TORONTO – DNSSEC Workshop
Wednesday, October 17, 2012 – 08:30 to 14:45
ICANN - Toronto, Canada

STEVE CROCKER: ….org and the button up there that I cannot read quite is open DNSSEC consortium effort in Europe, have all been pioneers, leaders in DNSSEC and strong sponsors and the reason why there's a free lunch today. Alright, let me take you on a little tour, this is my traditional quick survey of things and tweaked a little bit. You're moving that so that I have to move the slides, okay I can do that.

…category that they were calling regional that includes exactly just SU and EU because these are operated under ccTLD rules and yet they don't correspond to a single specific country. The last category are ones that you can find in the root zone that aren't associated with anything because they were put there for test purposes. And the reason for breaking it down this finely is so that because other people are doing surveys and publishing statistics…

…more participation by reporting. Anybody that has any ideas on that or wants to plunge in and help – be absolutely delighted. Here's the projection for the beginning of next year and for the middle of next year, and for the beginning of 2014. No real change here and that really reflects a lack of inputs that we've gotten, and I'm sure what the actual facts will turn out to be will be much better.

All this data is available if anybody wants to play with it or analyze it, just contact us. Here's a region by region look just sliced for today, or

for this month. I won't take you through the longitudinal – that's Africa, here's Asia Pacific, Europe. And as you can see, Europe is filling in relatively nicely, and a few more and it will be essentially color it almost done. Latin America and North America and I expect to see, let's see – we have an announcement, right, that it's going to be signed momentarily; next month I understand, right.

So that's the survey geographically and with the numbers, happy to take any questions or suggestions. Excellent, either it's too early or I've covered everything perfectly. I also have to apologize that I can stay for a little while this morning, and then I'm obliged to run off and do less useful things.

JULIE HEDLUND: Thank you Steve. Please join me in thanking Steve. And now I'd like to ask if you are part of this next panel, please do join the main table here. We do have some of the other panelists here already, and in the meantime I'll get the slides set up. So now we are moving on to our second panel, this is the panel discussion on DNSSEC activities in North America. It's split into two parts, we're going to first start with updates from the gTLDs, ccTLDs and then we'll have updates from ISPs.

And I'll just make a note for the program, Valeri Stoyanov from the Department of Homeland Security was not able to join us. But in his place we're very pleased to be able to have Doug Mawn sitting over here to my right. And without further ado I'm going to turn things over to our moderator for this session, Jacques Latour from CIRA.

JACQUES LATOUR: Thank you. Okay, so first of all welcome to Toronto. I hope you're having a great time. Today we're going to talk about DNS activities in North America and I'll start with my presentation. I'm with CIRA, .ca. And basically, as you can read there I'm pretty big, we expect to have the zone file signed by November 12th. It's been a long journey, more than a year. We're not even exactly sure when we started working on this, but at least we know when we're going to get it done.

The key event that occurred September 4th was a key signing ceremony. We had key people from the Canadian government present at the ceremony, and then we programmed all of the HSM for production. All of our information in the DPS is online and up to date. Next slide, but you're missing some. So one key thing we did at CIRA was we looked at all the lessons learned that all the different TLDs had with DNSSEC and implementing DNSSEC.

There was a lot of different things that happened out there, and we took that in account to develop our DNSSEC solution. So we developed a high availability resilient solution that incorporates most of the lessons learned that we've seen. So what we ended up doing was we designed a dual independent signing engine, and I'll cover that quickly in the next slide. But basically we signed a zone using two different technologies, and then we do differential between the different zones to detect if there's any issues with either zone at that point.

So what we did is we developed a comprehensive validation process for DNSSEC. So we do a lot of tests, compare zone files, we do a lot of check and then if anything goes wrong we don't publish the zone file. So, it's a manual intervention at that point to figure out what happened

or why. I guess a lot of you know in the past there's been a lot of different service impacting issues with different TLDs. There were DNSSEC software issues, key management, implementation issues at the infrastructure level, and also some operational issues. So we took all of that and built this solution.

So basically what we do is we sign one zone file, the unsigned file with open DNSSEC, we do the same thing with BIND and then we bring the two zone file on the level two validator and then we do a bunch of checks there. And the intent is that if we see an issue with either open DNSSEC or BIND or any anomaly, anything that goes wrong, the level two validator won't publish the zone. So throughout this process we actually worked a lot, we're a sponsor for open DNSSEC so we decided to use the latest version and make it functional for our use and production, even though open DNSSEC says we're running an alpha version which is not recommended for production, but it does work because our level two validation says it's all good, so far so good.

One key point to note is, if you look at the diagram on top, there's a PRD which is our production site, and the bottom piece says BAK or backup site, and all the signors in both locations are actually live all the time. So if we have a failure at the primary site, if it blows up or whatever, other cryptographic material is present online up to date and signing at the backup site.

So this is – you'll all have access to the presentation, you can read it – but basically we do level one validation before we do a lot of that to make sure the integrity of the zone file is good before signing. After we sign it we do a lot of tests, LDNS, valid DNS, we check the KSKs to make

sure it doesn't change. So basically we do a lot of different tests at that level, and that's where the lessons learned came in as a lot of the tests are specific to specific issues that occurred. And we ended up generating a pretty good zone file out of it.

So this is what we're doing, November 12th is goes online. After that, our next project is to get DNSSEC in the registry. So either we take DNS key or the S record or whatever. So that's going to happen early 2013. And then our next project is getting the ISPs in Canada to do DNSSEC. According to what I've seen at Tech Day, about .5% of the recursive over in Canada are DNSSEC enabled, so I think that's 12 or 13 of them, not a lot.

Our next step is to go work with the registrar and get them to do DNSSEC and then promote the .ca registrant. So the last bullet is the ICANN meeting in San Francisco; that was my last bullet is we're committed in doing DNSSEC. I think that was 18 months ago, so we still are.

MATT LARSON: Good morning everyone, I'm Matt Larson from VeriSign and the program committee asked me to give an update on .gov. So that's what I have for you.

JULIE HEDLUND: Just one second, evidently the slides have dropped out of Adobe Connect room for some reason. So I have to put them back in, I'm sorry about that.

MATT LARSON: So here's some background for you on .gov. as you may well be aware it's used for US Governmental agencies, both the Federal Government but also State and local governments, so .gov has been in the news for the past several years because of the mandate from the General Services Agency of the US Federal Government to – excuse me, the mandate is from the Office of Management and Budget; too many acronyms on the slide.

So people I think tend to think first of .gov for US Federal, but it does have State and local domains in it. In fact only about a third of the nearly 5,000 domains in there are actually the US Federal Government. So VeriSign has been operating .gov on behalf of the General Services Agency since early 2011, so coming up on two years. We're doing it with FIPS 199 High as our guidelines. FIP is Federal Information Processing Standards and the "high" means that if this were to fail it would have a critical impact on a particular agency or organization.

So that gives us a fairly high bar that we have to meet in order to run gov to those specifications. DNSSEC is important to .gov. As I said it's been a discussion for several years because of the OMB mandate. It's been signed since early 2009 and the transfer to VeriSign for registry services two years later. We believe that's the only transfer of a signed TLD from one registry to another so far, and we pulled that off without incident.

So we have a cloud signing service that we're about to offer and that will be included with the domain registration charge for all .gov registrants, just to make it that much easier for a particular agency or

organization to sing their zone. It's certainly not required. If they have any other mechanism or other vendor they can do that, but we're just offering this to make it absolutely as easy as possible for .gov registrants to sign their zone.

So here we go, this is the infamous OMB mandate, just to put a face to name as it were. And you can see the date on this. And the intent of the mandate was to have every second level .gov zone signed by the end of 2009. That hasn't quite happened yet, but it's a work in progress. So with thanks to the folks at NIST, this is a chart that shows over time the progress in getting things signed. So as you can see – and we have no legend, I apologize for that. I believe the green is the signed zones. So it's slow but steady progress.

And just because this is North America and I had the slides, I went ahead and put in a comparison to show .com and .net, just to have the latest statistics out there. So you can see here a chart that shows the number of signed .com names in green and the number of signed .net names in blue. Those two big spikes, the first one in June was from the UK hosting company and registrar OVH and then the next huge spike is from the Dutch registrar TransIP. So they both signed a great deal of the zones that they hosted and sent DNS records to the .com and .net registry.

So I just checked the current count, we have a website called scoreboard.verisignlabs.com that's always got the current count of signed names. And we're at about 120,000 .com right now and about 20,000 .net. And this is just a pitch for another VeriSign Labs tool. Dwayne [Wessells] who works for me has done really great work on this

DNS debugging tool that lets you put in a domain name and see exactly from the root on down all the key material, all the DS records, what's happening, if it works or doesn't work.

And that's the very brief update that I had. Are we going to take questions at the end Jacques? Okay.

DOUG MAWN: So I'll go ahead and give a little bit more detail on the .gov, Matt and I probably should have coordinated slides. But let me just give you a little bit more detail. As Matt mentioned, you can go to the next slide Julie. As Matt mentioned, the mandate came out in 2008. The numbers here actually started in 2011. There wasn't a concerted effort until March of 2011 within the government to try to push DNSSEC, some of the agencies had done it, most of them hadn't. So if you actually look here, of the 111 agencies 18 months ago, we had a significant number that had not deployed DNSSEC.

So this has been the progress. This slide is a little dated, it's March. We actually have to my understanding more compliant than non-compliant today, so we're above the 50% mark. But that's on the agency side. If we go to domains, next slide. Totals of domains, you can see again, slow progress between signed and unsigned domains within .gov. But again, we're getting there and getting people on board. It's been a little bit of a challenge.

As you can see, we still have a significant percentage. I think we're, these slides are dated. I believe the last I saw, and even Matt had it, was about 70% signed, which is what I understand the number is so. Go

ahead, next slide. So that's our improvement chart. We have to show that the UN Government is making progress and improvement. So I actually think on the Adobe Connect it might be cut off on the top, but the key here is the title has to do with DNSSEC validation.

So, some of you may be familiar with the standard that is NIST 800-53. NIST is in the process of revising that standard and it's revision four. And revision four requires all government systems to do validation. So, that's to be published I believe later this fall. And what we expect to then start to see is all systems, we have a ranking in the US of systems are either low sensitivity, medium sensitivity or high sensitivity. And in the past the only ones that were doing validation were high, and now all systems will be required to validate.

As you can see we already have some number of those already doing DNSSEC validation, but with an additional mandate and requirement, we hope, from the NIST side that will actually help push validation even further on the US Government side. So just some final statistics – 36% increase over the course of a 12 month period in agencies, 40% increase in domains, 43% decrease in the number of non-compliant domains. And we tried to estimate the cost savings by not having to operate 205 domains that were determined to be unused and we got rid of them, so this is an initiative led by DHS, but across the Federal Government for trying to push DNSSEC forward and it continues to proceed. That's it.

JAMES ANDERSON: Hello and thanks for having me join the panel. My name is James Anderson, I'm Project Manager at Neustar and I'm going to talk about a lot of the DNSSEC that we're doing at Neustar. If I look a little new it's

because I am a newcomer, so when you have questions please be gentle. Neustar operates a couple of services we provide for our customers. Obviously what we're probably focused on here primarily is our registry services and of the number of TLD type domains that we operate, or that we host on our services. I'll focus a little bit later on specific details of the ones that we operate.

We also have another service which I guess in the context of this conversation has to do with the second level domains, or enterprise customers. This one's called the Neustar Ultra DNS; I'm just going to mention it, in some of the components that we do, some of the services that we do for DNSSEC there as well to help drive adoption. However, both platforms, they're inter-related and obviously the teams talk to one and other and we are motivated by the same design goals for the services.

One common theme you'll see between the two projects, or the two services is an abundance of caution, in order to get DNSSEC up and operational, at the same time providing a level of service that our customers have come to expect for these services. So, moving into the registries that we actually operate – I'll just give you a timeline here and I'll tell you some of the statistics about them.

.US was the first one that we went on as far as signing the zone. We did that back in December of 2009. You'll see a timeline bar there and the next end of that timeline is when we actually start accepting DS resource records into the zone for subdomains. You can see there's a distance in that time there again that theme of caution. You can see as the next two registries that we operate are much shorter time periods

so there's a learning curve there so we're able to learn from it and move quicker.

The next section here is dealing with our SLD customer system, the Ultra DNS. And I'm just pointing out here is a snapshot of the user interface so you can see that if you have customers, or for the customers of ours that have interest in using DNSSEC, the system is there and available to use. We can actually turn it on. Again with the abundance of caution. We have not made it so that it is always on automatically for the customer, we actually have them ask for the feature. And then we turn it on and we expose them to it through this user interface.

And here then can actually select which particular domains they want to have signed, and then we apply the DNSSEC signing policy to it. There's a lot of detail in there, certainly take a look if you have any questions later we can go into the specifics of it. Regarding some of the lessons learned, some of these apply to both the enterprise side and also to the TLD side. But one of the things we find when we're talking with our customers about DNSSEC, and I'm not sure if this is probably a common theme for all of us, is without a lot of operational knowledge of DNSSEC, a lot of people are turning to us to say "how is this best performed? What signing policies? Which crypto algorithms should we be using."

So rarely do we have people come to us and say that we need to have X, Y and Z as a signing policy. Our services as far as DNSSEC, we've approached this as this is something that we're doing on behalf of the internet and for our customers and its enhancement to the protocol. So we don't have any charge for passing it on to the customers. There may be operational costs in terms of turning on the service, that has to be

borne by the organization but that's not something that we pass on the terms as like a charge. I think that's all the time we've got.

JULIE HEDLUND: You have 28 seconds.

JAMES ANDERSON: Okay, thank you for your time.

JULIE HEDLUND: Jacques, do you want to take some questions for the first of these two panels or do you want to wait and do it at the end? How would you like to do it? So yes, we'll save questions for the end of both of the sections of this panel discussion, so we'll move to the next presentation.

CHRIS GRIFFITHS: Hello, I'm Chris Griffiths from Comcast and today I'll be covering our effort, DNSSEC on the validation side. Next slide please. So we began working on this back in 2008 and we finally signed and finished signing all of our domains as well as turning on validation for all 18 and one half million customers that we have in the United States. So I've used this slide a couple of different times and thanks to the VeriSign folks for this. This shows at the time when we were signing in January 2012 this is where we started signing our domains.

And it's interesting, Matt showed this earlier, next slide please. We've got this huge bump obviously for additional signed domains. The key thing to note is you now have 18 and a half million subscribers actually

validating these, so that's a pretty interesting metric to take note of. Obviously with the signing and dealing with operational issues is not without issues. We've had a number of specific items in several of the TLDs, most notably in .gov. But we've actually started working with social media and other things to actually engage actively in this. So we've actually created a Comcast DNS Twitter account and other things to actually be proactive.

We also post updates on our website, dns.comcast.net, so that way folks can actually see the activity for DNS as well as interact with us, check our cache, look at the activity that's going on so we can be more proactive in this. So we've actually taken it to the streets as it were to deal with the issues. So obviously one of the issues that we continue to see is missed key rollovers, timing, other kind of associated issues that seem to be pretty prevalent kind of thing in the industry. So it's something that we definitely want to call out to folks that are actually actively signing their domains.

It seems that the tools have gotten better; it just doesn't seem that people are actually implementing them correctly. So that's something to take note of if you are thinking about singing your authoritative domain; you actually have a lot of people actually validating that now. So it's something to take note of if you're interacting with folks. The other things is looking at organizations like DNS OARC, I mean how do we leverage those kinds of organizations and others to actively get the word out, get engaged, get tooling and other kinds of things.

Comcast is one organization, we don't expect to solve everybody's issues with validation, but it would be great to have more of an industry

wide engagement in that space. So a couple of high level notes – we've seen through obviously larger amounts of validation, we've seen increased CPU, higher byte sized counts associated to this. We've actually seen some interesting attack vectors now ranging on our network, which is quite interesting. We've also seen a significant amount of fragmentation on packets coming through our network associated to this. So it's something that we're keeping a close eye on, but it's definitely we're now fairly well scaled at this point and we're pretty confident things are staying steady at this point with the infrastructure.

In quick highlight at least, what we've seen, authoritative zone signing is somewhat resource intensive associated to the systems that are going. We've made some significant upgrades in that. we've also been leveraging and looking at specific items within CDNs and GLSB; we're also working in the industry to try to get some of those things solved, so that's an active work item that we're pursuing.

And just to speed things up, for the most part we have a significant amount of metrics that we're starting to gather associated to SERVFAILs and also specific attack type things in our infrastructure, so we're keeping a close eye on that and we'll be talking about some of that actually at the next [NANO] that's coming up. And I think that's it. Thank you.

AXEL SGUIN: Good morning, I'm Axel Sguin from Videotron. Today I'm going to talk about our plans to implement DNSSEC on recursive DNS and our authoritative servers. First as I'm not sure everyone knows about

Videotron, we are an ISP in Quebec and we provide internet, cable, phone, mobile phone and cable TV. A year ago our plan was to implement DNSSEC on our recursive DNS. We decided to start on recursive DNS so to protect our customers from virus attacks and also because we thought it would be easier to [data] and recursive than our authoritative servers, and also because CIRA had not signed .ca and our registrars does not support DNSSEC yet. But currently we plan to implement DNSSEC in 2014.

We started by doing some tests on our recursive servers and we saw that the CPU increased a lot more than we expected and it was over the max threshold we defined in Videotron. So we decided to upgrade our DNS infrastructure first before we implement DNSSEC. So the lesson we learned is that we underestimated the technical requirements for CPU for instance, and also we under evaluated the operational aspects – how to deal with authoritative server that failed DNSSEC validation; how do we inform our customers; how do we make sure they don't believe it's our fault and how do we manage negative trust anchors. And also, we are sure there will be other unseen issues.

So what we plan to do now to implement it is we'll have to work closely with our customer service. We'll have to train them to use the DNS tools for example and any other tool. And will we contact the domain administrator when the validation fails. We plan to manage a blog like Comcast does; we thought it was a very good idea. And we'll start with a pilot and we'll do a progressive transfer for our customers to make sure the network is ready and the CPU will increase not too much.

And also, we don't know yet how to manage negative trust anchors, which is something we'll have to work on. For the authoritative servers we haven't done much yet. But we know we cannot afford to lose access to our domains because we have services like emails that rely on our authoritative servers. And also, we are responsible for business customer's domains and I'm sure they don't want to lose access to their domains either.

Also we were waiting for our registrar to support DNSSEC, but now we know that CIRA will take our DS records directly. That's it. Thank you.

JACQUES LATOUR: Okay, so I guess now we're ready for questions.

STEVE CROCKER: Can you say something more about the registrar situation in Canada. How many registrars are there that serve CIRA and what's their attitude about, or expectation about supporting DNSSEC?

JACQUES LATOUR: Right now we haven't, well we did talk to most of our registrars about DNSSEC; they're not in a rush to do it. Some of them support it. So I guess eh key thing is we need to have a good value proposition package for the registrar. And one thing I've noticed is that pretty much every ccTLD that are doing DNSSEC, they've built some sort of collateral to tell registrar how to do DNSSEC. We should pull all that together and have one common pitch and package with the good facts and that would certainly help us get registrars – I'm not sure what to do there.

MALE: I have a question for Chris – does Comcast have any data that it wants to share on the percentage of queries that they can actually validate out of the total volume of queries incoming?

CHRIS GRIFFITHS: It's very small. In comparison to the overall we're many billions per day, it's a small, small portion of that.

STEVE CROCKER: Let me just, have you compared the numbers that you're seeing against the numbers of signed zones known in com and net and so forth? It should track in some sense and not track in the sense that they'll be disproportionate if there's some that are frequently referenced versus others less so.

CHRIS GRIFFITHS: I think – yes. We actually have internal metrics tools that look at specific not only signed zones but also ipv6 enabled content as well. So we have all those metrics internally to look at things and also compare that to what's in cache versus what's out of cache. It's not, it's kind of lost in the noise right now. Not to say, I mean we have a significant amount of zones signed but I think the actual content and other things hasn't reached that yet.

JULIE HEDLUND: Could I remind people when they ask a question to please state your name and your affiliation. And we do have a microphone here in the middle of the floor for folks who may not be sitting by a mic. Thank you.

DAN YORK: It's Dan York with the Internet [Site]. Doug I had a question for you on the gov side. What was that NIST document number again that NIST is in the process of revising? And I have another questions too but.

DOUG MAWN: 800-53, and it will be revision four, so R4. The two controls that are key are security control 20 and 21. Those are the two that talk about secure name addressing and resolution. And that's kind of the last step on the government side as a requirement mandate for all agencies with respect to validation.

