My experience as a registrar is that outside of the ICANN/RIR community no one knows, wants or cares about DNSSEC. Two registrant requests for around three years, .004 per cent of registrants. It is viewed as another way to slow things down so affects SEO/end user experience. Another way to DOS yourself, way too easy to get wrong/break. Another way to D-DOS others, reflection attack, and broken. The whole zone idea is outdated in my opinion. We've not had zones as such for over ten years. It's all been BD-driven from multiple source systems." His continuing comment is, "I.e. people aren't sold in it solving a problem, but see it as causing them."

SPEAKER: The comment is so noted, but we're here for people who want to solve the issue of DNSSEC.

ALEX [MAYOVER]: Alex [Mayover]. I was wondering, Jacques, you said you had an interface for registrars or for DNS operators already in your registry that allows the updating of the data? Or was that a plan?

JACQUES LATOUR: As far as I got is that line on the PowerPoint slide. [laughter]

OLAFUR GUDMUNDSSON: Any final questions?

DAVID LAWRENCE: I just wanted to add one additional comment, as far as nobody is asking for this. There are actually some pretty big people asking for this - not the least of this is the US Federal Government under the auspices of an executive order from the Office Management and Budget, that say that all of their domains are supposed to be DNSSEC secured, and so this is an issue that really affects them. No matter what you might think about the general market across domainers, parking a bunch of domains, maybe they're not as interested in this problem, but there are some pretty heavy weight sites that are involved.

OLAFUR GUDMUNDSSON: To follow up on that one, there are some of the new ccTLD domains that have a very strict DNSSEC requirements for registrations for something like .trust, .bank, .insurance and others. So yes, there are going to be certain market sectors where DNSSEC is going to be important.

RUSS MUNDY: I'd like to do a very slight reprise of our morning Panel of the ten-year anniversary of the Workshop. It's that about two years prior to that Workshop, Steve and I hosted an after-ICANN Meeting about doing DNSSEC within the ICANN realm of things. We had registries, we had a couple of registrars, and Steve and I at that point, our primary orientation was the IETF world. So you might say it was an IETF meets the ICANN. The first shock was that it was told to us, in no uncertain terms, that the registrars were an important and critical aspect of this, and secondly that the vast majority of names and name server operations were not conducted by the holders of the names - rather they were conducted by registrars.

So at that point there was a gigantic hole in the IETF specifications for DNSSEC about doing this whole flow we're talking about right here. The principle output we got from the registry operators at that time was - and this is 12 years ago - "There is no way in the world that we would ever be willing to accept a relationship with anyone except the registrars. It's just not structured for doing that." That's something I wanted to point out, to keep in mind, as we're going forward. This is along-standing challenge and it needs to be thought about in those terms, because that's the way that everything has been built from pretty much the beginning of the whole ICANN structure.

OLAFUR GUDMUNDSSON: Thank you Russ. Panelists, final words? If you can answer my questions about timelines, that would be interesting. Duane?

DUANE WESSELS: Timelines? I don't know. I'm reluctant to try to predict the future. I don't know.

SPEAKER: There are two timelines? Building a solution - that's not complicated to do? The policy pieces? It's going to drive the solution, right? If it's just EPP or something we can do stuff quickly, but it's figuring out how to make all the lines work well together that's going to be the challenge, and the timeline for that. After IANA, I mean.

JIM GALVIN: I think it's important in our discussions to separate our problem space into three things that I would suggest. Our Panel here started out being initially focused on a particular technical problem, and technical people should work on technical problems - the problem exists and we know it does, but that technical problem exists in a second category of problems, which is policy. There's a question of you need something, but how do you make it happen? Can you make it happen? Is there some kind of compliance structure that you can create? Those discussions have been going on for a long time and will probably continue for a greater length of time.

In the context of this Panel we've talked about the fact that the DNS operator - as a general term, not the business structure that some people have - they're not generally considered a part of the discussion in this ICANN community. That has created the technical gap that we've been experiencing. The third space of problem, which this Workshop deals with to some extent, and has over the years - and there are plenty

of other forums that deal with it - is the whole marketing and business decision. Part of motivating it is two things. One is the policy requirements of making sure the technology is there, but you also have the business side of it, the marketing side of it. Do the registrants need to know about it? Do the users need to know about it?

