BUENOS AIRES – DNSSEC Workshop
Wednesday, November 20, 2013 – 08:30 to 14:45
ICANN – Buenos Aires, Argentina

UNIDENTIFIED MALE: Wednesday, November 20, 2013, 8:30 to 14:45, DNSSEC Workshop.

UNIDENTIFIED FEMALE: Good morning, everyone, to the DNSSEC Workshop. We're going to start momentarily. We do want to try to stay on time today. What we would just ask is to preserve the front seats here for the panelists. Otherwise, please do come up to the table. Particularly, we do want people at the table in order to facilitate participation. So anyway, we'll start momentarily and thank you all for joining.

JULIE HEDLUND: Good morning, everyone. I hope it is a good morning for everybody. Thank you very much for joining us today at the DNSSEC Workshop at the ICANN meeting in Buenos Aires, Argentina, on the 20th of November 2013. We're starting late, but I think we'll be able to catch up the time as the day goes on.

To start with, as usual, we are very pleased and fortunate to have with us Steve Crocker. I hope all of you know Steve. He is CEO of Shinkuro and he is also the chair of the ICANN Board of Directors. Without further ado, I would like to turn things over to Steve.

STEVE CROCKER: Thank you very much, Julie. It's both a pleasure and somewhat of an embarrassment for me to be here. I was reflecting back on the origin of this sequence of meetings, which I think has been anybody crucial in facilitating and fostering the adoption of DNSSEC across the world.

I first got involved with ICANN as chair of the Security and Stability Advisory Committee, and one of the topics that we took up within that committee was the need to push forward on DNSSEC. We had a number of discussion sessions and so forth, and one of my colleagues, Bruce Tonkin, took me aside and I was trying to remember exactly when it was. It was after the Tunisian meeting, which was early 2000 when he said, "Enough effort. We've got to make this bigger. We've got to separate this off and make it a bigger project."

In short order, we were able to do a number of things. One of them was to create this sequence of sessions separate from the primary track that SSAC runs along. This has really been a stellar effort with – you see on the screen there a list of people on the Program Committee. We put a lot of work into each and every one of these sessions. There's a standing call once a week of the Program Committee. Canceled a few of them, but that's the basic pace that this runs on all year round looking ahead at the next meeting, and oftentimes looking two meetings ahead.

Julie runs an absolutely incredible operation. If you have a small country that has a military that is not in working order, just invite Julie down. The country will not be the same when she leaves. I've now gotten involved in the political side of ICANN and I get less time – much less time – to stay focused on these kinds of topics. So I'll apologize now that

I'm going to have to run off. Let me back up, if you would, to the title slide, to the previous one, and acknowledge the sponsors that we have.

Just going around the slide from left to right, Afilias, GoDaddy, dot-org, dot-se, dot-ca, and VeriSign. There's no such thing as a free lunch. These guys are the ones that are paying for your lunch today. The sponsorship is much appreciated. We may need to pass the tin cup around and expand the sponsorship over time.

Moving forward. We also held – and again, this is something that I regret that I wasn't able to attend. I'm interested in feedback actually. How was this, implementers? Was there good beer? How many people came? There were probably a bunch of people who came who aren't in the room at this early hour. Again, sponsorship helped. Then we have [inaudible] for Canada, ISERVICES Systems, JPRS, NIC-ar our host for the whole conference here, and NomiNet.

This is actually another very interesting piece of history in the sense that this meeting here that we're in was the original form, and then over time we added DNSSEC for beginnings, and then added after that this implementers gathering. So that's a maturation of getting more fully fleshed out and in a broader reach.

The evolution of the process here is one of the positive things. It happened a lot by people who have come to these meetings and said, "Gee, here's an idea that I think you could have," and [inaudible] response is, "You're now on the Program Committee." We've been very fortunate to have very positive responses from a growing set of people. So it hasn't just been the same old people with the same stale ideas getting in a rut. So that's been very helpful.

Let me move on. So here's the program for the day. Color-coded [inaudible]. The green area – the more green you are, in a sense. Novice, very green. Intermediate, less so. And expert, appropriately grey and fading. I think we'll just move right into…

One of the things that I've been doing as part of our day job at our small company, Shinkuro, is we've been heavily involved in trying to look at some of the gating issues for DNSSEC deployment and also tracking a number of things.

We have a database that we keep expanding that has the status of deployment in the top level domains. That's been our focus. Next slide.

We keep track. We ask five questions of every top level domain operator who shows any signs of being interested or moving along the track toward DNSSEC deployment. These five questions have evolved over a period of time. The five questions have answers that are dates.

The questions are when do you plan to (or when did you, depending on whether they've already done it or haven't) enter experimental mode? Experimental mode means laboratory experiments or any kind of technical activity within the TLD, not necessarily visible and not necessarily part of an operational system. And there's no direct way to check on that, except to ask what their plans are or to ask historically when they did it.

Similarly, we also ask, "When did you (or when do you plan to) announce that you will in fact deploy DNSSEC in your zone?" That is important because it represents a commitment – a public commitment

– from the organization, and almost uniformly sets the clock for when it actually happens.

Now, that question is not designed to ask when it will actually happen. It's only a question of when the institution made the commitment, which in my view is an important milestone.

The next three are the various stages of actual deployment in a way that is visible on the operational system. So the state we call partial is the zone is signed, but not taking delegations perhaps or not otherwise in operation.

The next stage is DS in the Root, which is the same as partial, except that the DS record has gone into the Root. We didn't start out with that, but when there were enough TLDs in operation, we wanted to be able to reconcile our database with what was observable in the root zone. The transition is usually fairly quick from partial to DS in the root.

Then, the last state, operational, is fully up accepting delegations from subordinate zones. That's not easily detectable. The first two – partial and DS in the root – are directly measurable, but operational requires interacting with the operator and hearing what they have to say. Next slide.

We keep the databases up to date as we can and we take a snapshot once a week and pump out some statistics. These are our statistics as of a wee and a half ago. We subdivide things in two dimensions. One is primarily the g versus the ccTLD dimension, but we have a small little sliver for SU and EU, which are operated under ccTLD rules but don't correspond to a single country or territory, so we've called those

regional. The point here is anybody else who does measurements, we want to make it easy to compare the statistics.

The other slice that we make is classic versus IDN, where classic means the ASCII strings that used to be alone. We had another category that we reported on regularly, which was test TLDs. There were 11 IDN test TLDs in the root zone and they were decommissioned and taken out of the root zone, and so we just folded that down.

So what our numbers show here – oh, and what these numbers are measuring is the visible numbers as of that date. That means either they were DS or operational, so this means at the very least they had a DS record in the root.

So we're showing 108 out of 313 as the lower-right box in the total. So 108 have DS records in out of a total of 313 that are in the root zone. And then the various subdivisions there. Next slide.

And then we map all of this using the color coding. Well, I guess the color coding is slightly different from the one that I had on the front. We evolved this over time. The good news is that there actually is quite a lot of various shades of green there. Oh, I remember. We changed the color coding because through Dan York making a pointed suggestion.

Russia takes up a lot of space. Canada and the U.S. and Mexico and Brazil over in the western hemisphere. We'll go zeroing in on this in a minute. But this is the basic picture that we have. Again, these are all measured as of November 11th, a week and a half ago. Next slide.

This is the same data with a somewhat different presentation. We have this available in a PDF that one can zero in on and get much finer details. It's always available if people want it. Next slide.

Region by region, I'll just take you through the five regions. So this is the map of Africa. I guess it's not a surprise that it's not as fully filled in as some of the other regions.

On the other hand, it is quite heartwarming that there is as much activity as is shown there, and my expectation is that over the next year, this will become a lot denser. I'll just hazard a guess. It's very hard to get accurate data about the future, even though we ask. What we found is what people actually do very often is the head of what they said or different sometimes [inaudible]. It's much easier to get historical data. So I'll just hazard a guess that we'll have between 50% and 100% more countries filled in in some fashion a year from now. Next slide.

Here's the North America, which is simple. The North America region is really just – [inaudible] the way the regions are described, it's just really the U.S. plus Canada. I'm not sure there's much else in there. Next slide.

Here's the region we're in. We have Brazil, Mexico, Chile, Uruguay, Columbia. My geography is a little weak. What is the country that is nestled on the top of Brazil there? No, Costa Rica is up in the – yeah. Or one of. Yes, that's my problem too. Then you have in Central America some countries. Next slide.

Here's the Asia-Pacific region scaled down so we can get the whole scope of it. India, China, Mongolia. And even over on the left you have Iraq and Iran moving forward and Australia coming alive and New

Zealand has been in the root for a long time. And of course Japan, one of the leaders in the whole field. Next slide.

And here's Europe, which is in pretty good shape. Good enough shape that the ones that are not complete are the ones that are standing out, but this is rapidly filling in. I think that's about it. Is there another slide? No. Oh, sorry. There is important things.

So we have relatively recently put emphasis on DNSSEC history project. And when I say "we" let me back up a bit. The Internet Society has a program called Deploy 360 which focuses on important technologies that need to be adopted. Am I mangling this too badly, Leslie? Is that a decent description? Jump in and correct me when you get a chance here.

One of the details is now we've been working closely with the Internet Society on DNSSEC deployment with Dan York, and then one aspect is to try to capture what the history of the DNSSEC deployment effort has been DNSSEC started in the early 1990s, so we're rapidly approaching a quarter century of activity on this, which is surprising and a little bit daunting that it's taken that long to get here. Am I doing your slides?

UNIDENTIFIED MALE: You can keep going if you want, Steve.

STEVE CROCK: No, nope. Don't want to do that. We'll just segue over. I'll pause here. That's my set of slides on what the current coverage is and a little bit of retrospective on the effort here. We've tried to structure the program

at each of these meetings so that we cover both a current set of technical issues and also a spotlight on what's happening in the deployments themselves with extra emphasis on activities within the region. And it's intended to be a highly interactive session here. So with that, I'll stop. I'll be happy to take any questions, turn the floor over to Dan. I need to leave in a minute or two because I'm not just double booked today, but sort of triple booked in various times. I apologize again.

DAN YORK: Thanks, Steve. I'm Dan York for the remote participants. Just to emphasize the great work that Steve's team has been doing to come up with these statistics. I will also mention that in partnership with Shinkuro, we're publishing the DNSSEC deployment maps on our Deploy 360 site. So if you go to that, to internetsociety.org/deploy360, there's a link on the DNSSEC side for maps. And I realized this morning, it's not on the menu. It will be shortly, but there's a menu choice. You can pull down there and get to them. But we are publishing these maps. It's actually just deploy360/dns/maps and you'll see these maps. And we're publishing them periodically, whenever there's a new set to go. Julie, why don't you go on a page?

It's actually appropriate, Steve, that you were introducing this because it was actually an e-mail from you that began this project back in 2010. I was not involved. I joined the Internet Society in late 2011, but this happened before then when there was an effort made to go and capture some of the history of how DNSSEC was created, with the idea being partly just for historical record to understand what happened,

what we did. But also as a way to capture lessons learned for people who look at going and developing protocols and developing systems like this that would use DNS, etc., in the future. And not just DNS but in general.

So the purpose, as it mentions there, is the document, the ideas. It's at this URL. It's a wiki that's up there. There was a substantial amount of work put in in 2010 to go and create this. A lot of content was poured in. A lot of people contributed. And then as many of these projects go, it kind of tailed off for a while – for a long while. And then we've been working this last while to start to get that back going. We had a number of good suggestions and resources sent to us from people in this room. Julie, I think you can go to the next slide.

We're open to people participating. Please take a look in there and do it. You can just send an e-mail to the address there, the dnssechistory@isoc.org and we can set you up with an account to go in and edit directly in there. If you've got some content but you don't feel comfortable editing in the wiki we're open to that as well. We've received some pointers to that. We'd like to make this a solid repository of content. The end goal may be to turn it into more of an e-book type of thing or PDF in some way that can have a stronger narrative and go through and explain really what happens.

We're also looking to add some multimedia aspects to it, too. There's been some interviews with people and some other pieces that we'd like to kind of stitch into this to really show, to bring that to life in a different way.

So that's the DNSSEC history people. We'd love to have your help. Just see me while I'm here today or send us an e-mail, and we'd like to get you started. More people editing would be great.

STEVE CROCKER: I just had a thought while we were listening to you and plunging through this. We should set it up so that each person who's been involved has a place to jot down what the history is of that person's involvement or the history from that person's perspective. Every [RFC] has a little section called IANA Considerations and another section called Security Considerations.

What goes in there varies wildly from one [RFC] to another, but the mere fact that those sections exist triggers a lot of things that wouldn't have happened if there hadn't been anything. So we ought to have a little section that's just DNSSEC history for the contributions for everything, and then that will generate a bunch of raw material which we can then mine and gather from a personal perspective, without necessarily trying to be comprehensive.

But I think that having everybody feel that they're part of the history and that they can say something I think may be important. And even sort of taking a page from our emphasis on multi-culturalism, write it in your native language. We'll be able to gather all that.

DAN YORK: Thanks. It's a good suggestion, Steve. And like I said, it's a wiki. I'm glad to give anybody here an account to go in there. I'd love to have people just contributing notes like this even. If you want to just go in and create

a page that you're just dumping in your own notes, that would be great. So [inaudible] and that's the end of this.

JULIE HEDLUND: Thank you very much, Steve and Dan. And please join me in thanking them for all of their wonderful work. [applause] And now I'll ask the panelists for the regional update panel to please come fill around the front.

Welcome, again, everyone. We are going to move to the panel discussion. Before we do that, though, let me just mention lunch for those of you who manage to last that long – and I'm not suggesting that it's a long hard slog or anything. Your program that you should've had either in front of you on the table or on your seat, on the other side of that is a ticket to lunch. If you leave the room, be sure to hang onto that. Lunch will be in the room, so if you manage to stay here and you're in the room, you get lunch, so that's your reward. There will be some tables set up outside as well. We will, again, try to keep on time. But I'll mention this again as more people come in the room. Do hang onto your lunch ticket.

Now I'm just going to bring up the slides for the regional panel. We also have Luis Diego Espinoza who is joining us remotely and we'll be getting him on via Skype. Also, unfortunately, Oscar Robles from dot-mx has had to go back to Mexico. He won't be able to join us this morning, although we do have his slides available in the Adobe Connect room and online. Sorry, I see my Adobe Connect quit.

And then those of you who wish to use it, thanks very much to Luciano from dot-ar. We also do have simultaneous translation, and there are some devices around. I know that Luciano will want to give his presentation in Spanish and also that others may wish to do as well. So just one moment. I have to get the Adobe Connect room back up.

UNIDENTIFIED MALE: Luciano, do you want to just as the panelists to just give a short identification of who they are and their affiliation, since we'll need to do that anyway, while Julie and the tech people are working on getting the room back up? Will that be okay? Thank you.

LUCIANO MINUCHIN: Good morning, everybody. I'm Luciano Minuchin from Argentina. I would like to introduce the rest of the panel members [inaudible]. And I will introduce the other members of the panels that will talk about DNSSEC in Latin America.

We have Cristian Rojas from NIC Chile. Gonzalo Romero from dot-CO. We have Carlos Martinez from LACNIC. And we also have remotely Luis Diego Espinoza and he will join us in a short while.

Okay, let's start with my presentation. There may be some technical problems. We all know about that because we are all technicians, so this happens. Let's wait a few more seconds.

Okay. We are part of the Legal y Técnica secretariat of the president's office of the [Argentinian] Republic. There you have our e-mail, so if you

want to get in touch with us. Gabriel Brenta is the CEO of the computer systems.

We're going to tell you about the history of NIC Argentina and DNSSEC. When the people at ICANN proposed us to talk about DNSSEC, we had certain doubts and we wanted to tell them what we were able to talk about. NIC Argentina is quite an old entity in the region.

Here you have some historical data. It's one of the oldest in the history. We turn 25 years old this year as a registry and we were one of the first ones in the region. So it took lots of time. We made the first Internet connection in Argentina from the Project Ministry of Foreign Affairs and then the official registry was created.

But during that time, we kept on moving in the technical field [inaudible] was maintained. In 2011, the president's office decided to introduce a change in domain name registry. And so from the Ministry of Foreign Affairs, it was directly transferred to report to the office of the president, because that is what the president thinks that it is very important in Argentina and in the world.

It is also important to point out something. In 2011, the National Domain Name Registry was created. Since then, we have been working controlling the operation. But there you can say August 2011, but it was August 2012, and we took over the technical control. So we changed completely the platform including anything that you may include when you do a migration.

Here we have some details of what we had to manage, which was our road ahead. Currently we have 2.4 million domains for the region, which

is really very important. As you can see, most of them are dot-com, dot-ar. That is what happens in most of ccTLDs.

But in Argentina, we have the largest [proportion] of domain over total population in the region. So this is quite significant. Perhaps this is what makes the difference without a ccTLD. Our ccTLD is for free.

When we took over this separation, we asked ourselves, "Why DNSSEC? What are the benefits of DNSSEC and how to implement it?" We participated in several forums [inaudible] LACNIC, LACTLD, ICANN. Several regions. Everyone was talking about DNSSEC and said we want to make some research about that. We are quite a significant registry and we have to be updated in that technological process.

So we took a definition that was how to arrive in DNSSEC. This is a technology to be applied to the DNS, but in a ccTLD, this has an additional value because it's part of the value added to security. So we took certain definitions that we defined [inaudible], an ecosystem in general including everything related to data validation regarding users. We thought it was important to have this process in a sequence, in a [staged] manner. So we had an old technology where no DNSSEC was available, was [inaudible] other technologies that perhaps we were willing to introduce.

So we needed some legal and formal framework for it. DNSSEC is the last link in a chain of giving value, giving value added to our users. So we started with data validation. That was the very first link in the chain.

So there was a change you need not to be a registry or have technical data in your page, but now we request people to validate their data as

persons or as companies based on individual registrations and standard registrations we made in our country.

So we believe this will end in DNSSEC. It's not just the technical issue, because certainly we may find the zone and the correct domain but it will give us a name, and the name will be the right name, the correct space, but we do not have the information or what happens before that final link so we don't know whether the data of that domain are validated, whether it completes and complies with the legal framework and all the standard samples applicable in Argentina.

So to start with this journey, we have to make a significant investment in technology. We upgraded all our hardware platform, changing 100% our platform at the level of security, service, storage, everything. We have to change infastructures for all sectors and then we were able to update our DNS versions that [inaudible] or DNSSEC. Within the process, we also decided that we have to have [inaudible] networks.

So we needed in the region a diversified operation, so we decided to hire suppliers that might provide DNSSEC services distributed all around the world.

Within this process, we also defined to be a recursive DNS service provider, particularly for the government areas. You can see dot-gob.ar. GOV is a different "V" than the one you use. This is a definition taken in Argentina. They used to have the GOV with the short V and then we decided to shift it to Spanish and to put the GOB with the other "B" that is the translation of government.

The main topic within the ccTLD was a security issue. We are focusing on that. We are focusing on security. DNSSEC is related to security, so we need to focus on providing the service on the government domain names because we depend on the president office, and this is for us the most [inaudible] and we can provide security to people who would like to enter data, provide critical information, personal data, in certain governmental webpages. So we want that to be validated.

We also have dot.tur.ar and this has to do with tourist agencies. We have a lot of online traffic, many invoicing processes and the purchase of touristic packages, so that should be within the [zone] to be assigned.

We also started working with financial institutions from the political point of view, and we started working within the banking system. Now the whole banking system is signing the root zones with the DNSSEC and this helps us to address the phishing issue within Argentina.

We are now deploying different and studying different models. We are understanding different models and participating in different issues together with Brazil, Columbia, Chile, Mexico, and Costa Rica. They have models in which we are interested and we are trying to see which of them we can adapt to our idiosyncrasies and our way of work given the size we are now managing in our zone. We want to work with this region and models.

We are interested in moving forward on the DNSSEC issue and this is a [inaudible] request from our perspective. We want to have the collaboration of everyone. We would like to receive the input from everyone interested in working with us in this project and to move forward with the DNSSEC project in order to sign our zone. We believe it

is important not to reinvent the wheel, but to take the best examples and best practices to important the DNSSEC in Argentina and to work together with other actors in the regions and with other ccTLDs in the world. I think we need to achieve a joint work. So thank you very much for your attention. [applause]

If there is any question, you can ask it.

UNIDENTIFIED MALE: You mentioned that you are offering recursive DNS to some government organizations. Are you validating the other side of the DNSSEC? That is one of the projects we are now undergoing. Any governmental action has a theoretical framework that should be implemented before getting into the technical aspect, so we are now working on the theoretical framework and we're working with the technological organization within Argentina and the governmental agencies.

We offer that as a service. We have a technical [inaudible] the government agencies are very interested in this and I think this is a short-term project and we want to finish this for the very beginning of next year.

UNIDENTIFIED MALE: In your presentation, do you have a timeframe for when you expect to see DNSSEC implemented in that?

LUCIANO MINUCHIN: Yes. We have an objective and we want to start signing the zone in six months approximately.

JULIE HEDLUND: Any other questions before we go to the next panelist? Then our next panelist is actually not here with us, but he is with us remotely. As I mentioned before, Oscar Robles will not be able to join us and also cannot join remotely, so we'll move ahead to Luis Diego Espinoza. He's joining us via Skype. His presentation is the panel discussion DNSSEC Activities in Latin America, which I will bring up here.

I apologize to the people in the Adobe Connect room, but we'll have to take a short break after this panel in order to fix our technical issues. What I will do is post the link to the presentation that we're showing in the Adobe Connect room so that you'll be able to reference the slides. But in order to try to keep us on track here since it will take probably about 10 minutes to correct our technical problems, we'll go ahead and move to the next presentation.

