CR - DNSSEC Workshop
Wednesday, March 14, 2012 – 08:30 to 13:45
ICANN - San Jose, Costa Rica

Patrik Fältström: …that ICANN is arranging. I'm the Chair of SSAC, Patrik Faltstrom, and I have the pleasure of having Steve Crocker - that during the years I've arranged this workshop with, with Julie - is also together in the first panel. One of the reasons why I really wanted to be here and welcome all of you, I will go even though DNSSEC is an important issue that I am interested in; unfortunately I have a few other meetings in parallel so I will go out and in through the workshop.

But just because Steve and I are here, both of us, we would like to mention to all of you that exactly today, ten years ago, the Board made a resolution to create, to formulize SSAC. So I would like to congratulate Steve for initiating this. SSAC, I will thank all of you and all of you that have working with us in SSAC during the years, and thank you very much for coming.

Steve Crocker: As long as we're being scribed and we're on the record and people are listening, I'll just add a few other keywords. The genesis of SSAC actually stretched back a little bit more than ten years ago today. The events of 9/11/2001 triggered inside of ICANN just as they did across the globe a reaction to maybe it's time to look more seriously at security issues. In the case of ICANN, they held a workshop in November of 2011 - quite a good workshop with the slides still available online. I was not present but many other very good people came and gave presentations.

On the strength of that, the formative process for SSAC was started. A number of quite excellent people were recruited and then I was asked if I would Chair it.

Vint was Chairman of the Board of ICANN at the time and he said, “Well, just get it organized - six months it will be fine.” I knew right then that that was an underestimate by a certain amount. Then for the next eight or nine years I chaired SSAC and it’s really been a fantastic trip.

Within SSAC we started to push DNSSEC and it was tough because we couldn’t get enough concentration of effort. One of our colleagues, Bruce Tonkin, took me aside, I remember vividly, in Tunisia and said, “You’ve got to pump it up, get separate funding and make a separate project out of it.” Pieces fell in place.

We put this series of meetings in place and have managed to make quite a success of it, and so we have two great traditions actually - we have SSAC and then we have this effort - the DNSSEC workshop series - and a lot of people have put a lot of energy into it. It’s been really very rewarding, very successful and I get to take a certain amount of visibility. I get a certain amount of visibility from it, but really the credit belongs to the people who put all of the work into it.

With that we’ll continue, on the SSAC side, Patrik has done a fantastic job of taking over and bringing SSAC up to the next level. It’s become a respected institution and all the more so with the team that’s there, including the staff in particular, Dave Piscitello. Julie makes the trains run on time; Steve Sheng has just been really excellent.

Alright, welcome everybody to the DNSSEC Workshop. We’ve also had the benefit of sponsorship which provides lunches for all of you. There is a free lunch as long as somebody else is paying for it. The Program Committee, an all-star team - Diego, from this region and Lance Wolak, Russ Mundy, Simon McCalla and myself, with Julie keeping everything flowing.

Next slide; those are the sponsors again. Next slide - that’s the program, we’re doing it. Next slide; keep going. As a small project that I’ve been pushing with help from my team at Shincuro, we’ve been trying to keep track of DNSSEC deployment around the world. We have a set of maps that I will flash through in a minute.

It's really intended to do a couple of things. One is we can see what is happening today but also it keeps track of both retrospectively what happened in the past and prospectively what's anticipated to happen which is always an estimate that might change. With that, let's just move forward.

This is a map as of January 1, 2006, so we're going back more than six years ago. What's important here is, the color coding is yellow is experimental; the orange-ish color is formal announcement that there is an intention to implement DNSSEC; green is partial operation; blue is DS in the root - and of course that couldn't have happened back in 2006 - and red is fully operational, accepting delegations, up and running. We'll flash through.

The next one is half a year later. Let's see we can go back and forth. I should know who that is - Bulgaria maybe? Here we are - Brazil announces that they are going to be and then they become partially operational, and now we're moving forward 2008 - midyear 2008, 2009. There is Australia and the US and India and Namibia and various pieces of Europe. It's a little disproportionate because a single country that has a lot of territory creates a disproportionate visual effect.

This is mid-year 2011, so this is fundamentally about two years ago. The red is fully operational. This is pretty good stuff and here is more and more. Canada coming alive. Actually this is the projection for July this year. I thought Canada was running. We might have errors in our database. We've put a lot of work into getting control of it and I'm not sure we've got 100% control. What we do have - the only thing I can tell you that I'm very proud of - we do have a way of updating the database so that it gets better over time, so please do report any things that are missing or wrong and we'll be there. There is the projection for mid-2013 and here is 2014.