So you're talking about validation versus provisioning for things being signed. So three categories of problems, and in our discussions we have to be careful to focus on only one of them at a time - technical, policy and business. As far as timelines go, heck, I've been doing this for 25 years so your crystal ball is as good as mine, as far as the future is concerned.

DAVID LAWRENCE: David Lawrence, Akamai. I just wanted to basically echo what Jacques said. The issue is policy. Policy drives the technical specification because once the policy is determined the rest are just pushing bits, and we do the Internet, we know how to push bits - it's not hard. Once you settle on what the policy is, I'll turn around and write you the software in a week. That's the big hurdle.

OLAFUR GUDMUNDSSON: Thank you all. My hope, in organizing this Panel, was that we would be able to talk about things in a slightly different than has been done in the past, educate people about what's going on, and start the dialogue among the various parties that have to be involved in the policy process, so we can maybe do something good at some point in the near future. I thank you all for attending. I thank my great Panelists for participating,

and Julie and the Program Committee for giving me the small time slices. Greatly appreciated. You do a good job on that. Sorry about being late with the slides. [applause]

RUSS MUNDY: On the part of the Program Committee I'd like to say thank you very much and thanks to the Panel very much for a new and invigorating discussion that we need to carry on forward.

SPEAKER: I'd like to expressly thank Olafur for finally pushing forward with this, because this is a problem we've know about for a long time, and the reason we're here is because Olafur finally decided to do something about it. So thanks.

RUSS MUNDY: While Wes is getting set up, I'd encourage people… We didn't really get to talk here about next steps coming out of this, so I'd ask people to join this mailing list - the DNSSEC-audo-ds - so we can talk about what we do next and how we address this issue in this space, because this is really something that's obviously an impact for certainly large customers and people who want to do this.

JULIE HEDLUND: With that we're moving along to our next presentation. That's Unexpected DNSSEC Failure Strategies with Wes Hardaker from Parsons. Thank you Wes for joining us.

WES HARDAKER: You're welcome, again. This is going to be similar to my last one with a different topic in mind. This is designed to be a brainstorming session. There are better experts in the room about some of this material, so please pipe up if you feel you have something to add. One of the things that happens, let's say you go through my previous talk about how to do the right steps and how to monitor and manage to make things don't go wrong, what do you do when something does go wrong? That's key. The best thing to do is have a strategy in place. I'm going to go over your operational panic-binder - what do you do when things go wrong? We'll talk about some DNS failure strategies and some DNSSEC failure strategies. You need an operational panic binder really for both. A lot of people might already have one for the DNS side, and you might not for DNSSEC.

Then we'll talk about documenting your lessons learned a little bit at the end too. So good operators - and these are people that have been trained through failure, really - they realize that they need to have stuff written down so that when things go back they can reach up on a shelf and grab a binder that carefully outlines what they have to do, what commands need to be run so that they can do it as fast as possible when your brain is not working because you're panicking. So you document things like procedures and how-tos and what-ifs, and every time you run into a new problem you add pages to the binder so that your knowledge base is growing.

Then when that person retires you can hand the binder to the next person and information is already documented, written and transferred

and you don't have to try and train somebody within to weeks to know everything that's in your head. So you document everything. Bad operators, they just panic. They don't do anything else but panic, and then it takes time and then you work your way through the failure eventually. Everybody does get through it, but it takes longer. I searched for "panic binder" and it turned out someone's selling it. You can buy this. On Zazzle there's this account called [Love Teas Mugs], and they actually sell a panic binder. You can go and buy it and put your pages in it if you liked it. I like it. what goes in your panic binder? Whats' the point of it? What problems can you foresee? What problems have you had? All these types of concepts should go in there.

For DNS for example you have problems with your servers, one goes down. One of your servers is out of synch, which happens much more than I think people realize and is one thing you should monitor. You can have problems with your network link or routing problem. Those types of things affect your DNS operations too and ought to be in your binder even if they're duplicated in your routing binder. You could have problems with your parents. What if your data is out of synch? Or problems with your children. If your children are under a D-DOS attack and they suddenly want you to redirect their name servers to somewhere else because their link is slow, you've got to know how to do that really quickly for them too.