LUIS DIEGO ESPINOZA: Hello, good morning. I'm [inaudible] this morning. I'm [blind] with the Adobe Connect, but I will tell Julie that [inaudible]. I'm sorry for the font. Maybe it's a little bit small. I was thinking about I made a mistake with a map, because you can see the map, there's a yellow country there that in the last presentation [inaudible].

I've been working for a few years with DNS and ccTLDs, and more recently I've been [inaudible] DNSSEC and I noticed a few things. Here's the first one. In Latin America, there are more or less 39 countries, more

or less 39 ccTLDs and a little bit more of gTLDs. But thinking about ccTLDs. And according with this map, we shall borrow from DNSSEC deployment. The green area are the countries with their [DS] anchor on the root. Then you can see a lot of green, but the [inaudible] the quantity of countries [inaudible]. There's only a few. You can see the name of the countries. On black font is the country that doesn't have [DS] on root servers.

I have been chair of many useful technical workshops with many good technical and not technical friends from the region. I think many of them are in that room right now. There's a lot of workshops supported by ICANN, by LACTLD, by ISOC. I recently have been in the LACNIC meetings and they have a track of DNSSEC and this is a good thing. I start looking for since when they have a DNSSEC workshops in their meetings, and [inaudible] something like 2010. Maybe Carlos can correct me, but I think it's 2010. You can think about almost three years given DNSSEC workshops in only LACNIC and many workshops with LACTLD.

What are the effectiveness of these workshops in terms of the [inaudible] country codes with the [DS] and root? Well it's not too much. You can see – maybe not. I don't know the size of the presentation there. But you can see something like nine or ten countries [inaudible]. You can see I split some of them with blue and some of them with green, because the example that Brazil, Chile, Trinidad and Tobago, and Costa Rica all of them has implemented DNSSEC development and some technology. It's in the process of development.

This is the natural behavior of many of the academic ccTLDs – or ccTLDs that come from academic. They have their own technology. They want to do the things by itself and they have their own capacity to [inaudible] DNSSEC.

The other ones, most of them [inaudible] other companies like affiliates or other companies. It is outsourced. Later we'll tell you why this is important.

In terms of [inaudible], it doesn't matter how they get the [DS] on the root. But in terms of helping the region to develop more ccTLD [assignments], then this is important because if some of them it is outsourcing the services of DNSSEC then they cannot maybe provide a lot of technical help with other countries with – they want to sign with DNSSEC.

I was asking myself if there's lack of technical capacity in this [inaudible] assignment, I don't think so. I think they have a lot of technical capacity. They have a lot of experience running and managing DNS servers. And not only a DNS server, a country code DNS server [inaudible] think about the many security issues, performance issues. I know they have a lot of technical background [inaudible] to implement DNSSEC.

The other thing I was thinking about this. Maybe lack of [inaudible]. I don't think [inaudible]. Most of us in this room, we know if you want to sign, you don't need a lot of hardware or software. Lots of the software is open source and if you want to do it by using hardware, you can use [inaudible]. You can follow some of the workshops and you will find it is not too expensive. Well, if you want to spend money, you will spend

money. But it's not that expensive. It's not that hard to implement DNSSEC.

Then I think there is another reason. Let me check my notes. Okay. Let me take a few seconds and think about [inaudible]. We have a lot of workshops from many organizations and the effectiveness of the DNSSEC [inaudible] after years of this is only less than 30% of the countries in Latin America. Think about all the small countries in the Caribbean, for example, or many countries in Central America. It's a very small area and [inaudible] there. Next slide, please.

We are on the third slide. DNSSEC Neighbors Implementers. This is my proposal. If you see a Latin America map in two dimensions or any flat map, you see the distance and access in [inaudible], but it's not true. By example, to cross from Buenos Aires to Santiago, Chile, you need to fly across the Andes Mountains. They're a nice view, by the way. But it's not easy to get from Argentina to Santiago. I know there's a lot of [inaudible] there. But when you have the real physical work, there are some issues. By example, it's not easy to get from Panama to Columbia by [inaudible]. It's very difficult because [inaudible] the place.

And there's another issue too. In terms of the people, maybe a cultural thing. By example, it's very well-known that the Costa Rican people and Nicaraguan people are not the closest friends in the world. I have a good friend there. It's nothing to do with personal things. Maybe it could be a little bit difficult to establish some relationships with the Nicaraguan people if that help comes from Costa Rican people. It's maybe not easy. Maybe it's easy to get help from Honduras, for

example, or get help from Mexico by example than help from Costa Rica because of cultural issues.

The other thing I think about is the language. In Central America, we all speak Spanish. But in the Caribbean, most of them speak many languages of course, but English and maybe Papiamento or maybe Dutch in some cases. Then the language could be an issue in that area.

My proposal is this. We have Latin America. We can explain a little bit in sub-regions. By example, in the Brazil area, the right side of the map, there's a [inaudible] can maybe Brazil, they really have [inaudible]. They're very, very willing to help all the time. Maybe they can help Uruguay, Paraguay, maybe Argentina to get their ccTLD assignment. They are neighbors.

Then the other part of South America, maybe Chile can help Peru, Bolivia, Ecuador. I don't know. I mention Columbia because even if dot-co is assigned by affiliates, I know Gonzalo is there and he is a very helpful and very active person in this area. And I know he is willing to help some other countries to get their ccTLD assignment. Then Columbia maybe can help Venezuela or Ecuador.

In the case of Central America, as I told you, maybe Costa Rica can help but maybe Mexico too. And even if Mexico – I'm not sure about this, but I think [inaudible] is not on the root right now. But they are on the way. They have a lot of technology there. They have a lot of expertise. I think they can help some other countries to get [signed].

In the case of the Caribbean, I knew the manager from dot-sx and I know maybe he's willing to help the Caribbean or maybe [inaudible] is not yet [signed]. But I think they can be helpful in this area.

This is my proposal, basically. Next slide and the next slide. Divide and conquer. This is my final message about this. Thank you.

JULIE HEDLUND: Thank you very much, Luis Diego. Do we have any questions for Luis? Please go ahead Luciano.

LUCIANO MINUCHIN: Good morning, Luis Diego. You presented a definition that there was not much need for a huge investment to implement DNSSEC but you said that you may invest if you're willing. So what's the difference between investing more money than not investing so much money?

LUIS DIEGO ESPINOZA: I know there's a lot of people there that can answer this better, but in my experience, this really made the difference between first of all the assignment process, in the documented process by itself. Then if you follow some standards, some [inaudible] standard like the standards used in the [certification services], you will find you need to invest a little bit of money in some hardware.

By example, some of the hardware you may need to invest are a safe box to keep the keys safe. Maybe you need to invest in ceremonial procedure and you need to buy some people out of the [inaudible] to be there in a certain ceremony and these kind of things.

Well if you have a lot of signs – I'm not talking about the big ccTLD or big [inaudible]. I'm talking about the amount of [signs] you must do. Maybe you can think in some [inaudible] hardware to do this. But you can start without this big and expensive hardware. You can start with a simple [inaudible].

Or in the case of dot-cr, we started using the PPM chip that is provided in all servers for free. But this is a very particular implementation. I'm not sure if everybody will go with this. But it's useful and secure because the PPM chips have some level of security and it's good.

The thing is you need to start with something. Then you can do it only with software and a [certain] investment. Think about that and [inaudible] people to think about this process. After that you can start to specialize or split the process. Then you need to start buying a few things. It doesn't make a huge difference in the system. [inaudible] doesn't make the issue different.

The difference will be if you're trusted or not or if you are more trusted because you follow standards and you have a safe box and you do the things in public, that kind of things.

JULIE HEDLUND: Any other questions for Luis Diego? Then thank you very much and we'll move to the next presentation. Luis Diego, please stay on the line. We may have some more questions at the end. The next presenter is Carlos Martinez. I'll bring his slides up momentarily.

CARLOS MARTINEZ: Good morning, everybody. My name is Carlos Martinez. I'm coming from LACNIC. I listened to Luis Diego's presentation. Even though we haven't talked before, there are some common areas between us and I'm going to point them out. The purpose of my presentation is twofold.

First I'm going to speak about the implementation of DNSSEC at LACNIC, and then I would like to send a message not to the operators of ccTLD or [big] ccTLD is because the message and the word of DNSSEC has been quite widespread. But I'd like to talk to the operators of small and medium areas of zones, and then I will speak about how costly it may be to implement DNSSEC. I'm going to show you an example where you can see that DNSSEC may be implemented at reasonable cost. I'm not going to say a zero cost, but a small one.

So I have a slide that is a message that should not be repeated this environment because it's quite clear. But I like to stress time and again that there is no excuses to implement DNSSEC. We have no excuses. For a long while, the excuse not to sign the zone was that the root was not signed. Well now the root has been signed for three years. In fact, it was in July, so the root has been signed for three years. So we have to look beyond that.

What we are building having a DNS tree that is signed makes an important tool. We are going to have a directory that is reliable with digital [signs] and spread all over the world. So when you say that in those terms, we can see the scope and power of the tool we are building among all of us, so we should not waste any time in trying not to complete it so that this will become a technology useful to do some other things. For instance, if you [inaudible], there is a Working Group

of IETF called DANE and I think it will have a significant impact on many things we have and we will do in future years.

DNSSEC is not a solution to all the problems at a DNS system, but it certainly helps. It's not the silver bullet, so that when you implement DNSSEC you're not going to have any more problems. That is a must. If you operate a zone, you have to [inaudible] directly.

What's the role of LACNIC and the DNS tree? We have 20 or 30 direct zones (dot-com, dot-net) but these are very small zones. There is not much challenge. But I'm going to mention them because my message is addressed to that. You can do DNSSEC in small zones at the low cost. A major role as the operators of DNS is we go through the reverse DNS. It's not a TLD. It's not a ccTLD. It's not represented any money. But sometimes behind it we have lots of applications and technologies that do [inaudible] DNS queries, particularly the [inaudible].

Even when many people do not have their reverse DNS updated and people realize that the reverse should be updated when something fails over – for instance, when you don't receive the e-mail – here I included a summary timeline over process. In fact, when I joined LACNIC staff, by October 2010, this was my first mission if you may call it [inaudible] and I must recognize that the learning curve was quite high at the very beginning. A series of concepts that for anyone reading them for the first time, they're not quite friendly and intuitive.

Then when you start thinking about them, you understand all the pieces in the puzzle, but DNSSEC is a technology as well as RPKI. So you have certain things in common in this respect.

By the end of 2011, after the training, study and all that, we started signing some zones which you can see in the previous presentations called “Experimental Stage” and the areas that we chose were the direct zones, no [inaudible] critical but some other direct zones and ip6.arpa because if the IPv4 reverse are not updated, the IP6 are not updated. I can count it with fingers on one of my hands only. So the criticality there was not much important.

So when we analyze the risk, if that would be a problem, that will be the minor of the problems so this is why we chose it. We did some key rollovers in the trials. We took some technical definitions regarding software, and in the beginning of 2013 – as a matter of fact, January 1, 2013 – the reverse zones of LACNIC’s IP4 and IPv6 changed and were signed.

Even though the zones had been signed a bit before, January 1st was the official date and the [DS] registries were updated to the root through the IANA interface for this maintenance.

In IPv4, you have some corner spaces regarding to the [RX] space and the Legacy spaces that need some more analysis [inaudible], but they are basically soft.

By in terms of receiving the DS records from our associates, we may do it manually. If somebody is interesting, you may talk to me, so we may insert your DS records manually, and by mid-2013 we will have support for DS records and the provisioning system. The point is that the project for different reasons has to be postponed and I think by the beginning of 2014 it will be ready.

What about the architecture in signing our zones? This is called as the hidden signer architecture, so you have a machine behind and I would like to focus my presentation on that because you have a server that is the ones that signs in a hidden fashion. This is why it is called a hidden signer [inaudible] that is not reachable through the Internet because you have an IP that is not a private IP, but it's not routed. My idea was that it only should have IPv6 in that server, but that idea was rejected because the operators did not like it.

That server acts as a master server and there you have the zone files, and it's signed periodically and then you transfer the zone to the servers that are NS 1 and NS 2. Apart from NS 1 and NS 2, we have some other slave servers and we have secondary servers from [ours] and other organizations like NIC Brazil. And the transfer [that stems] from that other [nodes] are not from the hidden signer but from public servers, so there is a chain there.

An assigner does not appear in the NS records, so there should be no query. Even though it is not reachable, no query should go there.

So how we generate the zones. The zone files are generated periodically in the provision and system of LACNIC, so [inaudible] delegations. And there are text files that are periodically copies every four hours, as a matter of fact, to the sign engine. The sign engine in fact – and I want to take all the [inaudible] out of it, because I'm going to try and [inaudible] because you may spend – and it may be [inaudible] of money. You may waste a lot of money, but you may do it and implement it by spending a small amount of money. We are not using HSM, or the HSM is the hidden signer itself.

So we maintained a KSK offline, but when we need them, they are inserted through a [inaudible], for instance. So we haven't found risk analysis we've made for ourselves. We haven't found that there was much needed, except for that. And to include HCM, at that point that investment was not supported by the data we have. It doesn't mean that we're going to operate like that forever, but something that has to do with our current use.

In terms of software, when we started, the only alternative was open DNSSEC. Open DNSSEC is a tool that at that point in time was the material I'm speaking about late 2011. It worked okay, but it was quite rough in some aspects. But it has matured a lot in this last two years. Open DNS has matured a lot.

And the other alternative that is working again and I'm using it from the direct LACNIC zones is BIND 9.9 with something that is called auto-dnssec. So it's like magic, because you may just set out and generate the correct key pairs and set up what is called the [timing] metadata of the keys when you pretend to [inaudible] become effective or rolled over. And if you generate a new pair, the BIND 9.9 will roll over the keys by itself.

And to conclude, because I have no more time, the message I want to leave with you is precisely this. Set up like this one it's cheap. It's not expensive because it's the amount of that hidden server and additional switch if you need it. So it's less than $10,000 in investment. Much less depending on the country where you are. In our case, it was $7000. So we bought a good server with [inaudible] sources, etc., and we have an additional server – a backup server – if a catastrophe arises. But an

investment in [inaudible] was not really very high, and I think this should not be any excuse so as not to implement DNSSEC.

My final message. A TLD level. All TLDs know exactly what they should do, but my message is from one level down. If you operate a secondary zone or small zone, you have to work on signing those zones, the zones you operate in.

Once again, and I quote Luis Diego, the message of our corporation. There is a [inaudible] if there are operators that are small enough so this may be a very high investment as well, we have to take some of the hindrances out, because if I have trust with some of the operators, I do not need [inaudible] Luis Diego, a country that has my same culture that we have a very good relationship between operators and it's perfect. I think it's acceptable that other organizations may sign [inaudible] areas and may provide service to [inaudible] zones through a scheme like this one.

So those are some conclusions, but I've already mentioned them, so I should not go over again. Thank you ICANN for letting me be here with you on this panel. [applause]

JULIE HEDLUND: Muchas gracias, Carlos. And that's all the Spanish I have. Any questions for Carlos, please?

RICK LAMB: How are you doing? My name is Rick Lamb from ICANN. I had one question. First of all, great presentation. I agree with everything you

said. Simple is good. It's not very expensive. I think it's important to get that message across.

My question is for your risk analysis. Did you consider the risks from internal attacks? So from a rogue employee or something like that. Just wondering if you've thought about that.

CARLOS MARTINEZ: Yes. We considered that. The sign engine is in a data center. We lease it through NIC Brazil and we included that in our risk because there are servers that our PKI is there as well, so we took advantage by risk analysis with them before.

JULIE HEDLUND: Then we'll proceed to Gonzalo Romero and I will bring up his slides here momentarily.

GONZALO ROMERO: Good morning, everybody. Thank you very much, Julie. And thank you, ICANN, for giving me the opportunity of being here and sharing our experiences and challenges in DNSSEC.

I know that I have to be brief in this presentation, and this is my agenda for today. This is just a quick look to the technological deployment of our ccTLD, some updates in the implementation of the current EPP, our awareness and strategy and transfer of knowledge to the interior of the country, the state of affairs at the domain level, the challenges, and of course I will open the floor for questions and answers.

As Luis said, our case is somewhat different because we as a private company that grant a concession of the domain to the Columbian government. We took over that domain three years ago and our provider of service records is NEUSTAR. So it was not much complex to us to deploy DNSSEC to the zone or to the ccTLD [inaudible]. So basically experience of NEUSTAR would add a domain like .BIZ or .US.

It was not much complex for us to sign the zone. So it took out two months for a deployment as well as the other models that NEUSTAR has implemented before. We announced the implementation at ICANN 45 in December 2010 Cartagena, and the press release was made March 1, 2011.

So, very fast. Very fast because of the advantage of having a [inaudible] NEUSTAR. A strategic [inaudible] that is really very strong in the record industry.

So these are the policies for the area. So technically I'm not going to detail all of them, but the most important one is that we do not have a certification scheme for registrars. Everything is done through the [update] of EPP and all the information related to the historical process and what we do at DNSSEC is in our online content over the Internet.

With respect to the implementation update of DNSSEC, we are migrating in the definition secDNS-1.0 as defined by RFC-4310 to secDNS-1.1 defined by RFC-5910.

This is related to the EPP management of the DS registries and the DS records in the aggregation modification and withdrawal of records. This deployment will be done at several stages so that the registrars may

take their time to adjust their systems and to help the registrants deploy the same.

In terms of awareness and transfer of knowledge, year after year we have a DNS Tech and Sec Day. The first two years we focused ourselves on DNSSEC heavily. We have asked for collaboration in ICANN, ISOC, NIC Chile, LACNIC. Now I'd like to thank them because we receive much support from them.

The last time we held it three months ago in August 2013, we have cosponsors. The Columbian Chamber of Technology and Information that manages the IXP and we have people from the technical community that partially makes decision in ISPs and hosting providers for government, education in the institutions as well as private institutions with respect to the financial and banking sector.

We have a virtual community that we created three years ago. It's 50 of now. We're talking about [receiving] stability and security over there. Of course we discuss issues related to DNSSEC. In general, we update our blog to talk about the issue in our ccTLDs.

First of all, we're trying to work on raising the awareness of the government that in all the [inaudible], they may [inaudible] DNSSEC in the provisioning of technology services for different online government projects. So we have a project quite important with the Ministry of Information Technologies, the communication in Columbia, related to this fundamental. These basic points have included in the contracts, included in the call for bids and in those comments for proposals that they make.

Anyway, we're working with the academia, the universities mostly so as to sign [inaudible] domains and their edu.co. And also we're working an ISP in Columbia to work and offer services directly [inaudible] zones for the DNS customers.

This is the current status of [inaudible] domains when compared with the domains we manage. On February 2012, one year after having signed it, we had 1.2 million domain names signed and only 59 were signed before. Before the World Internet Governance Forum at Baku, we had 113 so we doubled that figure. We had 1.365 million domain names. March 2013, you can see only 113 and 1.470 being managed, so quite a low figure. And in October we had around 200 domains signed.

This is a reality and we cannot hide it. And of course we are confident that the deployment will keep on growing while the registrants gain awareness of having their domains signed.

Apart from the technological perspective, the question is what is the issue? Why that low number of domain names signed in our zone given the fact that we're the registry and we have [inaudible] in charge of this generating added value and given the fact that our registrars offer services to the registrants to sign the domain name.

So these were the main answers that we received. The registrar provides these. It is a security issue. They had some problems with phishing or any threat. And the other reason has to do with the lack of technical knowledge in terms of DNSSEC. And registrants do not [inaudible] by themselves without the registrar's promotion of the product or service, and sometimes the product is not reachable because it is not cheap.

What are the challenges? Well, as we said before, this is not only for the region but for the interior part of the region. We need to keep on working with the relevant actors – the ISPs, the [CERTs], the academy sector, the government and private sectors regarding DNS resiliency and stability issues. And these have to do with technical issues related to the DNSSEC. So when people come aware of all these security issues and resiliency and stability issues, we believe that DNSSEC will be adopted. ISPs and local registrars are very interested and they are now offering their registrants the [inaudible] zone.

As I said before, the agreements in terms of technology should include issues such as DNSSEC and issues related to resiliency and stability.

When it comes to Internet security awareness in relationship to the domain name, this has been increased in the region. This is very good and this will promote the topic.

When it comes to security issues, in Columbia the [curb] has been interesting in terms of corporation and this will imply efforts in the private as well as public sector.

We also believe that certain topics such as open DNS and some other issues referred by Carlos, these are tools that are very easy to use and every day they will be used and managed, and IPv6 is relevant for the Internet infrastructure and we consider that DNSSEC and [inaudible] issues are required for the Internet security, stability, and resiliency. Thank you very much.

JULIE HEDLUND: Thank you very much, Gonzalo.

DAN YORK: I just want to say I appreciate what you relayed here in terms of the awareness strategy and campaign, so I just want to say thank you for passing that along and sharing that because I think that's information that we're all looking at around what are the best ways to move forward with that, so thank you.

GONZALO ROMERO: You're welcome. I am to work very hard on this every time. We continue doing this kind of job inside our country, inside our region as well.

DAN YORK: I can also say having attended one of your.CO technical days that there was a great session here and I would encourage people from the region if you have not attended one of them to go and see what the .CO folks have put together. It's a great event.

JULIE HEDLUND: Thank you. Any other questions for Gonzalo? Then we'll move along to Cristian Rojas from NIC.CL and I'll pull up his slides here momentarily.