DAN YORK: Okay, my other question, thanks for that. The other question was you mentioned that some of the agencies had pushback or issues, what were the kind of bigger barriers that you saw from the agencies.

DOUG MAWN: It's an unfunded mandate, so it's been a significant culture change. It's interesting that even with a mandate from 2008 it's taken us four years to get where we are and we still have 30% of the agencies to go. There's been plenty of discussion about "well maybe we should take budget away from CIOs if they don't do it"; that would be an interesting

incentive, but it really is a culture change. I mean the technology is not the problem right, it's the operations within a government CIO shop and being willing to pay for things out of their hide.

But we have plenty of agencies that have done it, that have published what they've done. This is really not that hard to do it's a culture change.

PAUL [RATAT]: I have a question. So we've seen one incident where Nasa.gov got expired and it took quite a long time and a lot of complaints from people before that was fixed, like it was taking hours or maybe even days or a day. Are there any plans to collect this information and share this information other than the DNS mailing lists where a lot of people in the room are on, and maybe thinking about some automated way of dealing with known failures? And this is in general to the public. And as a subquestion to that, if everyone starts using, or if more people start using resolver steps on their own machine independently of ISPs, how are those people ever going to find out about these false positives and can we help them or not.

DOUG MAWN: I think that's an issue that's larger than just .gov, I mean I think that's an issue we're going to have overall as more and more authoritative zones get signed. I think one of DNS OARCs major successes is the DNS operations mailing list. We now have thousands and thousands of people there and that's become the central clearinghouse for reports of that nature. So I think for the time being we've got something that

works, but I agree it's something that we need to work on as an industry the more DNSSEC is deployed.

JAMES ANDERSON: I tend to agree also that as validation moves close to the edge it's going to be absolutely impossible for folks, the average layman using mobile devices or other things doing validation potentially to figure these things out. So we absolutely have to come up with some options prior to that becoming the standard.

ROLAND VAN RIJSWIJK: I have something to add to that. By the way, I didn't introduce myself before, Roland van Rijswijk, SurfNet in (Inaudible). Perhaps for the ccTLDs that might be a little easier because we have a deal with the guys from our local registry SIDN where we send then data on validation fillers that we see, and specifically during the big large uptake that they've seen in the past couple of months. I think that's proven a valuable tool to ensure that they could chase up any registrars or operators making a mess of things, and that's kept the number of failures and problems down in the .nl zone to something like not 5%.

So I think that works very well. So for the ccTLD folks here, or ISPs that operate mainly in one country it might be worth doing deals with your registry to help them chase this up.

CHRISTIAN: Hi, my name is Christian [Litton]. I'm from the .nl registry. I have a question for the gentleman from Comcast. As Roland said, we're seeing

a big uptake of DNSSEC in the Netherlands. And we're now trying to persuade the ISPs in our country to also enable validation, which is a tough task so to speak. One of the reasons that they're kind of reluctant to do it is that they are afraid that their customer service desk will get overloaded with questions because you know DNS domain names do not validate correctly. What are your experiences in that regard?

CHRIS GRIFFITHS: So we've certainly had our issues with a number of different high level domains, some of which have been clearly documented. We went into this completely aware that there would be operational issues, that's why we've been very proactive in standing up websites, making sure that we're actively participating in forums and other things with our customers that are experiencing these types of issues.

The other thing is, and we've documented it actually as part of a proposed draft at the IETF, is associated for negative trust anchors to deal with specific validation issues during a time when potentially there's a large domain that's impacted and a wide breadth of impact to customers so that we'll stop validating specifically for that domain during that issues, while we resolve this specific issue with the domain holder. And then hopefully after that we can disable the negative trust anchor.

So we've leveraged that in the past. We've tried to slow down the use of that over time, because again, we're less interested in turning off validation, especially in those failures, and more pushing the onus to the domain holder. Similar to the model that we have now, where domain

owners need to be responsible for their domain content, rather than the actual DNS resolvers. So we're looking for hopefully people to leverage tooling and other things to get better in this space.

MALE: I've got a question – doing negative trust anchors, kind of dangerous I think, so you need to have a good practice around that. So is there like a framework for doing this properly, analysis has been done?

CHRIS GRIFFITHS: I'll speak to that. We actually published a draft associated to try to document this process at the IETF, so at least people understood why we're instrumenting it and how we were performing it. We do view this as a short term, not the long term evolutionary step for people to maintain these things. It's not meant to this. This is just in the time so we can operationally manage our servers without having impact to our customer base. We clearly state that this is a couple of year type of thing. We don't expect to use this long term. It's a proposed draft.

DAN YORK: It's Dan York with a question for Matt. On this question around validators, I know your team was recently starting to do some work on a validator search, research project in the validating. Can you speak to that? I know Dwayne was working on that.

MATT LARSON: Sure. We started to look at DNSSSEC validation trying to detect DNSSEC validators passively in the wild based on the query traffic that we see.

There are several people attempting this and we recognize we're only one, but the nice thing is that our data roughly matches up with what other people are saying. So it's between 4% and 5% of sources that we see to a particular subset of zones that are showing evidence of validation. And we're doing that by sending first a response in a signed zone that doesn't validate, which induces in some but not all validators, it induces another query to one of the zones authoritative servers to check like did the signature get stripped, is there a man in the middle, let me try again.

And so we're taking that evidence of querying a second time as proof of a validator. And we recognize that's not perfect because we're in a bit of a gray area of the standard, it's up to the implementer to decide whether or not to do that particular retry. But at least some of the major implementations do that. We know that one implementation that doesn't is what Comcast uses and that's Nominum's. And that's not a comment on Nominum's validator it's just an implementation choice.

So the short answer to your question is right now we're seeing between 4% and 5% of sources validating.

DAN YORK: Dan York, I have a question for Chris. Chris you mentioned in your slides about the important issues we have with CDNs and load balancers and such, and you mentioned that you're looking at solutions or looking into some of that. I'd be curious to know what way you're going with some of that, because I agree it is a critical issue for DNSSEC here.

CHRIS GRIFFITHS: One thing we're finding in talking with some of the folks, and we've had a couple of different meetings and there's been broader meetings as well with some of the CDN players that we work with. While there's been significant uptake on the iPv6 side, there's less engagement on DNSSEC. So it's something that we're trying to resolve in the near term. I think there's some complexity obviously with signing content delivery networks which really is somewhat difficult in their current design, in some of the discussion we've had with them.

So certainly we've asked for the various folks that we work with to start working on this. We expect this will be a multi-year kind of process.

JACQUES LATOUR: I invited Videotron here so I might as well ask you a question. The question is – I'll answer the first one – have registrars asked for help from CIRA; the answer is no. You can send our keys directly to us; yes. And the question is what do you need, or do you need help from the community, from CIRA, what help do you need to do DNSSEC within your infrastructure, or what kind of help have you seen so far or…?

AXEL SGUIN: Of registry DNS we've done quite a lot, like we've done tests in our labs, so we should be quite okay. Maybe I'll have some questions for Chris Griffiths when we are trying to implement it, and I'm sure we'll be doing the authoritative servers to sign zones and I'm sure I'll have a lot of questions for the process and how to do that safely. And I'm sure I'll ask for your help at this time.

RUSS MUNDY: This is Russ; we have a question from the chat room for Chris. "How many validation errors are you seeing on average per number of lookups of the things that are coming in that should validate that don't? Do you have numbers you can share on that?"

CHRIS GRIFFITHS: Not actually looking at my dashboard, we do have those metrics internally. It's few and far between. Usually when we see these types of things, for the most part there's not a lot of traffic going to the stuff that we're seeing. When we do see significant ones though we do post them to the dns.com guess.net website. So there's an active blog; as soon as we see that and we get reports we'll publish that out. It actually goes out to Twitter and other things automatically as well.

RUSS MUNDY: Okay, as a follow up then – you're really making great use of social media as a way to get information out into the world about what's going on in sort of a broadcast kind of fashion.

CHRIS GRIFFITHS: Yes. Well it's broadcast but we also engage two way when we see DNS issues, even ones beyond just DNSSEC. If there's other related DNS items, domains or other things that happens on a daily basis. So we actively engage in our users and other folks through social media. We've found it very useful.

RUSS MUNDY: And if I could follow up with a question that I have for both Axel and Chris – have either of you looked at enough data, or have enough data to see if there's a difference in impact on validation; whether it's an NSC zone or an NSC3 zone. In other words, especially since you mentioned Axel that the validation was really heavy; do you happen to know if they were making great use of NSC3 versus NSC?

AXEL SGUIN: What we saw was just in our labs, so we didn't make any difference between NSC and NSC3.

CHRIS GRIFFITHS: And I don't think we've drilled into the data specifically for variation between those two. I know in the lab there was no difference associated, at least from what we saw generating high levels of traffic inside of our lab.

JACQUES LATOUR: So one observation is CIRA, one thing we did is we walked around in the country – well we took the plane because it's too big – but we did talk to a few ISPs around because we're promoting DNSSEC, we're promoting iPv6 in Canada, it's coming along, we're talking. And we keep getting the question "Do you have the facts. How much CPU power do I need to expect to increase? How much more memory do I need to increase on my authoritative? How much more bandwidth do I need to do?"

So if we could have some sort of a chart or a cheat chart that says "if you've got a million subscribers you plan an 80% increase in your infrastructure," or 20% or 10% and that way at least we – I'm sure collectively we have that information somehow, and that would be very useful when we have discussions. "This is what you need for DNSSEC. This is the operational process you need to support. This is blah, blah, blah."

CHRIS GRIFFITHS: I've actually covered this a couple of different times and I think it may be relative associated to your specific environment, right. I mean we did an analysis a number of years ago when we were looking at this for iPv6 as well on our DNS platform. And we came away, after doing the analysis and we said "okay we simply need to upgrade our platform," and that was a handful of years ago.

So those were three or four year old servers, around that time that they just simply needed to be upgraded. We expected that. And we planned kind of in combination to do the upgrades associated for v6 and DNSSEC at the same time. So we kind of get the at least uplift on the analysis from that. but I would say that there's probably, because of the variation in networks and associated traffic that you may see, I don't know a one-size fits all kind of thing might not make sense. But certainly there may be an industry there to analyze things and potentially give recommendation.

JACQUES LATOUR: We're out of time? One more?

STEVE CROCKER: Steve Crocker, I just want to follow up briefly. I don't have any first hand data but I was listening actively a few years ago to these questions and the three parameters, just to repeat, that are of interest are the amount of memory increase, the amount of CPU, additional CPU needed and the amount of bandwidth necessary to convey the larger packets. I'm trying to remember, I had a rule of thumb for these three figures that may or may not be relevant or even accurate at the time.

My impression was that the increase in CPU requirements of computing was not very much, so I was a little surprised that that turned out to be an issue here. Memory needed to be multiple and bandwidth needed to be multiple.

RUSS MUNDY: A couple of years ago, I was just quickly looking for the citation, I don't have it as handy as I'd hoped. But there was a RIPE report done by Olaf [Kaufman] before he left RIPE that has for authoritative servers a good set of formulas and approach for estimating the computing and bandwidth and memory requirements. And those seem to I think still be useful figures. We don't have anything that I recall, sort of a broadly usable basis for validating load yet. And I think JPRS was working on that but I don't think anything has been published. But there is some other activities that are studying, but for authoritative servers, that RIPE report I think is about the best.

MALE: One final thing to add to that discussion, it seems to also depend very much on what software you use on your recursive name server. Because we use [unbound] from [NL Net Labs] and we have seen a negligible increase in CPU consumptions. I was very surprised by what the guys of Videotron have seen as well because CPU, that was not an issue. Memory – eh, bandwidth is the big, the thing that goes up most.

JACQUES LATOUR: Now we're out of time? Okay, so thank you. I'd like to just one last observation while I've got the mic on. All the information that we have, I strongly believe in your site, the 360 DNSSEC site. So if we can all together put all the information in one spot, we need to pick one spot to go. Because if we have bits and pieces of stuff all over the place, if we centralize it would be a lot easier for people to get it done.

DAN YORK: It's Dan York. Sure the deploy 360. And part of what we're trying to do is to help do this and bring together information. So to the degree that we can help in that we're certainly glad to do that; that's our charter.

JACQUES LATOUR: So thank you panelists, great session.

JULIE HEDLUND: Thank you Jacques. So we'll do the switch to the next panel and I'll ask Russ and Roland and Jim Galvin to come join us.

RUSS MUNDY: Well, now that we've done our quick shift here. I am Russ Mundy, as Steve mentioned earlier, and this panel is one of the ones that we've enjoyed a lot in previous sessions and I hope we do this one also. It's DNSSEC in the wild; the idea being what are some of the things that are really important to report to the community that have occurred, some of which were expected some of which weren't. And so we have two panelists with us today, and Roland I'm going to let you say your last name because I always butcher it whenever I try, and Jim Galvin from Afilias. But Roland will start off for us here.

ROLAND VAN RIJSWIJK: Okay thank you Russ. My name is Roland van Rijswijk, that's the easiest way to pronounce it in English anyway. I work for SurfNet which is the national research network in the Netherlands. And I want to tell you a little bit about some of the experiences we've had with our DNSSEC deployment and specifically issues that we've run into with the bigger packets that DNSSEC causes, and fragmentation.

So I've put one slide at the beginning to just briefly explain the problem to you. What you see in this slide is a recursive caching name server at the bottom that's sits behind a firewall and an authoritative name server at the top. And the firewall that is front of the recursive caching name server is configured to block IP Fragments. Now, what happen is if the cache sends a query to the authoritative name server, which is arrow number one, and it asks for a DNSSEC signed answer – it might get a big packet back which gets fragmented and these are arrows number two and three.

So the packet is too big to be sent in one go and the first fragment, arrow number two, goes through the firewall, arrives at the recursive caching name server, everything goes fine. And then the second packet is being sent, which is the latter bit of the actual data gram and that gets blocked by the firewall because it's been configured to block fragments. The recursor will start waiting for the second fragment to arrive, which of course never arrives, and after about a timeout of about 30 seconds it will send back an ICMP and a control message to the authoritative server, arrow number four, to indicate that fragment reassembly failed.

So that is a brief overview just to tell you a little bit about the technical details. We've been doing research into this specific issue, and I'll tell you why in the next slide, but into the likelihood of this issue occurring on a live network. And it turned out that Nicholas Weaver of [Netalyzer] had already done some research and about 9% of all internet hosts experience problems receiving fragmented messages. And indeed our own research backs this up.

We did this specifically for DNS and DNSSEC and we see anywhere between 2%, and 2% is definitely confirmed, and 10% of all recursors that query our authoritative name servers that are experiencing problems receiving fragmented data grams. So why did we start diving into this? Well this problem really bit us. We signed our zone in 2010, were the first secure delegation in the .nl zone. And within a week we were experiencing problems. And actually the problem was that I had a queue of colleagues standing by my desk telling me that I'd broken the internet. And that was very unfortunate.

Digging a little bit deeper, it turned out that all these colleagues were customers of the largest ISP in the Netherlands, which has 2.5 million users. And they were blocking fragments on the edge of the service network. So that meant that all their resolvers were unable to receive fragmented responses, and since they'd recently switched to new DNS software, they were now asking for DNSSEC signed responses, so they were asking for big responses, which they were unable to receive.

And even though they weren't doing validation that meant that they weren't getting any answers for us and that meant that my colleagues couldn't read their email from home, couldn't read their website and couldn't use our voiceover IP service. And so of course I told my colleagues to call the ISPs help desk and explain this problem to them and the help desk said "SurfNet is doing something wrong." Which is a problem for us as well and which is the reason for us to dive into this issue because users cannot distinguish between the ISP doing something wrong here and us making a mistake.

And since DNSSEC is not t status quo for most domains at the moment, the ISP is very likely to blame us rather than look into their own core network. Luckily I knew the engineers at the ISPs and was able to convince them that they had an issue and they fixed it. But they still haven't changed the settings on their firewall; they've actually changed the settings on their recursors to indicate that they cannot receive big responses.

So what are some solutions to this issue, because obviously noticing a problem is one thing, coming up with solutions is the real deal. And what we did was first of all we dove into all the RFCs and had a look and

the RFC that actually specifies that you should be able to receive big fragments of responses is RFC 2671 which his quite an old RFC that describes the DNS zero protocol. And Paul Vixie, who is the editor of the original RFC is working on an update of that. And in the updated version they're actually changing their stance on fragmentation and they're explicitly including recommendations that people that implement this RFC should check whether or not they can actually receive big fragmented responses.

Unfortunately that was not in the original RFC, so I would say 95% of all people that operate recursors leave the setting of their software set to the default value which is that they accept big responses up to 4K in size, which means they should be able to support fragmentation, and unfortunately they don't. So we tried to find the solution at the authoritative site to see if we could do something about this problem ourselves.

And what we did is we set the maximum response size on our authoritative servers at such a level that we avoid fragmentation on the authoritative side to give ourselves some influence in dealing with this issue. Now obviously if you do something like that you want to be sure that you're not introducing new problems. So what we did was we did some bench marks to see how recursors dealt with finding DNSSEC signed domain names and what the influence would be of changing settings on the authoritative side.

Now the first slide I'm showing you here gives you an overview of the normal way that recursors would operate if they're not blocking fragments on a firewall somewhere and they're sending a query for a

signed domain name. What you see from left to right is Window Server 2012 Unbound from [NL Net Labs] and BIND from IC, and what you can see is they're all performing pretty well. These measurements were all done with an empty cache, so there is some priming delay in there, but they're all performing anywhere from 150 and 400 milliseconds on average to get the first answer for a signed domain out there.

Now if we put these resolvers behind the firewall that blocks fragments then we see a dramatic change. Window Server 2012 is actually unable to find an answer for a signed domain in any reasonable amount of time. And the average amount of time it can take before it can give you an answer is about 18 seconds. Now by that time the user will have already decided that the website is broken and they will have gone away.

Unbound does a lot better. The performance degrades by a factor of two, but Unbound has a fallback mechanism built in that means that if it doesn't get an answer to the first query within, I think it's about 400 milliseconds, they will send a second query where they lower the buffer size that they can receive to something that avoids fragmentation, which means that they will get an answer in the second go. And as you can see for the BIND craft, that BIND does get an answer a lot quicker than Windows. BIND also has a fallback mechanism, but BIND waits about five queries before they decide to send a query that has a smaller EDNS buffer size set so they avoid fragmentation. But there it's a factor of 10.

So what we did is we changed the – on the authoritative name server we changed the maximum response size on the authoritative side to a

value that avoids fragmentation on Ethernet, and we retried our bench marks. And what you then see is that Windows Server is still performing pretty poorly; the average is about five seconds before it gets you an answer, so users will still probably go away and decide that the site is broken.

The performance increase in Unbound isn't that dramatic; BIND does a lot better because it's more likely to get an unfragmented answer now if it queries one of the five name servers for our domain. And if we go to the next slide we change the settings on two authoritative servers, now I forgot to mention we have five authoritative name servers for this specific domain that we're dealing with. If we change the setting on two of them then it really becomes significant what the change is.

Windows Server now gets you an answer within two seconds, Unbound is nearly down to its original performance if fragments weren't getting blocked and BIND is now down to a slowdown of a factor of two. So that is a huge increase. And what this tells us is that we, as DNS operators, can do something about this issue on the authoritative side. And that means we can deal with this issue, which may be stopping up to 10% of our users resolving our domain, and that is, I think, very good. So we're now doing this in practice.

The slides that I showed you before were all experiments in a lab environment; these are slides from our live environment. In normal operations about 30% of all responses that we get back get fragmented and about 60% of all host sent query authoritative name servers receive fragmented responses. Now what we see the ICMP FRTE, that's the fragment reassembly time that exceeded. So where a resolver was able

to receive the first fragment but not the second one; that was about 1.3% in normal operations. And if you avoid fragmentation, obviously that drops down to naught%, and that means that these people who were unable to get an answer before were now able to get an answer from us, so that was very helpful.

Obviously if you decrease the maximum response size on your authoritative name server you may be introducing new problems because some of the answers will no longer fit in the smaller responses. So we did an experiment with that as well. We had a look at the (inaudible) repository which has a lot of signed domains in there, and sent queries out there with varying response size to see if we would get back truncated responses.

Now the table shows you the results for the default response size for K, the response size 1472, which means you avoid fragmentation on internet. And the response size 1232 which means you avoid fragmentation on iPV6 minimum NTU. And what you can see is that for 4096 and 1472 it is unlikely that we will see a lot of truncated responses for DNSKEY queries which are traditionally some of the biggest responses you can get. For 1472 you may see up to 8% of responses getting truncated, but we had a more detailed look into which domains these were and these were mostly experimental domains that had more than the normal amount of keys in their zone.