Of course the future projections have historically turned out to be underestimates just because we don't get reports, and then all of a sudden some things happen. This is the local region. This is the northern half of the Latin American and Caribbean and here is the southern half picking up Chile. Here is a sequence that takes statistics from the same database and shows the status and apropos of my remark about underestimates for the future, what you see are a level estimate in the out years here. As I said, that's almost certainly an underestimate as we get more data. This is what's known as of now as opposed to what the facts will turn out to be, which we can find some other time.

Any questions? Is this useful? Yeah? It's worth doing? It's taking more work than I had in mind when we set it up, but these things always do. So with that, that's the end of my short introduction. We have a fantastic program setup here and it is my deep regret that they boosted me up in the stratosphere where I am no longer allowed to do anything technical.

Julie Hedlund: Please join me in thanking Steve Crocker because unfortunately he is going to have to leave us I think with his busy schedule. We're just very, very pleased that he could join us this morning, and also for his continued support of this very important workshop.

Russ Mundy: I'm Russ Mundy. In conjunction with the work that Steve's doing that shows up on the maps, looking primarily at how to illustrate the deployment of signed CCTLDs, we're also trying to establish a mechanism to measure the availability and usability of DNSSEC. This is a tool with a couple of screenshots - it's called DNSSEC Check. It runs on a batch of different platforms and it's designed for people to have the software - we've got it for an Android phone and other portable devices as well as regular computer platforms. You can run a check and find out if DNSSEC will work from your current connection point. One of the things that we're trying to do is establish a database to collect where DNSSEC actually works and where it doesn't.

The submission is purely optional for those running the software. We would ask that people would send the data in so we could get a larger database. We don't have this part of it integrated into any mapping mechanism yet, but in fact it is an effort that we'd like to spread on to the community. The URL for getting the software is there on the slide and so please grab it, try it out and if you... let's go back one slide, Julie. You'll see the top tool is actually making use of the Comcast validating resolvers. They're all green. Incidentally when you run the tool here at the ICANN meeting DNSSEC works, everything is all green. The bottom picture there is a shockingly good picture of a hotel internet access point. The only thing that it doesn't return properly is at the AD bit but in fact, if you're running the validating resolver on your end machine, you can still do DNSSEC without it.

You can make a lot of determinations by yourself once you get used to using it, so please everybody, pick it up, give it a try and if you're willing to please send your data in. We'll have more information about what we've got next time.

Julie Hedlund: Thank you very, Russ. At this point we're going to go ahead and switch to our first panel. I'm going to switch the slides a little bit so just give me a moment and then I'll turn things over to Luis Diego Espinoza who is moderating the first panel. One moment please. Just one moment and I'm going to make a change in our Adobe Connect room, the slides aren't showing up there properly. Thanks for your patience. Thank you for your patience. I'm going to go ahead then and welcome Luis Diego Espinoza who is moderating this session, the panel discussion is on Challenges and Benefits of DNSSEC for Latin America and deployment updates from that region and others. I'll go ahead and turn it over to Luis. Hold on.

Luis Diego Espinoza: Good morning, I'm really glad to be here because we are working a little bit to implement DNSSEC product here. I was keeping an eye on all of the development of DNSSEC for Latin America. This morning I have these participants - Gonzalo Romero from Colombia - nice to meet you. I didn't meet you before. Frederico Neves who is over there. He's very common in this environment. He's doing a great job with the .BR. Roger Castillo from Mexico.

Deimon Tencio – he's from Banco Nacional de Costa Rica. He was invited because it's part of the development in Costa Rica DNSSEC implementation. Joonhyung Lim from Korea. I let the speakers to present. First, Gonzalo, go ahead.

Gonzalo Romero: Good morning, everybody. My name is Gonzalo Romero. I am the Chief Security Office of .Co Internet. We are the .Co registry in Columbia. Please let me talk a little bit about us. We are a private company. We launched on 2010 to manage and promote the .Co domain. We have a concession contract with the national government of Colombia. Our partner for security and IT is NeuStar. Our DNS servers are within the UltraDNS Constellation and they are managing now our rapid domain compliance for monitoring the malicious activities within this zone.