CRISTIAN ROJAS: Good morning, everyone. As my colleagues, I will deliver my presentation in Spanish. I am Cristian Rojas. I am an engineer working for NIC Chile and I will speak about the experience we had with DNSSEC in our project. Next slide, please.

We started with the project some years ago because our staff members usually attend international meetings where they discuss these issues – IETF, LACNIC, etc. So after these workshops, the idea of implementing DNSSEC appeared in order to improve the security for our client because we want to provide them with the best service, gaining more experience for the region and even for us, and to be able to share this experience with our Latin American countries and be updated in terms of the core business, which is the DNS. Of course if this does not affect the stability of our service and our objective was to sign the zone before the root, but we were not able to [interface]. However, we did it.

Now let me tell you about some history. We started with our internal actions in 2004. We started with some first lab tests. In 2007, we started with our concerns about DNSSEC and about the signing of the root zone, to improve the trust chain. So our technical group together with the Lab members – NIC Chile Labs – created a team that determined the internal implementation or deployment of the DNSSEC service in order to sign our root zone.

In 2009, we had our first testbed. It was an official test, a formal test, for the DNSSEC. In 2010, we started to follow the network and we had the root signed with DURZ. This was not validating. This was a [inaudible] or fake signed and we followed the same steps. So some months after, we had an [SLD] which was not validated. We worked with that [inaudible], and at the end of 2010 we end with a real KSK without sending the DS to the root. We did it in April 2011 and we have delegation signed DS and the acceptance of DS from [inaudible] was performed in 2010.

We have been in full production with the project and we are not having operational issues generating any problem for our clients. During the Implementation Project we had to decide on the focus, whether we would have a technical implementation defining the policy or else a policy defining the technical implementation. In fact, it was a mixture of both approaches.

We needed a policy compatible with the implementation that we could do. And on the other hand, this policy should help us to have an audited and applicable process. This was [placed] in a DPS based on other registries – for example, .SE – and before being offered to the public this was validated by our internal group, but it was also validated by an external group of advisors. For example, Richard Lamb. We received some comments and improvements for our document but they found nothing invalidating, so we were in the right way.

Another issue implemented was the generation of scripts defining the stages of the actions implemented in each of the stages. For example, during the rollover the idea is to avoid or to take the operation – to take decisions – and these decisions should be predefined based on the decisions of the group and how to act in case this process does not work as it is expected. Of course we are including the physical and logical security because this has to be embraced not only from the software perspective. We also need to include roles and analysis validated so as to avoid issues so that we can have an auditable system. This is not because we have doubts about our people working with us, but this validates the process and nobody can object the project.

When it comes to the next steps, well, we need to improve the DNSSEC adoption by the community because we are not very successful in terms of the domain names that are signed. The volume that we have is similar to the one mentioned by Gonzalo. We need to start training the community focused on some of the main actors or key actors involved. For example, the ISPs, some hosting companies, the government, universities, financial institutions. That is to say organizations having higher interests than the end users who are not interested in DNSSEC.

Another step we would like to take is to improve our scripts because we may have certain conditions or certain issues not covered yet, so we need to improve in this aspect and we would like to [inaudible], so the improvement of the automatization of certain steps that are now being carried out in a manual way.

Here I would like to highlight that when we started with the project, we had to decide whether to automatize from the very beginning or else to perform this manually. We decided to work manually because we could have a better understanding of the protocol. We have been carrying out the operation for a couple of years and now we have the necessary technical knowledge to go to another stage so that we can improve and have other automatizations, too, such as DNSSEC and the tools provided by BIND. So thank you very much. [applause]

JULIE HEDLUND: Thank you very much, Cristian. We have just a little time for some questions, please.

CARLOS MARTINEZ: This is Carlos Martinez from LACNIC. I have a comment more than a question. I would like to highlight the final remark, Cristian, and I would like to quote something I said at the very beginning which has to do with the learning curve of the DNSSEC. There is not only a DNSSEC learning curve in terms of a new registries and the interaction between the [signs] and the DNS, but also we need to focus on the operational aspects and I second what you said at the end because we need to have a maturity period and we need to gain knowledge so as to be able to assign and have tools necessary to sign the root.

JULIE HEDLUND: Please join me in thanking our very helpful and experienced panelists here who have given us a lot of very good information to think about, particularly for also Luciano for moderating the panel and for also ensuring that we have the simultaneous translation as well. So, thank you.

I'm going to then ask the next presenters, Russ Mundy and Zheng Wang, to come to the table and I'm going to take a moment to fix our little technical issue here. We did have a break scheduled. I think we'll probably run into our break, so you just have a couple of minutes to stretch your legs. I'm not sure where the coffee is, but we will try to make up the time as we go so that we are in particular being able to finish when lunch is served most importantly.

UNIDENTIFIED MALE: Folks, if we could start taking our seats again, we're a bit behind. We're going to try to catch up on time some.

JULIE HEDLUND: Thank you, everyone. We're going to go ahead and get started with the DNSSEC for the Enterprise panel. I'm going to turn it over to Russ Mundy.

RUSS MUNDY: Welcome to the panel session for DNSSEC for the Enterprise. This is something new for our workshop where we've not really had much [inaudible] of using DNSSEC in the enterprise before. We do have two presentations and we're going to try to catch up a little bit on our time. Am I first? Okay. I will just go right ahead.

For the DNSSEC in the enterprise, the first question is, "Why?" Why bother? Why worry about it? Well, the thing that I'd like to point out here is even though almost everybody in this room I think is associated in some way with the DNS industry, you each operate and have an enterprise that you're either in charge of or a part of and you should think about incorporating DNSSEC into your enterprise so as those that are outside of the DNS industry start to look at it, you'll have some experience in this space yourself that you can draw from. Frankly, that's where a lot of our experience comes from and we have helped those that are outside the DNS industry and that's why we wanted to spend a bit of time talking about it today. I'd love to get feedback questions that folks might have for this, too, for other experiences you might have had.

Within the use as an enterprise for DNSSEC, many of you realize this even better than I do, but the DNS name that you have represents you as an enterprise and that, in many ways, is one of the most compelling

reasons why you want to make sure your name and your representation is as it should be on the Internet.

One of the important ways to ensure that is to use DNSSEC in terms of both signing your zones and facilitating its use by validation and incorporating that in various capabilities you provide. If you have software that you provide to your customers for their use to get to your facilities, think about including validation as part of that. Next, please.

So the capabilities. The biggest place where we see DNSSEC in use, at least close to the enterprise level, are websites. More and more websites are assigned. Two examples up there. Of course, the ICANN website itself is signed and a number of websites and activities associated with the DNS industry and activities are becoming more signed all the time.

There's also some new and exciting capabilities emerging out of the IETF such as the DANE capability, the ability to have enhanced security for e-mail and new security capabilities are being examined that are built using the DNSSEC that is out there. So it gives you new security capabilities.

So this is the browser that is produced by the team that I lead. It's called Bloodhound. This particular displays at our website that is tailored to encourage and support the use of DNSSEC. You can see you get a DNSSEC check there at the top. Next.

And if you don't have DNSSEC – and we happen to run one of our hijack demonstrations – you can see that Steve Crocker is saying that DNSSEC

won't solve world hunger, and this only appears if you are not using DNSSEC. Next.

This is just an illustration of how many queries there are to fill one of these large commercial websites – weather.com, foxnews.com, cnn.com. Many, many queries just to fill one page. Any one of those can be hijacked. Next.

And when do we do it? We ought to do it now. We ought to start doing it now, making use of the technology that has been built that is available.

And how are you going to do it? Well, you want to look at your roles in the enterprise at the enterprise level for how DNS itself is managed because whether you're talking a registry or registrar, you want to integrate DNSSEC into your normal operation. The exact same thing you want to do at the enterprise level. Whatever set of functionality you are using to operate your DNS today, you want to use those same general functions, those same organizational responsibilities for doing DNSSEC.

For instance, a number of organizations may not actually have a formal assignment of who is responsible for the content of their zone in the enterprise. Maybe it's some IT guy sitting off in a corner and they make the decisions. Well, that's fine. In other organizations they have a senior officer of the organization that's actually responsible for okaying the content. They may not be the ones the fingers on the keyboard, but they're the ones that say, "Yes, you can put this name in," or "No, you can't do this." So those are the people that should be engaged and involved in the decisions themselves. Next.

This is an illustration that I use in a number of my presentations. On the far left is where you actually deal with the content of the zone, where you decide what that content is going to be. Up at the top of this triangle, after you go through your organizational registrar – and you may not think of it as having an organizational registrar, but functionally, you'll have an organizational registrar – and then you'll have an organizational name server operator that may be in your organization or it may be outsourced in some manner. Then the content is in the live and running DNS and it's actually used on the right-hand side. So there's many activities involved.

So part of incorporating this into the enterprise is making sure you know who those organizations and activities are and that you coordinate this properly and plan it in advance. Next.

So after you've gotten the roles and the people filling those roles identified, you need to make sure that each of the functions that are doing the various roles for their part in the overall operation are able to support DNSSEC and that's really the next big major step. After you figure out who's doing it, you've got to make sure that they can do it. Next.

Okay. And after you've done your planning aspects, one of the big challenges is often getting your registrar engaged in the DNSSEC process. Honestly, there's still a great deal of limitation in the availability of registrar support in DNSSEC. One of the ways to increase that support is for you as customers of registrars to go ask for it, because many times – and I'm sure we'll hear from Michele in the next panel – that's one of the reasons why the registrars don't do DNSSEC.

Nobody's asking is what they're saying. So as an enterprise, as a user who is purchasing names, ask for it.

So what's next? It's going to give you the ability to have a stronger security posture for today and for the emerging technologies tomorrow. That's really the key aspect of what DNSSEC does for an industry or for an enterprise in an a particular industry is it allows you to not only do more and better security today, but to be creative and to create and make use of other security technologies that emerge in the near future.

So that's it for my presentation. I wanted to keep it as quickly and short as we could here and we'll just have maybe a minute or two for questions, if there are any. Michele?

MICHELE NEYLON: I'm not going to ask a question. I'm just going to confirm what you said. Speaking as a registrar and speaking as the chair of the Registrar Stakeholder Group, I cannot think of a single member of ours who is saying, "Oh, my God, I'm being inundated with requests for this." James Bladel from GoDaddy has been on DNSSEC panels in the past and to paraphrase what he was saying, if it was a product that they were behind, they would've killed it because there just wasn't any demand.

Following the session is going to be a bit about DNSSEC from the registrar perspective and a couple of things we'll be looking at. But if there's no demand, we're commercial entities. We're not charities. We're not going to spend time, money, energy and effort building out something in the hope that somebody might at some point in the future

hypothetically come along and pay us wads of cash for the service. That's now how these things work.

I get very, very frustrated when I hear some of the hardcore technical types going on about, "Oh, but it's the right thing to do." It's like, okay, yeah, sure. If it was free, maybe. But developing stuff properly. And as you all know, if you screw up in your DNSSEC, bad stuff happens – and it happens really, really quickly. And it's binary. Either it's working or it's not working. There's not much in between.

RUSS MUNDY: Thank you. Any more comments or questions? Okay, let's move right on to the next presentation.

ZHENG WANG: Hello. My name is Zheng Wang from CONAC. I would like to talk about DNSSEC deployment enterprises from the perspective of economics. Here is the agenda.

First we would like to model DNSSEC deployment in a multi-stakeholder game. Several entities are involved in the DNSSEC deployment. They are [inaudible] who decide whether to request for [inaudible] signing service, and the registrar who decides whether to provide DNS service for the [inaudible] and the registry who decides whether to sign the TLDs and the roots.

And the [inaudible] resolver must be provided by ISPs who decide whether to open DNSSEC service, and the end users who decide whether to request DNSSEC validation. Each stakeholder has basically

two DNSSEC options: DNSSEC on and DNSSEC off. The root is already signed. We do not discuss root here. So the remaining problem for the game is how the other stakeholders behave in the game.

We'd like to discuss the strategies of each stakeholder one by one. First, enterprise roles. DNS caching resolver operators, they can be classified into two types. The first is the self-serve companies. This means they deploy DNSSEC on corporate infrastructure. And the second type is the ISP is mostly provide DNSSEC validation for its Internet users. In China, the ISP is dominant in terms of the percentage of Internet users. The other role for enterprises is domain name registrant. This means they deploy DNSSEC on their own domain names.

The game takes next basic assumptions that DNSSEC deployment is basically driven by the economic considerations of each stakeholder. We have several observations for the assumptions. Economic incentives for each stakeholder may depend on DNSSEC options in other stakeholders. And DNSSEC deployment is hardly ego-driven from an economic perspective. I already provided the analysis. The analysis may be suggestive for finding a way out for the game.

Now for the ISP in the game. The ISP is an independent entity in the game, because they are not the data originator or registrant or they're not the data provider, because the data is provided by the registrar and the registry in the game. They are not the data requestor. They are requested by the end users, so they are only the intermediate in the resolution system. So they don't have so much care. They do not care so much about the DNS message integrity. The end user [is] registry, registrant, and the registry.

So DSNSSEC deployment requires significant validation cost for them. This means DNSSEC is a large investment for little revenue for them. So we're going to conclude that for ISPs, low economic incentives for the DNSSEC deployment and they are unlikely to be driven by the proactive actions of other stakeholders.

Registries need to deploy the incentive in the TLD. This incurs significant signing costs such as bandwidth, computational resources, protocol support. And DNSSC deployment is much dependent on the DNSSEC strategies of its registrars.

If registrars are DNSSEC-oblivious, DNSSEC off is maybe a better option for them because they either can incur minor impacts on revenue. On the other hand, if the registrars support DNSSEC, DNSSEC off is a better option due to the revenue risks consideration. Here we do not consider ICANN's DNSSEC efforts in requirements for new gTLDs.

We can conclude that for registries, economic incentive for DNSSEC deployment emerge only if registrars provide DNSSEC service.

Most registrars in China are also the largest hosting service providers, so here we integrate hosting service into registrants. For registrars, DNSSEC means significant signing costs and other costs and the strategies of registrars depend on the DNSSEC actions of each registrant. If registrants require DNSSEC service, DNSSEC service was worth the investment. If the registrant is DNSSEC-oblivious, DNSSEC off is a better deal because they don't need to invest much in DNSSEC.

We can conclude that for registrants, economic incentives for DNSSEC deployment emerges only if registrants request DNSSEC service.

DNSSEC deployment may bring extra costs for the singing service, so the registrant has to decide whether DNSSEC deployment is worth the cost. The strategies of registrants depend on the willingness of end users to initiate DNSSEC queries. If most end users require DNSSEC validation in its queries, DNSSEC will be necessary for the protection of the registrant's DNS data.

On the other side, if most end users send DNSSEC-oblivious queries, DNSSEC off is a better strategy in terms of cost-effectiveness.

The conclusion is that for registrants, economic incentives for DNSSEC deployment emerges only if end users request DNSSEC in their queries.

Finally, the end users. The end user may have their query delay increased and processing burden increased if they deploy DNSSEC and they request DNSSEC. They may install an [inaudible] to stub resolvers to deploy DNSSEC and the action of the end user depends on the DNSSEC readiness in both the authoritative side and the [inaudible] side which means that the caching resolvers, the registrars and registries and ISPs all provide DNSSEC service.

We can conclude that economic incentives for DNSSEC requests from end users emerge only if registrars and registries and ISPs are DNSSEC ready.

So to summarize, the analysis above, we can draw dependency graph of the game. From the graph, we can conclude that promoting DNSSEC at the registries and/or registrars without stimulating other stakeholders is not enough for promoting DNSSEC because DNSSEC [inaudible]

registries and registrars alone cannot necessarily provide incentives for other stakeholders.

And the awareness of end users and registrants is very important for DNSSEC deployment because the actions by any of them can provide incentives for other stakeholders, except ISP. And ISP's position is very special. It is independent of other stakeholders, so we must take external funding, guidance or subsidy to promote the DNSSEC for them.

In China, China government has already initiated investment on the upgrade of DNSSEC ISPs. They are part of China next generation Internet project. Thank you. Any comments or questions? [applause]

RUSS MUNDY: Thanks very much for your presentation. Do we have questions or comments? Dan?

DAN YORK: I thank you for working through this analysis. Many of us have talked about this, but it's nice that somebody took the time to put it together into a document like this around that. You highlight many of the bootstrapping issues that we've had around here just in general with DNSSEC. The challenge I think is complicated by this ecosystem that you outline.

We've looked at promoting it to end users, for instance, and we started a bit trying to promote end users to go out and sign their domains and ran immediately into the issue that when they would go and try do that, either their registrar did not support DNSSEC. We've had people leave

these workshops and say, "I'm going to go home and sign my domain," and they go back and they immediately find the registrar can't support it or the registrar could support it, but their DNS hosting operator didn't do it.

You're absolutely right. We have this ecosystem challenge of bringing the whole thing together. So thank you for highlighting it all in there.

RUSS MUNDY: I have one question. Recently .CN just had its DS record into the root. Congratulations. It's been very recent, but have you been able to see if that made any difference from your perspective to the overall ecosystem structure that you're describing, that your TLD or your primary TLD is signed and in the root?

ZHENG WANG: Actually, [inaudible] initiative that DNSSEC efforts several years ago. They have a long test on DNSSEC deployment in [inaudible] infrastructure in China. I think it would take a very cautious step. It was DNSSEC deployment because [inaudible] ccTLDs [that worked]. We have already development DNSSEC related software and hardware to protect our DNSSEC infrastructures in collaboration with Internet community and to Chinese

RUSS MUNDY: Great, thank you. I think one of the things from both these presentations that are very important is to take away from here is to go raise the demand. Identify that you need support from the various

activities that you are acquiring support from whether it's product, whether it's service providers. In fact, some of the enterprises that we're working with to do the DNSSEC for the enterprise have literally changed their service providers.

When you do that make sure the service provider that you're leaving knows why you're leaving because otherwise they won't have any incentive from your departure to consider doing DNSSEC.

As Michele said earlier, there's just almost no spoken demand from the consumers with the registrar. It's the same thing also for name service providers. Be sure to examine that and let those out in the service provision, product provisioning world know that this is something that you as an enterprise, and hopefully your enterprises will each look at doing this yourself.

We'll end this panel now and move on to the registrar panel. Thank you people. If we could have Michele.

JULIE HEDLUND: While we're doing this I've restarted my machine and I'm going to try to get Adobe Connect back up since you didn't probably see it here but the people in the Adobe Connect Room were without slides for just a little bit. So I'm going to try and get that fixed.

MICHELE NEYLON: Good morning everybody. Here we are again talking about DNSSEC from the registrar's perspective. I've got two speakers with me this time. On my right we have Mr. Patrik Fältström. Most of you already know for his

wide and varied number of activities. He's the Chief Scientist Researcher with NetNod. It's always nice to deal with Patrik. He's such a sincere and polite little Swedish lad.

On my far left we have Rob Villeneuve from the Momentous Group. He's the CEO of part of their registrar business. For those of you who don't know how I am, I'm Michele Neylon. I'm the CEO and Founder of Blacknight. I'm also the Chair of the Registrar's Stakeholder Group.

The thing is you shouldn't take yourself too serious when you're talking about DNSSEC because if you do everybody falls asleep. We thought that we'd add the cartoons to the slide deck. Part of the reason why we've been talking about DNSSEC and registrars is, as many of you know, ICANN has recently introduced a new contract for registrars. All registrars who want to offer new TLDs have to sign on to the 2013 Registrar Accreditation Agreement, which is a great big long boring contract but unfortunately you need contracts for these things.

Within the contract and in its various addenda there are certain operational obligations that are quite new. There's one about IDNs, there's another one about IPv6 and the one which you guys care about is DNSSEC. For those of you who haven't read the wonderfully long and terribly exciting contract and the operational bits, don't get too excited. You haven't won. You're not going to force us all to offer a fully comprehensive, end-to-end, all singing, all dancing.

I’m sorry Dan. Dan York by the way for those of you who can’t see is widely gesticulating at me and getting all excited because that's what Dan does. By the way, Dan, you are looking very dapper. That's not

what's happening. There's a requirement for a level of support for DNSSEC within the new contract.

I'm going to hand over to Rob. Rob's going to speak a little bit and then after he's done his bit, so will Patrik. If you want to interrupt us, if you have questions, if you could politely raise your hand that will be really nice. We don't want to do death by PowerPoint. I'm a strong believer that if you fly halfway around the world just to look at a bunch of PowerPoint slides it's a bit of a waste of a flight. Rob, go ahead.

ROB VILLENEUVE: Awesome. Thanks for that introduction. I'm new to this group. I just wanted to say hello and thanks for having me. I'm certainly not a DNS expert but I guess I'm supposed to be a registrar expert so I'm here to talk to you about what's happening in the RAA.

As Michele said, I'm the CEO of the Registrar Group at Momentus. We operate four commercial registrar businesses. We've signed them all up for the 2013 RAA so we are very well aware of our deadlines on January 1st and our obligations to DNSSEC and I hope to cover the nuts and bolts for you today.

I also want to give a shout out to my [inaudible] boys here on the left because they've been pumping me up this whole time. Michele told me I had to put pictures in my slide deck. I didn't want to put a big giant picture of my face, so I put a big, giant picture of my dog.

MICHELE NEYLON: Which makes a nice change because I usually put cats in mine. Cats and dragons.

ROB VILLENEUVE: I don't think there's any metaphor there that the dog is leaping.

MICHELE NEYLON: This is actually his dog. I have seen photos.