So for “normal” signed zones, if you dial down the maximum response size on your authoritative name server to 1472, you’re unlike to increase the number of truncated responses. Now if you go down to 1232, then you see a dramatic increase in truncated responses. So if

you want to avoid fragmentation on iPV6 as well, you may need to look at your DNSKEY set size before you start doing that.

So, how to move forward for this – I presented on this at the RIPE meeting in Amsterdam a couple of weeks ago. We've actually written this down in a draft recommendation. The URL that's on the slide will take you there and we're going to do some more work on that. Obviously if you're operating a resolver, if you're an ISP, please, please, please check that the maximum response time that you advertise is actually something that you can receive because you, even though you may not be aware of this you may be blocking your users from resolving DNSSEC signed domains.

And we've also got, for those of you about to start deploying validation, we've got a White Paper out there. It's all creative concept license, so grab it off the internet, do whatever you like with it. But that explains how you should set up a validating recursor and it includes information on this specific issue as well. Thank you for that.

DAN YORK: Do you want to take questions now?

RUSS MUNDY: Yeah, let's go ahead and take some questions since the other topic is somewhat different.

DAN YORK: It's Dan York. Two questions – first of all, on those first experiments that you're talking about, the changes that you saw in Window Server

2012, Unbound and BIND, those came out simply because you were changing the maximum response size in the five servers you were operating?

ROLAND VAN RIJSWIJK: No, we had a set up where we changed the maximum response size on the authoritative side, so we didn't change anything on the recursors; we changed it on the authoritative side.

DAN YORK: Sorry, yeah the authoritative side. So you made the changes on the authoritative server and that showed that; interesting. So on the issue about the truncating and the 40% truncation of DNSKEYs which is just interesting, does your draft, is that where we should look to find o=more of what you thought about answers around that?

ROLAND VAN RIJSWIJK: No but if you want I can get you information on that. That's not in the draft. The draft is really targeted at implementing a solution on your authoritative name server rather than going into the data that's behind that, but I can get you the data if you want.

DAN YORK: Ok well I was just curious, maybe briefly what do you see about how do we deal with that fact? I mean there seems to be a fundamental disconnect here because if you wind up reducing the maximum response size to allow the fragments to get through you also have this issue with DNSKEYs which would seem to fundamentally break things.

ROLAND VAN RIJSWIJK: Yeah that is a difficult issue. For iPV6 actually this problem is a little bit worse because on iPV6 you will only do fragmentary assembly at both end points of a connection. So if you have a firewall that sits in the middle, that is very likely to break stuff and we've seen that those firewalls will be likely to be blocking [path and new discovery] packets as well, so that will drop down the MTU to 1280 very quickly. So on iPV6 this is a serious issue and we don't have a clear and cut solution for that. Sorry.

RUSS MUNDY: Yeah, let's just have one more question and then we can go on to the next presentation.

HUGH REDDLEMEYER: Hi, my name is Hugh Reddlemeyer, I'm from Toronto Linux Users Group and I'm sort of naïve about this, that's a warning. It sounds to me as if you're ameliorating the problem by fixing the wrong place. It seems like the right place of course is to fix all the firewalls or the resolvers. That sounds like well there are going to be 100 TLDs that you can fix it at maybe and a bajillion resolvers to fix, so it sounds like it's easier to do the way you are. But then you listed actually three pieces of software that are the resolvers, and wouldn't getting those three software producers on board to put fixes in…

I mean I know it's a configuration problem, but if they were made more resilient to configuration problems. There are only three places it needs

to be fixed and the perpetrators of the problem would be the ones that suffer rather than everybody else.

ROLAND VAN RIJSWIJK: Yeah that's a good observation. Yes it would make more sense to fix this on the side of the people actually having the issue in the firewalls, but as you mentioned that is a vastly larger group, and also these people may not have implements on that specific firewall. Fixing it in the resolver software would make sense, but actually as you can see from the results that we got, the people from Unbound and [NL Net Labs] and BINDS ISC are actually dealing with this.

And Unbound does pretty well right now, and the people from ISC talked to me after the presentation I gave at RIPE and they're actually changing the way BIND is dealing with the fallback in case of not getting answers due to fragments getting blocked. So I would expect that the performance of BIND would increase in newer versions because they're reworking their software in the fall of 2012 and they're hoping to get a new version out there. But it's a good observation, yes.

ROLAND VAN RIJSWIJK: So, this presentation is a bit more positive than the last ones. Rather than dealing with problems I'm going to tell you about a little success story. And it's going to be a story about the DNS signor migration we performed this summer and nobody noticed that we did it, so that was a big success. And the first question obviously is why migrate DNSSEC signors? As I introduced in the last presentation, we've been doing DNSSEC signing for a while, we were one of the participants in the

opening DNSSEC project so we started off with a very early version of open DNSSEC for our own set up.

And because of some limitations of the hardware that we were using we had a fairly complex set up and we were using shared keys. So we were sharing DNSKEYs between multiple domains and that turned out to be not a good decision in the end. And we wanted to migrate away from that and go to a much simpler set up where we had DNSKEYs for every separate zone and we wanted to migrate to new signing hardware as well, which supported this by allowing a larger number of keys to be stored in the hardware security modules that we were using.

As a sort of analogy I used the magic roundabout, those of you who are not aware of what the magic roundabout is, Google it because this is actually, it exists, it's real and only Brits can come up with a traffic system like this. Because it's a big roundabout consisting of five smaller ones and it's hugely complicated. And we wanted to go from that to something simpler. So I have a picture of another roundabout here, this is the Arc de Triomphe roundabout in France, and we wanted to go to a situation where every zone can have their own keys and operate completely separately from all other zones, just as the cars are doing in this picture. There are no lines on the road. They can go wherever they want and that should be the case for our zones as well.

Unfortunately that has a number of side effects as well. If you're doing a migration you want to avoid a big issue, so we don't want to be the poor cyclist that is cycling around the Arc de Triomphe roundabout here and get squashed between all the cars. So we came up with a couple of guiding principles. We wanted to keep manual zone editing to a

minimum because as soon as people start interfering problems start occurring. And especially, I mean obviously if you're doing something like this you're sitting somewhere in a terminal room, you're in a high stress environment because if you make a mistake your domain is going to go offline and it's horrible. So we want to avoid doing manual stuff.

And obviously we wanted the migration to go as quickly as we could make it, and keep it to within a day so that at least we would have a restful night's sleep after we had a successful migration. We started preparing about a year beforehand before we started doing this. Even before we got the new [HSNs] we started writing down what we needed to do. And what is shown on this slide is I made a scan of some of the diagrams that we drew.

And what we tried to do was draw all the different chains of trust that we would have if we were going to migrate from one signor to another signor and they're both completely independent. This is a little bit more legible than my hand drawn doodling. These are diagrams that we created from what we had on paper and it shows you in different colors and following the chain of trust from the delegation signor all the way down to the resource records, what the chain of trust would look like at any stage during the migration.

And we created, I think about eight or nine of these diagrams for every step of the migration, and we found that this really helped us do the migration. Because we could be sure that if we did the migration in the steps that we had figured out that the trust chain would always validate because we could draw a path from the top to the delegation signor all the way down the resource records.

Obviously we tested this with a non-essential domain first. Unfortunately these are a bit hard to read, but you can look them up on the slides, the slides are online. We used DNS phase from [Sandy National Laboratories] to visualize the KSK change that was actually taking place. And it's shown in these diagrams that if you see the difference between diagram one and two you will see that the KSK has been switched or the delegation signor has been switched. And the difference between two and three is that the old KSK has now been dropped from the zone.

So, the actual migration took place on July 4th this year. It did take a little under a day and nobody noticed anything. So that sounds a bit like an anticlimax but for middleware guys that's a big party. Because if nobody noticed anything, we did our job right. We learned a lot from this. We published the results on our DNSSEC blog, dnssec.surfnet.nl. There is also a document available that has all the diagrams in there that we created to do the actual signor migration.

I created ASCII [Art] versions of these diagrams to contribute to a draft that Peter Cook, in the back of the room, is writing on DNSSEC operator change. And hopefully that will help him along as well, and help you people if you want to migrate from one signor to another. And obviously that is also if you want to migrate your domain from one registrar to another. And that was it, thank you.

RUSS MUNDY: Okay, let's move on to Jim Galvin now and then we'll take a final set of questions at the end. Jim, please?

JIM GALVIN: Thank you Russ. Actually that last presentation is a nice segue here, I don't have any slides and that was an explicit choice on my part in preparing for this. I really only have one point that I want to make, and one message and so I'll just give you a little bit of background leading up to that point. Afilias has been part of DNSSEC and the deployment of DNSSEC for over five years now, so we have quite a bit that has gone on internally with all of this.

I liked the last comment that you were making there – it's nice when you can make a change and nobody notices and you know that you've done your job right. And in fact, that really is the message that I have to offer here; that planning is everything. And if you put the appropriate amount of preparation and planning in then all goes smoothly and nobody really notices. And we've heard that multiple times over already today.

Jacques started with his discussion about CIRA and their plans for launching DNSSEC; Comcast's' Chris Griffiths didn't really say it too loudly when he talked, but they put a lot of planning and a lot of effort into what they were doing before they launched validation in their system. I've been around DNSSEC a long time. I was there in 1992 when the working group first started to create the standards for DNSSEC, and Afilias began its work in 2008, which as I said, for those who might have a little trouble doing math, was pretty close to five years ago.

We're a registry service provider. We have 17 TLDs, 24 domains under management and obviously as a side effect of that we have one of the

largest DNS infrastructures. Our role in DNSSEC is really threefold. We do the signing, and with all the key management that goes with it for our TLDs. So he talks about migrating one DNS signor; we have obviously complex of signors to manage all the key management for 17 TLDs. And of course we have to be able to accept the key information from registrars and then you have to provide the DNS services, so those three things.

And as of today, we have all but one of our TLDs signed. The only one that's not signed is because that's the way that TLD needs it to be for what they do. My real only bullet point in a presentation as I said before is that planning is everything. And we really have not had any significant issues in our infrastructure since we started and got involved in this and everything that we've done up to this point.

We are just, as I like the phrases that Jacques was using this morning, I would use a similar phrase in describing – we're very risk adverse; we have a high availability, high resilient system. That was essential. You want to do this thing and nobody should notice. Except that at the time that we were getting involved in it you wanted everyone to know you were doing it, so you kind of had to tell them in advance you're leading the charge.

We really were early adopters, and I do want to take credit for two things in this process. I mean we made significant contributions to the deployment of DNSSEC. Afilias was the folks that identified the bug in RFC 4310. Now for those that who don't keep those numbers in the back of their head, 4310 is the DNSSEC enhancements to EPP that allows the registrars to provide the DS records, the key information and

such back to the registries. And it resulted in the publication of RFC 5910 with the appropriate changes that made all that work. And that was all a credit to our planning and our testing that we did before we allowed signed delegations to launch in registrars.

Another big thing that we hear a lot about in DNSSEC deployment today really is about key management. People talk about rollovers with enterprises. There's also a part of that puzzle is registrars and doing transfers; changing your DNS operator when you have DNSSEC engaged. And it was Afilias back during our testing that identified the timing issues that are associated with DNSSEC transfers and calling out the distinction, making a very clear distinction between DNS operations and registration operations.

And there's a lot of work in the community these days dealing with timing considerations in doing transfers and making all of that happen. And we had a wonderful success story over here with Roland and what's going on there. So that was a lot of work and that was several months of working. We had a couple of registrars that we worked very closely with who actually practiced registration transfers between them in order to work out a lot of those issues and to understand where the problems were.

So we started in 2008. We launched sign.org in 2009, which was the first gTLD to be signed at the time, and the largest with almost nine million domains under management when .org launched. And then we launched signed delegations into org in 2010, June 2010, which was in fact before the root was signed. I'd like to point that out too. Of course to be fair I have to give the credit to .sc who really were the first folks to

launch DNSSEC and they learned a lot along the way and they were the first ones to discover all the fragmentation issues.

So that was very important too and I do want to give credit to folks who do those kinds of things. In September of 2010 we launched internally what we called our project safeguard where the goal was, at that point, to sign the rest of our TLDs, and of course, bring on board more registrars and start that process. And that was a nine month process during which we made arrangements with all the rest of the TLDs to get them signed. The one last thing that I want to point out here, again going back to the presentations this morning, Chris had this on one of his bullets on his slide but you didn't really say too much about it at the time; you had sort of a question about it.

We talk a lot about the technical issues with DNSSEC, and there's a lot to be learned there. And most of the people in this room are here to learn about DNSSEC from a technical point of view. But for those who are service providers, you don't want to forget the rest of the team that has to be involved. One of the things that we had to do being an early adopter was internally training operations as well as development staff. I mean the DNS side of the business obviously was prepared for DNSSEC and they were moving along, but had to get into the registry and you have to get the rest of the company on board.

And you have to get operations on the other side, consider your NOC, your Network Operations Center, they have to do the monitoring and management and dealing with all that. But customer support, the customer support team is a big team. And in our organization they are a fairly large team and a large point of the organization, and we had a

lot to do there. We also started training programs for registrars. Part of our project safeguard was building materials to bring registrars on board and get them ready to do all of this.

And there's a lot to be done there. And we often shortchange that in these workshops and these presentations, so I want to just bring that back out and call that out for us too. So planning – that's my message, thank you.

RUSS MUNDY: Okay, thank you Jim. I think we really have seen today that there is some very good, positive things going on out there as well as – my that's a surprise we didn't see that one coming, which we've had both talked about today. And so I want to now open it back up for any questions that folks may have for these panelists in particular, or if folks have other items that are of a similar "I've been surprised by X" – this would also be a good time to tell us about what you were surprised about. Do we have any comments or questions of that nature? Oh my. Anything in the chat room Simon?

MALE: Roland, I'll throw a question out to you as far as are you going to be capturing some of your migration experience in a larger document or anything?

ROLAND VAN RIJSWIJK: The specific migration experience that I talked about here is completely documented. I'm not planning any other migrations at the moment. So that is fully documented and available on our blog and on our website.

MALE: Sorry, I recall you saying that now.

ROLAND VAN RIJSWIJK: That's alright.

RUSS MUNDY: Well one of the things I would like to just highlight here – Peter is back there – is the DNS Operations Working Group at the IETF which Peter is co-Chair of. And there has been a number of documents sent through that working group that has been very helpful to the broad community. And I would encourage folks if they have comments, suggestions and I know you worked with Peter for providing some Roland, but I think how you would handle the fragmentation; that may be something that we might look at getting into a BCP possibly. Because middle boxes will continue to be problematic for a while and it might be worth the effort to try to get that documented in an IETF spec.

ROY ARENDS: Roy Arends from Nominet. Roland, I think what you just described is basically an instance of a DNSKEY rollover, when you changed from one solution to, when you switch one solution to another solution. Is that correct?

ROLAND VAN RIJSWIJK: Yeah, the migration was implemented as a rollover, yeah.

ROY ARENDS: Okay and in the DNSKEY rollover there is basically various ways of doing it. One is literally double DNSKEYs and another one is double DS records. Could you highlight which one of the two you picked?

ROLAND VAN RIJSWIJK: Yeah we did a rollover with double DNSKEYs and that's documented as well. The reason we chose to go for that one is that we wanted to do a migration that involved minimal interactions with a parent and would work with a TLD, and I'm not sure if there are any out there, but it would work with a TLD that allows you to have only one DS. So that is the strategy we chose. In the end we could have gone for the double DS because our registry supports I think up to six delegation signor records, but we specifically chose that one so that we could have an experience that would work for everyone.

RUSS MUNDY: Okay, any other questions? We are almost exactly on schedule here, and it is time for a coffee break. And I noticed a little bit ago an odor of burning in the room, so it looks like they've already set up the beginnings back there of the lunch. But it's not lunch time. It's only coffee break time. So we have a 30 minute coffee break. And please be back on time because the next item is the Great DNSSEC Quiz led by Roy Arends, and it should be a fun event. Thanks folks.

JULIE HEDLUND: Thanks. Please join us in thanking this panel.

Just to remind everyone that we'll start up again precisely at 11 for the Great DNSSEC Quiz, and if you don't have a quiz form look for some extra pieces of paper lying around on the chairs, there's some to my right, and be sure to get one. But we will start precisely at 11. Thank you.

ROY ARENDS: Hello everyone. We're going to start in about nine minutes. If you don't have a form yet Julie's going around with a quiz form. You need a quiz form later for the quiz. Thank you.

JULIE HEDLUND: Everyone, this is the DNSSEC Workshop and we will start very, very soon; in fact in just a few minutes. And we will then have the great DNSSEC Quiz. If you do not have a quiz form there are some forms there on the table just the second table in from the doors in the front. We'll start in just a few minutes, so please finish up your break and join us.

Everyone please come in and take a seat, we are going to start the Great DNSSEC Quiz as soon as I can get the meeting back together because I see I've lost my connectivity. How nice. But please do come take a seat and we'll get ready shortly.

ROY ARENDS: Shall we start? Cool. My name is Roy Arends; I'll be hosting the second DNSSEC quiz. Last time we had a prize, this time we don't have a prize, but the prize is eternal recognition. And just as we had eternal recognition of the last winner, well there goes eternal recognition. No, the last winner was Matt Larson from VeriSign. We do 14 questions; we do it in pop quiz style. And what that means if you put your name on a form, you can form a group; folks at a table can form a group. You can play individually. Put your name on the form. When you're done with your questions you give it to your neighbor.

He will then check the questions for you. So after we're done with the questions we'll go over them. Cool, first question. Sorry, the hints – sometimes more than one answer is correct; sometimes none of the answers is correct. You get a point per correct answer. So for instance if A, B and D are correct, write it down. If you have all three, perfect. If you also highlighted that C was correct and C isn't, you lose all the points for that question. Okay, let's go.

So, which top level domain has the largest deployment of DNSSEC? Is that Germany, Sweden, the Netherlands or Brazil? I need to clarify things a little bit. What I mean with the largest deployment of DNSSEC, the largest, because there are a few protocol lawyers here right? It is the largest number of second level domains which have DS records in the top level domain. By the way, when we go over the questions, if there's any discussion on what the proper answer should be, I have the last say. I win.

Cool. Second question – which of these top level domains deploy DNSSEC? Is it .ec for Ecuador; is it .tk for Tokelau; is it .tv for Tuvalu or is

it .mx for Mexico? No that's not intentional. It can be all of them. Number three please. Which keys are mandatory in a DNSSEC signed zone? Is it a ZSK; is it a KSK; are both mandatory or are neither of them mandatory. And the protocol lawyers are puzzled now. Okay.

So there's a bit in the response, and it's the A D bits. What's the A D bits stand for? Is it authentication denied; is it anno domain; is it access denied or is it authenticated. Guys let me know if I'm going to fast, so I'm just going to go to the next slide. What does the D O bit stand for in a DNS query? Is if DNSSEC Off; DNSSEC On; is it DNSSEC Okay or is it disallowed? Next please. This is a fun one. What does 257 indicate in the DNSKEY records? Is that a DNS zone key and secure entry point; is it a DNSSEC zone signing key; is it algorithm 257 or is it NSC3 shall one, or is it CCLVII?

What are valid DS algorithms? So which of these can I use as a has algorithm in the DS record? Is it A – [SHA-1, is it SHA-256, is it SHA-384] or is it ghost R34.11-94? Next please. When was the root KSK rollover? So the KSK is the key signing key; was it in July 2010; was it in January 2012; was it done on both of these dates or was it done on none of these dates? Number nine – which top level domain has the largest ratio of signed delegations versus all delegations? So is that DE; is it BR – just the top level domain – or is it .gov or is it .uk.

Number ten, what does a C D bit stand for in a DNS query? Compact disc; checking disabled; cryptographic device or change directory? Next question, what were the very, very first DNSSEC RR Types? This took me a while to figure out. Is that [R-say NXD NSEC]? And what I mean with the very first DNSSEC RR types, I'm talking about that's been put in draft

internet standards or RFCs. That's what I mean with the very first DNSSEC RR types.

Next please, what does KSK stand for? Key signing key; the kill switch key; the key switch key or kappa sigma kappa? What does ZSK stand for? Zero switch key; is it zenith singing key; is it zone signing key or is it Z series key? That's a difficult one. And the last question, what is a DPS? Is it a DNSSEC problem statement; is it delayed protection service; is it DNSSEC policy statements or is it an alternative acronym for ICANN, the Domain Preservation Society?

Cool. I want you to give your paper to your neighbor so he can check it for you. Now I'm going to wait a few seconds. Too bad. Okay, so are we all set? Remember more than one answer can be correct and I've got a whole team of protocol lawyers here who will probably keep me honest, but like I said I have the last work. Okay? Cool. Here we go.