Regarding the statistics and milestones, we did one million registered domains in less than one year from global second level launch. Our renewal rates are 65% - much higher than any other TLD launch in the first year and we are on track to grow to two million domains in two or three years. Regarding credibility and awareness, T.CO is used by Twitter as the URL shorteners like 110 million tweets a day. .CO is used by Google as the official URL shortener and domains like A.CO, K.CO, Z.CO and Cloud.Co are used by Amazon in their products. If you need some additional information about us, just go to our website.

We got into DNSSEC, we announced our signing in the ICANN number 39 in Colombia and Cartagena in December 2010. We implemented the signing during January and February and we finally announced in a press release our deployment and our signing on March 1, 2011. We followed the same models as .BIZ and .US and we respect the same standard policies. We recently rollover our KSK and the most important thing we are doing for making the adoptions really easier is we don't need any certification or special requirements for validating the DS records so the registers can submit it by EPP updates.

From the local perspective on the ONS, we do .CO DNS Tech and SEC Day. We are working on this for this year in September. Last year we did the event on July 27th. We had 60 participants, most related with the ISPs, the government, the academy and banking. We have very good speakers like Edward Lewis from NeuStar, Kaspersky [Dianic] from Chile and LACNIC, among others. As a result we built a CO-DNS virtual community in which you can find videos and all of the information related with the event.

This year we are planning to do the same event in September which is already LACNIC sponsored. We are inviting right now Comcast, CloudFlare OpenDNS and Ilumintel for making presentations. From the global perspective, we are working on several articles related with how to sign .CO domains within our zone, celebrating our first anniversary after the signing of the zone.

Our status now - by February 2012 we have 59 domains signed, very similar to that .BIZ and .US. Four registrars manage those domains. Eighteen domains also include private registrations and related with Latin America presence. Six of the domains are registered by Colombia registrants and one by a Peruvian registrant. This is a chart of early adopters in which you can see that almost half of the domains don’t have a webpage. The third part is related with E-commerce sites and six domains are redirecting to non-safe sites.

We did a survey with the Latin America registrants. They told us the following, “Registrar provides me the service as an added value.” “DNSSEC is DNS is a security matter issue.” “My website was hacked before,” and when they refer others to DNSSEC, all the time they receive answers like, “What is this thing?” And the most important relevant issue is that no registrant signed by themselves without register promotion of the product.

Our challenges are we need a strong community and knowledge transfer interaction between the registry, the academy, the government and in particular the ISPs for validation regarding the DNS security issues. When you ask local ISPs and tech personnel during conference and related, what is DNSSEC, they didn’t know about that. On the public sector IT products, all of the requests for proposal should include DNSSEC as a must. We are working so hard locally regarding the knowledge of domain names, which is very, very poor in our country. However, the internet security, awareness and proceedings are growing. We have now two Colombian CERTS certified by a diverse community and we have a public policy in cyber defense and cyber security.

From the global perspective combined with innovative solutions like OpenDNS, DNScript and Bind - the last version of Bind - which includes inline signing on NXDOMAIN redirection. We think that the DNSSEC adoption may grow so that people can have more confidence in the entire DNS infrastructure. We think, finally, that as IPv6 is relevant and required for internet infrastructure, DNSSEC is relevant and required for internet stability and security. That is all, thank you very much.

Luis Diego Espinoza: We'll leave the questions for the end. Going to the next presenter, Frederico Neves from .BR.

Frederico Neves: Good morning people. I will give a brief update on .BR and deployment and our current activities. Nic.BR is a not-for-profit organization. We run .BR and some other infrastructure services for the Brazilian internet like internet exchanges in 23 cities and some other coordinations among the Brazilian internet like the [Brazilian CERT, the statistics] and other things. We are 120 people company and get directly to the point regarding the history of the .BR DNSSEC deployment. We started during the standardization of what we call the DNSSEC peace process during the ITF. And that work finished up there in the first phase around the end of 2004, beginning 2005. Then we decided to... we had some firm plans to deploy DNSSEC in .BRs.

We started July 2006 with five small zones. .BR is divided in 60 plus zones. We had in mind that DNSSEC was a first [season] service, so we started since the beginning with DS connections in our entire interfaces and direct interface that is a web one and an EPP interface for registrars. We finished deployment in January 2009 with the three large zones and signed it with nsec.3 - that is to solve some problems that we have with... I will not tell some problems, but some issues that some registries thought were in actually the DNSSEC base standard.