ROB VILLENEUVE: For those of you who need a little refresher, the RAA is the Registrar Accreditation Agreement. It is our contract with ICANN and it governs how the registrars operate their gTLD businesses. I think it's important to note that it is an optional upgrade for registrars to sign the 2013 RAA. There are previous versions. Just yesterday we were getting an update on the adoption rate for the 2013 RAA. Certainly adoption isn't moving at lightning speed.

That's where the DNSSEC updates are contained. They are not contained in any previous RAA. But the previous speaker was looking for an economic incentive to get registrars on board and they found it. It's new gTLDs because registrars must sign the 2013 RAA in order to support the new gTLD program. That's pushing registrars to go.

As mentioned, many of the requirements in the RAA are due January 1st. If there's any registrars in the room, they know that if they signed prior to January 1 you had a little wiggle room to implement those, but if you sign on or after January 1st, those are obligations as of day one.

You want to see the contract language? There it is. I debated for a long time whether I'm going to read it to you. I think I'll skip it. I'll break it down for you instead but if you're interested you can get the RAA at that link down below off the ICANN website. It's section 3.19. That's it. I will not read that.

Here's how it looks. You have seen this chart a few times but this is specifically from a registrar's perspective. But when a registrant wants to set up DNS they must speak with their DNS operator. I'm sure this is a process that everyone in this room knows very well. The DNS operator will provide some information back to the registrant that they must somehow get to the registry and that's where the registrar comes in.

The registrar deals with all forms of domain name setup from the registrant's perspective. They will pass us the DSKEY. We are then obligated to make the adjustments at the registry. The contract reads that we must do so over EPP.

MICHELE NEYLON: Patrik, go ahead.

PATRIK FÄLTSTRÖM: It's actually to this picture. I just want to point out that in some cases the registrant has the ability to appoint the DNS operator as a technical contact which means that [inaudible] can contact the registrar.

ROB VILLENEUVE: I missed an arrow there and that would probably simplify the process a little bit. I think it's important that we highlight those red arrows

because the contract itself speaks specifically to the communications between the registrant and the registrar and the registrar and the registry. What Patrik just outlined is not contained within the contract itself.

The other note is that registrars are often DNS operators themselves, so this box around those two box means sometimes we do offer DNSSEC but that is not governed by the contract. Really the contract specifically just talks about passing DSKEY records between the registrant and/or a representative of the registrant and the registry over EPP.

The obligations in the contract. The contract also mentions that we must do so in a secure manner. It's very loosely written. What it means to me is that when we're dealing with security measure and we're dealing with domains and attacks like hijacking and such exists and man in the middle attacks, the registrar could be a focal point for an attack. It's not simply just passing information back and forth but it's doing so with authentication and authorization and auditing and all the normal security practices that a registrar would normally put in place for domain updates.

As I said, the contract specifically mentions EPP. This is a bit of a sticking point for me. I personally don't feel it's necessary we use EPP. Registries often provide registrars with other means of updating domains. Usually it's the form of a secure website where the registrar or its representatives can log in and make small adjustments to domains, which is in my opinion the perfect way to handle requests which are of complexity and very low demand.

When requests are complex and of high demand, of course it facilitates us to automate the process and that's to use the EPP protocol between us and the registry. However, for requests where there is very little demand we would be done already if this is how we could do it is just use the registry portal instead.

Some other considerations – this is probably more for the registrars in the room than anyone else, but if you look through the rest of the RAA there's a whole bunch of obligations we are required. One of which is WHOIS data requirements. They have to follow a very specific format. If you look very closely, there is a DNSSEC field within the WHOIS response which signifies whether that domain is signed versus unsigned.

Also, there's going to be some technical challenges around domain transfers – inbound domain transfers for registrars which choose not to support DNSSEC given the fact that inbound domain might already have DNSSEC enabled. Other considerations for registrars that registries often have an onboarding process to support DNSSEC, which often means some specific implementations for that registry and certainly their own policies and procedures.

MICHELE NEYLON: Just to expand a small bit on this. Some of the registries, it's more than just an onboarding. They actually go through an entire certification. Some of the registries will not allow you to do anything with DNSSEC unless you're certified. Let's say for arguments sake if you wanted to move a DNSSEC sign dot-org from Rob's registrar to mine, you won't be able to because we don't support DNSSEC.

ROB VILLENEUVE: Correct. So there's certainly some challenges that we see there that are not addressed in this contract. And some other obligations that we would have to take up with the registries themselves in order just to support that connection.

The final point that I wanted to make was you can't do any of this from a registrar perspective without supporting the customer, providing some education. Even though we are a very small piece of what it takes to set up DNSSEC, we are always the front line for what happens when the website goes down. It does us very little good to try and slough off the request on to some other party, be it the registry DNS operator or somebody else. It's on us to take up the support burden for the other operators as well, with the other actors as well.

Finally some simple other considerations. The RAA does not apply to ccTLDs. We have individual contracts for those. From a registrar perspective who's rolling out DNSSEC you might consider doing it for ccTLDs. Obviously registrars that want to support DNSSEC should do so for their own domains. That's something we are currently in the process of doing. It also helps us test the waters to see what DNSSEC is really like from the registrant's perspective because in that case we are the registrant.

As I said before, when the registrar is the DNS operator they're not obligated under contract to support DNSSEC, but of course to support the cause, that is something that they should to look into.

Again, more for general information or more specifically for registrars, there is help. Often registries will provide a tool kit which allows us to implement the EPP section of our communications. There's also a universal open source tool kit which registrars use. Registries often provide software extensions for those tool kits that gives us the communications out of the box so to speak and we're left with the integration problem from the development side. I'll skip the schema part.

This is my last slide. As I said, I'm new to DNSSEC so here's some resources that I found useful. I'm sure most people who are familiar with DNSSEC already know all of these resources and probably some more. The one at the top is the one I wanted to highlight – the Registrar Stakeholder Group. We are doing some outreach to recruit more registrars and community participation.

As a registrar, what I would want to point out is those registrars in the room who are not members you can get a lot of support from the rest of us. When it's a contractual obligation we're all required to do the same things, we often work together in order to make those things happen.

MICHELE NEYLON: It's only $500 a year. Wonderful value. If you are an ICANN accredited registrar and you are not a member of our Stakeholder Group, please join up. Patrik, you're up.

PATRIK FÄLTSTRÖM: Thank you very much. What Michele explained is that yes I am Head of Research and Development and other things. At NetNod we run root servers. We run slave servers for maybe 45 ccTLDs and lots of other kinds of stuff. Next slide please.

Responsible for distribution of Swedish Time. A lot of hands on work there. It's also the case that I happen to own 50% of a registrar that concentrated on being a registrar for ccTLDs. Given that we hear so much good words about what's happing in the detailing community for some weird reason we decided to concentrate on the hard part. ccTLDs which are by far the most complicated situation. We decided to do DNSSEC from the beginning, which was not very easy of course. We also decided to start with our own domain names and specifically with IPv6 and DNSSEC and not to expose anything to customers before we actually had it ourselves.

One more thing. To be able to know really how this worked we decided to implement everything ground up on ourselves including EPP. One thing we found is that as soon as we started work with multiple registries, specifically ccTLDs, as I will come to later, using those prebuilt packages does not work. This is one of my stronger messages. Next please.

This is how most registries that I communicate with – and it says gTLD here but it could be any kind of registry. Most registries do believe that they have registrars that work with them and the registrar has multiple registrants and then you have top level demands. This is how the policy, this is how instructions that are sent to registrars are assigned like this. Also, the information that registries want registrars to send to

registrants are written in a way so it's pretty clear that the registries think that the registrants have domain names in only those registries, which is a little bit confusing. Next slide, please.

Quite often it's what the registrar has to do is to rewrite the whole thing. This is normally how it actually what it looks like. You have two different registrants. They have domain names and different TLDs. They use different registrars. If you're lucky they only use one. They use multiple different DNS hosting providers and the situation actually kind of messy.

Luckily the positive side is that there are more and more people and parties and organizations that do understand that this is a mess. I'm actually – for example we have this panel. But it's also the case that I actually do get calls and contacts from multiple registries and multiple other registrars that ask for my experience.

MICHELE NEYLON: So basically what you're saying is this panel is a sales pitch for your services, Patrik?

PATRIK FÄLTSTRÖM: To some degree, because we are so tiny so it doesn't matter. We don't have any competitors really.

MICHELE NEYLON: Well so are you, but never mind.

PATRIK FÄLTSTRÖM: No, no, no. Take it the other way around. Even though I want people to wake up and say that this is a real mess, I want to end with a positive side to say more and more people understand this. Next slide please.

My picture very much looks like this where I think there are two different kind of lines. You have the contractual agreements but then you also have different parts which is where information flows. In this case for example you have three different domain names that the registrant has. All of those domain names are in this simple picture handled by one DNS operator to the right. The DNS operator, to make it easy, the registrant has made it possible and the registrar do accept the DNS operator to be a technical contact for the domain name.

The registrar in turn talk with the various registries and pass information to them. This looks like a complicated picture but this is actually a simplified one because the situation can be more complicated. If we just start with this picture and try to move things in this direction, I think that's a good start. Next slide, please.

Here we start to come to the various different kind of issues. The first thing which is all of us registrars say, "Oh it's so expensive to implement DNSSEC." If it was the case that all the registries actually used the same flavor of EPP and everyone handled the process and policy around DNSSEC the same thing, it would not cost so much.

Implementing this for more than one registry is a royal pain. When implementing EPP from bottom up, I can say that even though we're implemented for half a dozen registries, which is not so many but still adding one is in the order of 200 to 300 man hours to implement a flavor for a new registry per registrar. What registrars want I claim is we

don't care what kind of EPP flavor you use. We want to be able to use the same code, exactly the same protocol for you as a registry that we use for other registries. Registries around the room and elsewhere, please harmonize your EPP protocol. Thank you.

One thing I don't understand is there is specifically one ccTLD at the moment that I'm working with that is now introducing EPP for their ccTLD and they are rewriting their own EPP stacked bottom up. Currently they're trying to find bugs in the greeting message. I think there are more other things to do than that. Anyways, next slide.

Specifically with DNSSEC as we saw we have this RFC. The problem is this that we also saw before that this isn't the RFC there are two different forms for me to face. Next slide please.

Red and black didn't really work. This is my fault and absolute not Julie's or anyone else. In the protocol I was error director when this protocol was approved. This is why I can complain on it because it's my fault. I should never, ever have let this ROC through.

This RFC say there are two different forms of interface that the registry can support: the DS or DNSKEY. This or has as we saw earlier slipped into the RAA. Can the registries please agree on one? As a registrar I don't care. I have chosen to use DS in my implementation because I start with a [dot-sc] and [dot-sc] did chose DS.

That means that I will not implement DNSKEY. I cannot do that. That absolutely cost too much. Either all of you move from DS to DNSKEY or you move from DNSKEY to DS. Make up your mind. There should not be

a “or”. Note here the contract allow registries to agree on one of them. We registrars, at least from my perspective, do not care. Pick one.

Why is this sort of complicated? You have all of this different kind of information passing pass. A DNS operator passes DS or DNSKEY to the registrar. The registrar passes DS or DNSKEY to the registry. The register places assign DS in their zone. Next.

But now you have to start to look at what actually happens out there in the market – if some registries want DS [others] DNSKEY. That is one of the problems. It's also the case as Michele pointed out changing DNS operator that is hard already from the beginning. Changing the MS records to make sure that the zone is always up. Doing that with DNSSEC as we know is pretty darn difficult. Changing registrar is difficult, specifically if the registrar supports different mechanism for this.

Being the DNS operator and not registrar is of course a quite complicated situation. This is one of the reasons why we see certain movements in the market regarding competition or non-competition where, for example, we encourage customers that want to run DNS themselves and run DNSSEC to either allow us to be the master and handle the keys or to implement the API we have to be able to do Automatic Key Generation because key rollover is kind of difficult.

The last thing which is really what's happening is that if you look at the registry and the registrar as sort of one data base, the registry do have a database and the registrar sort of have some information, which is a mirror of the registry. Having a multi master database we know is quite complicated. Doing updates in the registry without doing it in the

registrar is also sort of very difficult with EPP. You have to send notification.

Because of that I'm a strong believer in not doing changes in the registry without doing the change actually in the registrar with some very specific exceptions. For example, when it is the case that domain name is not renewed and i's actually terminated, etc. Some law corporations. But otherwise all changes are done in the registrar that is then pushed to the registry. Keeping things in sync is really, really hard.

When started to talk about that you might be off sync or out of sync and talking about key material. You don't want to be in that situation. It's hard enough when changing DNS operator or changing registrar. Next slide please.

What people are talking about in the IETF at the moment is trying to find out a band mechanism that makes this easier, that you have an out of band mechanism for the bootstrap. Then they can use other kind of mechanism. For example, if you already have trust via DNSSEC and the data's published, you can then sort of use that to inherit that later on in the process. Next slide please.

There is for example one draft that Warren is working on down there that is talking about the ability to fetch information from the child. If it is the case and the situation is such that the DNSSEC material can be pre-published in the child zone, which by the way is not always the case. But if that is the case and the child zone is signed and you have done the previous boot strap it's kind of easy to pre-publish things or publish things in the child zone. Very simple. Fetch information from there.

I like this, but I don't like it if the registries start to use this mechanism to fetch the data directly from the child zones because that means that the registries are bypassing the registrars. What I'm nervous about at the moment is that just because of the mess with different DS, DNSKEY and whatnot and high cost for implementing DNSSEC that some registrars. specifically the large ones that have much higher cost than what we for example have because they have not implemented DNSSEC, there might be an interest from the registries to move faster forward and start to bypass the registrars and get the DNSSEC information from the child directly. That would not be a good thing.

Having the registrars fetch the information from the child zone will be really good. Today we don't have a standardized way to move the DNSSEC material from the child zone to the registrar. Each registrar, including us, have their own private to private API but it's even more non-standard than what the registries are doing with EPP. I myself sort of violating much more of the standardization than what I'm complaining on here.

But if the registrar is using this, that's fine. We'll still keep the competition issues, the ability for registrars to compete regarding DNSSEC, which is one big sort of advantage for a small registrar like us. Don't forget when discussing these kind of things what path the information flows. I don't want to have too much changes in that. Then I think that was the last slide. Yes, thanks.

MICHELE NEYLON: Thanks Patrik. Thank you, Rob. Let's open this up I suppose a bit for more discussion. Warren, what a surprise. Hi, Warren.

WARREN KUMARI: If people are interested in what Patrik was just talking about, during Dan York's panel there's going to be some discussion of that draft and some details that addresses much of what Patrik was saying.

UNIDENTIFIED MALE: Which is coming up next right after this one.

WARREN KUMARI: There's the Root Key rollover apparently in between.

UNIDENTIFIED MALE: My bad. I'm sorry. Root key rollover first then we'll have that discussion.

ANNE-MARIE EKLUND LOWEINDER: I'm Anne-Marie Eklund Löwinder from dot-sc. I have also a strong message to the registrars and that is to make sure you use secure channel to exchange the key material from the child because I have seen very, very bad examples. That is something to take care of.

MICHELE NEYLON: [Jacque]?

[JACQUE]: First of all, we're trying to make it easy for registrar to work with us. We're implementing. We're going to accept a key or a DS or both or whatever you want to give us. We'll take it and we'll make it work. Our goal was to make it super easy for the registrar, the customer. But with the [CDS] stuff to automate the exchange of keys, the last thing I saw

was that the registrar was to poll the child to see if there is changes. That's more work. This is code you need to write to see if there's new keys to publish. I thought the whole goal was to make it simple. You're adding more work on your site to be synchronized. But it's a chicken and egg I think.

PATRIK FÄLTSTRÖM: I'm all in favor of having a standardized interface between the DNS operator and the registrar. If it is the case that one of those interfaces to be implemented I don't see any problem implementing that. If I look at the cost for implementing that interface and the cost for implementing the per registry specific notifications that I need to be able to receive for each individual registry I communicate with if the registry is the one that is polling that is much, much more work than having me polling the child because the registries do not have a standardized notification mechanism.

MICHELE NEYLON: Jim Galvin?

JIM GALVIN: Thank you, Michele. Jim Galvin with Afilias, a registry service provider. I'll speak a little bit to a couple of things that Patrik said there. On this issue of DS versus DNSKEY and which one takes in 5910, to a large extent we don't really care. But I view it from kind of the same position that a registrar does or a service provider with a lot of registries. We don't get to decide. We're driven by what they want.

We can sort of provide some advice and recommend one versus the other, but as I recall those arguments of DS versus DNSKEY, at the time that that standard was created there were a lot of politics involved in that. Part of it is nation states, which I guess always seems to be the problem maybe in some of this, decide what they want to use.

The issue comes down to algorithms. That was the issue that we ran into at the time and why even we agreed to allow for the choice. I don't think that you get to take the blame in allowing for the choice. It was sort of driven by the community and that's what it wanted. Let me pause there. It looks like you want to say something.

PATRIK FÄLTSTRÖM: Absolutely. That is what I see now. From where I am I'll say that there is a higher interest of only supporting DNSKEY by the registries that would like to set a policy on what cryptograph they are using to create the DS. Remember that the registry is the one signing the DS, so absolutely as a registrar to understand that they should make choices for whatever algorithms and crypto and whatever they are placing in their zone.

That is also from a registrar perspective. We're only passing data from the registrant to the registry, and today it's pretty difficult for such a simple thing that if we are putting up a web page where people have their domain names and they're going to sort of copy and paste over a secure channel, Anne Marie – over a secure channel I promise. [Inaudible] is better, but over a secure channel.

But if people are going to copy and paste in the web interface the DNS material, just having the different web forms for DS and DNSKEY

depending on what TLD it is the client work with. I just don't know how to do that in a way that is possible to educate the customer. It's really, really complicated.

I just encourage everyone to try to support one. Yes. I really liked all the registries that support DS and DNSKEY because that makes it easier for us. As I said, we have chosen to work with DS. But I don't want to choose. I'm happy to change to DNSKEY, but I don't only want to change to DNSKEY if that is what I can use for every registry.

MICHELE NEYLON: Dan York. Okay Jim, I'm sorry.

JIM GALVIN: I'm sorry. I'm only half done. Actually you say registries want DNSKEY. We don't. We want DS.

PATRIK FÄLTSTRÖM: You want DS. Okay. But the others want DNSKEY. I decided I don't care.

JIM GALVIN: The reason why we want DS instead of DNSKEY is because we don't want to have to do all of the algorithm support. Now you're down to the issue of nation states and registries. They want to choose what algorithms are used for things. Creating the DS means that we have to do all of that instead of just taking it in.

PATRIK FÄLTSTRÖM: So everyone in the room you now understand what situation we registrars is in. You ask why we think that it's costing too much. You might still think that we're stupid but now at least I hope you understand.

JIM GALVIN: No, no. We're in the same place. I'm agreeing with you. It's a problem. It's an issue. The second thing that I wanted to get to though is you're talking about using the protocol that Warren's going to get to when we get there and talk about it. I actually support the idea that registrars should do that polling and should get that data and then push it up into the registries. I like that solution.

Part of the reason for liking that, though, is because the alternative is I as a registry have to do that polling and I'd rather delegate that and distribute it out to the registrars. Otherwise, that's a bigger responsibility on registries. Also, as you said, it maintains the retail relationship in the right place. Thanks.

MICHELE NEYLON: Thanks. Dan?

DAN YORK: Before I do that, can I yield to – Warren did you want to? He's shaking his head.

MICHELE NEYLON: You're all being so ridiculously polite to each other. It's hilarious to watch from up here.

DAN YORK: I can be rude then if you'd like me to do that. I want to emphasize a number of the points. I won't because of the time we have here, but I think Patrik one point you made though that's critical. From looking at a deployment perspective, this issue of the registrar communication and getting this information is a critical one.

But the other one you also mentioned is this idea around DNS operator to registrar communication and the fact that all the registrars have their own separate proprietary APIs. This is a challenge beyond even what we've highlighted here is this issue that we need to look at that as the next step in some way. But I don't know that we'll ever get there.

MICHELE NEYLON: Actually, just speaking to that speaking as Chair of the Registrar Stakeholder Group, we've had DNSSEC updates and things from various parties over the last few years. There was an initiative to collaborate between the more technical staff of the registrars and the DNS operations community. Some work around this kind of possible standardization or something. Speaking exactly to this but how you can interact with the registrar. It died. It just died a painful death. The thing is it comes again back to this demand. Supply and demand, chicken, egg. Call it what you will.

JIM GALVIN: On that same topic, though, I guess one interesting point would be do you have a sense of how many registrants wind up hosting their domains with their registrar versus using external DNS operators?

MICHELE NEYLON: Totally without checking our own database probably I don't know 80-plus percent. The third party DNS providers that we see people using it's either because you're talking about, say, a country code where we happen to be the registrar choice for most people. Then they might use somebody else for currently the hosting piece. I don't offer it.

Other third-party DNS providers maybe it's because they're using that for a whole load of things and they've got some funky options that people like. But I think that a lot of people, even if they're hosting their websites elsewhere and they're not using us for the hosting, they're still using our name servers which causes all sorts of interesting legal issues at times. But that's maybe out of scope here.

PATRIK FÄLTSTRÖM: You also have lost the other separate DNS operator all the enterprises that want to at least run the master zone and manage the key themselves that need to have a registrar.

MICHELE NEYLON: Warren looks like he's about to explode. Go ahead, Warren.

WARREN KUMARI: Thanks. I think I'm just going to suggest that maybe the details on what Patrik was talking about we should discuss later after. I've mumbled about this draft because some people have read it, some people haven't, and so some people are very confused as to what's going on.