Which top level domain has the largest deployment of DNSSEC? Which one? Perfect nl, so that's one point. Second question please? Which of these top level domains deploy DNSSEC? Sorry? None, very good. So if you have written down none, or you didn't write anything there that's one point. Number three, which keys are mandatory in a DNSSEC signed zone? Is a ZSK mandatory, is a KSK mandatory, are both mandatory or neither mandatory? I'm sorry? Yes, so there are a few right answers here.

If you have ZSK, ZSK and a KSK, they're not really that different except for one bit. That one bit makes it the KSK or the ZSK, so you can actually use either or both, but you need to have at least A or B, D is correct and C is correct. So it doesn't matter what you've written down.

Okay. So everyone gets a point, exactly. What does A D stand for in a response? I'm sorry. No, just one point. So what does A D stand for in a response? Guys? It is D – authenticated. No, it's authenticated. Yes it is. Okay, yes. Okay what is the right answer?

MALE: D – that's what Donald wrote down.

ROY ARENDS: Exactly, thank you. Number six, so there was one point if you answered D. What does the D O bit stand for in a DNS query?

MALE: C

ROY ARENDS: That's correct, well done. Next question, what does 257 indicate in a DNSKEY record. I just want to hear a letter, guys which letter?

AUDIENCE: A

ROY ARENDS: Perfect. Number seven, what are valid DS algorithms? Is it A, B, C or D; which one are valid? All of them. All of them are valid DS algorithms. So this one, hold on – if you have A or just B or just C or just D you get one point. If you write up two you get two points. Did you write up three, you get three points. Did you have all four, you get four points.

When was the root KSK rollover? Was it July 2010, was it in January 2012, did we do it on both of the above dates or none of the dates above? D is correct, none of the dates above. In fact, we're currently discussing…

[background conversation]

ROY ARENDS: Oh! Oh is this when you go from a [dersky] to a fun, fun, fun. Sorry, I stand corrected; I stand corrected. Well no, none of the dates above right? Oh perfect, it's A by the way. Thanks guys. I didn't count the [Ders] rollover. I'm actually talking about the regular key rollover, but okay.

RUSS MUNDY: Rollover was in the question so it should be D.

ROY ARENDS: Well no.

[background conversation]

ROY ARENDS: Okay I'm the boss. If you have A that's correct, if you have D that's correct. So you get a point either way. Which top level domain has the largest ration of signed delegations versus all delegations? And I'm

talking about DS records in the top level domain for second level domains. So is it de, is it br, is it gov or is it UK. That's correct, that's D. I'm very, very pleased to announce that Nominet, .UK, has 50% of their second level domains signed.

[background conversation]

ROY ARENDS: 100%? Okay. So we have 50%. It's only 18, so we have nine signed. So if you D that's correct. What does the C D stand for in a DNS query?

RUSS MUNDY: Roy, I thought gov was at 70%?

MALE: Yeah wasn't that the stats? Where's Matt Larson?

RUSS MUNDY: Gov is right about 70%.

MALE: Yeah, that's what he told us today.

ROY ARENDS: Well I dint know that answer before I made the question.

RUSS MUNDY: But you can't go against what we just saw.

ROY ARENDS: I thought I had a research team at Nominet.

[background conversation]

ROY ARENDS: Thank you Oliver. So over 4000 delegations in .gov and only 1500, something like that are signed. And the UK wins again. Okay. So anyway, let's move on. Number ten, what does the C D bit stand for in the DNS query? B is correct, checking disabled. And eleven, what were the very first DNSSEC RR types? And I'm going to allow two correct answers here. So is it A – [R-say NSD NSEC]; is it B [Key NX SEC] or is it C [Key NSEC and RRSEC], or is it D [DNSKY, NSEC 3 and RRESC].

B is correct, however, A is correct as well. The very, very first internet draft that had any mention of DNSSEC has instead of a key [RSA] and had instead of an [NXS] record it had [NXD]. So answer A is correct and answer B is correct. Why is B correct? Because…

[background conversation]

ROY ARENDS: Because that very first draft is very, very hard to find. It is there and it was only briefly there, because a few months after the publication of

the very first draft, December 1994 I think, then the answer B was correct. Number 12, what does KSK stand for? Is it a key signing key, sill switch key, - okay I'll move on from here. It's the key signing key. Number 12, what does ZSK stand for? What's the right answer? C, zone singing key. Number 14, what is a DPS? Is it a DNSSEC problem statement, the delayed protection service, a DNSSEC policy statement or domain preservation society? C is correct, DNSSEC policy statement.

Okay, what I want you to do now is add up all of your answers, sorry add up all of your points for these answers. And I'm going to count down, first I go up and then I go down to see who the winner is. Oh perfect you have a prize? Fantastic. Okay, does anyone have more than 14 points? One, two, three, four, five – oh you DNSSEC geeks. I have five people more than 14 points. Okay, whom of you have 15 points? Jacques Latour? Oh from Estonia yes, what is your name? Thomas Claussen.

Okay and that's Oliver Goodmanson, anyone else with 15 points? Oliver was it you with 15? Okay. 16 points? Okay. 17 points? I think we have a tie. If I haven't seen any other hands, it is Rick Lamp and Dave Knight, both from ICANN. I wonder if they might have access to the slides; Julie? [laughter]

JULIE HEDLUND: I took them down.

ROY ARENDS: Oh yeah you took them down; that's true. Okay guys. I understand that a prize is actually on its way. You will get your prize in a minute. Next

to that, until the next meeting you have eternal recognition. Thank you all for participating in the DNSSEC quiz. I've got a minor point to make, if, and that's only if, I know that the DNSSEC Deployment Working Group, the folks who basically set the agenda for this meeting, they have the last word on this. But I'm out of DNSSEC questions.

So if you have questions that you would like to see in the next DNSSEC quiz, send me those questions and I will incorporate them in the quiz. Okay, thank you.

JULIE HEDLUND: Thank you very much Roy. And so now we are ready for our next panel, which is encouraging DNSSEC adoption and what has worked and what hasn't. So I'm going to ask that panel to come and join us at the main table here. And our webcam went away again.

[background conversation]

SIMON MCCALLA: Okay, thank you everybody. I've realized, doing that quiz, just how unworthy I am to Chair this panel. That's a reminder I need to revise more. Anyway, the purpose of this panel is to talk about how do we encourage DNSSEC adoption. And we had a very similar panel at the ccNSO session yesterday, and we had some very interesting discussions about ways in which various technical and monetary ways in which we could do that. So I'm very delighted to be here talking about that subject again.

We've got a fantastic panel with us today. We've got Torbjrn Carlsson from the Internet Infrastructure Foundation; we've got Ondrej Filip from CZNIC; we've got Chris Hesselman from SIDN Labs; we've got Vincent Levigneron from AFNIC; Frederico Neves from .br and Yoshiro Yoneya from JPRS. So thank you all and we look forward to hearing your presentations. We'll happily take questions during the presentations; we'll also have a quick roundup at the end of the session as well. So firstly, I'll hand over to Torbjrn.

TORBJRN CARLSSON: Thank you very much. My name is Torbjrn Carlsson and I joined .se in 2005 when it all began, our deployment of DNSSEC. In 2009 we changed our business model, we went into the registry registrar model starting using EPP and then I became the head of the registry and have been that since then. Okay, as you all know, we were the first TLD to sign the zone, and we also were the first TLD to have a commercial launch.

And in 2009 our Board set up a goal. They said we should have 50000 signed domains in the end of 2009. And we were working very hard, but we failed. And in 2010 it was the same goal, as you see on the figures on the slide, we failed that year too. But in 2011 things changed, and I'm going to tell you how we did it later on in this presentation. The goal in the business plan for this year is to reach 350000 signed domains, and let's see, because we're going to use the same method as we did in last year.

What we also have done is when we went over to the EPP in 2009, we regarding to the registry registrar agreement, we did it mandatory to our registrars had it mandatory to remove DS records. Now we working

on a new registry registrar agreement, I think it will take effect next year. And in that agreement we probably will make it mandatory to handle DS record all the way. The conclusion of this slide is that we have failed in our attempt to create a user demand. We tried very hard for many years.

We were advertising, we were sending out newsletters to the registrants because at that time they were all direct customers to .se. And we had online training, everything, but we didn't succeed in that way. One good thing was that we put on some target groups and some failed and some has succeeded. Another of the registrants that has failed was all the banks in Sweden. We were working very hard together with them for two years. I was probably in eight meetings with them during that period, but they are still not signed.

I mean they think that they're focused on other security mechanisms to handle the problem, but it doesn't. But anyway, the two other focus target groups was of course the registrars and also the ISPs. And we have succeeded very well on those target groups. What we did in 2011, we changed our strategy. We see it now as an essential upgrading of the infrastructure. And that also was adopted by the ISPs in Sweden. They did understand this message and they also see the same result as we do.

And for this, I think this is the reason why all major ISPs in Sweden today validate. As you have seen in several presentations in these days here, we have a very high percentage of resolvers out there who are validating. The problem was that most of the registrars, not all, they are in a [key roll]. I mean because they can send the DS records to the

registry and they also running the DNS for their customers. Actually more than 90% of our registrars run the DNS for the registrar. So they were a key factor for success.

And they still, when we start talking with them in late 2010, they say "we ain't going to do any investing in DNSSEC before we have a customer demand"; so the same old story. But we changed that because we made actually two things. We invented a kickback system and a discount system. Not so much money, but money enough to change the way that the registrars were thinking. They started to do those investments that was totally necessary to handle this.

And what we also have done is that we are putting our two major target groups, the registrars and the ISPs in the same room. We have meetings twice a year. We also have a very active email list where we can discuss different topics, solving problems. And this is necessary because you can't go into a situation where your large ISP has taken the decision at the very high level, the management level that they are turning validation on. They cannot put it on, put it off, put it on; that's not the way. Because then we're going to give DNSSEC a very bad reputation.

But problems do occur. They do. Every week we have problems with resolvers that are blacklisting, I would say correct, authoritative servers out there. So you must work together and I think we have succeeded very well. And we are a small country, it's very easy for us to have the local internet community together and well-organized. I think one thing to mention also about the discount and kickback – the Swedish

Government, they have used nearly the same method to succeed with all the authorities in Sweden.

Almost all of the authorities now in Sweden and they are quite many of them. They are signed and that's because the government was handing out some sort of contribution for those who are signing, and that succeeded also. So things look quite well now in Sweden, I would say. Okay.

SIMON MCCALLA: Thank you very much. That's fantastic. I'm going to hand it straight over to now to keep us on time to Ondrej Filip.

ONDREJ FILIP: Hello everybody. My name is Ondrej Filip, I'm from the Czech registry. I must say I was quite delighted by the previous presentation because we have a sort of personal competition with the internet from .se and I'm glad that they plan to have 350000 by the end of the year because who has more domains pays for beer for the other, so it's a very important competition for me.

So we have about 37% domains signed. We are close to a million domains in [.nz] so it's about 370,000 domains. And you know you can check the numbers at our webpages – www.nic.cz. So what has worked or what hasn't worked or at least what has worked worse than we expected – first of all we realized we had to avoid the word "DNSSEC." That's something that really doesn't work, definitely not in Czech language, but I assume probably not in other languages. So when we

wanted to discuss or somehow market DNSSEC by the end users, we had to use very simple words.

So we usually use something like “secure domains” in our language or something like that, so it’s very hard to tell the people that they should check whether their ISP is validating or whether their domain is signed. So it definitely has to be written (inaudible). Also some very technical tools that we prepared for the technical community, like the DNSSEC validating resolvers didn’t bring much value. It’s probably much better to talk directly to ISPs and try to force them to validate, try to somehow motivate them.

And the last thing, we had a lot of downloads and we presented it many times, but honestly it didn’t get much intention, is the DNSSEC hardware tester. It was a tool that you could download a software for Windows, Linux and Macintosh and you can test whether your connection is ready for end user side validation. And again it was too technical for many people, so some of the techies tried to download it that was basically everything that has happened.

Now those are issued that we really spent some energy and probably if we were to repeat this we wouldn’t do that anymore. But what has worked, our work with the registrars. There are two or three aspects of it. First of all technical, we a little bit amended the EPP so every domain can have a link to an object, not a DNS record, but a DNSKEY so multiple domains can share a single DNSKEY, which is usually the case by the registrar that signs all the domains by default.

So if they do a key rollover or some operations like that they just update a single object in their database, so that’s easy for them and they like it.

But of course more importantly, we have some economical incentives, also marketing incentives. We have a certification program. So any registrar that is (inaudible) or end user can get a number of stars from one to five, and for them it's quite hard for them to achieve five stars without supporting DNSSEC. And they all wanted to have five stars, so that was also one driver for them.

And last but not least, we have a co-marketing program where we pay back some of the money to them if their marketing campaign is related to domain .cz. And that money has a cap based on the number of domains they register. But if they sign this cap is much higher, so that's why they are motivated to sign domains because they can get more money from us.

Something that has worked very well is direct communication with mainly ISPs and also some major sites and also government. We just in very simple words during some technical conference with some drinks possibly, we talked to the technical guys "Hey guys we have this issue. We would like to secure the internet, can you help us. Can you start validation?" Surprisingly this worked very well. We are a small country. We basically know each other, so we could meet those guys, talk with them.

And so many ISPs, even the big guys in the country started to validate. And the same applies for the government, many sites are signed. Many big [eships] and newspapers are signed in our country. And last but not least, oh it's not last actually, our supporting tools, probably many of you use Firefox add-on. It's a tool that gives you visuality of the domain you are browsing whether it's signed or not signed, so this is for Firefox,

now we extended to Chrome and Internet Explorer as well. So you can download that plug-in and you can see whether the website you are browsing is supporting DNSSEC.

And also DNSSEC HTML widget is also on the homepage of CZ NIC. If you enter it you'll see immediately whether your ISP is supporting validation and iPV6 as well. And we developed some more tools, so check back at nic.cz if you are interested because everything we do is open sourced so you can download it, use it, whatever you want.

And again, we are communicating very often with the press, with the media and in every press release we talk about DNSSEC, or almost in every one. And we have a long term good relationship with the technical media, so DNSSEC is very, very accented in their articles and things like that. So to wrap up, we have 37% and we are growing. All the major registrars support DNSSEC, and the majority of them, they sign all the domains by default and we are talking about registrars with more than 90% of market share, so really almost everybody.

A very good situation is on the validation side. So two or three cell phone operators validate – Telefonica Czech Republic and Vodafone. The same applies for the largest DSL provider, which is Telefonica again. And almost every B2B ISP validates, so that's very good. Many important sites were signed as I think I mentioned. And last, and very important thing, DNSSEC became a part of the official government strategy called Digital Czech 2.0. And that strategy is stated at every governmental to be signed and that this should be promoted to users in the Czech Republic. So it became a part of the national strategy, or it's a

draft of the national strategy at least, so I hope we will (inaudible) operate it from the document.

So that's all from my side. Thank you very much.

SIMON MCCALLA: Thanks Ondrej. We just have one quick question from the floor from Dan.

DAN YORK: Ondrej, it's a great amount, excellent progress on what you're doing there. On the validation question, what did you do to be as successful as you are with getting all those ISPs to do validation?

ONDREJ FILIP: As I said, it was quite surprising. We just came to the technical guys we were meeting in the exchange points for example, and the internet exchange point meetings, and we just tell them "you probably see our marketing activity, we need to help on it. We cannot offer you much. We will do a press release and we are an independent organization, so this press release is good media coverage. But can you help out with that; can you just start validation?" And those guys said "Well yeah we will inform management and we will do it." And it was done in about a month.

One more thing that was important, they have an argument we needed to deal with. And they said "If we will start validation and because we have large number of domains and some of them are broken, if we will start the validation all consumers will see less website and customers

from the ISPs they are not validating." So what we had to provide for them was a tool that periodically checks all the signed domain and checks whether they are not broken. And if they are we usually inform the end user and delete the broken signature.

So that was a tool we had to provide and also we provided a hotline, phone number they can call 24 hours in case they would face some problem with DNSSEC.

DAN YORK: So you're taking on that monitoring for the cc domain then as far as which sites have broken signatures?

ONDREJ FILIP: Mm-hmm.

DAN YORK: Okay. Interesting. Thank you.

SIMON MCCALLA: Thanks. So without further ado, I'll pass on to Chris from SIDN.

CHRISTIAN HESSELMAN: Thank you. My name is Christian Hesselman. I'm with SIDN. SIDN is the registry for the .nl domain, that's the Netherlands. A small country in Europe as you can see on the map over there. We're a not for profit private organization and our zone file currently consists of over 500 million domain names. And we work together with around 1700

registrars. Since the beginning of September we're the largest DNSSEC zone in the world. We have over one million signed domain names.

And the way we accomplished this is like many of our peers, we followed what we call a collaborative approach in which we closely worked together with our registrars, and in this case also Power DNS, one of the manufacturers of name server software, and also Dutch Government agencies. Actually there should be two of our registrars in the room right now – there's (Inaudible). I'm not sure if you guys are around here. They're not here. That's too bad. Anyway, they should be here at the conference so maybe they'll show up later on.

So what we did is our strategy was to coordinate the deployment of DNSSEC in the Netherlands of course, promoting mass signing. And our, let's say, activities basically revolved around two major parts, consisted of two major components – one was the two year discount program for our registrars in which they got an 8% discount on the domain names that they signed. And this basically resolved the issue of not having a business case for them, as there was no customer demand yet. And the other major component of our activities was the what we called the sharing of DNSSEC knowledge.

Our registrars indicated that they expected from us to take the lead there and basically help them become more knowledgeable about DNSSEC. So we set up a website, it's called dnssec.nl, with lots of documentation, blog posts, videos and whatever else. And the major asset there is that it's in Dutch. So many people in Holland speak English, but having the same material available in Dutch is a plus.

Well in addition we had a flawless introduction of DNSSEC tier two back in May, so that also helped of course. And we have a very active account manager who was frequently interacting with our registrars. As you can see in the picture we started out with nine high profile registrars, but the uptake was so quick that we currently ended up with 239 registrars doing DNSSEC. If you look at the interactions between the registry and the registrar then you can see that it required a huge effort on both parts, lots of interactions.

But that our registrars now have let's say a unique selling point in that they can offer DNSSEC to their customers and they also actively advertise that on their websites, and they also have an international advantage because their one of the first registrars internationally in Europe for example to become DNSSEC enabled.

On the registry side it was also a very intense process with an organization wide impact. We got lots of publicity out of it, so that's a good thing. And of course, the most rewarding thing is that we contributed to a safer internet. The other two stakeholders in our let's say collaborative approach were Power DNS, like I said; it's a manufacturer or DNS name server software. And we worked together with them because more than 50% of our registrars use Power DNS as their name server software.

We financially supported them and they provided tech support to the registrars. We also interacted with the Dutch Government agencies, and they got DNSSEC on what we call a comply or explain list; which means that whenever a certain technology is on that list, a Dutch Government agency is required to basically purchase equipment or

software that has that technology in it. So the result of all these activities was what you can see in this graph.

The red like is the uptake of the DNSSEC signing in the .nl zone. And we're currently roughly at 1,283,000. So our next steps are basically four things. One is we plan to work on secure transfer since we're a large DNSSEC zone. This is something that we're going to run into soon. We're starting to interact with ISPs in the Netherlands to basically enable DNSSEC validation, so that's what we call DNSSEC tier three. And we're also working on a tooling to basically crawl the entire .nl zone to check which domain names validate correctly and which don't. And finally we're working on our registrant communication program. That's it. Thank you.

SIMON MCCALLA: Thank you very much Chris. Does anyone have any questions for Chris before we move on? Okay. So moving on next we'll have Vincent on please, from AFNIC.

VINCENT LEVIGNERON: Yes it works. Good morning, my name is Vincent Levigneron and I work from AFNIC. I joined a long time ago. We are waiting for my slides. I see there is a big clock just in front of me, but don't worry, no pressure. I will be very brief because we did almost nothing if we compare to (Inaudible). So I'll be very brief.

AFNIC operates six ccTLDs for now. The largest one is .fr with almost 99% of all domain names registered for AFNIC. The other ones correspond to smaller French territories and share the same registration

and publication [roles] as .fr. We are also backend registry for 17 new gTLDs. And of course DNSSEC is part of the package. DNSSEC was introduced at AFNIC in September 2010. For the DS registration it was launched a little later, 18 months ago through our web interface and EPP.

When we started DNSSEC we met some problems due to our technical choices and zoning tools and (inaudible) for instance was not the best way to (inaudible) stable but it was for now. And during key [duration] phases and when we rolled over our keys we had some problems at the beginning. And we were able to find many bugs in lots of different tools. It seems CIRA is still finding ones, that's what Jacques said in his first presentation. And since we launched the DS registration the system is now stable.