Here's an example page. They look like everything under the sun. They can be very specific like this one, which lists "You should SSH to the slave, run RNDC reload, if that fails then stop the service entirely and restart it, and if that fails…" So you can go through the series of steps and eventually by the end of the page you'll hit the part where it will

start working. Some people have much slower ones, "Just go reboot the sever." That's even better than nothing. What does your panic binder with DNSSEC look like? What should it contain? There's a number of new things. There's a number of things that may not be in there yet, if you only have a DNS related one. There's probably less than your binder already contains. Half of the problems with DNSSEC are related to just networks, computers, outages and links and stuff - so the content you're going to be adding is actually not as big as you might think it might be.

But as we talked about earlier, DNSSEC increases time-related problems, it increases the need for contact information. We talked earlier about how you really have to know your children and parents better. Do you have canned responses for your support staff? The people answering the phone lines saying, "I can't get to my bank.com's website," do they have a script to say, "We know that something is happening, we are resolving the DNSSEC-related issue right now"? All those things need to be thought about ahead of time if you want to minimize your impact. That's DNS true for all of them.

Let's go through some examples of DNSSEC stuff. We have signatures. What happens if your signatures expire? How do you resign it? What happens if your augmented software doesn't work? Are you able to go and do it by hand? Do you have the instructions for that immediately at your fingertips so you don't have to go and read manuals and figure it out? How fast can you do it? When you do so, how do you push out an update? How fast can you do it? Time is likely to be critical on all these steps. It's very similar to needing to update an A record quickly. If your web server needs to move very suddenly because you've had a machine go down, it's the same process. You've got to update that A record as

fast as you can. This is not new information, it's just at another time when you might need to run through that same set of steps.

How long until all the caches out there are flushed? Just because you've updated it, well, if your TTL is on your signatures and your data records and stuff, what's the longest length of time that your support operators will know you're still going to get calls, even though we've fixed the problem? You have to have responses for, "Your ISP is going to take a while for the data to flush the cache. It should take four hours at most." You can have a countdown timer - "You're down to one hour and 38 minutes left, sir." Again, are you testing for these kinds of failures in the first place?

So what happens if you have a missing DS record? What happens if you deleted your old and you forgot to update the DS record? How do you create the new one quickly and publish it to your parent? Do you have the website written down somewhere so you can get there? Is it an administrative request that has to go through some other channel? How are you going to get that key to them? How are you going to get that DS record to them? Similarly, how are you going to get it from your client? If you are the parent and you detect a failure, or someone calls you instead of your client, or somebody calls your client, how are you going to negotiate that with rapidity?

Again, how are you testing for this? How do you know there's a problem? Are you going to wait for the phone to ring or are you going to have a testing and monitoring procedure in place so that you'll detect it before the phones start ringing? I can tell you which one is better. What about compromises? What about somebody stealing your keys?

How are you going to fix that? This is the big one - this is the panic scenario that everybody really worries about. What happens if your keys get stolen? How are you going to generate new ones? How do you update them as quickly as possible? How do you put them in place and update your parents? How are you going to resign with the new ones?

This is a scenario where you really need to know your software in and out. Whatever you're using to sign your zone and generate keys, this is not something you want to be reading manuals about. That's not something you want to do quickly. How long will it take to propagate? Again, all these types of situations are very similar - how do you have contact information for your parent so you can push their hot bottom? If you're an important client, they may be willing to jump for you a little bit. Is anybody using your key as a trust anchor? If you are a TLD of any kind, especially in countries where you could imagine government offices and things like that that not only have the root zone as their trust anchors, they might have your country key as well.

If that's the case, how are you going to push that out really quickly to all the people that might have it? Unfortunately, it's one of those things that you can't know; if someone's using you as a trust anchor, unless they've told you. RFC 5011 documents how to roll keys slowly to make sure that everybody can follow your key roll and switch their trust anchor, but that doesn't work in the case of a compromise, and it does talk about that a little bit in the document. Again, this is not necessarily super new. It's very similar to a very fast NS record change. In the same way that your DS record is pointing to your existing key, well your NS record is pointing to your existing name server.

If you suddenly lost your network where your name hosts were being served from, and you had to move it to a new IP address, it's going to be the same sort of problem. These are not new, it's just you have to realize how to run some new commands for new material. The update mechanism is very similar. Again, are you testing for these key mistake changes? If you make a mistake, will you know ahead of the phones ringing? There's also other things like algorithm issues. Unknown algorithms with some important validator out there. There has been cases where, especially like Google's name service for a while, validating 8.8.8, we didn't know one algorithm, and some major people got together with them and it's all been worked out now.