MICHELE NEYLON: Just one thing. I would remind some of you within the technical community when we're talking about ICANN and gTLDs please bear in mind that it's the registrar whose neck is on the block. We sign a contract with ICANN. We are responsible for the domains. It doesn't matter a damn whether you think we're not doing a good job with the DNS. You're not the ones who can lose your livelihood and have your contract terminated for something weird happening. Russ, go ahead.

RUSS MUNDY: I had one question relative to the resellers of registrars and the new RAA agreement. Is there any expected relationship in terms of encouraging or fostering provisioning for DNS capabilities by the resellers at all as a result of this?

UNIDENTIFIED MALE: We don't have resellers directly but I did reach out to a few of our friends in the Registrar Stakeholder Group who do support resellers to say, “Okay you've looked at this provision. What do you think?” The simple answer was we'll extend our APIs to our resellers to allow the key records to be sent back. It was as simple as that.

There was no further communication or push or emphasis on support of service. It's just that they would enable the reseller to send the records to them and manage the records.

MICHELE NEYLON: Just adding to that. The 2013 RAA is the first time that the concept of reseller has actually ended up in the contract. This is one of the things that I know a lot of people have been kind of struggling with. For a lot of the registrars our thing is, well look, we're the ones who have the contract though we are also conscious of these entities existing.

I think one of the challenges for registrars at the moment when looking at the 2013 RAA is that that entire document took 18 months of intense negotiations. There was a lot of backwards and forwards and some of the language that's in there when you look at it you might say to yourself, “What the hell does that mean? Where does this come from? Why is it there?” So you talk to ICANN staff and you say, "Okay, there's this paragraph. There's this obligation." They go, "Yes, yes, wonderful. Isn’t it?"

We're like, "Okay, that's great. What the hell does it mean?" How are you actually going to check for that? One of the things from our perspective is anything that's an obligation for a registrar is something that ICANN can potentially take a compliance action against us on.

But if we don't understand how they’re going to check it, then it makes it quite hard for us to understand if we're complying. It doesn't matter whether this has to do with something very, very technical or something more policy [and legal]. Patrik, go ahead.

PATRIK FÄLTSTRÖM: Being a sub-registrar for the gTLD, we are not an accredited registrar, [inaudible] point that out, partly because it's extremely difficult for a small organization to actually get the insurances that ICANN requires. So we can simply not sign a contract with ICANN. We cannot be, for legal reasons, a gTLD and an accredited registrar regardless of how much we would like to.

We're a sub-registrar, but let me tell you it was not hard at all to find a registrar that handled DNSSEC. We are completely DNSSEC compliant even though we're a sub-registrar. That works.

The second thing is that we are, though, a registrar for many ccTLDs and we have sub-registrars. From our perspective, specifically as a registrar that has sub-registrars, when we have been working with our legal department or with the legal departments of other registries – for example .LC – I think our view is just like Michele talked about is that it's we as the registrar that has the contract with the registry. We are the ones that have to make sure that everything that is done under that contract is according to what's in that contract.

We are really nervous about having even the concept of sub-registrars. So in general we are objecting to that. Because if we are doing it ourselves, or a sub registrar or whatever, should not really matter. Because every text that is about a sub-registrar that might imply that there're certain things that are not responsibility we have but instead directly between the registry and the sub-registrar.

All of you that are ccTLDs, I'm not saying that you should not talk about sub-registrars. You might allow it or whatever you want to do. But don't fall into the trap to just by default have it just because ICANN is talking about it. Think about what the situation is in your context and make a conscious decision.

Because we have for example, as I said, sub-registrars. Some registries are perfectly happy to only put all requirements on us. And we as the registrar have absolutely no problem taking absolutely full responsibility both for us and for our sub-registrars. We're just passing the contractual requirements on to the sub-registrars.

MICHELE NEYLON: I think we're kind of running way over here. Just one thing I would kind of say again is that, for a lot of the registry operators, you view yourselves as nice little islands. You forget that from the registrar side we're dealing with lots of you. Doing something new and funky and inventive doesn't actually help us because we're dealing with so many of you.

At the moment, registrars like ourselves are dealing with maybe 50, 60 or 100 different domain extensions across Cs and Gs. In the new gTLD world that number could go up several multiples, or not if you make it hard for us to integrate with you, be that for DNSSEC or for anything else. I say this about anything. Anything you're doing if you get funky and inventive you're actually shooting yourself in the foot. Am I going to end up giving you the last word, Jim? I am, okay. Go on.

JIM GALVIN: I just wanted to point out that there's a new working group that's looking to get started in the ITEF for registering EPP extensions. I just think it's important to close on that point. Registries who do have their own things should seek to get them registered and be added to the list so that it's much easier for people to see and maybe that'll help consolidate some of these differences or bring them together. Thanks.

MICHELE NEYLON: That's a very good point. I think at least one of our staff is involved with that. The more you combine things – because what we've seen is two registries, same function – but no, It's a different command. Why? Why for the love of God would you do that?

UNIDENTIFIED MALE: Registrars please push on your registries to bring them up.

UNIDENTIFIED MALE: Thank you Michele for continuing your efforts to talk about this and to speak about this both here and within the Registry Stakeholder Group. So thank you for the work you do.

JULIE HEDLUND: Please join me in thanking this group. Now we'd like to suggest a slight change in the program. Since some of the topics in the automated update of DNSSEC information are related to the conversation we've just had in this panel, we are going to swap that with the Root Key Rollover presentations. We're going to move ahead to the panel discussion on Automated Update of DNSSEC Information. So that is Dan

York with Francisco Cifuentes, Ondrej Filip and Warren Kumari. Please come on up.

Then we will follow that with the Root Key Rollover presentations. We're still behind our time. We can probably start lunch a little late unless of course our stomachs all revolt. I'm going to switch slides while the panelists are coming up. Thank you.

DAN YORK: Welcome. We're going to do this. The order I want to do is I want to have Warren talk first about the Automating Maintenance of Delegation of Information. Then I'm going to follow with Ondrej and Francisco here. I want to do Warren first here. Okay, yep. You're all set. Warren let's take it away.

For everyone who's remote as you heard Julie say we're switching the order of the sessions here. We're going to be doing this and then Root Key Rollover. Our goal is to wind up with all of these fairly quickly so we can have the lunch that's coming in here.

Russ is telling me we're just switch things a little bit more and do some lunch and then we'll do Root Key Rollover depending on the timing. Warren, let's go.

WARREN KUMARI: Alrighty. Let me try to tell Adobe not to explode anymore. You want to reconnect Adobe quickly?

DAN YORK: For the folks who are remote, we are yet again experiencing some Adobe Connect information. We'll put the slide link in the room while Warren continues to speak here.

WARREN KUMARI: While we're busy doing this this is going to be discussing two drafts that we have in the IETF. These are about automating the maintenance of DNSSEC and other delegation information. Hopefully it will address some of the issues that Patrik brought up and also hopefully make stuff easier for registrars. Especially if Michele's still around. There you are hiding behind Dan.

What's the actual issue that we're trying to solve? Well, rolling DNSSEC Keys is hard. Actually it's not really the rolling of the keys that's hard. It's the publishing of the new keys that's hard. Currently if I want to roll the keys on the domain that I own I have to roll the keys, get the new DS record and then I need to log into my registrars web interface. Chances are I've forgotten my credentials, which means I need to do password recovery. Then I need to log in and then choose domains and then find the domain I want to manage and then scroll up and down. Click mange and then click manage DNS information and then click manage DNSSEC information and then click bulk upload and then cut and paste the new DNSSEC information and for some reason my registrar likes this in a different format to what the tool generates. So I have to add and remove some spaces and then curse a little while and then try it again and then curse some more.

And I also need to figure out if I'm replacing all of the DNSSEC Keys or if I'm just adding a new one. This is confusing to most people and they

manage to screw it up. It's also fairly dangerous. Many of the DNSSEC outages have been key rolls where either the human just forgets to do it or makes a typo, something like that. In many cases registrants outsource their DNS operations to a third party. In these cases I think this actually bit Dan once.

The operator emails the new DNSSEC information to the registrant and says, “Please upload this.” If the registrant doesn’t see this obviously that doesn't happen. The zone goes bogus. One of the solutions I have seen proposed to this is the DNS operator says, "Well just give me the credentials to your registrar and I will log in as you when I need to do that." That seems like a really bad idea. As Patrik and a number of folks have said, "This doesn't end well."

So what we're proposing in this draft is that you simply publish your new DNSSEC Key information in your current zone. You stick it in a new resource record that has a C in front of the current type.

If this is your new DS record, you publish this in your zone with a C in front of it. If your parent is one of those that prefers DNSKEYs instead of DSs – and this is a religious argument. There are reasonable arguments on both sides. But if your parent prefers DNSKEY we can still accommodate that. You publish your new DNSKEY in the zone. You stick a C in front of it.

DAN YORK: Warren, to be clear, too, you're publishing both. Your DS record is there and you're publishing now a new CDS record, etc.

WARREN KUMARI: Yes, you can actually choose if you would like to do that because some people want to do prefabrication of keys. If you're a sane child – sorry, the C in the CDS stands for child. If you're a sane child you will publish both. You have the right not too though.

Now what happens is your parental agent will come along and will poll its children and if it finds one of these CDSs it will publish it. So who exactly is this parental agent?

MICHELE NEYLON: Sorry, this is me asking really dumb questions because that's kind of what I do. Is this a new type of DNS record you're creating or you're repurposing an existing one?

WARREN KUMARI: Yes and no.

MICHELE NEYLON: Oh come on.

WARREN KUMARI: The IANA has already allocated it to us [inaudible].

MICHELE NEYLON: Let me rephrase that. So this is not something that is currently supported in any software, apart from something truly experimental that probably lives on some weird server that nobody can actually use.

WARREN KUMARI: Yes. On a [inaudible] box.

MICHELE NEYLON: But it's not standard at the moment.

WARREN KUMARI: Not standard yet. So who's this parental agent? This is a new set of terminology. In the RRR world, the child is the DNS operator or the registrant. The parent as you would expect is the registry. In the RRR world the parental agent is the registrar. There's a reason that we're using new terminology. That will become clear in a minute.

The way that this works is the registrar will poll all of its children every now and then looking for CDS records. This is a standard DNS lookup. Nothing special here. Just a different type. Then the child is running standard DNS software and they will respond with CDS or CDNSKEY. As I say, standard DNS requests. Standard DNS name server. Standard response.

The parental agent will then pull the C off the front. Basically different way to stick it back to the original resource record type and publishes it in the parent using whatever protocol it currently uses. Probably EPP or whatever it currently uses.

The reason we have the new terminology is in some cases the parental agent and the parent are the same organization. This is very common in things like enterprises, educationals, some ccTLDs. If that's what they want to do and Patrik will probably jump up and down and shout, "No,

no." But it's the ccTLD's right to decide to do that if they really want. They then publish it how they currently do it themselves.

Another very common use case is the DNS operator is the Parental Agent. This is when the registrar runs DNS on behalf of its registrants. In this case it can continue to use what it currently does. Doesn't have to use CDS. It might choose to use CDS anyway because we're expecting this to be built into a bunch of tools. A bunch of tool vendors have already said they're going to support this. Either you use what you currently do or use this if it's easier.

Some additional details – polling. Yes, we're currently specifying polling. This is actually designed just as a framework. We expect there to be additional triggers if people would like them. Additional drafts specifying how to trigger this. If you're a registrar who doesn't want to poll because you think that's heavyweight, you could have a button that people click. You can supply a standard, simple restful interface.

Basically it's just a trigger that says, "Please go and do this work." You don't need to authenticate it because the system self-authenticates itself, which will probably make Anne Marie happy. The key upload now happens in a secure manner.

There's another solution called CSYNC that compliments this. It does the same sort of thing but it's for name servers and glue. It's simply a Type Bit Map of what records should be copied. Related; not the same thing.

The difference the CDS/CDNSKEY draft talks about DNSSEC stuff so new DS records, new DNSKEYS. CSYNCH is used for other stuff. Name servers

and glue and potentially also as a trigger for CDS if you'd like to do that. Questions?

DAN YORK: Go ahead Michele.

MICHELE NEYLON: Thanks. Again, I'm just asking kind of dumb questions because I'm not that much of a geek. So you're creating a new type of DNS record, so you'll probably get the likes of BIND and things like that to support it. I suppose it's more of a question this was more of an observation that if you manage to get it into BIND you still need to get it into our interfaces. That can become a bit of a challenge.

For us as a registrar, unlike Patrik's registrar, we didn't build everything from the ground up. We've taken software from third party vendors and we've ended up in some ways it's been fantastic. It's been great. I can rely on a third party and throw money at them and they make stuff happen. But the down side is that if I need to make stuff happen faster than they like it, I can be waiting a long time. I suppose it's more of an observation than anything else.

WARREN KUMARI: We understand there is some more work for registrars here. Hopefully the fact that zones don't go bogus as often means you'll get less calls, less support issues, things like that. We have a registrar side proof of concept. This is not complex from the registrar side, but obviously if someone else has difficulty at all you need them to add the support in.

Another thought is registrars might want to charge for this as an additional service.

DAN YORK: I have a comment over here, but Russ, it looks like you want to respond to this. I think I know where you're going to go.

RUSS MUNDY: One of the things that you get into anytime you make a change of this nature you have to have the software to actually do whatever it is you're specifying. There are in fact a batch of tools out there. We produced a whole gaggle of them, DNSSEC tools. We will likely have a support for this and many, many of the DNSSEC tools, including ours, are open source, freely available. And so it becomes a matter of expertise as opposed to dollars in most cases, but dollars if thrown at it sometimes might expedite too.

DAN YORK: Do you have a response to this? Alright Patrik. Come on.

PATRIK FÄLTSTRÖM: The reason why I support this even though of course it will be a cost is that one it has nothing to do with the user interface, which is expensive for translation, it's language and whatever. It is something that is done behind the scenes between us and the DNS operator. That's cheaper. It is a mechanical way of filling data into our database. No humans involved. That's relatively cheap.

The second reason is that I will of course not implement this unless I do see people agree that this is how it should be done, because I don't want to implement two of these different kind of versions. The third one I still see this being cheaper to implement than the various different kind of notification mechanisms that I would handle if it is the case the registries starts to start of sort of accept these sort of things.

Yes, it is a cost. I will have caution. But I think so far it looks pretty darn good. If it is the case then we just stop here.

DAN YORK: Thank you. Michele, you do have an obvious point that, yes, obviously getting out there in the software is the first step. Getting that deployed into the actual community of people operating the servers is another issue. We have time for one more question here.

UNIDENTIFIED MALE: Sorry. I said I think it got covered with some of the discussion of what I was going to ask. Thanks.

DAN YORK: Perfect. Any other questions? Warren you want to respond? And then we need to go on.

WARREN KUMARI: As I say, this is still a draft. We would very much like to talk to registrars, registries, people who might implement this to make sure that we cover

what they want and to make sure that we solve their use case and make the system as simple for them as possible.

DAN YORK: So perhaps this is an opportunity we could talk to Michele about how we get this out to the Registrar Stakeholders as far as for comment. Okay, go ahead.

MICHELE NEYLON: One of the problems with anything involving IETF stuff is that the number of registrars who are on any IETF mailing lists you can probably count with, I don't know – do you get past the fingers? Do you get to the toes? Probably not.

This is something where I think Dan and ISOC and your ability to take these ridiculously complex technical things and break them down into manageable and understandable nontechnical language. That's where you might come into play. If you can get me something in simple terms that my members can digest without having to resort to, "Oh God I'll have to run this by our sys admins," then that might be something.

If you can say, “Right, this is a technical solution to a problem. This is probably going to maybe save you money and maybe generate revenue for you,” and you can actually put that in terms that we can understand simply, then yeah, get that to me. I will happily share it with our members. Now I can't guarantee that any of them will give a damn or that any will reply. That I can't do.

DAN YORK: Sounds good. Well we appreciate that. I took an action on that. I'll work with Warren. We can see about if we can come up with something around that.

MICHELE NEYLON: Well, you know where to find me anyway.

DAN YORK: We do, yes. With that I'd like to move on and have Ondrej speak about DNSSEC Automated Tools. They're going to switch seats here for a moment. For the folks who are remote we apologize. We're still having Adobe Connect connection problems so we're probably going to again resort to – we're trying to get back in there. And then we will go with that.

Let me just begin with an introduction here as far as Ondrej is involved with the CZNIC or CZ.NIC depending upon how you wish to pronounce it. They create a good number of tools around this and have been one of the folks providing a lot of great support for helping make DNSSEC more deployable out there. I believe that is what we're going to be hearing about right now. I'll turn it over to Ondrej.

ONDREJ FILIPE: Thank you very much.

DAN YORK: For the remote folks, it crashed again. We're just going to keep on going.

ONDREJ FILIPE: Thank you very much. My name is Ondrej Filipe. I will go a little bit against the stream because there is many people talking about increasing the number of DNSSEC penetration. I will do exactly the opposite. I will talk about how to decrease it a little bit.

Just a short introduction. I know we are one million domain and we have very large R&D departments. [Inaudible] actually bigger than the registry, so I always say we are an R&D company with a small registry attached to that. We do a lot of stuff for the good of the Internet and for DNSSEC as well. If you are interested, check the web pages.

One of the flagships of our development is registries [inaudible]. That's an open source registry running mainly .cz and CZNIC. However it's deployed in many other countries. It's completely DNSSEC ready, fully automated. Since I presented the software last in Durban I will not repeat. If you are interested, you can check the presentation. That's about the registry software and it's related to this presentation.

One more thing that will help you understand our situation – we have a fairly good DNSSEC penetration. About 37% of domains are signed. Again, you can check those numbers. We have daily statistics from that. Penetration's very high.

One more thing I need to explain before I will jump into do presentation, it's all data structure. That's something I will also enter the discussion about DS records or key record or DNSKEY. The structure for domain is following. We have a registrant, domain holder. That's something usual. It's hard to present in such an environment I must say.

We have a certain number of administrative contacts and then we have two special objects which can be attached to a domain versus name server set, which is a list of name server plus a technical contact and a keyset, which is very similar object. It includes some DNSKEY, so some key material; and again technical contact.

Why we do this is because multiple domains can share just a single NS SET and KEY SET. If a registrar has 10,000s of domain which have the same setup, they can use just a single object in the database. This helps especially with acute rollover because [inaudible] registrar can just update one object and all the domains are okay and the DS records are recalculated for them.

That is the situation. Now what's the issue we wanted to solve? We got a very large amount of domains signed. Some of them became bogus. We saw that especially during the transfers between registrars the new registrar forgot to update the key material. Some of the registrars are just not very good in technology. So we face some percentage of errors. Of course the more domains are signed, the more number of failures we face.

That was a problem not just for those domain holders but also for ISPs because when we started to talk to them and we told them, "Guys can you start validate?" They said, "Well, we would like to but if you will start we will see less domains in the market than those that do not validate." That can be a problem and we don't want to solve those problems so we will not start validating." That was an issue, and then starting to do something with that.

What we did, we checked the registry. We explored where those errors comes from. We started first round of cleaning the problem. The first thing we did a small change in the EPP. That was that we delete the secure delegation that pointed to the KEYSET in case there is any change on name servers.

If you wanted to update name servers, you need to explicitly re-add the secure delegation. Then we are sure that this is really what is meant and that there's not just some error. It helped in many cases, especially during the transfer set between registrars or if the domain was transferred from DNSSEC-aware to DNSSEC-ignorant registrar.

But in some cases, it didn't help. Some of the registrar have Smart registrar system and when they saw that some object was deleted they added again so it didn't help. This is the first round. It helped in many cases and decreased the number of errors but we had to continue.

So we started a second round that was much broader. We went through all the zones and tried to detect the bogus DNSSEC signatures. We set up a simple mechanism for removing those delegation. Of course there had to be some DS records or DNSKEY reference. The name servers were reached so it's not the [lame] delegation. If name servers can be reached it's a different problem so we don't have to care about DNSSEC.

For five consecutive days we saw that either no DNSKEY in the zone or it's bogus or the signature has expired and the trace from root zone failed. In such case, we started to do something with the domain. That something is influenced by the registrar decision. When we presented them what we are going to do some of them say, "Yeah, please delete it. We don't care." [Inaudible] so please act on behalf of us.

Some of them just minority said, “Yeah, could you send us a list of those failures of the bogus validation? We would like to do by also something with that.” Minority decided and that’s fine.

Of course deleting something within database is not so easy, so we’d rather to be very careful and not to make any mistake. We divided the situation into two different problems. If it’s a problem which is related to some well-known KEYSET – some KEYSET which is used for thousands of domains or ten thousands of domain – then we just simply delete it because that’s obviously some error.

But if the DNSKEY was related to single domain, we’d rather contact the domain name holder. Usually we called the man and ask him, “We saw this problem. Are you aware of that?” Of course when there is something wrong with the system – if for example there’s more than 100 secure delegations to delete a day or any other condition, we stopped the process and checked it manually.

Here are some numbers from this attempt. We started two years ago, August 2011. During August we deleted about 3000 DNSSEC signatures the reference to DNSKEY. Also we presented this result to the registrars and some of them fixed their EPP script interfaces and stuff like that.

Since September 2011 we started the second round. During this month we deleted about 1200 references to DNSSEC. Again the registrars continued fixing their interfaces. Since that during 2012 and 2013 we delete about 9 bogus DNSSEC references a day. In a year we can say that the error percentage is below 0.1%. That’s probably something we can [inaudible] rate in such a huge system.