The initial phase was a kind of manual process with manual rollovers and a lot of interactions with the operation team. The keys were secured by a crypto file system, so this initial phase of deployment that ended in May 2010. Leveraging the route DNSSEC signing, we learned from the process actually before it started. The discussions of the process and the ceremonies and we grabbed some good things from there and we designed our own ceremonies and we have been running this process since May 2010. This is what we call our second phase and it's based on two ceremonies a year. We have backup sites and our KSK are kept in HSMs in both sides and we have completely automated rollover system and deployed since that time. This is what we call a complete professional DNNSEC deployment for .BR.

The deployment strategy - one of the ideas that we had is to create kind of safe havens in .BR for sponsored TLDs like we created by request of the Judiciary Power in Brazil they choose .BR - it's an SLD. On that SLD to get a delegation you need to be certified that you are a Judiciary Power organization and actually you need to have a DS in place in a signer zone, so this is mandatory. This was October 2007 and in September 2008 we created the B.BR that is a TLD exclusive to banks. You need to be a real bank certified by the Brazilian Central Bank. There is a human process to get your delegations inside of this zone and DNSSEC is mandatory too.

In parallel of all of this at the time we beginning in early deployment, we didn't have any kind of automated, we didn't have Open DNSSEC in other tools, so we decided to build our own. We built one tool that is freely available in its own version - 2.0 now. We had probably more than seven releases since the beginning. That is called a DNS [Shim] and the target of this tool was actually hosting company providers. We like to provide a kind of security master for these guys that have hundreds of thousands of zones - small ones, with a small amount of records. This was like 2007 and then in 2010 we decided to start dogfooding from this piece of software and we started to provide direct services for customers that want their hosted zones.

There is not a single information in the interface for the end-users that this is a DNSSEC signed zone. It's completely transparent to the end user. With that deployment we got to 8% of the .BR delegations that are currently in 2.8 million delegations, are currently signed since December 2010. We have been giving trainings in operators meeting in Brazil and we are continuing to outreach ISPs and others and hosting providers. There you can see, if you look at this graph it's a little bit difficult, but between 2006 and beginning, of end of 2010 you can see that we had probably a pretty small deployment. I should have put another graph with a better resolution for this part of time. But we had until the end of 2010 a little bit more than 1,000 signed delegations. That was pretty small amount of signed delegations and then we started to provide the service and now we have around 230,000 signed delegations.

With the events of software like Bind 9.9 that we have the bump in the wire signer; and especially in the case of hosting provides, Power DNSSEC that it was available since mid last year, we will probably see a larger growth in the market because as we are providing this we are trying to raise the bar for the registrars so we are trying to push them to provide better services.

The challenges and benefits - I think we are still in the early we start to collect benefits from DNNSEC in the upcoming years, so the work that we are starting to see in the standardization process with the conclusion of the first documents on DANE in the last couple of weeks and we will probably start to see… we are already seeing some interesting drafts trying to solve security problems that we are struggling with, other deployments like trying to secure the routing system. We are now seeing new ideas leveraging the DNSSEC and work that is happening at DANE. I have - I don't know if it's "hope" is the correct word but I have a gut feeling that we will see pretty good things in the near future.

Luis Diego Espinoza: Our next presenter is Roger Castillo from .MX. Please start.

Roger Castillo: Okay, good morning. As Dr. Crocker said, we've been running DNSSEC, well he showed in the graphic, we've been running DNSSEC in the experimental fashion from some time ago. We've still not signed the .MX zone at this time, but we are planning to do it soon. I'm going to tell you something about what we've been doing to be ready for DNSSEC. One of those things, it's collaboration with ITESM – that's the Technical Institute on Monterey. We've been sponsoring research projects to test the DNSSEC platforms and anticipate possible problems with DNSSEC, trying to avoid risks and be ready to provide guidance and support to adopters.

One of those projects is called "My DNSSEC." It's a project which goal is to implement DNSSEC at the application level allowing the user to verify if a domain is validly signed. It's a browser plug-in that displays an icon in the status bar showing the DNSSEC status of a domain name. I think it's something similar that DNSSEC validator that we saw a few minutes ago, but it's developed as a plug-in that goes into the browser. It is a collaborating project between Nic Mexico and DNSSEC and ITESM. We've been providing guidance to the research project participants to know how to build that implementation.