But they initially were starting to roll out some pretty major changes using an algorithm that Google didn't use, and they found out pretty quickly that that might be important; that everybody's using that algorithm. What are you going to do? And what are you going to do when the phone rings and you find out that there is somebody out there that's running a pretty major infrastructure that can't change overnight? Are you going to explain to them the need to upgrade? Or are you going to push an additional DS record for them just to make them happy? Because you can have more than one DS record. You can have one with [shar 1] and one with [shar 2] IPv6 and things like that. There's ways of publishing more than algorithm.

What if an algorithm is broken? I chose the worst one. What if ECDSA suddenly dies? Do you have the ability to generate new keys and new signature types really quickly, and to change your infrastructure quickly? Do you know how to do that if something suddenly comes out in the crypto world that nobody was expecting? Learn how to switch quickly.

This is an example of some interesting binder materials. Victor Dukhovni, who's the person who authored the DANE SMTP draft, he has had lots of people come to his website and test their DANE SMPT deployments. The really good thing about the DANE SMTP world is that it's getting really high pickup.

There are 1,000 enterprises and major zones that are now using protected email over DANE and SMTP. Compare this to the web world where there's less than 1,000 - and the specification has been out for years - the DANE SMTP draft is not yet a full specification and the ramp growth is going through the roof. Everybody's wondering what the magic bullet for DNSSEC is. It sure looks like DANE SMTP might be it. Hopefully it might be published soon. Anyway, this was Victor's top ten list of things that he has seen; operational mistakes that people have made, and they're not in any particular order, and again, they're Victor's, not mine. But the number one on here is that DANE and DNSSEC is seen as a fashion statement. This is his personal pet peeve; that people sometimes do stuff to look cool and then fail to follow it up with operational practice.

In this case, you fail to have the binder ready, you forget to resign, you forget to change your TLSA record - it's just because you did it because it looked popular at the time. Do make sure that you're ready to go - not only now but as time rolls on, for anything in the crypto world that you want to do. There are failures of automated signing. We talked about that before - where people are failing to resign their zones on time. There's failures to upload the TLSA records before updating the cert. Sometimes people roll their TLS certificates and then they think, "I have to go change DNS." It has to be the other way around. You have to put

the new one in the DNS so that people can get to it, before you install it on your server. That's a really common one.

The other common one is that DANE TA says you're not pointing at your certificate but you're pointing at your parent certificate. One of the requirements in the document is that the server has to be configured to send not just your certificate but your parent's as well - otherwise the DANE algorithms have no way to match things up. Sometimes that doesn't happen and that's actually a hard one. There's unsupported types. There's incorrect data in there that people have hand-typed some parameters in the TLSA records and got stuff wrong. Not every implementation of Postfix has TLS so you publish a TLSA record that say, "I promise I can do authentication and encryption. "

When you publish that and your software doesn't support it on the other side, people won't talk to you anymore. So make sure that your Postfix is 2.12 or greater. That's where they started including TLSA support. Actually, STARTTLS is earlier than that, fortunately. On the receiving side you don't have to support TLSA. Firewalls filter out TLSA queries. This has been the long bane of DNSSEC - that packets are dropped because they're too big or there's types in them that don't recognize. If you have intrusion detection or some software in the middle that's doing active stuff for you, make sure it's up to date and that you talk to your vendor to make sure they're not going to be dropping stuff that you suddenly need, because it's new technology and they haven't implemented it yet.

Then of course there's broken name servers or not complete implementations. These are the things that he's seen in lots of his

testing, and as I said, he has 1,000 people that are up and running. He's testing a couple of hundred thousand domains. It's up since the last time I looked. There are a lot of people doing automated stuff. They're testing domains that don't even have TLSA records, but somehow they're chugging through it on his site. You can find a lot of that data on that website there, tlsa.info. What else? Here are the pages that ought to be in the front of your binder. I don't care what your problem is. These are the pages that should be in the front. How do you talk to your parents?