Conclusion. If you will have a lot of domains a high penetration of DNSSEC you will face some errors, so be prepared for that. Of course, this may discourage some ISP to validate. We did something with that. We cleaned up the issue, and after that the majority ISP signature [inaudible] started to validate. Almost all ISPs or cell phone operators currently support.

The DNSSEC chain is complete, of course except the end user validation, but that's a different issue. ISPs validate and the whole DNSSEC traffic is quite secure in the country. Thank you very much.

DAN YORK: Okay. We have time for a couple of quick questions. Anyone? Russ?

RUSS MUNDY: Ondrej, when you're using one key for a large number of zones and you do the Key Rollover do you resign and republish all the zones, if you will, in synchrony or you do them in some sequential basis using the same key?

ONDREJ FILIP: We have just one zone, so I don't understand the question.

RUSS MUNDY: I understood what you were saying is the second level zones that a large number of them are signed with the same key. When that key changes is it…?

ONDREJ FILIP: What the registrar just does is he updates the KEYSET so there are currently two keys in the object. Then he's starts slowly to resign all the zone that he holds. After the process is finished he just removes the first KEYSET and that's all. Just two transactions between us and the registrar. Everything, the job is done by the registrar so it's very easy for them.

RUSS MUNDY: So then the registrars, for the most part then, are doing their resigning of those multiple zones with the same key in a somewhat sequential manner as opposed to one giant batch.

ONDREJ FILIP: Honestly, they have tens of thousands of domains so it takes some time to resend them all. Usually I know the process for some of them were more than weeks. That's why there needs to be some time.

RUSS MUNDY: Thank you.

ONDREJ FILIP: Of course we recalculate all the DS records and we have dual DS records during the period in the zone.

DAN YORK: Okay, Warren?

WARREN KUMARI: Two related questions. One some people specifically want their zone to be unvalidatable, serve as a test domain. Two, for ones where you've removed the breakage, have you had any customers who've got grumpy because suddenly their zones unsigned?

ONDREJ FILIP: Good question. That's why we call them manually. That's why we inform them. Honestly once it happened that the man said, "Yeah, that's on purpose. I really want this to be broken." And we said, okay. Then we are fine and we just mark this domain that's okay. There's an exception in the script. Super majority of people said, "I don't know what you are talking about."

I will continue work. Don't be afraid we will just delete something in the database. They said, "Do whatever you want." Some people say, "Yeah, thank you for calling me. I will fix it." That's the result. Just single man said "Yeah, it's on purpose."

DAN YORK: Thank you very much for that. One more [inaudible]?

UNIDENTIFIED MALE: If I was lost please forgive me, but how often do you check the bogus status in the registrant?

ONDREJ FILIP: As I said, it's daily. Every day we run the script through all the way.

DAN YORK: Please join me in thanking Ondrej for that presentation. And now for something a little different to move into a different range with automated tools, Francisco is going to talk to us a bit about a different cryptographic backend. So we're going to get a little deeper into the puzzle here. I'll turn it over to Francisco.

FRANCISCO CIFUENTES: Hello. My name is Francisco Cifuentes. I am a research assistant on NIC Chile Research Labs. I'm going to talk about DNSSEC automation. In particular, about Key management automation. Our work is called Threshold Cryptographic Backend for DNSSEC.

On ICANN 40 we proposed a system that follows the layout shown in the slide. It has a zone database system which store DNS records. DNSSEC zone generator that converts the DNS records into a valid DNS zone. Signer Robot, which keeps every DNS record from the zone database system with a valid signature, and a cryptographic provider that provides every cryptographic function that signer robot may need.

In simple words, both BIND key management solution and on open DNSSEC follows this architecture in some way. We used open DNSSEC by giving it a new cryptographic provider [inaudible].

I'm going to focus on the cryptographic provider. There are some needs that the cryptographic provider has to satisfy. Zones need to be re-signed periodically. The keys must not be closed.

In order to satisfy these needs many DNS deployments have chosen Hardware Security Modules (HSMs). That is a very secure and fast cryptographic cover to satisfy these needs. To communicate with this

hardware the signer robot uses the PKCS #11 API developed by RSA Labs. But there has been some problems by using HSM. First, hardware fails. In 2010 there was a problem with the [inaudible] domain because hardware failure of HSM.

Also there is a problem because HSMs are expensive. That can be a problem to a smaller organization. Ones who employ DNSSEC. There is software implementation of the PKCS #11 API called SoftHSM that is developed by the open DNSSEC team, but that implementation can be vulnerable because someone can copy the cryptographic objects from the file system easily.

What we propose in order to replace the Hardware Security Modules is a Threshold Cryptographic Backend. It is distribute cryptographic backend that has many models that can be each of them can be different machines. It has a signature dealer on n nodes, a number of nodes that make the work in a distributed way. If you want more information about these you can ask for it later.

On one side we have open DNSSEC. On the other side we have the Threshold Cryptographic Backend that was implemented at the time [inaudible]. It was missing what is in the middle the PKCS #11 API layer. That's what we have done recently.

On the right you can see in the blue box is the Threshold Cryptographic Backend that was implemented at the time of ICANN 40, and in the red box is what we have known personally. It has PKCS #11 API layer, Hardware Simulation Module that simulates every semantic of the HSMs – in particular the cryptographic objects management.

Communication module that communicates to the Threshold Cryptographic Backend through our Rabbit MQ.

This system has many properties. It is distributed, fault tolerant, robust and secure. It is distributed because a private key is split into shares and then distributed among the nodes. In that implementation one of machines generates the key and immediately sends to the nodes through our RabbitMQ. Also it is this simple because the signing procedure is called in each of the nodes making the whole distributed process okay.

It is fault-tolerant because a subset of the nodes can fail and the signing process will be completed successfully. For example, if we have five nodes, we turn off two of them then the signing process can be completed successfully if we choose the parameters well.

It is robust because failures and attacks can be reduced implementing nodes in both different programming languages and operative systems. In technical implementation we have to use java programming language, but we can use every operative system that [inaudible] has support on.

It is secure. That is one of the main properties of this system. Because no one holds the complete private key. It is distribute among the n nodes. In [inaudible] implementation as I said before the machine signature dealer splits the key into shares and the shares is the only things that start in someplace.

It is secure also because more than k nodes – k is the parameter of the system – have to be compromised to authorize faked signatures.

Summarizing what we have done here, basically PKCS #11 API provider that uses the Threshold Cryptographic Backend implemented at the time of [inaudible]. Actually signs DNS record.

What it is not is a fully compliant PKCS #11 API implementation. We have only focused on the functions that open DNSSEC Version 1.3 uses.

There is future work here by completing the PKCS #11 implementation in order to make it usable directly from BIND or any other software in any other use case of the PKCS #11 API. Also we have future work by testing this on a real zone set. If someone wants to collaborate, just contact us please. That's it. Questions?

DAN YORK: Thank you, Francisco. Do we have some questions? We have a bunch in there. I saw Roy first. Go ahead.

UNIDENTIFIED MALE: Regarding HSM as you were saying is it a special appliance or it can be intel server or some hardware? Is it special hardware appliance, HSM?

FRANCISCO CIFUENTES: No, you can use any computer.

UNIDENTIFIED MALE: The software, can it be installed as a virtual appliance like on [inaudible] or [inaudible] server?

FRANCISCO CIFUENTES: Yes, you can. Actually we have tested this on [inaudible].

DAN YORK: Thank you. Roy?

ROY ARENDS: Thank you for the presentation. I found it very, very interesting. I work for Nominet, the UK operator. You mentioned UK Nominet. I just wanted to point out that the issue that we had was not due to a failing hardware security module.

What happened was one of the many hardware security modules failed and then we decided to roll to a new system and we made a small mistake there. This mistake would happen if we used it software based backend, any backend basically. So independent of the hardware security module.

I just heard you saying that your backend is basically a software based backend. So this doesn't necessarily have the same security features as a HSM backend. I think you've solved the redundancy issue, which is very nice. A fundamental thing that you've implemented is a NFM scheme where you need to have at least n partners of n systems to cooperate to generate a signature. Is that correct? I'll take it offline.

DAN YORK: Roy's going to take that offline. I saw Rick, and then I've got Warren.

RICK LAMB: Thanks Roy. This is Rick Lamb. This is really cool stuff. I remember seeing your presentation, one of the earlier papers on this. I assume first of all it's open source?

FRANCISCO CIFUENTES: Yes, it will be published on our [inaudible] repository.

RICK LAMB: Okay. That's really cool. My second question is have you considered incorporating time into this? In other words computing the RR sig in the distributed fashion. Because right now the problem is with the standard PKCS #11 interface if you have an insider attack someone could generate an RSA good for 10, 20 years so you're kind of hosed.

But if you pushed out don't be tied to the PKCS #11 interface, if you pushed out the calculation the full [inaudible] calculation and distributed that you'd have a set and forget system. Anyway, my main point is this is really cool stuff. Thank you.

DAN YORK: Thank you Rick. Warren?

WARREN KUMARI: Something that was unclear to me – and apologies if I missed it – is if you're using something like Shamir's Secret Sharing algorithm and then having the distributed bits actually combine a bit and have a single person do the signing or if the signing itself is actually distributed amongst all of the nodes?

FRANCISCO CIFUENTES: The whole signing procedure is distributed. Did I answer your question?

WARREN KUMARI: I guess we can chat more offline.

DAN YORK: Thank you very much Francisco for bringing this research here. Roy, if you could come up here and get ready to be on queue for the Great DNSSEC Quiz because I realize that you and I are what's standing between everybody here and lunch, so we're going to try to do this quickly.

This actual example of what Francisco just talked about is a great part of what we have tried to bring to this DNSSEC workshop. I'm speaking here as part of the program committee that we'd like your feedback a bit about these workshops. We've been doing them as Steve said for a number of years. Russ is telling me eight years that we've been doing these workshops with the ICANN meetings. We're doing this.

We'd like to get your feedback. Here we go. We'd like to know how to do it. We've put together a little survey, which we'll put the URL out in a moment for all of you, but basically we'd like to know a little bit about you and comments about these workshops – what you'd like to see, what you'd like to hear.

We've got a sense from a good number of people that generally this seems to be a good format and people like it. But we'd like to hear from you first of all if you agree with that. If you think it's a good format, let

us know that. If you think there's things we could change, more of some of the types of things. Would you like to see more research like what we just saw from Francisco?

Would you like to see more operational suggestions? Would you like to see more case studies like we saw this morning? Would you like to see more funky tools? Would you like to see more cat pictures from Michele?

Whatever you'd like to see inside of here we'd like to hear back from you. We've done this. We've put together a little Survey Monkey thing. I have to say, I'm using the royal we. I should say that Julie is the one who did this. Thank you, Julie.

But we would like to have you go and take a look at this. That's how I'm going to leave it. The URL is here. We'll put this out into the various DNSSEC lists. The mailing lists are out there. We will also put it in the chat room and we would ask you, please go take a look at this. Let us know what you think because we as the program committee would like to hear back from you.

Any immediate feedback, questions? Anybody else? Then with that I will give you the last thing between us and lunch, which is the tri-annual – because three time times, The Great DNSSEC Quiz. For those of you who are new here – Roy are you going to explain this? It's not on or not up.

Roy, also just watch out. You're about to whack the webcam that the remote viewers are seeing. Remote folks we're getting the AV folks to take a look at this.

JULIE HEDLUND: While we're doing this. Remotely we are taking a lunch break from 12:30 to 1:30. This quiz is something we're only doing in the room I'm afraid. It's not something that's online. If we put it online everybody would have the answers and that would really not be all that fun.

You can go take a break and we'll be back at 1330 Buenos Aires time.

ROY ARENDS: Thank you everybody for joining me in the Great DNSSEC Quiz. We've been doing this for several ICANN meetings now. I think this is the third year in a row. Since DNSSEC is really not that hard and I'm the one who has to get all these questions together what I did was basically take a couple of new questions and take a couple of old questions.

If you've played this quiz before you'll probably recognize some of the questions. Hopefully not any of the answers. Anyway, so the way this works there is a form on your desk. If you don't have it, it looks like this. You can use basically any type of paper. There are 12 questions. Please put down your name on the form.

The way it works after we're done you're going to give your form to your neighbor and your neighbor will check your answers for you. If you win this, you will get a free lunch. Just to test this, also if you win this you have eternal recognition. Who remembers the last winner from last year? You remember the last one or you were the last one? You won it last time. Who knew this? Eternal recognition.

First question please. Some hints. Sometimes more than one answer is correct. If you think more than one answer is correct just put down all

the answers you think are correct for this question. However if you get one wrong all the answers are wrong for that question.

Next question, please. Which country code's Top Level Domain was the first to deploy DNSSEC? Was it Puerto Rico? Was it Sweden? Was it Denmark? Or was it Germany?

DAN YORK: No fair that we have some of those people right here.

ROY ARENDS: Next slide please. Which generic top level domain was the first to deploy DNSSEC? Was it .gov? was it .org? Was it .museum? Or was it .info? Michele as the world's DNSSEC fan you should know the answer.

MICHELE NEYLON: No. I can make an educated guess.

ROY ARENDS: Next, please. This is a little bit more technical. Which RFC has nothing to do with DNSSEC? Is it RFC 2065? Or is it B. 4035? Is it C. 2535? Or is it D. 4304? Nope

What does DS stand for? Is it A. Delegation Signer? Is it B. Delegation Security? Was it A. Delegated Signer or was it B. Delegation Security? Was it C. Domain Signed? Or is it D. Delegation Signer?

Number five. What does RFC 5011 convey? Is it a way to roll over trust anchors? Or is it about Hashed Authenticated Denial? Is it about Secure dynamic updates? Or is it D, nothing to do with DNSSEC?

Question six. What is a DPS? Is it a DNSSEC problem statement? Or is it B. Delay Protection Service. A Delay Protection Service makes sure that you have a delay. C. DNSSEC Policy Statement? Or D. Domain Preservation Society.

What does the D obit stand for in a DNS query? Is it DNSSEC off? Is it DNSSEC on? Is it DNSSEC [inaudible]? Or is it data out?

When was the root key rollover? I'm talking about the key signing key not the zone signing key. When was the root key rollover? Was it July 2010? Was it January 2012? Or was it on both of those dates? Or on none of these dates?

Here's a hint. If you want to have three points if these answers are correct you could actually choose A, B and C. But depends on if they are correct or not.

Question nine, please. How many different root server organizations are there? Is it A. 11? B. 12? C. 13? Or D. 14?

Number 10. What is the country code's top level domain for Curacao? Is it A. CW? Is it B. SX? Is it C. CR? Is it D. AN?

Next please. What does the AD stand for in a response? Is it A. Authentication Denied? Or is it B. [inaudible]? C. Access Denied? Or D. Authenticated?

This one is new. What is the oldest currently registered domain name? Is it A. Rootservers.net? Is it B. Symbolics.com? Is it C. Mitre.org? Or is it D. Nordu.net?

Thank you all for playing. Make sure you have your name on the form and please give the form to your neighbor. Okay, Julie, can you go back to the first question please?

So which country code was the first to deploy DNSSEC? That was Sweden. Well done. The correct answer here is B, Sweden. Anne Marie if you would have gotten this wrong, then…

Number two which generic top level domain was the first to deploy DNSSEC? Was it gov? Was it org? Was it museum or info? It was museum, C.

Which RFC has nothing to do with DNSSEC? Was it A, B, C or D? Anyone? Okay the answer is D. D has nothing to do with DNSSEC. RC 4304 nothing to do with DNSSEC.

What is DS stand for? I think my voice memory basically gave it away already. The answer is D. Delegation Signer.

What does RC 5011 convey? This is question five. RC 5011 answer is A, a way to rollover trust anchors.

Number six, now what is the DPS? Many of us think maybe that D would be a good answer. But the actual answer is I think C. Is that correct? DNSSEC Policy Statement.

UNIDENTIFIED MALE: Can we put it to be A?

UNIDENTIFIED MALE: More people might think A was a better answer even though it's not the right one.

ROY ARENDS: What does the O stand for in [inaudible]? The answer is of course C. DNS Okay. Number eight when was the root key rollover? Was it in July 2010, January 2012, both dates above or it hasn't happened yet?

The answer is D it hasn't happened yet. To be fair to be very, very clear there was an initial key rollover. Hold on. Hold on. There was an initial key rollover except it wasn't in July 2010. That was basically for the Mickey Mouse key that really didn't mean anything to the real very first key.

Nine, how many different root server organizations are there? I've got some bonus points for this one. Is it A. 11? B. 12? C. 13? Or D. 14? Anyone?

It's not C. There are 12 root server organizations out there. There are 13 letters you'd actually be right. Of those 12 here's the bonus question of those 12 this is going to be interesting, how many are not U.S. based? If you have three as your answer you can add one point. There are three non U.S. based root server organizations.

What's the country code top level domain for Curacao? Is it A. CW? Is it B. SX? Is it C. CR? Or is it D. AN? Now we have one person in the room

who knows all about this. This is [inaudible]. He has a very, very long history of dealing with all of these little individual…

UNIDENTIFIED MALE: I am correcting his score so I can do whatever I want on this question.

ROY ARENDS: What did [inaudible] wrote down?

UNIDENTIFIED MALE: He wrote D. No I'm just jokin,. A.

ROY ARENDS: A is correct. CW is the country code top level domain for Curacao. The last question. Sorry. What does AD stand for in a response? Is it Authentication denied, Anno Domini, Access Denied or Authenticated? The correct answer is D. Authenticated.

The last one what is the oldest currently registered domain name? Is it A. Rootservice.net? Is it B. symbolics.com? C. mitre.org? D. nordu.net? Anyone? B, symbolic.com is not correct. Symbolics.com was the first in the dot-com genre. But another one was first. Mitre.org was the very first one in the .org zone.

The correct answer is nordu.net. Nordu.net is the very, very, very, very first domain name registered. It was about 15 March 1985. That's it.

Can you please hand your form back to your neighbor? Hopefully your partner has basically added up the score. If not he needs to do that

now. We're going to count back from basically 18. Who has a score of 18? I'm not sure it is actually possible. I'm just going to go from there. 17? Anyone? You need to shout because I can't hear everyone at the same time. 16? 15? 14? Come one guys. 13? 12? There's no one who has all the questions correct?

11? 10? Anne Marie and [inaudible]. Anyone else? And Richard Lamb. We have a divided by three first place. Let's just continue just a little bit. 9 anyone? Points it's not questions, points.

Let's go down. Let's start from zero. Who has no questions correct? Be honest. 1? 2? Perfect. Well done. Just out of curiosity, Michele how many did you have correct?

MICHELE NEYLON: I wasn't playing.

UNIDENTIFIED MALE: I tried to get him to.

MICHELE NEYLON: I would have probably got four or five of them right maybe. But a lot of the ones like the RFCs I going, “I have no idea what that was.”

ROY ARENDS: Thank you everyone for playing. I think is lunch is ready on this side. Julie?

JULIE HEDLUND: Everybody thank Roy. Thank you, Roy. It's the best part. You will notice that we are missing a key element mostly. That is tables. We asked for lunch in this room and we did get lunch in the room. And we found that tables didn't fit. There are some small tables outside. Otherwise I'm afraid you'll just have to improvise. I apologize for any spills that may result. I think I'll make you sign a disclaimer so you don't blame ICANN for that. No just kidding. Enjoy lunch and we will be back precisely at 1:30.

UNIDENTIFIED MALE: And to that point. We are running a little bit behind, so please do come back as quickly as possible. If we can be ready to go at 1:30 that would be ideal. So thank you.

JULIE HEDLUND: Actually more to the point, we'll start without you.

UNIDENTIFIED MALE: Right. Be here or you lose.

JULIE HEDLUND: We're getting started up here momentarily. Thanks, everyone, and just so you know, we're going to go back in time a little bit in the program, that is, and we're going to do the DNSSEC Root Key Rollover presentations with Russ Mundy and Rick Lamb. So come on, get a seat at the table and we'll start momentarily.

RUSS MUNDY: All right, folks. We're about to get started here. We may not have our cameras, so it's just the root key rollover so we'll forgo the camera if we need to.

JULIE HEDLUND: There is a camera. It's just not [inaudible].

RUSS MUNDY: Okay, there is a camera running.

JULIE HEDLUND: See its right there. He's recording it separately.

RUSS MUNDY: Okay. All right. If everybody could take their seat, we'll get going here for our afternoon session. Which, this is a reschedule of what was originally the morning session. This is a panel describing the recent SSAC publication about the root key rollover. It is SAC063.

Okay, so it's a scroll-through. Okay.

JULIE HEDLUND: I don't think it works. I can see if it works.

RUSS MUNDY: I can just do the scroll. That's fine. No problem. Yeah. Okay, well, we're mostly on the screen. It only went one way. Okay. I'll let Julie take care of moving it when we need to.

The SSAC, for those that may not be familiar with it, is an advisory committee of ICANN for security and stability and we, as a group, I'm a member of SSAC and there are several other members here in the room that just happen to be here also. We issue advisories to the community. There is absolutely nothing binding about any of these advisories. They are truly advice. Hopefully useful advice to the community. So this is advice about the root key rollover itself.

One of the points that we have identified that is part of the document when you read the details is this document does not provide any advice on the quantity or timing of when or how often you ought to do root key rollovers. It deals with topics that you need to think about and consider and plan for as part of root key rollovers. You can see the general overview there on this slide, which is the general sections. It's really the sections that are in the report. It's not moving here.

JULIE HEDLUND: I can do it here.