All of these ccTLDs are fully DNSSSEC operational, which means that we represent 20% of all [the] ccTLDs Steve Crocker presented in his first presentation. But after just one year of operation we only had 50 signed zones with DS announced, which involved 16 registrars. We found out that other registrars had signed zones but without DS announcement. And we decided to conduct our first survey. The goal was to prepare our infrastructure to an unexpected growth of the domain names signed, and we had various answers.

Is that the end of the slide because there is something missing? Okay, I have mine. So the beginning was not very explosive, as I can say. But I think in six months we have constant growth with 10 new registrations with DS per day. And more than 100 new registrations since three months because our largest registrar decided to propose DNSSEC as an

option and in his future plan he will sign complete zones. As you can see we are far behind the registries represented in this panel, but we are at the very beginning of our DNSSEC promotion plan.

The number of signed zones is now higher and will reach 1% of all AFNIC domain names, which are now signed. We hope that we will be as successful as you in the near future. Yes I am almost out of time but it will be okay. Some of our largest registrars as I told you still plan to propose DNSSEC and have planned to sign all their domain names in the near future. And that's why we decided to launch a five year DNSSEC promotion plan alongside our registrars.

But the promotion plan is not only about registrars and we also plan to ask domain name holders as well as larger ISPs for validation for instance. And of course all the registries will successfully experience to find the best way to increase DNSSEC around this and to find a collaborative approach to deploy DNSSEC. And I have lots of interesting things to do according to the various presentations. I am over. It's finished.

SIMON MCCALLA: Thanks Vincent. Anybody have any questions? Great, thank you for that. Oh we've got one, apology.

JACQUES LATOUR: Jacques Latour from CIRA. So one thing that seems to be coming along is the TLD operator, it looks like the TLD operator is responsible to monitor the signed zone to make sure that they're, the signed domain

to make sure they're valid. And then there's a lot of discussion around that. Who's doing that right now?

MALE: We have been doing for ages now. But we have been doing that for the delegations too. When we started to provide DNSSEC we just extended the service to check signed delegations too.

MALE: And I think is said that we do monitor it and try to fix the issue.

JACQUES LATOUR: So I guess the question is should that be a best practice or?

MALE: Okay, what we do, we are by databases checking all the delegations which had occurred during the last 24 hours. And then we check them and sending out emails to our registrars in the morning.

CHRISTIAN HESSELMAN: We developed a tool that enables registrars to check online if their domain names validated correctly. That's something that we will be building into some sort of crawling engine where it can continuously check whether or not domain names validate correctly. But the responsibility, I think, is with the registrar to make sure that they set up their infrastructure correctly, but we can then help them if we see any problems.

VINCENT LEVIGNERON: In AFNIC we are obliged to use a checking step when you propose a DNS configuration and of course we check for the DS. And that's why today we can say that 100% of domain names which are signed are (inaudible) correct because we check the same for each time you ask for modification of [NS and DS registrar].

MALE: But are you doing ongoing monitoring or is it just when they first enable the zone and upload the records?

VINCENT LEVIGNERON: This is the first time the modification but we don't check it after, not for the moment. It's something we planned but not yet.

MALE: Thank you. I'm just kind of building on Jacques question that we are seeing that some of the zones are doing that kind of ongoing constant monitoring and I was just curious more too how prevalent that was.

SIMON MCCALLA: Operator, is the remote mic working?

JOE [AMPLY]: Joe [Amply], ICANN. This is not directly related to any of the presentations that I just saw, but since I have to skip out of here in a few minutes I think it's interesting material and I thought I'd mention it. At

one of the functions of IANA with relation to DNSSEC and the root zone is we publish the trust anchor. We publish the trust anchor out of band of the DNS protocol using http, and we provide various means of checking the authenticity of the data. And we track how often that trust anchor is downloaded.

So these numbers we thought would be interesting in terms of uptake of DNSSEC. We assumed that people would receive the trust anchor from here. To date, well up until a couple of months ago, what we saw was a fairly steady low number of thousands per month retrieval of trust anchor material from the IANA. We imagine that many of these validators that are validating are probably configured by people who know what they're doing so perhaps many people are not using the out of band method.

But in the month of September, that monthly average of a low thousands increased somewhat. And in the month of September we logged 450 million downloads of the trust anchor from the published location where it come from. And a little further examination revealed that most of, well pretty much all of that additional load happened after September the 19th. So checking user agents and comparing the calendar with known other events in the industry, the launch of ios6 on iPhone's, iPod's and iPad's has suddenly resulted in a community of potentially 450 million additional validators in the world.

So in some sense this stuff just got a little bit more real. So if people are interested in the other side, apart from signing, interested in the prevalence of validation on the end location, it's I think the case from our perspective that this is no longer a phenomenon which is based on

validators and ISPs and now this has moved firmly in the domain of end user devices. So now we have operating systems that are really sort of designed from a human interface perspective for 12 year old children and grandmothers to use, which is now potentially doing DNSSEC validation.

MALE: Joe, do you have any data to show that they're actually doing validation?

JOE [AMPLY]: Well, all that I really want to talk about today is what we see from the IANA side. But surely there are many iPhones in the room held by people who know how to run TCP dump and they can draw their own conclusions about what the device is actually doing.

SIMON MCCALLA: Joe, on behalf of the program committee, show of hands in this room, I think it would be a really fascinating presentation if you could come back to us in Beijing and show us some of the results of that and get some proper numbers on that, because I think that would be really interesting.

JOE [AMPLY]: Yeah I'd be very happy to do it.

SIMON MCCALLA: Thank you.

RUSS MUNDY: One thing to add to that is Windows Server 2012 also has a built in mechanism for grabbing the root trust anchor from the IANA site. So I would assume that once deployment of that kicks off you're going to see much bigger numbers again.

JOE [AMPLY]: We look forward to is, more traffic in this area is good. One thing I would add is that I don't think we've been clear enough in the way that we've designed this thing and how we expect validators that are bootstrapping to validate the authenticity of the trust anchor material that they receive. And now that we have a very large number of largely admin list devices doing this stuff it seems important to get it right. So we're going to make an effort over the coming months to try and progress these things in conversations in places like the IETF to try and make sure that we're doing something that makes sense and that the method of secure retrieval that we think should be followed is actually being followed.

SIMON MCCALLA: Thanks. I'll just take one more question, we've got Paul and then we'll move on for the record.

PAUL WOUTERS: I just wanted to say that [Dabine] actually uses unband anchor to also grab the root key, so every [Dabine] installed will also generate this for you. But that's probably the thousand you were seeing before.

SIMON MCCALLA: Thank you for that. That's a really, really interesting discussion. Sorry Jim, go for it.

JIM GALVIN: Yeah one quick clarification to Joe. So he said 450 million downloads of the trust anchor, was that just a spike or is that the new steady state?

JOE [AMPLY]: Well not much time has passed since September 19th, so it's a little early to say whether what we're doing is tracking upgrades of Apple devices to ios6 and new devices that are shipped with ios6, or whether we can expect to see regular occurrence of this. We don't really know. Early to see from the outside, but yes, by Beijing we should have a better answer to that question.

JIM GALVIN: Well where did the 450 come from, over what time period I guess is the right question for right now.

JOE [AMPLY]: That was 450 million downloads between September 19th and September 31st. It was more than we were expecting. [laughter]

SIMON MCCALLA: Just a bit. Okay, thanks folks. I'm going to pass it over to Frederico now, from Brazil.

FREDERICO NEVES: Good morning. My name is Frederico Neves and I work at the .br registry. So basically we have been doing this for a long time now. We started with incremental deployment in 2006 and added DS collections in every single interface that we had for the end users we added the support. The initial deployment was pretty simple with offline signors. And then a little while before the singing of the root in May 2010, we revamped the system to have it completely in line with the characteristics of the registry – two signing ceremonies per year, back up sites and the use of enterprise quality hardware to the provisioning of the DNSSEC.

And then we picked basically three deployment strategies – one we decided to create some safe havens and promote DNSSSEC with that. And then we had three deployed during this time, three specific domains for the judiciary for banks and for the legislative power in Brazil. And all these domain names have DNSSEC mandatory. So if there is no DS there is no delegation. And this was one of the strategies and it attracted a lot of end use to the DNSSEC arena and this was good, but the amount of delegations are pretty low, especially because there are very restricted zones.

Then we wrote and provided to the hosting companies a piece of software that does automatic DNSSEC provisioning, it's called [DNS Shim]. And since December 2010 we started to use it on direct customers that we still have. We have a mix of [moding] in Brazil with direct clients and clients through registrars. And with these direct clients we are now, this week, 329000 signed delegations.

And since the last week too we started to auto-provisioning TLSA records, and completely automated so end users don't need to actually know how to do that. If they have a htps server and name provisioning through these two, you have just to click a button and we fetch over htps the connection and fetch the certificate, look if it's more appropriate to use H1 or 3 depending if it's a self-signed or a certificate chain through any of the 600 and something trusted certificate providers.

And then we ultimately provision the TSLA records. So on the side of provisioning data this is almost basically done in our case. And we have, in the third deployment strategy was the training and outreach to ISPs and service providers. And we have been doing this in the operators meetings in Brazil since the beginning 2006. And this is a continued work. But what you could see here is we have started deployment in 2006 and we had a pretty small uptake until we started to provide commercial incentives, like direct or indirect ones.

And then with these commercial incentives in late 2010, we started to have this uptake that is basically linear and as you can see we are getting around 200 new signed delegations a year. So outreach and training works but only for the techie and this needs to be completely automated for end users. They actually don't need to know that we have this thing going. And safe havens, they suffer the chicken and egg problem. Like the banks they have this safe haven that would probably have more impact regarding phishing because of the users having in their minds that this is a safe domain name not because it has DNSSEC on it.

But anyway, it's a first round chicken and egg problem. And the monitoring incentives, even indirect ones, that is what we are doing, we are not giving any discount but we are providing services for free, it just works. That's it. Thank you.

SIMON MCCALLA: Thanks Frederico. Any questions from the floor? Okay. Thank you.

MALE: I'll just say it's awesome to see the TLSA stuff coming in for [Dane]; thank you for implementing that. And anything we can do to help get that out is awesome. Thank you.

SIMON MCCALLA: Okay, and last but definitely not least, over to Yoshiro.

YOSHIRO YONEYA: This is Yoshiro Yoneya from JPRS who is operating .jp. The background of our DNSSEC deployment is we launched DNSSEC services last January. That means that DS registration to the jp zone is available now. But only 5% of registrars handles DS registrations, but they cover almost 20% of jp domain names. And the penetration of DS registration with signed zones [with registrars in] .jp is still very, very low. And by our observations we see 2% queries of DS to the jp DNS.

So what we did, there are several things we did. So one is DNSSEC promotion to registrars. We had several private seminars to the registrars and we did DNSSEC examinations with ISPs and hardware

vendors. And in the examinations we did performance tests such as authoritative DNS servers caching resolvers and small (inaudible). And we also did the registrar transfer test with registrars. And finally we published the report to the public in Japanese and with help of APNIC we published English report also.

And some promotion activities with the community, we joined DNSSEC JP which was a community to promote DNSSEC in Japan. And during the activity we published several kinds of documents to the public in Japanese. Because for Japanese English is not so familiar, the documentation in Japanese is very important, so the objective of DNSSEC promotion in Japan was to provide such kind of Japanese document.

And as a result the recognition and understanding of DNSSEC have improved in Japan, but DNSSEC adoption rate is still very low in registrars, ISPs and registrars. And the analysis of this, the promotion to ISPs, registrars are not sufficient yet we think. And promotion to registrars may be improved by giving more education to the registrars and giving incentives to registrars like other TLDs do.

But how about ISPs and registrants? The reason why ISPs and registrants do not adopt the DNSSEC to their zone or to their (inaudible), they are already recognizing the usefulness of DNSSEC but they are also recognizing impact of DNSSEC operational failure, which caused the name resolution failure. So that they are especially nervous to keys (inaudible) area because many DNSSEC operational procedures are automated recently, but KSK rollover is not. So that they fear for the failure because KSK rollover requires interaction between the child

zone administrator and the parent zone administrator, so there is a chance of failure because it is a human operation.

As I said impact of KSK rollover failure is causing a zone banishing which means a name resolution failure for whole domain names under that zone. So if that kind of zone banishing has happened, ISPs and registrars will receive a lot of complaints from the end users and the impact will remain until [they expect the validator] to be expired. How to mitigate the impact – there are some possible countermeasures but some of them are lack of feasibility or hard to implement in the average registrars.

So we are thinking about shorten DS TTL in parent zone; parent zone means like .jp. But there is not best practice yet. I'd like to discuss especially like you TLD operators or DNS operators to have such a best practice to mitigate the impact of zone banishing and I'd like to talk about the shorten DS TTL of the countermeasure. And such kind of preparation for possible failure will encourage ISPs and registrants to adopt DNSSEC I think. Thank you.

SIMON MCCALLA: Thank you Yoshiro. Do we have any questions? Okay, well I have a question for the whole panel and I want us just to consider. The story that we seem to be seeing so far is that actually reaching out to registrars and reaching out to ISPs seems to be having a good success. Should we be considering reaching right down to registrants and even internet users, or is that a bit of a futile exercise?

MALE: Well I think I was very clear in that matter. This is an infrastructure thing.

MALE: Did you mean companies or did you mean end users as persons?

SIMON MCCALLA: I think both.

MALE: Both, okay. We tried to reach the big companies, the big registrants that run the infrastructure that are usually capable of signing domains. And we made several marketing campaigns related to as I said the secure domains, so we tried to communicate with them that they should check whether their ISP is validating. We never tried to help them with the end user side validation, but we tried to reach them, tried to explain it's great if they see the green key. So in various [ways] we tried it and I think we were successful so far with it.

SIMON MCCALLA: Okay thanks. I'm going to ask you all one very quick question to finish, which is if there was one thing in your rollout plans for DNSSEC that you could say "that's the thing that made the biggest difference to uptake," what would that be? I'll start with you Vincent, right at the end.

VINCENT LEVIGNERON: Yes because I can start because we did nothing. So good advice could be just wait because we waited and now we have a gross of [DS unresolves], so perhaps it's good advice.

MALE: I don't think there's just one thing that makes it work. I think the combination is the unique thing that drives it; the combination of tooling, financial incentives, approaching ISPS, approaching registrars, etc.

SIMON MCCALLA: That's cheating.

MALE: I only have one thing on my wish list and that is that all TLDs are invoicing their registrars a lower price for both renewable and new registrations if they are signed.

ONDREJ FILIP: Yeah I have a very similar approach. We didn't make up different pricing for signed and unsigned zones, but we do something similar with the co-marketing. So I think that was the thing that really helped the DNSSEC penetration in the country.

MALE: So I see lots of success stories in the other TLDs so I'd like to share such kind of success story in Japan to [frustrate the] people out of DNSSEC.

MALE: I think that the commercial incentives, direct or indirect ones that we had done in the past did a great job. But that was in a phase that we were like with the chicken and egg problem. I think we are very close to a tipping point that we will have end users, because currently we only have the infrastructure secure, nothing else basically. Because we don't have any applications doing any kind of use of the information out there, but we are I think in a tipping point that when we reach this then we will have probably a market looking for that.

Even more than 95% of all the owners of domain names don't know anything at all about this technology, and they shouldn't know that. So I think that we are targeting the right audience – hosting providers, ISPs – and when we reach this tipping point that we are empowering end users with this technology, we will see a large uptake.

SIMON MCCALLA: Great, thank you. Well I can see that Jeff Moss and [Rick Lamb] are virtually salivating there because they've got lunch behind them, so it's a good reminder to first try to finish on time. I just want to say thank you very much to all of our panelists for an excellent discussion. Thank you. And I believe we have lunch, it looks like it's ready behind us. We are finishing now and having a lunch break and we should be starting again at about quarter past one. Thank you.

[break]

JULIE HEDLUND: Hello everyone. I just wanted to let you know that the DNSSEC Workshop will start precisely at 1:15. So finish up your lunch, get some coffee and dessert and if you are in the next panel, the Solutions to Help People Implement DNSSEC, then we'll ask those panelists, that would be Russ, Christian and Paul to join us just a little bit before 1:15. So anyway, just go ahead and make sure you've got some lunch and some coffee and dessert, and we'll start in about 10 minutes.

If Christian Rojas from NIC Chile is in the room, Christian we have your badge, which also is your Gala ticket. So if you want to go to the Gala tonight, or get into any of the other meetings here at ICANN without them questioning who you are, please come get your badge.

Please everyone take a seat. We're going to start in probably about 30 seconds. So if you're near a seat, grab it and be ready to cease your conversations. Thanks.

RUSS MUNDY: Folks if we could take our seat, and we're missing one of our panelists here, Christian Hesselman. Ah, here we go, great. First thing I want to do after our fine lunch is again acknowledge our sponsors, they're all up there. And this is the reason we're able to eat for free. Thank you everybody that sponsored this, most generous and most appreciated, and it works out really nicely especially when it's in the room like this. There were some really good conversations I think that occur over lunchtime. So if anybody hadn't figured out yet, I am Russ Mundy and I am Chairing this panel.

There are three of us on this panel and this is the panel to address tools for helping people do things in the real world with DNSSEC. And we are roughly a 10 minute presentation a piece and I'm the first one. So I'll just use this mic here. So the DNSSEC tools have been around for quite a while. It's one of the major thrusts of my team of folks, and our work is funded, as you can see in the slide, by the Department of Homeland Security Science and Technology.

We've had some other help over time, but by far DHSS&T has been the ones that have been behind getting these tools out so anyone, everyone in the world is able to do DNSSEC. And I've sort of changed and made up a new moniker – yeah it's how people do DNSSEC, tools for doing DNSSEC. There's a range of them, you can see different groupings of them. And the website is one that some of you will recognize. And you'll notice there on the front page, one of the little tools, which I'll talk about in a little bit, but that's the website shown of course through a fully validating DNSSEC resolver, another one of our tools.

So the main subset of the tools that I'll be talking about today are tools for various types of users of DNSSEC, users being sometimes the end users, such as those that will be using a browser or a cellphone to do DNSSEC. As well as network managers, network operators – so sort of two different grouping of things. So this is our DNSSEC check tool. As it says at the top, "help us measure the world." And what we're doing with this tool is it actually lets you do a live check in real time of the DNSSEC features and capabilities that are necessary to work.

And you'll notice on the left hand side, you'll see a gray B C C over there, and that's actually a grading from one of the reports that's out of the US

Federal Communications Commission that identified a way to mark grading for evaluating resolver use of DNSSEC around the internet. So it's available for Windows, Linux, OSX, Android – another Nokia device. So it's available for lots of different things. We'd like people to just grab it off the website and run it and report back what you get. And we've got real time graphing that shows there is progress being made, but it also shows where some of the weak spots are.

And you can see there the A D bit is pretty unsuccessful in lots of places. So for those people who haven't really looked at what happens when you use a web browser, this is an illustration, again that comes from DNS Packet Trace, another one of the tools that actually shows the number of DNS lookups that are required to occur when you go to those two websites. And so the first one, weather.com, you can see is a little less dense than the foxnews.com. CNN.com looks about the same as far as number of lookups as Fox News and it is color coated. The small amount of green you see there is actually the validated checks that have succeeded.

The browsers that let you, we do have a browser that's part of the tool kit and that checks the entire page. If you notice from the last set of lookups there's many, many lookups it takes to fill a big commercial webpage homepage, this is much smaller. This is actually screenshots from a demonstration. This is the legitimate what the webpage should look like. And without a DNSSEC validation occurring you could see that somewhere somebody along the line – it happened to be our team – faked up a DNS hijack of that website, and so only a portion of the webpage was substituted in which are friend Dr. Crocker admitted that DNSSEC won't solve world hunger.

So we tried to make something that was clearly fictitious, but anyone that was attacking would not want to make something look fictitious. But this is an illustration of how a portion of a webpage can be hijacked and substituted. So some of the tools for illustrating this, this particular tool is called DNSSEC Nodes and it's running next to the browser. And you can see it, it draws a pictoral illustration of what's validated, what hasn't validated and the things that are unknown.

If you look at that small red .on the far right hand side that is a name that exists on this website that intentionally fails validation. And in fact, that is the link that we hijacked on the previous page and put in a substitute story. So something can be on a page and fail DNSSEC even if the URL at the top of the page does pass. And so here's a slightly bigger illustration in a circular picture of the full website of all the nodes. And here is, you can look up any one of the nodes, see what its validation state is. And then you can also get a map that shows you all of the validation steps back to your trust anchor. So this is DNSSEC Nodes, it's quite a useful tool. It will run standalone and it will run on quite a few platforms.