If anything goes wrong with any of your stuff, probably 90 per cent of the time you're going to have to make a phone call or visit a website. Where's your account information? Where's your login or your password? Especially if you're sharing stuff across multiple people, because your registrar doesn't support multiple accounts. Where's the support contact? Do you have a special hotline because you're super important? What about your client? Do you have a paper list of your client DNS stuff if you need to look it up quickly because stuff is out of synch? Do you have a list of their name servers, either electronically or in some other method; so you can look up and verify stuff as fast as you can? Do you have contact information for your clients?

Most parents do not keep a list of email addresses and phone numbers for their clients. Lately that's improved, but if you go back even six years ago I think most parents would have no contact information for their children. So it's discussion time. I deliberately left stuff out. There's no way I was going to put it all into one presentation. What else do you guys thing is stuff that ought to be critical and go into the binder? What scares you the most? What are the ones that you're not sure how to do,

or that you do know how to do because you've run into that problem? Anybody?

DAN YORK: We've been in here for six hours. That's the issue!

WES HARDAKER: Okay, start panicking and freak out. That burns up the energy level. All , well, if there are none then I'll end early. Any last questions?

DAN YORK: Thank you Wes. Before we start talking about pieces here a bit, I do want to again note a thanks to the sponsors who are here. I see several of them in this room. From Afillias, which Jim who was here earlier, Jacques in .ca, DINE, they're around, .se, and SIDN, Cristian was here - I want to thank the sponsors because they have been vital in helping us continue to do this project, as well as Comcast and MBC Universal and MBA who helped with the implementers gathering. I also definitely want to thank Julie. I want to give her a round of applause on this. What Steve said earlier about the Program Committee is very true. We have a weekly conference call every week from now until the next time, every Wednesday at ten o'clock in the morning on East Coast Time we're on this call where we're talking about what's next for this session.

The Members who are part of that, it's a chunk of time, and Julie is the glue that keeps us together on doing that, so the support you provide Julie, it's there to do that. I also want to thank Kathy, who's joining us in these last two Workshops. Thank you Kathy as well. She's on the email

list, so she gets the email that we all get around all this too. We're always interested in people who do want to help more with these sessions, so if you're interested in being more involved, please do let us know, which brings me to my next point.

Just as we're ending this session we'll start to get prepared for Buenos Aires, for the next ICANN Meeting at ICANN 53. I've already had a couple of people offer suggestions of what they'd like to talk about for the next one. If I could pick on him, Cristian suggested that we ought to have a Panel around validation; getting more validation deployed within their country, region, things like that. Cristian is interested in being part of that Panel, so we'd be looking for others who might be interested in talking about what you may have done in your country, region, whatever, to help encourage validation on the validation side of things. That's certainly one area where we'd want to see much more of it happening. Anybody here interested right now? Jacques? No?

SPEAKER: Dan, you did say about the mailing list. Did I miss that you said what the mailing list was?

DAN YORK: Yes, I did earlier. For the other thing, this operator's issue, it's…

SPEAKER: I meant the mailing list for coordinating the Workshop?

DAN YORK: Well, that's a private mailing list for the Program Committee, but we are looking for more people who might be interesting in being part of that, so if you are interested find me and I'll be glad to talk to you about doing that. We're always looking for more folks who may want to help us with the ongoing creation; which a lot of it is figuring out what we want to offer the next one, what makes it different from the one before, and also finding the Panelists and speakers and people who might want to be part of that, and reviewing proposals. We put out our call for proposals, we got all these proposals back, and we try to accept as many as we can within the space. Sometimes it involves going back to the folks and saying, "What did you really mean by this?" or, "How do we think these might fit together to make something that's interesting for people who are there?"

The other thing is I have to complement Wes. This is the first DNS Workshop where we've had so much discussion about parents and children, and rules between them. We were having little side conversations over here about parents and… The other thing I noticed in Wes's presentation was you were talking about resigning stuff and resigning stuff, and I saw this in someone else's presentation too. We're all DNSSEC geeks in here, so when we see that we think about resigning, but someone else who's just reading that may look at it and say, "You're going to resign?" Maybe we should put another dash in there or something? I don't know.

Anyway, with that, I think that's my major comments on that, so let's come into the "how you can help" that we like to end with this session. Do you want to say something? All right. We like to say for TLD operators, the things we'd like you to do when you go home or come

out of here is sign your TLD. Let's get more of these. Let's fill in the rest of that map - especially on the ccTLD side. Let's fill in the rest of that map with green. This part here - accepting DS records - it sounds silly but that's a key part that needs to happen, and working with the registries.