RUSS MUNDY: You can do it there. Great. Even better. So we have five recommendations and I won't read them verbatim, but I urge folks to download the report from the ICANN SSAC website and read them in detail because, in total, it's about a 40-page report. The recommendation section and executive summary section are less than five pages total. So if you want to read a little bit less, read exec summary and then read the recommendation section to get the high-level view.

But recommendation one is really pointing at publicizing and working in conjunction with the community to make sure that it's as broad spread set of knowledge as possible that the root key rollover for the root zone is coming, and describe the mechanisms and the motivation why and what's going to happen so it's not a surprise to people.

Next recommendation is that the ICANN staff, in coordination with the larger community, that they should create a collaborative test bed working with the community to have a facility and a way, not necessarily just in one place but whatever the staff decides is the best way to approach it in the community – a way to test things relative to the rollover, prior to doing the rollover. Again, part of what we've seen experience wise is test, test, test, before you do the DNSSEC piece for real.

The third recommendation is dealing with developing and otherwise encouraging people to decide what breakage means with respect to a root key rollover, so we know in advance, first of all, what to look for; and secondly, the people have a much broader, consistent agreement as to what it means.

Fourth recommendation deals with developing procedures for rolling back to the current key if, for whatever reason, that becomes necessary. So this is something that, again, hopefully it won't be needed, but if it does cause some significant problem, we want to be sure that you can get back to the original key that's actually out there and in use now. That needs to include procedural things as well as technical things.

The fifth recommendation is really for collecting information and analyzing information related to the root key rollover itself and looking at that data collection and analysis of the data to use for deciding the frequency and things to watch for in future KSK rollovers for the root zone.

That's it, right? Or was there one more? Yeah, that's it. So those are the five recommendations in the SSAC document. I think, in the interest of time, let me just ask Rick to go and then we'll take questions after that if we could.

RICK LAMB: Hi, this is Rick Lamb. While Julie is getting that presentation up, I'll say one of the advantages of working in this community is we get to see each other often and we work closely together. Hopefully you'll see on my slides, they will – should – pretty much align with some of the recommendations.

To start with, we've been, and this is from the perspective not just of ICANN but a little bit of root zone design team. That's a team that was put together originally in designing the system that created the, or developed the architecture and the procedures, processes for the root zone itself. We've been able to [reinstiate] that group and this includes VeriSign, and U.S. Department of Commerce and ourselves.

This is what we're doing. We're starting to plan and develop our approach. You can read that as easy as I can. Based on input that we've received. Next slide please.

We're still in the very early stages. We met at the Berlin IETF, which I think was the end of July of this year. At that point, we had already gone through a part of a public consultation process with the community that talked about the KSK rollover and what kind of interest the community had. We've been identifying research and testing and the kind of outreach that might be necessary in the communication. Next slide please. Try to get to some of the meat of this because I know we're techies here.

Parameters, none of this is frozen in stone, but within that group, our discussions were that we're not going to do an algorithm roll for this first pass. We're not going to bite off way more than we can chew. An algorithm roll takes a lot more work and we're not actually going to change key sizes, either. That's the conclusion we've reached, but we're looking for feedback. And if someone could make a really strong case for elliptic-curve cryptography, hey, job security for me. Keep going.

The mechanisms. Of course, we're just going to publish the new trust anchors as early as we possibly can before it even shows up in the root zone file, give people as much time as possible. When I say as early as possible, the kind of time frames we're looking at are six month sort of thing. We will also support 5011 with its revolt capability. Next slide, please.

This is wonderful that the SSAC report actually recommends this. We realized how important outreach was and communication was during the DNSSEC deployment, so we're going to do that again, and that's very much a part of whatever plan we come up with is going to be a pretty heavy outreach. Of course, we all know that the informal consultations

are also very critical in this, where people feel free to tell us exactly what they think and what they think the right steps will be. Next slide, please.

5011 testing is one of the key things we worry about. Just a short refresher to those who don't know what 5011 is. It's a key rollover protocol. It has as one of its stakes actually revoking the current key. What's important about that is that's the point of no return. So if you are at 5011 and you see a packet that says revoke or a key structure that says revoke, that key is no longer good. We have to be very careful about how we do that and we need to make sure that works. There will be a public test bed. This will run for many months and have engagement directly from the community.

This last bullet is very important. Rolling the KSK, the biggest impact is going to be on the resolvers, so we're going to get up close and friendly with a lot of the large resolver operators and software vendors, i.e. Google and people like that, because they make up almost – some of them make 5% of the DNSSEC validations right now. Next slide, please.

Response. I have to say thanks to some of the members in this room that actually pointed this out. There is some definite problems when you deal with IPv6 and UDP and you start to increase the packet size due to the DNSKEY RR set, the record type in the DNSSEC that actually has all the keys in it. That's definitely going to expand as we roll. You have to introduce the new key and in the old key, there will be double signatures and no matter how much work we do to try to minimize the impact, minimize the packet sizes, we are likely to overrun that particular number. There is going to be a lot of internal testing done with that before we do anything else.

Of course there will be, as before, with the root, our ears will be very wide open, listening for any kind of issues that might be happening out there, as well as sensors. Next slide. Thanks.

All right, roll back. This was something even before the SSAC recommendations. Everyone at the table is so afraid of, “All right, what if we screw up? How can we do something? How can we roll back?” So this is very prominent in our design.

As I said, there is a point in the 5011 protocol where a roll back is not possible. In those cases, we certainly would not be going back to publishing the old key. But what we've done – none of this is in stone. One of the theories, one of the approaches that has been developed by some of our friends with Kirei, actually, who formed part of the original KSK rollover design team, was that we could delay the reject state in 5011 until much later in the process. We will have already rolled the key by then. The new key will already be in state, in place, but should something at that point go haywire and people start calling up ICANN and throwing tomatoes at us more than they normally do, we can then go back. So this is something critical. Next slide, please.

Future rollovers. There's a lot of discussion about while we're doing this planning, let's figure out the whole, let's come up with a plan not only for this rollover but all future rollovers. That's not what we're going to do.

Since this is the very first rollover that we're going to do, we're going to take this very conservatively, and we're going to learn from that first key rollover before we do anything else. If you looked at any of the comments from the public consultation period, they were people that

thought we should roll this three times a year, initially, to really get this ingrained. And then others maybe that said there's no need to roll at all. And so, that's a number we'll probably be looking for more feedback from the community on to try to get a better idea.

Right now, what we're looking at, what we see up there as something that seems reasonable. It should allow us sufficient frequency to make sure that we don't forget how to do this, but it's not so frequent that it's going to cost us a lot. Every time we roll the key, unless we change the key management procedures drastically, it does involve people. People traveling from far away like there are some people in this room who actually are the Trusted Community representatives that help us roll the key now. They have to come from a long way and you really can't expect them to show up at the drop of a hat. That's not fair. Next slide.

This is my last slide. Here's where we are. We really appreciate the recommendations out of SSAC and now that they're final, we're going to look at them very carefully and look at the whole report. Thank you, Russ, and work party members. We're going to summarize some of the inputs we've received from the public consultation process and we're going to also, before we run here, we're going to be excessively conservative. With all the new gTLDs having entered the root, we are going to try to fully understand what impact these things may have on the overall stability and security of the DNS before we decide to also add in additional issues such as KSK rollovers.

The last bullet is, taking all those into account, we are going to look at the KSK rollover timeline and try to look at it as conservatively as possible. In other words, we're not going to roll the key this year. I can't

say for sure, but I think we would not roll the key next year, either, so that's about as far as I'm willing to predict. But we're going to take this very carefully at first and once we've gotten all the information from this first exercise, we will then plan future key rollovers in a much more regular fashion, hopefully. Last slide, please.

Talk to us. I'm here. Just grab me. Hit me over the head. Do whatever you have to do to convince me what we've got to do. Feel free to talk to any of those members as well as upper level company staff as well, just to understand what's going on with the root key rollover. There's an e-mail address you can send it to. You can also just send it to richard.lamb@icann.org. That's if you want a faster response, you can do that. With that, that's it. Thank you.

RUSS MUNDY: Excellent. Thanks, Rick. Right on time. Let me open the floor for questions. I see Warren.

WARREN KUMARI: So Rick, somewhat of a loaded question. When the roll the key, when you initially roll the key, even if you do it really carefully, do you think there is going to be some breakage, or do you think there will be no pain at all?

RUSS MUNDY: He did say Rick.

RICK LAMB: Well, personally, no. I don't think there would be any breakage. I don't know if you mean breakage with resolve? Yes, breakage with resolve. I don't know if you're referring to the process we run versus out in the real world. Out in the real world, yes. Absolutely. We know that. But the idea is to try and to come up with reasonable metrics. Again, that was a really good recommendation. How do we determine when to roll back? Or when we've broken things.

RUSS MUNDY: The issue of breakage is a hard one because it can mean very different things to different people. This is one of the reasons why the SSAC says let's come up with a definition, whatever that may be.

RICK LAMB: I'm confident, as far as the internal processes stuff, that a lot of the code actually already has 5011 support built in it.

RUSS MUNDY: Other questions? I would have thought there would have been a lot in a room full of DNSSEC people. I guess everybody's confident that our root management partners are going to do it perfectly. Dan?

DAN YORK: So, I guess I'm not commenting, and I guess I'll speak for others, because at this point, what is there to comment on? We've all submitted comments into the process. We've seen the recommendations out of SSAC063. And the response Rick provided from ICANN is similarly lined up with that. I think at this point, we're just looking forward to looking

forward to what comes out of the next stage of this, which is really the analysis of what might break and the looking at that. So I don't think there's much for us to comment on at this point, personally.

RUSS MUNDY: Let me just add one comment with respect to the ICANN and SSAC process. There's been a recent, new addition to how the board is keeping track of recommendations that come from the SSAC to the board, and that is they are actually tracked. There's a process put in place to follow the recommendations and see what, whoever they're pointed at, in this case most of the recommendations are pointed at staff, and so there is a much more clear cut set of steps that should tie together the recommendations that have just been published literally a week ago, I think. And what happens next. So we'll be able to see that.

That's part of, I think, ICANN's initiative for making sure things are more visible than what they have been in the past. Okay, if that's it, thank you very much and we'll move on to our next panel. It is Dan. No, it's not.

JULIE HEDLUND: We're going to operational readiness.

RUSS MUNDY: Okay, operational readiness. Stuart and Jason and Yoshiro, please.

JULIE HEDLUND: We're starting out with Stuart. We're having sound problems again.

RUSS MUNDY: Oh my. Okay. Is Yoshiro here? I saw him. Oh there he is. He was behind me. Okay. Let me scoot down a little bit, give you guys a little more space here. I'm not sure how I'm going to do the timer here to keep people visible. Let me grab my – because the iPad is for the speakers. Okay. All right. So are we set, technically here?

JULIE HEDLUND: Yes, we are.

RUSS MUNDY: Okay. So this panel is addressing what happens when you use DNSSEC in the real world. What are some of the experiences, the good things, the not-so-good things, the "Oh, this is wonderful, but"? Our first presenter is Stuart Olmstead-Wilcox talking about the CA Registry. So please, let's just move right into your presentation.

STUART OLMSTEAD-WILCOX: Thank you. I'm Stu from CIRA and I'm just going to talk about what we're doing in our last phase of basically deploying our full DNSSEC solution within the CA registry and the choices we've made relating to a lot of the discussion today actually, as to how we've built our implementation.

So we've done it as a multi-phase project. First we built the back end – sort of a zone signing solution and signed our zone. That was completed at the start of this year and that's working well.

The next phase was to actually develop the DNSSEC support in our registry to allow our registrars to actually submit DNSSEC information into our registry and then publish that in an automated fashion. That

work is almost done and that's really what I'll really summarize a little further on in the presentation.

Then the final phase, which is one of the things that we're talking to a lot of people about here and getting a lot of great information about and from other registries. We've already committed to this phase, is how we promote the adoption, how we promote signing within Canada and trying to get some traction. Next slide.

This is the quick overview of the signer and validation process. Jacques has actually presented this a couple of times I think. Basically, we have a redundant signing process that uses Bind and open DNSSEC to sign and then there's a level two validation that checks to make sure that we get the expected result from both sets of signing before we publish. This architecture was designed by Jacques and built by our operations team. It really is working quite nicely so far. We do have 80 signed domains that are maintained manually right now within the registry, as well.

So DNSSEC in the .CA registry from a registrar perspective. The main and absolutely primary objective is keep it simple for registrars. Obviously that was a bit of a topic from one of our earlier panels. Keep going.

This is just a quick overview. Everyone here basically knows how this works, but in our particular case, we do have a web interface, which we call our .CA manager, that allows registrars to submit transactions into our registry, and we're also supporting EPP. We're adding the capability to submit DNSSEC information into our registry via both mechanism. Obviously, for EPP, we're following a 5910, and the business rules in our web interface follow the same protocol, basically.

As we've highlighted at the bottom, we're not trying to re-invent the wheel. What we really tried to do, in keeping with our core objective, is stick with the standard, leverage what we've learned from the community and then make it as easy as possible for registrars. Keep going.

Top part is just summary of the DS versus key data records from the RFC. Our decision, based on all of what I've just discussed, was that we wouldn't make the [or] choice as described in the RFC. So, we will support any of the interfaces. So a registrar for any given domain can give us DS, they can give us DNSKEY or they can give us both and we'll accept them.

The reason for that really boils down to all of the discussion that we've heard today. We've talked to multiple different registries over time who have made the choice of Key versus DS. At the end of the day, it seemed that maybe the reason that the RFC was written that way wasn't as technical, potentially, as for other reasons. It seemed that, with some of the operational issues that people that have been signed for a good amount of time that have uncovered, that this is maybe a better approach or a more, certainly for our registrars, an easier approach to allow them to integrate with us, if they've integrated with other registries.

So these are just specific details on decisions we've made in out implementation. Obviously, we're adhering to the schema defined in 5910. We've decided on a maximum of six DS records. We say and/or DNSKEY because we'll accept both but we'll obviously generate the DS. We accept all of the IANA specified algorithms for keys. We accept all

four algorithms for DS digest. One thing that we did do in our current implementation is, if we're given a – And when we generate the DS – sorry, I skipped one – we're using SHA-1 to generate the algorithm within our system.

When we're given a KNSKEY and a DS, so they're together, we actually generate our own DS using the indicated algorithm for the digest type and then we compare that with the given DS record, just as an extra level of validation to ensure that – or try to ensure – at least, that we think that the DS we were given actually is accurate, or at least what we think is accurate. That was actually a suggestion that Andrew Sullivan gave us a while ago and it seems like a reasonable thing to do to begin with.

The two optional elements that are defined within the RFC, we're not supporting. Currently, we just don't publish incremental updates in our zone. We publish once an hour, so the urgent attribute in our current infrastructure, we couldn't support. And we [inaudible] the signed and unsigned status within our WHOIS.

This is just sort of giving a bit extra information on our implementation regarding the DS or DNSKEY. I think the main things is that we're still adhering to the schema itself. So in [inaudible] for example, we can't mix. We adhere to the schema, so we can't mix a DS or a DNSKEY in that actual transaction. But in an update, you could have given us a DS and then do an update and give us a secondary key and we'll accept it is really the difference here. Go ahead.

So again, our next challenge, once we roll out the registry implementation, is to foster Canadian adoption, which has been

everyone's challenge I think to this point. So as I said, we've garnered a lot of information from the community. We certainly have started building a strategy around how we think we want to position DNSSEC for Canada. We certainly started talking to our registrars and trying to get their feedback on what they'd like to see from us. Also talking to ISPs and DNS operators within Canada to see what their state from a DNS readiness is, as well as how we could help them to move that along, as well. So that's going to be our focus most of next year.

And that's it. So from an implementation perspective, we do have a technical specification document we wrote for registrars to just explain our business rules and so forth. And that's all. Do you have any questions?

RUSS MUNDY: Thank you, Stu. Let's move on next to Jason Livingood from Comcast and he's going to talk about negative trust anchors.

JASON LIVINGOOD: Great, thank you. And bring up the slides. My name is Jason Livingood. I work for Comcast. We're a large ISP in the United States, and ironically enough, I'm also watching a live broadcast here on my laptop that's our company's 50th anniversary that we're celebrating today, so kind of a neat aside.

RUSS MUNDY: Oh, congratulations.

JASON LIVINGOOD: Thanks. So, diving right in, I thought the focus of this would be about negative trust anchors, which is something that I'll explain in detail, but in essence, we operate one of the world's largest recursive DNS infrastructures and we deployed DNSSEC a couple of years ago. This is all about one of the tools that we thought was pretty essential to supporting our roll out. Next slide, please.

DNSSEC validation, from our standpoint, is really great. It's wonderful, except in those occasions when it fails. And then, it's sort of a problem. What's interesting that we have observed is sometimes when people think that this happens, they think that it's the ISP, in this case, blocking access to these sites. We had a very interesting one, and we did a white paper about this a couple of years ago, NASA.gov, their signing failed and there was a news report then claiming that we were blocking the website. Tons of people then blaming us on social media and, really, this wasn't us doing anything wrong. It was simply the signing got messed up. We've noticed this repeatedly with domains that fail. Next slide, please.

A lot of people think, SERVFAIL, that's not good. They don't like DNSSEC. So sometimes things really get a little bit messed up operationally and people tend to blame the validators. It is very difficult to explain to your customers and to other people, the news media and so on that this is really an authoritative issue and that is out of the control of the Internet service provider. In many cases, people then say, “Well, if it doesn't resolve with these DNS servers that use DNSSEC validation, then you should switch to pick your flavor of non-validating resolver out there.” People tend not to switch back after that. People are really downgrading

their security when they do that just as a work around. Next slide, please.

What's a negative trust anchor? Primarily today, validation would fail for one or two reasons. One of two reasons. Excuse me. One would be an actual security issue. The other would be the second, with is an operational, process or technical error. And at the moment, really number two is the dominant one where it is an operational signing problem, key rollover type of thing.

As a validator, you really, prior to negative trust anchors, had one of two choices. One, you could do nothing, and that could be problematic if either it's a domain customers complain very loudly about, or if it is a major domain name that people are sending a lot of traffic to. So imagine Netflix.com, Google.com, [inaudible] and so on, something that is 10% or more of your traffic, that validation failing could be a real problem. You could do nothing and allow that pain to be there and customers to be upset by it and call in to your ISP, or you could turn off validation for all domains, which seems, at least from my perspective, an over-reaction.

So negative trust anchors means essentially that you're turning off validation for a single domain, and it's not like you're using a special signature saying this is actually legitimate when it's not. You're really just turning off validation for that one domain. Next slide, please.

And so, we at Comcast have been using negative trust anchors since shortly after we launched DNSSEC validation, or right around the same time. When we do so, we noted on our DNS information website, which is there, dns.comcast.net – I should note, we don't always do a negative

trust anchor when we notice these failures, especially when it is what we call a repeat offender where, say, domain or TLD that just can't seem to get it right. We try to help out the first few times, but after the fifth or 10th or 20th time, we sort of give up and say, “Well, they need to get better.”

And, of course, we continue to strongly encourage domains to sign, especially the big ones, and we strongly encourage domains that are signing their names to do so in a reliable fashion. Next slide.

We've taken this issue to the IETF, to the DNS Operations Working Group, and there's been a bit of debate about it, to put it mildly. One of the issues seemed to be, how long if you've documented that negative trust anchors exist, how long would you want that practice to be around? Most people sort of said, “Well, a reasonably short period of time is how long an individual trust anchor should live.” And what does that really mean? I think in practice, it tends to be one day or less in our network, but we're still having that discussion.

And the other, which is probably the bigger issue, is the discussion about is the fact that negative trust anchors exist a good thing in the long term, and should they be deprecated at some point in the future? If it should be, what is the right time for that? Our perspective is that, when DNSSEC deployment reaches some critical level of mass, that that would be an appropriate time, but we're not there yet, we don't believe. Next slide.

We definitely are hard at work. There's our studious cat. We are hard at work updating the draft. It's mostly based on my personal bandwidth. Because we had a little bit of push-back, I went and set out publishing

two other drafts to try and get some lower-level agreement on two issues. One was basically who is responsible for DNSSEC mistakes, and the other is around not switching resolvers when those failures occur. Next slide.

So the first document really talks about who is responsible for authoritative DNS mistakes and what it's intended to be is a reference that we can point customers and news reporters and other types of parties to to really understand, okay, if there's a DNSSEC validation problem and it's for, say, operational and technical reasons, who's to blame for that? Who has the power to solve that problem?

What we try to explain, or I try to explain, is that the power lies with the authoritative operator, the person that creates those records and puts them in the authoritative DNS. It's not an operator of a recursive server. And hopefully that will help. Next slide.

And then the second one here is – so if you have a validation failure, suggesting to folks that they try to route around it by changing their resolvers is not a good thing. They're really downgrading their security and they should stick with resolvers that are validating and they should wait for the authoritative party to resolve the issue or for someone to put a negative trust anchor in place. But it's not something you should just sort of go and switch to something that is non-validating. That is not a good thing from a security standpoint. Next slide, please.

So that's it. That's the high-level overview of negative trust anchors and happy to take any questions later on. But from our standpoint, we think it's a pretty essential tool for a recursive operator to have. We've heard many other operators of recursive servers say that they would not

deploy and turn on validation without this kind of mechanism as a sort of pressure relief valve, in case a major domain failed or it was causing some real problems. We think that's important, especially as we look forward to major domain names that represent traffic that's significant on the order of 10-plus% signing. That seems to me an essential tool for a network operator and DNS operator. Thank you.