My DNSSEC uses a local installed outbound server that can also work in proxy mode using an intermediate server in case DNSSEC packet cannot pass through the internet connection. I hope you understand that because I'm not really following. My DNNSEC implements a safe browsing mode in which only DNSSEC valid sites can be navigated. That is, I know, pretty much heavy stuff, but it's only developed as example, like an experiment and the plug-in is capable of doing that.

Here we show the plug-in states. We were advised to level up that precise icons to give some indication about DNSSEC. Maybe we could do much better with the icon design. The initial state is the default state when opening a new tab. Nothing is verified yet. The warning state denotes when we access a domain that is not signed in with DNSSEC. DNSSEC Wrong is used with a serve failed response is obtained. DNSSEC Okay is shown when DNSSEC chain of trust has been validated with the AD bit.

The development of platform support - we have desktop for support for Windows XP, Vista and Windows 7, Internet Explorer 7 and 8. I think they are currently working on some extension for Firefox and Chrome. It's also been tested only in proxy mode for mobile platforms and Symbian Windows Mobile because of the difficult… it could be very difficult to add a plug-in to a mobile browser. The plug-in shows the icon at the bottom of the status bar of the browser.

As I told you before, it's an effort supported by NIC Mexico and developed by students ITESM Monterey. They are Master's Degree students in civil engineering and advanced computing that are working on this kind of project. It's a better project. It's still on… it's better we're working with the development of it. I'm going to show you a small video show in its operation.

Okay, the browser opens; we're going to do a .SE website to show its functionality. It is in initial mode and then it will check that the zone is correctly signed. Next is a website - a domain name that is not signed. We get the other icon. Here I think, the system fails before showing the icon, but we're still working on that. The plug-in shows that there are problems with the site we are trying to enter because it is not correctly signed. But it fails before it can show the icon.

We have a test zone [assignment]; we have a provisioning website that is also in testing mode. We have a test set for DNSSEC and we are working with that plug-in for the end-user. That's it. Thank you.

[Applause]

Luis Diego Espinoza:

Well, (inaudible) abroad – let's talk about that later. Now is the time for Deimon Tencio. He will speak in Spanish if you need to check the earpieces.

Deimon Tencio:

I'm Deimon Tencio - good morning. I work at the National Bank's IT security. I now implement DNSSEC at the bank. It is one of the first banks in Costa Rica involved in this. It's quite major and together with the NIC we're doing the DNSSEC deployment. I would like to make a small introduction, something we all know.

The relevance for us when getting to an Explorer when we write the URL, in this case the DVNonline.url, we know that the DNS part is very important. It's been there for awhile and when we check at URL DNS is (inaudible) the resolution. Everybody, especially our clients, trust that query. But what would happen if when you write the URL you are redirected somewhere else, something that we don't want?

It is an attack in 2008 we must know Don Kaminsky who talked about DNS cache's poisoning. And today we can see different attacks, but all of them could come true at some point in time. The probability is quite high. Today attacks are directed to banking. One of the methods used for this type of attack is phishing - at least in Costa Rica it's quite common. There are the duplicated web pages so that people's information will let them get into the bank accounts of people, do millionaire transaction moments leading them to different accounts to be then withdrawn and commit fraud. In Costa Rica and throughout the world banks have been trying to implement security mechanisms. Many of us will know the extended certificates - this green bar in our Explorers or browsers let us validate where we are.

Another important thing is the multiple authentication factors we can implement in our bank sites. Something very important for us is user education. We have educated users so that they can look at the URL and that the URL they are accessing is the one they actually want to get to. But what has happened - what has happened is that attacks become more sophisticated. They don’t just use phishing, but they also combine this with farming techniques.

Farming can be summarized in three majors attack points. One of them is attacking the host of the client station. The last case where we’re able to see some two months ago was to a customer - they sent him an updated script of an Adobe and it changed the client’s system introducing the URLs of the banks of Costa Rica and redirected them into a different IP address. This IP address had the fake sites to capture information and then perform the fraud.

This is something that is out there and another farming approach is the changes in the DNS records. Our station is… there is a DNS with the queries and the translations of the names into IPs. But when this record is changed, it’s redirected to fake addresses. So anytime the hacker will change the fake DNS where we’re directed to, we are redirected somewhere else. These attacks have actually taken place and the (Inaudible) attack vulnerability report is back in 2008 is the cache [poisoning].