The next set of tools that I want to talk about are things relating to managing DNSSEC for network managers. Webmin is an open source project that has had some DNSSEC support in it for a while. It's quite popular in the open source community, used by many people to ease the administration of running many different services, primarily Unix based things. And what we've done is we have taken and integrated DNSSEC tools into that package. Right now it's just for CENTOS 6, we'll probably looking at more later on.

One of the problems with the initial Webmin integration was though they could sign zones they couldn't rollover keys. If you tried to do a key rollover with the original Webmin interface and capabilities it broke your zone. So it's done more properly with DNSSEC tools and you can rollover your zones, you can see the state of your zones at the bottom of the page. These are a set of other, this is a screenshot of the DNSSEC tolls focusing on the management tools in particular.

This is Roller D which is a standalone tool but is also one that we've integrated into Nagios. So this is a big screenshot; you can have a smaller one. And as those of you that have looked carefully at how you do rollover of a DNSSEC key, there are several stages you have to go through. And this works in conjunction with the rollover mechanism to show you the state of your rollovers. Small screenshot with lesser information. This is the Nagios integration. You can manage and monitor the state of your DNSSEC signed zones using your Nagios workstation, which a number of operators we understand are running Nagios today, so you can grab this plug-in and use it conjunction with your existing workstation.

This is ZABBIX, similar plug-in available for ZABBIX. And thanks for Frederico Neves for pointing us at ZABBIX saying that this is another nice open source capability and so we have the plug-in available for ZABBIX. And another more chart based layout for ZABBIX. This is a wide range of some of the recent emphasis that we've placed on managing your DNSSEC once it's out in place. Because one of the things that we've especially learned and heard from people that are doing the .gov zones is they have not effectively and efficiently done all of their rollovers, and they have caused other people breakage.

So we're trying to give people and make available tools so this is less likely to occur. And I wanted to say that our newest release is now available, it just came out a couple of days ago. And I have most of these tools on my laptop, some of them on the iPad and cellphones and stuff. So if anybody wants to see any of them or have any more detail, certainly feel free to catch me up afterwards, and at the end of this we'll have a question period.

That's the end of my presentation. Of course dnssectools.org is our website, though we do want feedback. Tell us what else you might need.

JULIE HEDLUND: Do you want to do all the presentations in a row?

RUSS MUNDY: Yeah. I think we'll do all the presentations then go ahead and take questions. Which one is next?

JULIE HEDLUND: Christian is next.

RUSS MUNDY: Christian, okay good.

CHRISTIAN HESSELMAN: We just saw a whole lot of tools that Russ talked about, and I'm just going to talk about one, which is going to be what we call the DNSSEC

Portfolio Checker. It's a tool that was developed by my colleague [Mic Shiben] and I am presenting here on his behalf. The DNSSEC Portfolio Checker is a tool that we built for our registrars to enable them to easily check whether their domain is validated correctly or not.

And we made this tool available in the form of two channels, one is a website the screenshot of which you can see here. Unfortunately still in Dutch, but if there is sufficient demand we can always make an English one out of that. So what you can do here is upload a file with domain names. You would go and it would then basically try to validate each of the domain names in that file and it will return a status which can be "secure," meaning that it validates correctly; it can be "insecure," meaning that there's no DNSSEC enabled at all' it can be "bogus," meaning that there is an error in the validation process, or "no data," which means there's no data in DNS on that particular domain name.

So that's one means to evoke the tool, the other means is through a RESTful interface, the URL of that interface is down there. And that's something you can use to check one individual domain name, for instance, using a script or something like that. So as I said, the main motivation for developing this tool is to help our registrars and as part of our DNSSEC deployment for .nl, but we also wanted to develop a beta version of a tool to check if this is something that would be on interest to registrars in the first place. And if yes, if we could move it into an operational service that we would make part of our operational process. So that was the second motivation.

And the third motivation was that we wanted to have some sort of basic tool for building the DNSSEC Health Monitor that we are currently

working on. That's a crawler engine that basically crawls the entire .nl zone to check which domain names are evaluating properly and which don't. It's actually a very simple tool. I forgot a box around the middle two boxes. The middle two boxes are actually the DNSSEC Portfolio Checker. It consists of a web service and a lib unbound validating resolver.

And you can then track with I through a client which is either a web browser or maybe a script that uses the RESTful interface. The middle two boxed are the SIDN Labs Network. That's an experimental network which is disconnected completely from our operational network. And it makes use of a DNSSEC enabled name server in our operational network. The tool runs as a KVM instance and it's written in GO and you can download it from github if you want.

So in addition to all the technical work we did for this particular tool, we also engaged in some communications with our registrars. A large part of that work was being done by our account manager who visited the registrars and talked to them about this tool, and in fact, the original request came from one of these registrars if we could offer such a service. We also sent out an email to make them aware of the tool and we posted it on various websites and blog posts.

So, some statistics – we basically logged everything that the tool had been doing, and it's been up there for two months. So since August 17, 2012. We estimate it's around 20 registrars that have been using it out of the 1700 that we have, so that's not a whole lot. However there are 239 registrars that do DNSSEC, so this is about 10% of them. About

39000 domains were checked, but this also included our own test runs, so it's a little bit skewed, I guess. I hope so.

MALE: While we have a pause I'll just ask a question. Do you want us to promote the use of this tool, this looks very cool.

CHRISTIAN HESSELMAN: Excuse me?

MALE: So you want the use of this tool to be promoted?

CHRISTIAN HESSELMAN: Yeah that would be very nice.

MALE: Okay, this is very cool. I just used the command line interface to go and it's very nice to be able to have a nice way to go and check a domain nice and quick.

CHRISTIAN HESSELMAN: Cool, thank you. So as I was saying, 39000 domains have been checked since August 17th and most of them are secure as you can see in the statistics over there. So in addition to the primary usage of making an online service we also used it lets say for some statistics on the entire .nl zone. So what we did was grabbed a random sample of domain names and fed it through the DNSSEC Portfolio Checker just to figure out how

many domain names would end up in "bogus" state, so which ones would not resolve properly. And it turned out there were 66 of them, so that's a .66% ratio of domain names that do not validate properly, which we think is pretty good.

And of course this was just a random sample and we expect that this can be improved a lot once we develop this DNSS crawler that I talked about. Another thing that we use the DNSSEC Portfolio Checker for is for secure transfers. So since we at .nl have a million plus domain names signed right now, we expect that we are one of the first ones to run into problems with secure transfers.

So what we did is we went to a registration system and took out all the domain names that were transferred as of June 1, 2012, so signed domain names. And we ran them through the Portfolio Checker it turns out that 801 of them were "bogus," so they did not validate properly. So that's 10% of the entire set of transferred domain names, which we think is quite a bit. So this is actually a very good indicator that some work needs to be done on secure transfers.

So coming to the conclusions on my presentation, the down side of the, well not the down side but what we figured out through the tool was that the interest from registrars was relatively low. So this is actually useful to know before we actually build this entire thing into our operational systems. So we will probably not do that. But we also found out that the tool is very convenient for people working at the registry because they use it to assist registrars who call them let's say to discuss problems with broken domains for example.

And we also discovered the 10% domain names that ended up in a "bogus" state after a transfer, so that was actually the use of the tool which we didn't anticipate before. So that was kind of nice. As I said, the next step is to use the basics of this tool to develop a DNSSEC crawler which is a continuous process that goes through the entire zone we estimate in around 20 hours, and that will give us an accurate insight into the DNSSEC status of the .nl zone.

And that's it. For technical questions you should probably contact my colleague [Mic], because he knows a lot more about DNSSEC than I do. Thank you.

RUSS MUNDY: Thank you Christian. Now we'll go to Paul Woulters speaking for RedHat today as opposed to no hat.

PAUL WOUTERS: Thanks. Do I get my timer?

RUSS MUNDY: I was going to give you the extra minutes.

PAUL WOUTERS: Awesome. Okay so I'm Paul Woulters; I work for RedHat and I'll talk a little bit about the DNSSEC integration that I've done for them. So for those who don't really know the setup at RedHat, we make an enterprise Linux operating system. We start from a community of free and open source software, some of it is written in house, some of it

elsewhere. The innovation really happens in Fedora Linus, which is the end user, developer, expert user, desktop system – that's where all the innovation really happens.

So when we break things or when RedHat puts in new features or new things that's where it goes, that's where it breaks, that's where we hope the expert users will give us feedback. Then once in a while those releases get stabilized and from that we cut a RedHat Enterprise Linux release, which then really becomes frozen, minimum changes, gets certification and all these things needed to make it an Enterprise OS.

For instance, people may remember the glibc upgrade. Some people are still having pains with the systemd upgrade migration from [System DNS scripts]. And selinux is also a tool that's actually really, really good and it gives you a lot of security, and it's being given people a lot of trouble. So a lot of people turn it off. The last half year I've actually been pretty active on the selinux rules for all DNS and DNSSEC related software, so if you've turned it off in the past, please try and turn it on again because it's really good.

As a packager we package many products from other people. You'll see a lot of the tools here are in fact from the Sparta team. We see open DNSSEC, bind, NSD, PowerDNS Unbound, and then DNSSEC trigger which people might be familiar with on their laptops here as well. We merged sshfp now with some other tools into a new package called hash-slinger, and we worked on openswan to add some DNSSEC support there as well.

So we were the first, as far as I know, to enable DNSSEC for default in Fedora; enabled the DLV as well because we really needed those non-

signed TLDs to be supported. And to ship keys and resolvers, so for years already when you installed a name server you would get signed answers and DNSSEC would be enabled out of the box. I was personally also responsible for the DNSSEC conf utility that shipped trust anchors before the root was signed, against the advice of many people in the room here.

And luckily we found a really cool bug before the root was signed, and so the rollover-or-die bug was found. I got a call at 4 a.m. from RIPE saying that something was happening and they really wanted me to change something. It turned out we did a bad rollover, package was hung up in the update system. And as such, the keys weren't updated and it triggered a bug in BIND to continuously refetch the keys from the RIPE servers. So these are things we really like to happen to find out about, but we really like these to happen in Fedora and not in [REL], and so that's where a lot of experimentation takes place.

So now we're moving towards things on the desktop where we wanted to work on the laptop and for the end user. So we set up a few infrastructure things with the Fedora hosted people. For instance we published TLSA records; we published a DLV record, we were signed a long time ago and we now do some specific services for hotspot detection. You're welcome to use them even if you're not using Fedora. The first URL you see is the static URL to detect hotspots. You're guaranteed not to get an http redirect and you're guaranteed that the content is of typed text and contains the two letters "OK."

If it's anything else someone is either "man in the middling" you or it's attacking you but most likely you're on the hotspot and you need to

authenticate. The second page is a special page where the [TTL is zero] to ensure that that entry will never be in your cache. And the idea about that is that it can be used to launch a webpage to authenticate through the web portal ensuring that you're doing a DNS lookup that isn't already in your cache so that you don't get timeouts.

So DNSSEC-trigger and Unbound is the combination that we use to detect whether or not you're behind a captive portal and to reconfigure your DNSSEC validating name server on the fly. And it works great. We've had some tremendous cooperation with NLnetlabs to get features and to get bugs ironed out and to really use this in production. I've been using this for probably two years now, and on top of that I run with selinux and [fips] mode and all the other extra checks there, so I spend half of my time debugging my laptop and half of my time doing other things.

But it's great. Well it's not great, it's good. DNSSEC-trigger plus Unbound works really well, but we need some additional features. We need DNSSEC changed to actually get a whole bunch of lookups to us really quickly instead of having to do all these TCP lookups when people are mangling are UPD Port 53 traffic. So we're doing lots of work on that and we're getting a great audience by using the Fedora users to report bugs to us. And in fact we talked to Olof for a bit in the last couple of days as well; he has some great tools he's working on and we're hoping to be able to support him by giving him that extra user base so that he can get more statistics gathered.

And if anyone else is doing similar work, please contact me so we can try and get your statistics gathering things into a larger community,

because that's really what we do and what we want to help with. On openswan we have done some work as well. One of the problems we have, this is the second largest problem after hotspot is that when you start your VPN your DNSSEC worldview has to change. You're connecting to some private that's not visible on the internet part of the name space and you need to tell your laptop that this is a special, unique not public part.

So the patches we've made ensure us that when you connect to the VPS – and again, this was stimulated mostly by me not being able to use DNSSEC while I was on the RedHat VPN. So what it does is reconfigured Unbound on the fly based on the IPSEC parameters received during the negotiation for the VPN tunnel. It reconfigures Unbound to divert the Redhat.com queries over to VPN. It ensures that it flushes everything in between so you're not mixing your internal and your external queries. So if I go crazy at home I can close my laptop, open it at the coffee shop, connect to the VPN and not have to worry about my packets not making it because the VPN uses RFC 1918 space and it's not available and I'm not on the VPN.

This works pretty well. There are some minor issues, but it works pretty well. This is the hardest problem yet that's not been solved. The DNS split, the VPN is one, there are more complicated splits where you have this and we need to better support this. There isn't much experience yet because there aren't that many organizations that have both internally and externally DNSSEC signed zones that if you walk the public view will actually conflict with each other. So we need to do a lot more work on this.

We started redoing the Unbound package a little bit to make it easier for those reconfigurations to happen. So if you would have an internal zone, to make it easier to add these more or less on the fly or through your puppet or some distribution method that the enterprise is using to do these kind of overrides. And then also for things like local data, for instance the nasa.gov that was unavailable you would want to somehow be able to provide a workaround for users. And we needed to change the packaging of Unbound for that.

This is an adaption that I made based on work from NIC CZ and OS3SEC and Peter from Holland, to add TLSA integration into the browser. So I took their plug-ins and they did DNSSEC validation already, so the only thing I really needed to add is to add the TLSA record authentication. I looked at the available colors, the traffic light colors are all taken so I picked purple. It is useful. You should really only use this when you're willing to break your connection a lot and this is a Firefox plug-in, you should really install Chrome to have a backup to authenticate to the hotspot because this will cause a lot of delays and there's still work to be done.

But the proof of concept is there; we can validate TLSA records in the browser without manual work and we're doing this to push people like Firefox into supporting this natively. There is also a fresh package called hash-slinger, which you should look up on Wikipedia what it actually means. But it adds the tools, sshfp which was already available but has been slightly updates, and the TLSA tool to create these records that you can use with DNSSEC protection. For those people who don't know, TLSA command will show you the records you can add in your zone.

Sshfp actually can do a zone transfer and garb all the A records and C names and actually generate all sshfp records for you.

There's no tool yet for IPSEC key but that should be coming up as well. So, the short answer, because I have 18 seconds left is if you're a tool developer please think about the crypto libraries you are using. For Fedora we can support everything and through Fedora and EPEL and of course [Ascentivis] repositories, we can support any crypto library we want. But if you want to be core of rather than selinux than there's only a few subsets of crypto libraries allowed. And if you have anything that uses MD5 please try and phase it out. Because if you're running in [fips] mode MD5 is not allowed, and that's actually a too large part of my day job in fixing software that assumes that MD5 always works.

Including if you're calling crypt, please make sure that you don't call string copies straight on the return of crypt because crypt can actually return a no pointer. And that I think is the last slide, no. Oh yeah, so we want a more native integration into network manager of the DNSSEC-trigger and Unbound tools, and so we're working on that. if you want to help catch me and we'll gladly talk, but this is still a couple of months away. But we really hope to fully integrate this into network manager to do optimizations of network detection for instance, like it would be really good if we can share our probes or at least remember the networks where we were at so we can more quickly establish a good network connection that has a fully functional DNSSEC capable DNS. And I think that must be the last slide. Okay, thanks.

RUSS MUNDY: Okay, thank you very much Christian and Paul. And now I'd like to open it up for any questions on any of the capabilities you saw described, talked about here or anything else related to it. Now's the time to raise your questions, go ahead Dan.

DAN YORK: Dan York. First just a general thing, thanks to all three of you; these are awesome, both sets of slides and tools, so thank you for all the work you're doing on that. Russ, I had one question for you which was sort of what's next for the DNSSEC tools project. I mean I know you asked us what do we need, but I'm just curious do you have more tools that you're looking at developing.

RUSS MUNDY: Yes as a matter of fact. You've already seen the emphasis being on usability, users, whether those users are operators or end users, and the importance of validation, the importance of getting the validation right. Some of the tools we're also looking at are tools to facilitate and help, akin to what the SIDN tool is but a somewhat different approach, and also to have more complete integration with the TLSA Dane capability into the validating browser.

So yeah that's the set of things that we're looking at right now, but truly we would like to get input from the community if there are things that we haven't seen, additional things particular segments would like. We're happy to receive input and there's a decent chance we'll be able to at least partially help, if not do what you're looking for exactly.

CHRIS GRIFFITHS: Russ, one thing that might be interesting might be, I'm not sure if your tools support that, but I have one of these network probes at home, which is from the [SCC] RIPE Atlas Project and it would be great to basically have a software version of that on your cellphone. So that you would be able to discover in which network you would be able to do DNSSEC with validation and would be able to store that somewhere in an anonymous way, thus getting an overview of what the uptake of DNSSEC is in the real world from an end user perspective.

RUSS MUNDY: Thanks Chris, and that's actually close to what we do with DNSSEC Check. And if folks are willing to send in reports from where they are, it is purely software and although it does take a manual initiation of it, is perhaps what you're suggesting is have something that would just run without having to manually initiate anything. It's just when you connect to the net…

CHRIS GRIFFITHS: Yes that's exactly right. The reason I'm asking is because at SIDN we are involved in a project with SurfNet and we sponsor let's say, we sponsor a project that enables universities to upgrade their campus infrastructure, and this includes DNSSEC. And since let's say the population at a university is generally willing to experiment, it might be interesting to offer them some sort of app they can download that runs in the background, I'm not sure if that's possible, and then this basically calls home and stores all this information about which ISPs do validation or not and those networks encountered by those students. So that

would be, we would be able to have access to a large user community there.

RUSS MUNDY: Yes and I like the idea. We'll certainly take that back and look at it. One of the questions that I have related to that is we're also looking to see if there are other folks that would be willing to participate in the data collection activities and storage and is that something that would be worth looking at too. Yeah okay, that's great.

MALE: That's one of the things we also want to help with the integration in network manager to gather that data and to make it easier for people to report and see what's going on, and also to share which networks are really good and really bad and maybe shame people into some better compliance.

HUGH REDDLEMEYER: Hi, Hugh Reddlemeyer from GTA [LOG] again. I'm going to ask another naïve user question. Networking is fragile in general, it breaks for lots of different reasons and they're not obvious to the end user. What would be great is a tool that knew enough of the whole stack that could tell you what's going wrong. You guys are talking about what's going wrong with DNSSEC and that's really important because you're adding a new layer of failure on top of all the old ones. But it would be really nice if you could have an integrated tool that would be a one-stop shop for what the heck's going wrong with my networking.

And I guess the only one I'm really asking this of is Paul, because he's the only one that's representing a company that does the whole stack. But I do think end users would really like to know not just what's going wrong with DNSSEC, but what's going wrong period. Thanks.

PAUL WOUTERS: Okay I'll answer that. So again, one of the reasons we wanted better integration with Network Manager is to facilitate the single interface towards the user. So whether the user starts VPN or the VPN disconnects or the Wi-Fi disconnects or the DNSSEC is broken, we want to merge that into one unified interface, which is currently with the applets that DNSSEC configures using its old separate from it. And that's one reason we want to integrate that, so you're right in that aspect.

As for the user experience in general, some of it is really hard because it's non-interactive. Like if you do a system upgrade in the background and there is no user and you do error reporting then there's no one who's going to see it. So that's a little bit harder, but there are also some efforts underway to make a more standardized version of logging to make that easier as well.

And then the third aspect is that the user experience for a large set of users is purely based on the browser and that's really not something we control, but we hope to steer them in such a way that they will do a good job and that we're not going to get any of these repeats of like SSL certificates where people are trained to click on "yes I want insecure."

RUSS MUNDY: And in fact some of the patches that we have for Firefox and Mozilla we have submitted into their system. They've yet to pick them up and incorporate them, but we'll keep trying and keep pushing. And hopefully, in addition to just the URL at the top of the page, just as you say a network problem is one thing, a problem on a web browser isn't necessarily one link and it's not necessarily the one you see at the top of the page.

Also in that kind of space, questions of this nature, if you could also submit them into the browsers and the OS vendor realm – I mean this is great and we really like the input, but also getting people to go directly to the providers. Because many times we hear there isn't any need for this kind of thing, so the more people that ask the better and more likely it is, the better the demand is and the more likely they're going to address it. So do we have more questions, comments?