Another piece - helping with statistics. One of the things we talked about is we've got these nice maps of TLDs, we have the validation maps that Geoff does through his magic Google Adwords thing, and we have a number of different statistics sites for second-level domains. We can get a lot of it for the new gTLDs through the centralized zone database, so we can know how many are signed, but we are looking to try to understand how many domains are signed at the second-level. So if any of you are TLD operators, if you have a way to expose those statistics; the number of signed domains, we'd ultimately like to ideally get to some dashboards that we can show that do it.

Some folks, like the PowerDNSSEC guys, they have some nice charts for some of the European ccTLDs. We'd like to get that in a larger range. Anyway, next slide. Zone operators, again, working with registrars, try to work with that. Help with statistics. Network service providers - we really want to see more validation happening. I think one of our goals for 2015 is we'd like to see Geoff's chart, that shows about 12 per cent validation, we'd like to see that increase much more by next time. We'd also like to see more service providers helping support DANE and that also means in provisioning interfaces too.

Website content owners - this is one we've been working with a bit but we're looking to do more, but quite honestly we have some

infrastructure things before we start promoting this widely, including the fact that a lot of website content owners, the biggest ones, wind up using the CDNs and the other DNS operators we just talked about in that past Panel in there. But we're really encouraging people to go and do that, and asking people to go out and deploy validators. One more? Yes, everyone: use DNSSEC! Share your lessons. We're always interested too in different kinds of presentations here. You had Wes providing a nice tutorial in this last one about what to do in your DNSSEC panic book, which is a nice thing that we haven't had that type of thing before.

We didn't really have much in terms of the tutorials here, but we're always interested in that. We're also interested in case studies. I enjoyed the fact that we had the ones in the Regional Panel this morning, including the man from sgNIC that said, "We're not there yet, but here's our plan to get that." Xiaodong Lee, a couple years ago, came here with his presentation where he talked about how China was going to sign .cn and he walked us through the process he went through. Those were extremely valuable for other folks out there. I wanted to give a special round of thanks to everyone who participated today.

I want to say thank you all for coming. A few of us will be around a little longer. We'll see you in Buenos Aires. Please get your thinking caps on for what you might want to present, if you're interested. Thank you very much.

JAAP AKKERHUIS: At a previous Workshop, do you remember the talks about the RIPE Atlas Probes measuring system? I actually have some with me, so if

people want to have a go at joining the Atlas please talk to me and we'll hand them out.

DAN YORK: Jaap has got Atlas Probes, so if anybody wants to take an Atlas Probe home with them and deploy it in the network back wherever they are, the Atlas Probe system is a wonderful system that's out there, that's helping us do measurements, that RIPE NCC uses. It has this little probe and you just plug it into a network and then it gets linked back into the Atlas network. Jaap's got about a dozen probes and he's glad to give them to people to take home. Put them in interesting places, yes. Two in your own network doesn't matter. Yes, we'd like more in various different coverage areas that they don't have them in. Africa, anywhere.

JULIE HEDLUND: We have a question in the chat. This again is from Rob Golding: "Is there a DANE primer, high level rather than techy, document that can be shared with business to explain why they need it?"

DAN YORK: Thank you Rob. The answer is we don't have one at this precise moment, but stay tuned. That's one of my persona projects for this year; to do a bit more with helping us get some materials out there for DANE. On that note I'll mention too: many of you know I'm employed by the Internet Society in large part to help with this kind of advocacy and promotion of DNSSEC and DANE and pieces like that. if you are looking for a piece of material that helps you explain something, like Rob just asked, please feel free to contact me. I'm at york@isoc.org. Part of

my mission is to either find or create that kind of content. So to the degree that I can help you, I'm a resource. Contact me.

Somebody else asked me today about how they can get started with doing this for their ccTLD, and I'm glad to help point them to resources. You're streaming? Where are we streaming to? To Kenya? Greetings Kenya. What?

SPEAKER: I want to add one thing because I don't think we've done it. We haven't thanked Dan yet. Way to go. [applause]

DAN YORK: Thank you all of you, and we'll see you all next time.

[END OF TRANSCRIPTION]