RUSS MUNDY: Thank you, Jason. Next, we're going to hear from Yoshiro, who is going to give us some of their experience in TTL lengths at .JP Nick.

YOSHIRO YONEYA: JPR.

RUSS MUNDY: JPR. Thank you. Sorry.

YOSHIRO YONEYA: Hi, this is Yoshiro from JPRS, which is .JP registry. Today I will explain our experiences that we change the DS TTL in .JP zone from one day to two hours. I explain about why. What was the background of these changes and how we selected the two hours and the explain about the conclusions. Next please.

This is the background. For using DNSSEC, there is a very big concern for the registrant and ISPs. If the DNS name resolution will fail – I'm sorry, if DNSSEC operation failed, then the DNS name resolution will fail. This is a

very big impact to the end users. The biggest mistake is usually what happened with mismatch in parent zone with DNSKEY in child zone.

If this situation happens, then urgent recovery between parent and child zone administrators are required. But this requires registrant, registrar and registry cooperation. Even though [inaudible] the influence of the name resolution failure will remain until the DS cache in validators being expired. So registrants and ISPs want to shorten the duration. This is background. So next, please.

There are two possible counter measures for this failure. One is a flush failed domain's cache in validators, but this is a very ad hoc solution and it's hard to reach each validators' operators because they are hundreds of thousands of ISPs in the world. So Comcast is not the only one validator operator. We have to reach many, many, many operators. This is almost impossible.

The second counter measure is a shortened DS TTL in parent zone. This could be an effective solution, but the [fact] is moderate value for DS TTL is not shared yet. This solution is possible because this solution is done by the registry or the zone operators. So this is based on the decision of the zone administrator. Next, please.

Before we changed the DS TTL, we measured our DNS behaviors. We investigated two JP DNS servers. We have seven DNS servers, but two of them taking, obtaining DNS query log. So we looked for the query of those two servers. But we also viewing DS graph and from the DS graph, we're monitoring out of seven DNS servers with DS graph and DSC graph shows the same number as the two servers. So we thought that only two servers, in investigation, only two servers will obtain whole behavior

or our DNS servers. The results of our analysis was that DS queries for whole DNS queries is about 3.5%. So the reason why DS queries is so many is another story. I do not explain here. But my query made some [inaudible], so if you have any interest, please defer to the URL here.

The existing DS queries which has a DS registration, the ratio of the existing DS query and whole DS query is about 0.08%. So only very few DS queries are [real] DS queries, which has a DS registration. So other DS queries are only for check if that domain name has DS name or not.

This graph shows the DS query ratio and existing DS ratio. On the left-hand side, the graph shows the DS query ratio and the right hand shows the side shows the existing DS ratio, so the existing DS query is very, very, very low. Next please.

So I will explain about how we decided to moderate DS TTL. We used a three-step analysis. Next slide, please.

The first one was thinking about similarity within the NCACHE TTL. So the DS TTL can be considered as a duration of influence when name resolution failure occurs. And NCACHE TTL is also the duration of status when query name did not exist. So there are similarity between DS and NCACHE regarding name resolution failure. For the NCACHE TTL, it's value is recommended from one hour to three hours. This is based on RFC 2308. So, DS TTL would also be effective within the range from one to three hours. Next, please.

We calculated, estimated the change of the DS queries if we changed the DS TTL. The top one is a result of our [inaudible] analysis. As I said, the DS query ratio is 3.5 and the existing DS query ratio is 0.08. So if the

DS TTL changed to three hours, the DS query ratio would not change because the existing DS query is very small portion, but the existing DS query ratio will be increased to 0.6, about multiplies eight times. Now if DS TTL changes to two hours, existing DS query ratio will be 0.9%. And if we change to one hour, existing DS query ratio will be increased to 1.8%. So next please.

This graph shows the how the existing DS query ratio changes. Next, please.

So finally, we considered three conditions, which value is most suitable for the current .JP. The three conditions are small, if how small, impact to the current JP DNS, and how it is enough to scale the shortening of the DS TTL. If the existing DS queries will not increase if DS and validators are increased. So [inaudible] was two hours because it was most moderated value for these conditions. Next, please.

So this is conclusion. We decided to shorten DS TTL from one day to two hours. This value is just what's for current JP DNS. This value will be changed in the future if we find much more suitable [value]. This event was happened on this last Sunday, 17th, so we changed this only about three days before. But after this change, I [inaudible] the log and find that the existing DS ratio is a little bit increasing, but the total DS query ratio is not changed so much as expected.

So please give your comments based on your experiences if you are studying to change the DS TTL, and I'd like to share it as a best current practice, especially for TLDs. Thank you.

RUSS MUNDY: Thank you, Yoshiro. So we've had some really good presentations here about real world experience and issues. I'd like to open the floor for questions or comments from folks. Warren?

WARREN KUMARI: Warren Kumari, Google. Question and comment for Jason. So Google DNS now does validation. We were not doing validation when NASA.gov stuff happened. We actually noticed a fair uptick in the number of people using our services because as soon as NASA.gov happened, a bunch of people sent posts on various things like Slashdot saying "Somebody change your resolver at 8888 and suddenly everything works."

Now we're doing validation. But I don't think we could possibly have turned it on without some sort of NTA-type technique in place. There are, however, a number of people who say negative trust anchors are harmful because it doesn't create an incentive for people running alt servers to actually do the stuff correctly and concerns about opening yourself up to legal liability because if there's a real hijack, you're telling people it's all okay. Do you have any comments on that?

JASON LIVINGOOD: Sure. Generally speaking, we have only been putting negative trust anchors in place when the administrator of the domain, the authoritative owner, contacts us and says, "Yeah, we messed up. Could you please do something here?" Or, where we notice it and we reach out to them and they confirm, "Oh yes, it was an operational issue."

It's definitely not automatic because then it could be that very risk that you mentioned, which is it a security problem for real or is it an operational issue? So I think that addresses that part.

Generally, are they harmful? I think it's better to have DNSSEC validation than not. And this is my opinion one of the ways you get to more validation happening.

RUSS MUNDY: Well, I have one comment, since I don't see any from the audience at this point, and that is Jason indicated that the negative trust anchor idea is not necessarily widely accepted throughout the IETF and the standards world. This is not a new problem. In fact, in the time frame between 2065 and the 4,000 series of specs, there were at least two major efforts to put in to the specs themselves this capability. And the working group rejected them very soundly.

So it's been an issue that's been raised before and has not been accepted through the IETF. It's a problem that is trying to do a balancing act between operations and the security perfection idea.

JASON LIVINGOOD: I think it's indicative or emblematic of a larger tension that you see from time to time at the IETF, which is you have a protocol developed and a sort of purist view of how to carry that out and implement it. Then you have a very different set of people whose job it is to deploy and make things work at scale – not at small scale; at very, very large Internet scale. That's where guys like me and Warren and other people come in.

There are simply things that you learn as a result that you have to adapt to. I know I and many other people and Warren and others are trying to help IETF become more open to operators participating and sharing their views about actually doing these things. The reality is that both of these communities, not only do they cross over quite a bit, but they need each other. A great protocol is nothing if it is not deployed. So, in the case of DNS security, I think it certainly holds true.

RUSS MUNDY: Roy?

ROY ARENDS: This is also to Jason Livingood about negative trust anchors. I actually like the idea. I think it's necessary and I think it ties into something a little bit wider. There's been some discussions within the IETF operations, DNS operations group, about the ability to remotely do something about – basically to flush a cache, if that makes any sense? Now, how that would look like in the future, I have no idea, but I can tell you, being on wrong end of things once in a while, we really would like to have a mechanism in order to flush a cache.

I know that negative trust anchors is not the exact same thing but it ties into that same discussion about the imbalance between those who make a mistake, those who consume it and the man in the middle who gets all the blame. Thanks.

JASON LIVINGOOD: Yeah, I think cache flushing mechanisms are important. I know Warren has a draft there in the IETF and that's a discussion that's starting. What you typically see are you get these ad hoc requests via some random mailing list, maybe it's [ORAC], maybe it's DNSOP, maybe it's NANOG or whatever, and I think one of the recent ones – maybe it was someone from the New York Times –they needed a cache flush. You get these requests via e-mail. How do you validate is this really the domain administrator or not? Should you do this? It would be nice to have that work in a more distributed and automatic fashion. I think that's one of the tools that you want in the tool set here.

DAN YORK: I was just going to comment that I think Jason, your comments are spot on about the deploy-ability of protocols versus the, and I would encourage people here and remote, this is a critical issue to get more operators and more people who are using these protocols to participate in the IETF in some form, even if it is purely just to go and read the documents and do that. In fact, I'll be talking about that in a moment when I'm up here, but I just wanted to emphasize that point. I think it is key to get people giving feedback on this.

WARREN KUMARI: Yeah, Warren again. So if there's no NTA RFC, one of two things will happen: (A) people won't be able to deploy DNSSEC because there's a huge cost to enabling it or (B) people will continue to do NTA but just not in a standard way, and neither of these are good outcomes for DNSSEC deployment.

JASON LIVINGOOD: Yeah, I agree, and I think that the key to understanding this is validators will do this sort of thing. Do you want it documented so people understand what it is and how it works and what the practices are around it and some level of standardization and some discussion about it out in the open? Or do we all wish to pretend it doesn't exist and, if we don't talk about it, that it doesn't really exist? And I don't think that's too realistic.

I think, generally, in sort of the post-Snowden world, so to speak, the IETF meeting a couple of years ago in Vancouver talked about this security more generally at the technical plenary and I think the IETF and many other technical groups in general are talking about how to increase the level of security on the Internet.

Certainly things like TLS for website access is one mechanism. I think DNSSEC is another facet of that sort of generally increasing the security of the Internet. I hope that, when we start to see after this meeting, a little bit more momentum around DNSSEC, particularly signing more big names, that that can be something that can help along that security road.

RUSS MUNDY: Erwin, go ahead.

ERWIN LANSING: Erwin Lansing, .DK. I'm not sure how many of you were in my talk on Monday, but that was actually my point at the end, and to be a bit

provocative about deploy-ability and offer people that work on standards, that we've got some people, especially for DNS, DNSSEC security, interested in previous [inaudible], we want to help you get it implemented at the lowest level, and we want to get it deployed and get some real-world experience with that.

RUSS MUNDY: Well, I think we really have reached the end of our time for this panel. Let's thank our panelists very much for their presentations.

JULIE HEDLUND: I just don't know what we should do with that question in chat. It was after…

DAN YORK: I have the unenviable task of trying to do about a half-hour's worth of presentation in about 15 minutes, along with wrapping this up. And there was a question in the chat room that we'll raise to Jason.

JULIE HEDLUND: No, it was to Stuart and/or Roy Arends. His name is Brett and he said [inaudible].

DAN YORK: Okay, so we'll raise that question to you guys that's there. So I'm going to finish up here with a little bit of just a piece about DANE and what happened at the IETF. For those who are remote, the slides are available there, so what we'll be able to go through this. Where do I click?

JULIE HEDLUND: You can't do it.

DAN YORK: Oh, I can't do it. Ha! All right. Okay, so next.

So just to basically remember what we're looking at here, when we talk about DANE and DANE protocol – I guess I should ask this. How many of you here are familiar with DANE? All right. So I'm talking to a lot of folks who already know this. For those who are remote, you can see this and we will just kind of walk through this. If you look at the slides, this is what we see in an SSL interaction. We have an HTTPS with a nice little green lock that goes on. And the question is does this have the correct certificate? Let's go on.

So the problem can be that a firewall or an attacker, somebody else can get in the middle of that and re-encrypt it with TLS, so you wind up seeing the correct lock. So let's go on.

A DANE-equipped web browser, or other device, other application, would be able to detect that this had happened and be able to alert the application or web browser that there was a problem and it was not the correct certificate. So, let's go next.

So this is what we're talking about protecting. DANE is defined in RFC-6698, and it asks this question of how do you know that the SSL certificate that you're using is the correct one? Go ahead, next.

One of the interesting things is that DANE is a container for TLS certificate or a public key of it, a fingerprint of it. That's a key point. That

is what DANE does is it specifies a new record, RFC-6698. It's the TLSA record. There are some other proposals that will have variations on that, but it's the same idea. It's a record, a DNS record, that is a holder of a TLS certificate. As I show on the slide, there's four different modes of it. One is where you say that it is this specific certificate, which is one of the modes that's there. One you can say, for this website, I will only accept certificates that are issued by a specific certificate authority. Okay.

There's also a way, a mechanism, where you can say this is the specific certificate I want, and this is the specific certificate, which may not be signed by a CA, a certificate authority. It may be a self-signed certificate. So DANE provides this kind of flexibility to let us go and have – to create a layer of trust, a trust layer, if you will, for TLS and SSL certificates and the usage of that. Go on to the next.

Now, DANE, we talk a lot about it in context of web browsers because it's an obvious use for it, but what we're actually seeing is a lot of interest in actually using it in other places. The folks who have done the post fix e-mail server have implemented DANE inside of that so that they can use it to determine, are they connecting to the correct mail server to go and deliver e-mail?

Just over the past week or so, a good number of the XMPP community have gone out and implemented DNSSEC in their Jabber servers so the Jabber servers are able to authenticate using DNSSEC – not authenticate, validate – that they are connecting to the correct server on the other end when they're going and delivering XMPP messages. There's some folks working on it within the void space to see how they

can use this when you need to go ahead and deploy certificates out to thousands of phones or applications. How can you go and do that? Next, please.

We've got a number of different uses. There's some links up here around a number of the drafts that are out there around using DANE with e-mail. There's a good draft called DANE operational guidance, which Wes Hardaker, who many of us know, worked on with a gentleman named Victor Duckhovni, who is behind the Postfix e-mail server. Basically, what he did was, while he was implementing DANE in Postfix, he basically wrote down, what was going on as he was going through this and came up with this draft, which he and Wes would like to make more generic. So they're looking for experience from people implementing DANE where they talk about this. They're trying to capture that information there.

Then some other ones. Paul Wouters wrote a couple around using it the PGP and OTRIM. Next please. So there's a number of places there.

I've got some pointers here, again. We maintain a page at the Deploy 360 around the DANE with DANE overview. There's a nice IETF journal article with it. And there's the RFCs. Next, please.

There's also some new tools that are out there. We maintain a couple of lists of that, the DNSSEC tools project has one, as well. Next slide, I think.

Okay. This is also a mailing list. I was going to bring this up later, so I guess I missarranged my slides. But anyway, this is a list you all are invited to join. A number of us are here and we're looking at how do we coordinate advocacy, really, around promotion of DNSSEC and DANE

activities. I would also say – it's going to come up on my IETF slides in a minute – there is something new with DANE that I'll talk about in a moment.

So that's the quick overview of DANE. I want to move into IETF. Last, two weeks ago, was IETF88 in Vancouver and there were about 12,000 participants from 54 countries that were there. There was a huge amount of folks on security. On the DNS side, there were really three pockets of activity. One was DNSOP, the working group, and actually, on a quick note, how many of you in this room were there? Yeah, look at all the hands. A number of the folks are here in this room. So there was also a side meeting on the DANE protocol that, again, found a whole bunch of us up in a room on the top floor of the hotel talking about DANE and things. And there was also another group called the DNS-SD extension, which is looking at using multi-cast DNS and DNS-based service discovery and using that, extending that beyond a local LAN.

Just, as a reference, that's like Bonjour and the stuff that you use for connecting on the local networks, seeing the number of Apple devices that we have around. All those things that will let you rapidly find a printer or something like that or another machine. This whole thing is how do you take that and move it beyond a local network into a multi-network environment, and how do I find the printer in my mother's house or something like that? How do I do that securely? And there are people looking at how would we do something with DNSSEC? What role would it play in there to help securely ensure we connect between that? I mention that purely because it was a momentary in there, but let's go on to the next slide, please.

In DNSOP there was a lot of discussion. As Warren will attest, there was a whole lengthy discussion around this whole issue of the automating of the transmission of the records that we just talked about earlier that Warren did about the CDS/CDNSKEY. It's great. The new draft that was talked about earlier came up out of the discussion here to kind of merge all this together and make it make a little bit more sense.

Following on Yoshiro's talk, there was some discussion there around DS queries and pieces. And also there's a couple of drafts that, again, Paul Wouters has been focusing on around increasing the efficiency of DNSSEC queries, and specifically, some areas around how can we basically TCP connections open, how can we keep some of the different connections to allow us to do more queries in a single connection? So there's some very interesting work going on there to make it more efficient. Next, please.

This is all sort of work that's happening in there. You can see here a link on the slides to where you can get the agenda and the documents that came out of there for IETF88. There's also another document I'll mention from Wes Hardacker, which is talking about DNSSEC Roadblock Avoidance. Basically, he was trying to capture a good number of insights, lessons learned about where there are roadblocks within the DNSSEC structure that need to be avoided. Next slide, please.

There was a side meeting that we had about DANE where a number of us looked at it. Some of the key points that came out of there was really, as a focus area, we need to look at how can we get more TLSA records deployed?

One of the reasons around this was that one of the push-backs we've had from browser vendors is they don't want to implement it because it will potentially impact speed. But we learned in the meeting, certainly, that browsers are looking at actually how many actual DANE records are out there. Seeing not a lot of them, they're saying, “Why should we bother with this?” So the more generation of TLSA records we can get, the better we make our case with the browser vendors and others.

Two quick drafts to mention. There is one that Olafur Gudmundsson is working on around terminology, which is something that is critical. And then also, we had a discussion. The folks at NIST have come out with a test tool that lets you test the validity of DANE certificates. That's what's up here and some more publicity around that will be forthcoming. So next please.

Finally, as mentioned by Jason a few minutes ago, there was a very strong focus on strengthening the Internet around what we can do to harden it against large-scale, pervasive surveillance. There was a technical plenary. If you haven't seen it, I would encourage you to take a look. It's a video that's up there and that page, ietf.org/live/ietf88/, has a link to the video as well as to other materials that are there, as well. Next, please.

It was, again, more summary of information you can get out of the links. Next, please.

The other piece I would mention, again, if you are not familiar with working with the IETF, I would encourage you people to go to this ietf.org/newcomers. There's a particular group – IPv6 and DNSOP – that are ones that could really use some operator assistance. So join the

mailing list, read the drafts, help provide comments. It would be very helpful for us. And that, I think, is it.

So with that, let's shift rapidly. I'm not going to take questions because we are out of time, but I'll be here to take some more questions. We're going to shift to the wrap-up slides that we have, and for that we actually have no time, so Russ's clock doesn't even get to get set. We're going to wrap this up by saying to people who are either here in the room or people who are remote things we would encourage you to do.

We would encourage TLD operators and registries to sign your TLD, accept the DS records, work with the registrars, help. Another aspect is help with statistics. You've seen some charts that we've had up here about deployment. We'd like to work with more TLD registries around how we can help provide more of these. If we go on to the next slide.

RUSS MUNDY: Zone operators, yeah, sign your zone. And one of the other things that I want to add that from the earlier presentation about enterprises, we're all part of an enterprise, in one way or another. Look at implementing DNSSEC throughout your enterprise. Make use of it at the enterprise level, as well as signing your zones and checking the validation. Actually go forth at the enterprise level and look at using applications like Bloodhound and other capabilities that make use of the validation, make use of the DNSSEC.

DAN YORK: And we want service providers, network service providers and ISPs who are out there, please get those deploying DNSSEC validators, DNSSEC

resolvers because that's another incredible part we need to make this happen, and of course, signing your own zones is important. And again, we want people to be promoting the DANE protocol. Really help us drive that because it's one of those areas that is new, that helps provide a solid reason why we can look at DNSSEC being used and provide some true value there.

RUSS MUNDY: Websites, again, sign your zones, but another important area is put in TLSA records actually, and that itself promotes and will promote the browsers making, being more likely to support DANE as a protocol. So, deploy the TLSA records in sites and zones that you control. Make use of it yourself.

DAN YORK: So everyone, we can say here, use DNSSEC yourself. We've got a number of different tools. Share your lessons learned. Participate in these workshops. And I will say as well, not only do we thank everybody who is here, but we will be having another one of these in our next session in Singapore. We will be doing another one of these. We're always looking for new case studies, new presentations, new tools. So for those of you who have been sitting her listening today, either in this room or remotely, and you've got ideas, we would love to hear from you. There will be a call for presentations coming out soon, and we'll start to be planning that next event. And we're always open to those ideas, if you have them.

RUSS MUNDY: And we make no promises that we won't ask you to compress your presentations because everybody today did so and did so very well. Thank you, everyone who participated and presented.

DAN YORK: And with that, we'd like to say thank you to everybody who's been here this entire time. We put up a couple of websites here, www.dnssec-deployment.org, www.internetsociey/deploy360, (we're missing the .org in there I notice) and www.dnssec-tools.org as well. That one won't. Hey, where's the, is there a .internetsociety new gTLD yet? All right, dot-less domain. Anyway. Those in this room will get that, actually.

We want to thank you all because there is a whole lot of work, too, in the program committee, and I think there are still a few members who are here. Who's on the program committee who's still here? I see Jacques. Okay, Yoshiro. Okay. All right.

I would just like to say there's a lot of work that's involved with this. A lot of people have been part of this to make it happen. And so I'd like to give a round of thanks to all of those folks, too.

And I have to say a final thing, too, which is we definitely need to give a round of thanks to Julie. Without her, I could tell you, all of this would not happen as seamlessly as it does. Well, all of those things. She is what makes this happen. Even when there are seams, it still all works through and it all goes on, so thank you very much. All right, thank you, everyone and let's go out and make DNSSEC happen.

[END OF TRANSCRIPT]