DAN YORK: I have one more – Dan York, I have one more question for Paul. The work you're doing is I assume for Fedora RedHat. Have you had interactions with other Linux distros as far as what they're looking at as far as adding DNSSEC validation into those other distros?

PAUL WOUTERS: We do talk amongst the developers on the various software packets and the mailing list themselves, so all NLnetlabs mailing lists and all the packets and servers. So we do talk in the community, it's not just that we're all by ourselves. We do also regularly interact with the people like the [W] maintainers and there's a large overlap of the people with

this interest. So there is talk throughout the community at large. I would like to see some more synchronization about what we need and what we want also on different levels.

And that's not just for DNSSEC, but for instance there's even discussions for when you enable [fips] mode on a machine, some people complain about pre-linking for instance. Pre-linking breaks the security checks in [fips] mode and pre-linking is purely a speed up measure for loading applications. And I as a security person say "well if someone enables [fips] mode then clearly they've decided to think that security is more important than speed, so just undo all the preloading and be done with it." But that runs into a lot of other people and for instance the glibc maintainer has a very strong opinion.

So I don't always get what I want as a security person, but I definitely try to reach out as far as I can.

DAN YORK: Thanks. I guess my question was more of do you have a sense of how far along some of those other distributions are in terms of getting this, getting DNSSEC validation to be part of it. I guess I heard before that [W] is, or was that you, I guess I'm just curious what are the other Linux distributions, where are they at in actually making it happen like in Fedora and RedHat.

PAUL WOUTERS: I'm the wrong person to ask about those questions [other than] distributions.

DAN YORK: Sure.

PAUL WOUTERS: But I think the main problem that's stopping this, my plan was to try and enable DNSSEC for everyone in Fedora 18. And my plans were to enable DNSSEC on Fedora 19. And at this moment I don't see that happening because if you think back to my slides, the number three issue is still an issue that's unsolved by anyone as far as I know – the key distribution of the internal versus your external zones. And some of those issues in combination with hotspot handling really has to be solved before we can enable this per default.

And until we've done that the consumers of DNSSEC are fairly limited and so people aren't paying too much attention to it yet. So we have things to do on that level. And then there's a whole other level of how do we go past [Bos Six]; and people are still using [Get Host] by name instead of get other info, and now we're going to tell them that even that's obsolete. Or as far as I know nobody is working on extending get other info to include the DNSSEC information, so I see sort of a convergence to the lib unbound API on one hand, but there's lib val on the other hand, there's the lib IOC and what are the people going to do, how are people going to get that information into the application to integrate better.

And then on top of that we have the problems of the key distribution. If an OS cannot assume that a resolver is running on a host it means that the applications themselves have to do the resolving. The problem

there is that if Port 53 is blocked they can't do it themselves or there's a policy that people don't want to do it themselves, so they have to trust the local resolver it's running. And so these are all circular problems on how to move forward into increasing this deployment, and there are still many hurdles that we have to pass.

RUSS MUNDY: With respect to the API issue, actually in this DNS issue this is some work that we've done earlier which you and I should probably talk about offline. But the API issue is an area that my team has worked on some for the last several years, and it really, we had several years ago general agreement from all of the major DNSSEC DNS software providers that they would like to go to a newer API that was DNSSEC capable.

But as we got more of the application realm folks involved, what they basically gave us for feedback was that they need a whole new DNS API, not just an extension to the current API that would do DNSSEC. And so that is a considerably larger job. It's not one that has been forgotten about, but it's not one that's being very actively worked at this point in time. I believe we are about out of time, so unless there are last urgent questions, I think we should thank our panelists here.

And also point out that each of us has a place for sending in questions, comments, responses about things you'd like to have, things you'd like to see in terms of what we talked about today. So this isn't your only chance to talk to us. So thank you folks and appreciate your questions. And now, I think Dan is next. So Dan York is going to give us a presentation on their Deploy360 Program.

DAN YORK: Alright, good afternoon. And I've got the official clock; this is awesome by the way. If you're ever doing moderation, I don't know exactly which app this is but – [BP clock], I've got another one. If you have an iPad and you're a moderator, this is an excellent app to have; it's a great way to keep people on time and on target. So my name is Dan York and I work for the Internet Society. One of our teams is focused on deployment and operationalization and the specific program I'm working on is called the Deploy360. How many people have been to our website?

Okay, good number of folks who are here. Yeah you better put your hand up Roland. You've given me comments. It's at internetsociety.org/deploy360 and our focus, our mission is really to provide real world deployment info, whatever that may be – tutorials, case studies, whatever it may be. And I guess similar to what Russ said before, we want to know how we can help you. Our focus is how do we take away the pain of deployment and how do we help get DNSSEC and iPV6 deployed in a faster manner.

So I want to put out the plea again – if you go through the site, take a look at what's there – we have a content roadmap of some pieces of information that we want to get up there. We'd love to hear your feedback. If you are deploying DNSSEC in some manner and you'd like to be a case study, we'd like to talk to you. We'd like to write up some of those and get those out there. We also are always looking for new tutorials and other information we can put there.

But I really want to talk about sort of what are the questions that we, what do we need to do and how do we get more validation, how do we get more pieces about this. We've been looking at this for the last year as we've been building up this program working with many of the folks in this room – Russ and Steve Crocker and the folks with the DNSSEC Deployment Initiative and many others around there.

And so this presentation, coming at the end of today is really sort of summarizing some of the trends that we've seen, much of which the pieces you've heard discussed today, and also give a few pointers for some of what comes next.

When we look at, and kind of what we've seen, this is no big surprise, I think if we look at the list of what we need. You've heard it again and again here – one of the keys to getting DNSSEC more widely deployed is to get registrars and DNS hosting providers on board. It's a key component of doing this. As we've started to go out and talk to people about DNSSEC and the power it's had I can't tell you the number of people that have said "Oh sounds great, I love it Dan. Let me go do it" and they go to the registrar and find they have no way to do it.

They can't go and click a button and they can't go and even ask for it. There are registrars that simply do not support it. We've certainly heard the value of validating name servers with Chris up here earlier and the folks from CZ and SE who are doing fantastic work. I want to dive into these a bit more. One of the things that I put this slide up here to talk about is within a lot of our communication we're a bit sloppy talking about what registrars do versus DNS hosting providers.

And part of that is because very often registrars and DNS hosting providers are the same. Registrars provide the DNS hosting. But we need to be clear as we look at this and communicate out externally that there are four different pieces of the puzzle. There are the registrants who choose to enable DNSSEC, or as in the case of Brazil or other places where they just have it automatically happen. Okay, but they have a role to play here. The hosting provider is of course the one who signs the zones, publishes the record, perhaps provides that UI for management and then ultimately sends that DS record to the registrar and the registrar is then sending that up to the registry.

Now you'll notice there's a couple of pieces in here that are still manual; we still have a very manual process between the hosting provider and the registrar. Part of this is that we've got a very common case out there where we have registrars who are also hosting providers. I have some domain at GoDaddy and I can go in there and pay a little bit more and click my little button that says "enable DNSSEC" and boom it just works. It's a beautiful thing from a user experience.

But it's because they're also my DNS hosting provider. If I use somebody else as a DNS hosting provider and I use GoDaddy as my registrar, it's a good old manual copy it from one web UI, paste it into the other. It's a painful process that not necessarily people are going to want to do. Yes it's easy to go highlight, copy, paste, but come on that's an error prone process that's part of that. And you see that with any number of folks who register their own domain and they want to provide some ability up there.

So what we see if we look at this is there's really three things that could greatly accelerate the adoption of DNSSEC; and that is one, if registries could make it as simple as possible with those DS records, registrars need to make it as easy as possible to get those DS records because DS upload, that's our one big issue that we seem to have here. And then the hosting providers need to make it simple and automated. And we've heard any number of solutions here today with people offering different services, signing services, just doing it all automatically; a number of the solutions are out there that are part of that.

I mentioned simplifying the registry hosting process, some of the folks today talked about how they just automatically do it. We do have some of these one click offerings, which are great. When I've shown this to some people about how easy it can be they're like "oh that's all it takes." And for the end users, for those registrants who are out there this is a beautiful thing when they can go and just put a button on it.

Here's another example from a DNS hosting provider, in this case Dyn, where they have again an "add DNSSEC" button at the bottom. Now I will say from a user experience point of view I've shown this to a couple of people and they kind of get put off by all these techie things that we love. So the key expiration, key size, these types of things. This is another example from the user, we have to think about the user experience and what's the user experience for registrants, for people who are hosting this, what does it look like.

Can it be just a simple button with maybe an advanced panel that then throws up these things that people who care about can go in a tweak those items, or is it just something that disappears like we heard today'

several people who just it automatically happens, set your domain up and go. But what is the user experience; this is a key part to making this work better for the end users. And I go back to this, simplifying the transfer of DS records. There's a couple of registrars out there who are playing around with APIs as I mentioned, one of them here, GKG net, a registrar who's been doing some of this.

Others have other proprietary APIs out there, there's nobody who I've yet seen who's got a standardized from a hosting provider to registrar side of this. Yes for registrars to registries we've got EPP, but I'm not seeing that necessarily being exposed to the DNS hosting providers to make this kind of connection happen. A lot of that still is all copy and paste. So here's another opportunity we have where we can go and look at how we can accelerate this to make this that much quicker.

Again, this is that piece and I think we've identified this. We just had a discussion a couple of weeks ago where we were talking about what are the major technical issues. Again, it seems to keep coming back to DS upload, DS upload. So if there's one thing I would put out to all of you in the community, this is a piece we need to work on. How do we make this part even simpler and easier for this whole process to work smoothly on?

I would also mention, and I want to call out Rick Lamb is here with the ICANN DNSSEC group who's been maintaining this list. How many people have visited ICANNs list of registrars? Okay, this is a great thing. I know Rick hopes that eventually this will go away; eventually we won't have to do this because every registrar will just support it. But in the

meantime it's a great list to start. But what I would ask all of you is send in registrars.

I mean I just heard today that there were 249 registrars in – who was that, is it .se, .br, nl; it was nl – there was 249; let's flood Rick's list okay. Make his list really long. I'm asking you to give Rick work. He's tired of playing solitaire, he needs something to do. So if you go to this page there is a link on there and please send him some stuff. I saw some other pages that come up today that talked about how many registrars that they had in those domains and they're not on Rick's list. So Rick's list needs to grow.

And also, there were how many, you're now up to how many that support .com; there aren't that many. We need more. And the other gTLDs and others. Send Rick items that are there. On the validating name server side, this is the URL that Mark Larson mentioned earlier today, it's a validator search; a project that VeriSign Labs is doing. There's a number of these projects that are out there. His is one, his team is working on this project where they're trying to go and quantify some of the work that's there. He's asking for community help too. He's asking people to put a little snippet of html into their webpages, into their headers that basically is loading two URLs in JavaScript.

And it's going to making two calls and it's helping them to gather some data around this. So if you've got sites that you're willing to help them in this project for, they've got some instructions on there about how to do this. So again, they're looking for help to try to build these metrics to say what is the percentage of DNSSEC validating resolvers out there. So it's another project that's going on out there.

We heard the story today about Comcast; we've heard about ISPs in Sweden and the Czech Republic and others who are doing this; that's excellent to see. We need to make more of that happening. Certainly education around there; customer education, more of those tools that we're seeing around how to go and do this. On the domain name side, really what we're looking for is how do we go and help get the enterprises and governments to do this. How do we get them to sign the domains to enable and install DNSSEC validating?

For the end users, for the registrants so much of it comes back to this very first bullet. Even if they are interested in it they can't do it, it's hard for an end user to necessarily go do it, outside of some of the TLDs who are here who have just made it work so well for the folks that are there. So we need to do that.

We also need to move out into more of the mainstream media and more of the mainstream conferences, the folks in that line, and start getting more information out there about the value of DNSSEC. And I want to talk specifically, how many people are familiar with what Dane does? Okay so I maybe don't need to go through all my slides here, but just for those who aren't aware, think about the process of what Dane is giving to us and think about it from an end user perspective, because people have asked what's the killer app for DNSSEC – I would argue that Dane gets us close as far as what it can do.

Because think about it, what Dane solves is this issue – and for those who saw me presentation yesterday at ccNSO this is the Obi Wan free presentation okay. I don't have my little pictures of Obi Wan in here; this is just diagrams. I was doing it yesterday for folks who did not know

about Dane. But we have this thing about I'm going to get a website, in a typical SSL as an example. I go and I get this, I get a TLS encrypted webpage back.

But the issue is how do I know if I get the correct certificate. How do I know that's the right one? And this is where Dane comes in. If we're here at this, I'm over at a hotel and I know that my DSNS is being intercepted and I know that everything is going through a firewall at the edge of the network; I know because they're putting a little banner on top of every single webpage that I surf, so they're intercepting this. They're breaking the TLS connection. I'm getting a lock icon; I still get my little green lock. I still think I'm going to a secure website, but in fact they've gone and they've broken the connection, they've resigned it and they could potentially be taking all the information off into log files including personable, identifiable information and everything else.

The issue of course is that we've got 1500 plus CAs that are out there, any of whom could be compromised, could have any issues with that. There could be signing certs that are being issued that are going back to these metal boxes, all of these different pieces. And so we get into a situation where we've got a case where a Dane equipped browser could potentially help with this. Because what happens is you get this TLA record we've talked about a little bit, and you see on the right hand side of the picture the DNS query comes back with a TLSA record and basically this goes and it's doing a hash – well depending on what's stored in TLSA, whether it's a full certificate or a fingerprint of it.

But it's basically saying "is this the certificate I'm getting from the web server." If so, then this is good. If not, then it fails. It fails the

validation. That's the goal of where we're trying to go with this. It provides a stronger, more secure web experience. Because if you think about it TLS, or SSL as it's commonly known, is encryption with a limited – and I'll argue weak – integrity protection. Because the integrity protection of whether it's truly who it says it is, is based on the fact of whether of those 1500 CAs that are out there and all of that. It's got limited integrity protection.

DNSSEC has very strong integrity protection, that's what it's all about. This is what it is. Combining the two of them, taking TLS, SSL and DNSSEC together is giving us encryption plus strong integrity protection. So we've got a very powerful message out there that we can say "this is how we secure the web experience." Now, there are some pieces of this that have been raised on some of the lists around "Well what if the corporate firewall requires that it proxies TLS connections"; there's some pieces that are still here. But longer term we need to get Dane out there and deployed in browsers and we need to get TLSA records out there so that we can even be testing this and working with this.

I commend the folks at the Brazilian registry who are doing this with the DNS Shim product, with their tools that are out there and making TLS records available. There's other folks, I know Paul's been working on stuff to publish TLS records with hashling or on other pieces like that. That's all good. We need to publish TLSA records. We also need to get this deployed into browsers and other things. Warren Kumari, who is not here right now but was here earlier, and yes he works at Google, but not in the Chrome group, was really saying "we need to encourage the browser vendors to be looking at how do they add in this Dane support."

Now the browser vendors have a zillion different things they need to implement, but they need to hear from us that this is important whether it's gestures of support, whether it's comments on mailing lists saying "this would be great, I would use it if Chrome were to support this." Warren informs me that he forwards any notes he sees like that over to the Chrome team. So I told him which mailing list do you want those to flood, we can arrange that. But he needs to hear this, browser vendors need to understand this because this will really help us move this forward.

Dane is also not just for the web. If you're in a Dane Working Group you've seen there's a draft out there about email, how we could use it to provide integrity around that. There's some folks saying "well we could use this for voice over IP we have an issues with in the SIP world around how to go and provide certificates for SIP end points to setup SRTP connections." It could be used in [Jabernix] and BP, it's a way to go and do this. And it's also of course using CA signed certs, but also using self-signed certs, so it provides a mechanism at which it could go and do that.

So Dane to me is an important part for how we go and move forward with this. If you're looking for information to provide some, we've put up a page on the Deploy360 site around Dane; we're going to be adding to that. If you go there right now you'll see a little video interview with Warren talking about some of this. You'll also see some other resources that we're going to be adding to it as well. Their use cases RFC as well as the Dane protocol are also very powerful to look at.

So again, as far as getting this out there, there are libraries that are adding to it that are already out there. A couple of them hosting providers, we need to provide a mechanism for adding TLSA records, and we need to start getting it talked about and discussed. So let me just finish up by saying a couple of words. Several of us, a bunch of us, some of the people in this world have started to get together and say "well what can we do to move this from a marketing advocacy promotion point of view, how do we do the next stage of the deployment and the marketing of DNSSEC and the advocacy around that."

We've come up with really four areas that we need to look at. One around what do we need in the way of better tutorials, you can read it on the page; what are the tools that are out there; what are the unsolved technical issues beyond this DS upload issue, are there more pieces that we need to be looking at. And then the measurement – how do we start to measure what's out there.

There is a mailing list that we put together called dnssec-coord, comes out of coordinating DNSSEC activities. You're welcome to join that. It is a public mailing list, you're welcome to join. We're planning some monthly conference calls to help support our communication in working on this. We've got some different folks, some of whom are in this room, who have stepped forward to say they're willing to help organize some of this or help coordinate some of these people.

So I would ask you to join that, to help us with this. We're trying to say we've got a tone of tools, we've got a ton of materials out there; how do we take this to the next level and really start to push the larger

deployment of this through promotion and advocacy. I'll wrap that up just saying again I'm with this program within the Internet Society. We'd love to figure out how we can help you. And I'm at York@isoc.org if you want to email me anything, and please feel free – uh oh, I'm already getting somebody here. Okay, ask me questions Patrik.

PATRIK FALTSTROM: Thank you very much. Patrik Faltstrom. One thing that I think that we have to be careful about – let me back off. I think this is a really good project, but as you also disclosed, and I'm probably one of the people that pushed you to start doing it, so I'm absolutely full of support for what you're doing and I will encourage everyone to join that is interested in this because it is a difficult problem.

And one of the things that are difficult is to use the correct terminology so that we know what we're talking about. And if we go, for example, to the webpage that Rick Lamb has, and this is something that I think that you have to be much, much more careful with your pictures. Rick Lamb's page is about ICANN accredited registrars that do handle, that accept DNSSEC, not registrars. There are a lot of registrars out there that do handle DNSSEC specifically in the ccTLDs that actually have deployed DNSSEC much more than the gTLDs that are not and cannot be on that specific list, but on other lists.

DAN YORK: Ah, good point. Okay we'll take that as an item that we need to perhaps figure out a way to – I'm looking at Rick right now saying – good point,

we'll figure it out. There's potentially a way we can come up with some kind of thing.

PATRIK FALTSTROM: I just want that if it is the case that you talk about specific problem for ICANN accredited registrars that you should use that term and not say registrars. That's my point.

DAN YORK: Okay but to your point there's a larger issue that we need to figure out how to list all registrars that are doing that, in this interim phase until we get there. And so whether that is hosted on ICANN or if we need to put it on some other site.

PATRIK FALTSTROM: That is another problem we also can work on. I hope you understand the point I'm trying to make.

DAN YORK: Yes.

PATRIK FALTSTROM: Good thank you.

RUSS MUNDY: There is other places that can have lists too. So that's an easy answer.

DAN YORK: Yeah that's an easy one. We have lots of websites we can put lists up at. I mean we're just pointing at Rick because he stepped up and started doing it, saving me from starting to do it or somebody else from starting to do it. So we can figure something out if we need to. His list is great.

PAUL WOUTERS: The update DS problem you mentioned as I guess the first biggest problem. Let me point to Draft [Routers DNS Up Secure Updates Use Case 00] – people should look over the document, see about the use cases, see if they have any more use cases. It's specifically important to realize that the world consists of more name servers that have relationships to each other that are not falling under an ICANN registry/registrar/registrant model, and that there's many kinds of updates that we'd like to see.

Imagine if we have a secure relationship between parent and child, we can do a lot more than just updating the DS record. We could update the NS record. We could update the [glue] because now the child can actually signal the parent securely about something. So that's something that's really useful and it's sort of on hold more on political than on technical reasons I think. So if people can comment on the appropriate IHF list on that that would be great.

And then my second point –

DAN YORK: Paul, could I ask you to send me that draft in an email or something because I didn't get it, but it sounds excellent.

PAUL WOUTERS: And then the second one is a much older one from June 12, 2001 and that is draft [Barwood DNS UP DS Publish]. That draft actually suggest that the child can put a copy of what it wants to be published as a DS record in a parent as a CDS record in its own zone to signal directly between the child and a parent to circumvent all of these problems with (inaudible) and cutting and pasting and whatever. I would really like people to also comment on that and say "let's try and move this one forward."

Again, I think there's more political reasons why people are nervous that child and parent zones shouldn't communicate together in the registry/registrar/registrant model that are actually blocking the enterprise people that really want all of this automated within their organization.

DAN YORK: Thank you Paul. And I see Mr. DNS OP Chair is coming up right after you, I'm assuming to respond.

PETER: Yeah, my name is Peter (Inaudible), I work for DENIC but I'm also the co-chair of the IETF DNS Operations Working Group and actually I am Paul's political reasons. [laughter] The point here, and maybe this audience can actually contribute to resolving this issue, the point is that we've seen a couple of solutions just that people can't agree on the problem and on the specifics of the problem. So we've seen a lot of technical approaches to solving this perceived parent/child interaction problem.

We've seen so far that this is something that is happening in [geek] circles.

So having real registrars and ICANN accredited or not that doesn't matter in that case, and real operators contributing to the use cases document or reviewing the slightly different problem statement in the various solution documents would actually help us gauge the problem space to understand to what extent this is really the problem in DNSSEC.

Personal opinion is we haven't come to that moment where this interaction is so heavy that the automation or absence thereof is really problematic, but I just might be wrong.

DAN YORK: Okay. So well maybe we can go have a beer and discuss that at some point, because I will argue that it's come back from a number of cases that this whole DS upload issue is a barrier for many folks. Now I'm going to get the hook so I've got to just wrap it there and say please, for those who are in here, I would second Peter's comment; we do need more comment around this whole issue, especially for those who are not necessarily in IETF circles.

And if you're not, if you're interested in contributing but are not fully into the IETF way, please feel free to use me as a conduit to get that feedback back. I'm willing to take that into the circles and provide that feedback. So thank you very much.

RUSS MUNDY: Thank you Dan. Now if we could have our next panelists, Lance Wolak is the Chair, so I'll step out of the way. What was the time on each of these Julie, was it five? Five, okay.

[background conversation]

LANCE WOLAK: Hi good afternoon everybody. I'm Lance Wolak; I'm with Public Interest Registry and moderating a very interesting panel this afternoon. It's our last session and we expect to go through this on time. But we do have some interesting material to go through, we may run a little bit over, but we'll stay as close to the time as possible. So this session is DNSSEC in the New gTLDs. We have Roy Arends of Nominet with us, Jim Galvin of Afilias and Patrick Jones of ICANN.

Just a quick thought or two before we get started; during the life of a signed zone certain transitions can occur. And this would include a simple domain name transfer to more complex transition related to a possible registry failure or DNS operator failure. So our panel members today will be reviewing a number of these situations or conditions for your consideration. So why don't we move on to Roy first, and he'll be going through secure zone.

ROY ARENDS: Julie, before you put up my slides, Jim Galvin and I, we coordinated our slides together and we thought that the order would be Jim first and then Roy, so let's do Jim first.

JIM GALVIN: Okay thank you, and moving to the next slide as soon as you get that up there. So I want to key off of a little bit of something Dan York just said in his last session – there is a really very important distinction to me to be made between the DNS operator and whatever that happens to be bundled with. He was talking about registrars and bundling the DNS operator, and I want to focus on DNS operator and the registry here and make that separation in this context also, because we're talking about DNSSEC transitions; transition of a DNSSEC services when a registry is going to fail. Let's focus on the DNS Operator failing.

It may or may not be explicitly a part of the registry, and in fact, a failure of that may or may not be related to the registry failure itself. Important thing to get out of that is the DNS Operator failing has a significant and irreparable impact on registrants and on their zones obviously. I mean if you can't look up a zone then even though the registrant and their website and any other services they might be having would work, the internet community at large will never be able to get there, never be able to do it. So it's useful to make that separation.

If you go back and look at, since we're in the ICANN context I'll point this out, SSAC did a document SSAC 47 where they talked about, commented on the ICANN registry transition process. And they make this point there also about making the separation between the operator and the registry. So the transition requirement is really one primary requirement and that is to minimize if not eliminate validation failures, including the DNS resolution more generally. So you just want to make

sure that you can always resolve the domain name to an address in an appropriate way.

And of course this whole process of DNS and DNSSEC is still getting a lot of attention. We've seen that here today. We've seen that in every ICANN meetings in this DNSSEC Workshop. I want to focus on one particular requirement that is necessary when you're doing transitions of your DNSSEC operations. And I also want to point out that this is not a complete technical solution that I'm going to be talking about here. I'm just going to focus on one particular technical issue and teen consider the risk management of that particular item that we're talking about here.

Okay, we seem to be frozen. I'll keep talking forward while she brings that up. The essential technical principle that is important when you're trying to transition your DNS services is that in order for validation to succeed at all times, the appropriate public key information has to be available when it's needed. And for this to be true during a key rollover, the next key or DS record has to be published in advance. It has to be available alongside of the old key. And that's even true, well it's true when there is no DNS operator change. I mean that situation is still true. But it's a relatively straightforward thing to do in the case of no change of the operator. You're just doing a key rollover.

So the essential action that has to happen in order for this to work in the most general case is you need to get the new key included in the old key set that the old operator, that the losing operator publishes. This is in order to get passed various kinds of timing issues that one has and

keys that are held in caches and the different kinds of behaviors that resolvers have with their caches.

You need the new key to exist in both places, both in the old place and the new place in order to ensure, in the most general case, that you have a transition and you don't have any validation failures. And it is important to point out that this is actually a pretty straightforward process, it's a little complex but straightforward. It can be executed when you know the transition is occurring and when you're going to plan that. And we saw that earlier today as Roland from SIDN was going through his whole process of trying to migrate the hardware in which they do their signing. When you plan this that was essentially, effectively a transition of an operator, moving your hardware; it's a key rollover. You can make this work and nobody can notice.

During an unplanned transition though a fundamental question is whether the losing operator will continue services. And that becomes the essential question that needs to be answered. You want two things to happen – one you need them to continue services because you need to make sure that your various caches and the information that's out there anybody who might have old signatures can still get old keys; that all of that information was available.

So the procedures for an unplanned transition is the same as a planned transition if the losing operator is going to cooperate and if they'll continue their services. If they're going to continue to be helpful in the transition process and make it work and ensure there's no validation failures then you simply have to coordinate the pre-publication of the next key or the next DS record and you can make all of this work. So the

problem is can you avoid transition, can you avoid validation failures if they're not cooperating.

And that in fact is really the concern here that I'm trying to highlight. It might actually be necessary to go unsigned before resigning. If you're losing operator doesn't cooperate in the transition process for whatever reason, they're either maliciously not cooperating or perhaps they just plain can't. The entire system has just failed and they're not there, then you can't move forward and you can't make a smooth transition.

So the observation that I make there with respect to EBERO, the emergency backend registry operator and what has to happen is we make the proposal that we establish this key relationship between the old and the new, and the new in this case would be the current operator. So when the new gTLDs would come out, since this is about new gTLDs and DNSSEC, you would have the EBERO be selected or some set of them be selected – I mean there are various technical options here in terms of the implementation, but you have to actively set up this key relationship in advance.

So if I'm the current operator I can immediately establish a relationship with one or more EBEROs right away and have those held in escrow perhaps; they might not have to be distributed right away. Again there are a variety of ways to implement this. But that's what you want, for this new key to be on hot standby and available and ready to go as needed in case you have an emergency. Thank you.

ROY ARENDS: Since my presentation is related to Jim's presentation I suggest we do questions after my presentation. Yeah? Is that okay? Okay. So we all heard Jim say how hard it is to do DNSSEC rollover between registries and registries, but this is not typical for a registry to registry transition. Thank you Julie. You have all kinds of transitions. Zones move from registrant to registrant, they move from operator to operator, from registrar to registrar. Folks do a DNSKEY update or an HSM update or DNSSEC signing software update. We've seen a great presentation from Roland on how to do that.

And I asked Roland today there are two kind of typical solutions, which one do you use. And he used basically the double DNSKEY and there's another one that's called the double DS records. Do we actually know why this is so hard? What is the fundamental problem? When you do a DNSKEY rollover there's a main requirement, Jim already pointed it out. Doing a DNSKEY rollover the zone needs to be seen by a validator as signed and valid. The slight issue there, slight problem here is that validating resolvers do cache DNS information. And when they cache – sorry, when records are signed, when a signature is signed by a key and the key thus needs to be related and available to validate that signature.

Now when you have two different zones, well essentially the content is the same but the keys are different, because you're transferring a zone from one registry to another registry. The last thing you want to do with that new registry is to use the old DNSKEY. You do not want to import an old signing key into your system. So basically you use two different keys. So assume you have an old key and signature and a new key and signature. We know that the old key cannot validate a new signature and a new key cannot validate an old signature.

Now if there was no caching this wasn't a problem. However, once these things are cached the resolver will not refresh them until the TTL for these records has expired. So this is what I call – and I apologize for the term; I had to come up with it about a week ago. This is what I call a DNSSEC Lockout. So the old key and new sig are cached or the new key and the old sig are cached and we know that they don't validate, but we also know that the resolver won't refresh it.

So this brings me to the next big requirement, and this is what we're trying to solve; this is the fundamental thing we're trying to solve. We want to avoid a lockout. So what Roland described this morning was a DNSKEY procedure, a double DNSKEY procedure. And this is also what Jim was referring to and this is really the best case scenario. What I mean by that, and this is not on your screen currently, what I mean by that is if you have the losing registry incorporate the new DNSKEY from the gaining registry, then everything is fine.

Because then it doesn't matter to which zone you talk; you at least have an overlap and the overlap is the new key. The new key is available from both zones. So validation works, caching works. There are still some timing issues to resolve but that's basically one of the ways to do it. So Jim really described the best case scenario.

PATRIK FALTSTROM: I'm sorry Roy, Patrik Faltstrom. I need to interrupt here. I'm a little bit confused here. You used the term registry, what do you mean.

ROY ARENDS: What I mean with registry is the signing operator of – basically the DNS zone operator. That's what I mean. What I mean registry I use the term registry in the context of EBERO.

PATRIK FALTSTROM: Okay thank you.

ROY ARENDS: Just to relate to EBERO, EBERO stands for emergency backend registry operator. And one thing an emergency backend registry operator intends to do at one point in time is to provide DNS service.

PATRIK FALTSTROM: Because in some of these changes we also have a parent registry that will be involved in some of these DS record things, so I just want to make sure that we invent enough terminologies for everyone to know what we're talking about.

ROY ARENDS: I have no worries that I will confuse people even further. Now in what I'm about to say the parent is indeed involved. So what Jim was describing was the best case. With an EBERO case it might not be the case that a losing registry wants or is able to cooperate. It might not even exist and no one might pick up the phone. So what do you do when the losing registry or the losing DNS zone operator is cooperating with you? What you do then is hopefully, and these are assumptions that you have to make, that the gaining registry has at last a full zone

copy, including the old signatures, and that these signatures in the old zone are valid for some time in the future.

And what you do then is basically equivalent to what Roland was describing with the double DS. And so I'm not going to go all DNSSEC on you. What you do is you add the EBERO DS records next to the old DS records to the parents before you do any transitions. So the DS record is part of a chain of trust, the current chain of trust is basically from the parent to the child and the child is the old registry, is the old DNS zone operator – before Patrik gets up. And you have basically a DS record that points to the new key in the new operator.

With DNSSEC at least one of these DS chain needs to work. So if you have one, two, 476 it doesn't matter; at least one needs to work, one chain of trust needs to work and you have a valid chain of trust. So what you do next is in the new zone, which is a complete copy of the old zone, you replace the old key signing key with the EBERO key signing key. You then add the ZSK to the zone. You keep the old ZSK. This actually is not a requirement but I just add the ZSK to the zone. And you sign the DNSKEY or R set with a new KSK that replaces the old DNSKEY signatures. And you sign the zone with a new ZSK while you keep the old zone signatures.

Now this sounds complex but it can all be automated and it is proven to work. What we've done here is we've basically reigned the zone and added new DNSKEY records without the need of the old DNSKEY. And the reason that it works is because the DNSKEY set does not have to be signed by the ZSK. It is the KSK, the key signing key that signs the key set, and we've just introduced a new KSK.

The third step is you basically redelegate zone to new servers, and after some seconds basically for instance in the root zone I think NS records on average two days, so you wait for a few days. All validators should have validated to the new zone on a new server and what basically remains is the last steps of the regular DNSKEY rollover. You retire the old ZSK. You retire the old ZSK signatures. Now note that I say "retire" and not "remove." Retire – there's a whole process in doing that and this should be all automated.

So if we go then back to the lockout scenario that I describe, also we switched the new keys and the old signatures are cached. Since the old DNSKEY is now available in the new zone that basically means that the old signatures can be validated by the old keys. So all rejoice, no lockout. And then for the second scenario there's the opposite. You have new signature and old keys and in this case the old keys are cached and not the old signatures. So you have old keys cached. The old signatures are available in the new zone and the lockout scenario is when you have old keys and new signatures.

Now these new signatures, they can only come from the new zone. And if you get a new signature we know that you also get the old signature. So the old signature is available as well, so we all rejoice, there's no lockout. And the reason that this works is – sorry, there's one point that I wanted to make. The timing here is critical because the old signatures, you can't regenerate them because you don't have access to the old DNSKEY. Timing is critical because these signatures have a limited shelf life.

So it might sound like a good solution when the losing registry or the losing zone operator doesn't cooperate, but what just happened is we doubled the amount of signature in the zone. So there is pain. If you have a very, very large zone with an enormous amount of signatures, you just doubled that. So why does this work; because this is essentially the double DS method. This comes from draft IETF DNS OP DNSSEC-key-timing-03 in section 332. And in this scenario, like I said, there's no cooperation needed from the losing registry. That's it. Thank you.

LANCE WOLAK: If we have a few quick questions we can take those now. We are running close to our time period. But I'd like to move over to Patrick right now, and then we can take questions at the end.

PATRICK JONES: Patrick Jones from the ICANN security team. My comments are fairly short and hopefully that will be a good introduction to a few questions. So over the last couple of years ICANNs been involved with working with the gTLD registry operators in the community. It started out as a gTLD registry failover program and a plan and we did a registry continuity exercise with some of the existing operators; that ultimately that work ended up going into the applicant guidebook as a proposed registry transition process.

What that's identified is that ICANNs role if there is an emergency transition that's needed would be fairly limited. We'd be involved from a coordination standpoint to ensure that there is a transition between the losing and the gaining operator as Jim and Roy mentioned, and

involved in the addition of the new DS records through the IANA process. There would also be a coordination role between IANA and the NTIA and VeriSign as through just the normal DNSSEC process.

What we've also had some discussion that ICANN will also have a facilitating role to encourage potential pre-publication of key material in the steps that Jim suggested. But also in providing a shared information path; sort of a way to share information between operators and so that way there would be an ease of transition from one operator to another in the event that there's a failure.

There's another area where ICANN may have a role and that is in messaging with the community and to registrants that might be impacted in the event of a failure. And those would probably be the ends of the role for ICANN unless there is a need for some greater coordination or collaboration with the community. So with that, I don't have any slides and hopefully there's some good discussion that can go more about those suggestions that Jim and Roy made about DS records and transition.

LANCE WOLAK: Great, thanks very much Patrick. Do we have any questions for the panel?

PETER: As of five minutes ago I still worked for DENIC and for full disclosure there's no stake in either new gTLDs or EBERO or whatever, so I'm just a concerned engineer here. First of all I'm a bit confused, so that's a question to the panel master rather than to the panel. What is the

purpose of presenting the drafts here? Is there an assumption that the technical discussion or the discussion of the technical gory details is going to happen in ICANN circles or in this forum in particular?

RUSS MUNDY: Well as one of the people from the program committee that was pushing for this, the whole topic of what occurs if things have to be moved around and what occurs with respect to the new TLD program was really the genesis for having the panel and the information, not necessarily to present particular solutions. It was get information out about the impacts relative to DNSSEC in this general space.

PETER: Okay fair enough, so that what I was getting at is this is really so involved and esoteric, or say sophisticated that even a three hour discussion, that I'm not starting now, won't be sufficient to mark out the details actually. I have a question for Roy actually. You mentioned, and that's the right slide there, you said "double DS method." On the voice recording you mentioned "oh yeah by the way you also double the signatures so it's a combination of double DS and double ZSK," right.

ROY ARENDS: To answer that first question, that is correct.

PETER: Thank you sir. So, my perception is that you were, both of you, Jim and you were working from a different set of assumptions. And referring back to the intervention I made following Paul, we've seen a couple of

times that people are working on solutions, but don't agree on the problem. Is there a certain set of requirements of assumptions that can validly be made? In your case Roy, you also make, and you mention that in all fairness, you had a certain set of assumptions about the timing, like the remaining lifetime of the signatures, the accessibility of the zone and so on and so forth.

So where would these requirements come from. Is it the requirements would be imposed after these methods have been discussed?

ROY ARENDS: No. The requirements come from the simple statement that how do you keep a zone secure while you do a transition. So the requirement is to keep a zone secure during transition. It's a technical question and we gave some technical answers to that today.

PETER: I would appreciate it if we could lower the flight level from stratosphere to somewhere where we don't need the oxygen masks, which means that yes I will agree to that high level description, but your scenario would not work if a registry engaged in say a signature lifetime of a day, except you can't do that rollover in half a day. So where do these, how justified are your assumptions in terms of regulating [triptoparameters] for the parties involved?

JIM GALVIN: Okay, so there are basically three levels here. The first level is when everything is working, the losing registry is basically participating in the

key rollover, the zone migrates from one end to the other end and both are happy. There's basically a divorce and one gets the house, the other one gets the dog and that's all set. So that's the high level, that's when everything goes right. There's no timing constraints there basically. The second scenario is the medium scenario where the losing operator doesn't cooperate; you can't sing your key that way. That's the mid-level.

The low level, the other extreme is when there's nothing there at the losing side. When signatures already have expired. So there are the three basic kinds of solutions. One is where everyone cooperates, one is where the losing doesn't cooperate but the information is still available, and the third one is if there's absolutely nothing there and you kind of have to go through insecure.

What I'm not here to do is set out requirements for, for instance, the new gTLD program or for the EBERO, what an EBERO should adhere to. What I'm saying is if you want to do a zone transmission and you want to remain secure, this is the way to do it.

PETER: Thank you. Just one quick remark to that, and that may end up in the situation where you have provided this set of three tools jointly and in the end parameters have been chosen the way beforehand that none of the tools will actually be applicable. Is that correct?

ROY ARENDS: That is correct.

PETER: Thank you sir.

JIM GALVIN: So let me also respond but put things in a following context, since Peter I also gathered you were also asking about just how technical a presentation we're giving here and if this is the right forum for it. Taking a step back, the requirements for a registry transition are laid out by ICANN in the EBERO Transition Plan and how all of that's there. And if you go back and look at SAC 47 we offered our comments on that transition plan and some issues about it, and of course all of that's been revised too.

So we came at this from a very simple statement of "you want to make the transition happen while maintaining the security of the zone." I would characterize the difference between the two things that you saw today from myself and from Roy is more a case of "I'm making the observation that without cooperation it's actually not possible in all cases to do a secure transition." What Roy is pointing out is, as you dig into more of the technical details you realize that you can actually affect this change, affect the transition without cooperation, as long as you do it within a certain limited time frame.

It's not 100% solution. It's a 90% solution or 95% I suppose, depending on your point of view, depending on some timing parameters. As you point out if the TTLs are less than a day things get really sticky. So that might provide some advice to registries to think about this kind of issue. But there is a window of vulnerability and that's the point. Based on

these TTLs and what's cached and their values, but even in the presence of that there will always be some part of the community that's at risk but the majority of it will be covered by this Plan B solution.

So it's the observation that there's a path through most of this. Oh okay, I'm sorry. Anyway, that's the way to look at this is we're really solving the same problem and he's offering a solution that works. To take this to a registry context it's about pointing out to registries in here and in these meetings since this is ICANN that you should care about this and you should care about (inaudible) transition and this is a particular issue that you should pay attention to in your own disaster recovery plans.

LANCE WOLAK: Thank you very much, thanks to the panel for this very interesting material. Thank you.

RUSS MUNDY: And thanks everybody for coming. DNSSEC Workshop has ended. We need to get out of the room I think. Thanks folks.

MALE: Somebody lost a power cord here. There's a power cord sitting here for a, looks like a (inaudible) laptop. If you've got a (inaudible) laptop, check your power cord. If anyone's missing anything please bring it up to the front desk up here and we'll hold it for them in lost and found.

LOUIE LEE: For all of you who want to participate in the discussion please come up to these tables up here rather than sitting on the sides in the regular chairs. If you're only observing and don't feel like you want mic time go ahead and be on the sides. But if you think you want mic time please come up to the table and we'll be starting momentarily.

[End of Transcript]