The part of the vulnerability of this process - there is a query by the name resolution servers, but we cannot leave aside DNS manipulation. At our companies today we have technicians who manage DNSs and we don’t know at which point in time they can get involved in fraud and change them. So for the National Bank, the introduction of DNSSEC is major. At least in Costa Rica maybe not many people know what DNSSEC is. I think it is a challenge for Costa Rica getting everybody trained and understanding that this technology helps us improve and make queries safer. Let’s go to the next slide.

The pros of DNSSEC that we have seen at the National Bank - we can browse more safely when we get into the bank’s URL. We help the client to be sure that he or she is entering the National Bank’s site. There is the use of email, not just through browsers and end resolution, by other systems such as email, proxies and other systems that use the DNS for queries. So there will not only be a vulnerability in browsing, but emails can be redirected as well. The seriousness of this problem - the insecurity of DNS queries - is quite an issue. That is why we believe that DNSSEC is a way to make sure about this type of services.

And then new advances in security as well - my colleague was talking of “My DNSSEC” - but there are different type of security systems deployed that will be like an add on to email, to proxies that will support a query validation that will be used in DNSSEC and the technology of domain signature to get better safety and security and internet services. From what we have been able to see, as to DNSSEC, we believe that there are many challenges for all of us, for our companies and there are many items here. One of them is the relevance of the upgrade of the navigators, explorers so that users can check that the domain they’re getting into through the validation *via* DNSSEC is safe. Navigators don’t have this now. They use plug-ins to validate DNSSEC, but Firefox, Microsoft with Internet Explorer will have to add this DNSSEC validation, so I believe that browsers will need to get up to date.

Another important thing is suitable configuration to support DNSSEC. This is very important. Many of DNSs worldwide - some of them have quite old versions and they cannot be expanded to the DNSSEC protocol. Efforts need to be made to update things and set them up properly so that DNSs can be validated and checked. Another major thing is the commitment by many companies to sign the domains. That is very important because we do have the technology and DNSSEC is here. In order to implement this, if we don’t do it in each of the companies’ zones, we will be working in vain. So I believe that that progress is the pipeline. The company that is deciding to pick this up - implement this security item - will have good results because it will give security to their clients.

And finally signature processing and delivery - progress has been made, but we need to move forward as to how to validate signatures and keys. We have the technical documentation, but for many companies having [HCM modules] for privates keys is pretty costly. This is the area where service companies was proud and will sign domains or provide this service to companies to sign their own areas. This is what I wanted to talk about, such as about the National Bank with the support of NIT, we have been able to sign a transactional area and we had, we will go forward to improve safety in our services.

[Applause]

Luis Diego Espinoza: Okay, our next speaker is Joonhyung Lim. Go ahead.

Joonhyung Lim: Okay, let's move to another reason. My name Joonhyung Lim from Korea Internet and Security Agency – KISA - which is also a .KR domain registry in Korea. First of all, I'd like to thank Julie and Planning Committee for sitting… giving me a chance to sit in here, although my late submission of presentation. Thank you.

Okay, I give you a quick update of .KR DNSSEC status very briefly. Right after the root GO was signed, we had been trying to sign .KR.GO. As you can see the top-level domain zone signing is just start of action for full deployment of DNSSEC. Everybody do a DNSSEC generally, but what they have to do is quite different. Each stakeholders do something differently. For example, registry signs the zone file, right, [dumps the DNS record] into their registration system and ISP builds up new cache DNS server. We are now also trying to support these Korean stakeholders, solving these kind of difficulties drive from different.

This is very specific issues generally you might not consider when you do your job for deploying DNSSEC. From some point of view, I believe that this kind of information is helpful to someone who is right before implementation level. We experienced the trouble with HSM device which is [high security module]. It was just because HSM doesn't support latest version of BIND. We asked to [bend the authority] and our problem was solved. But as you know, BIND merging has been three countries changing, so you must check everything as much as you can before implementation. So operational consideration is also important, I'd like to say at this point.

As you can see there are some other issues for HSM. There are two kinds of HSM - PCI tied and server tied. PC tied handling and managing a key set, isolate on that PCI device. For several types - can share with each DNSSEC master server so there is a difference to build up the system for DNSSEC.

Okay, integration solution for wide range and fast deployment of DNSSEC. We design plan to deploy DNSSEC validations, supported open cache DNSSEC and it's another thing too, we call this [Zenas]. It is to promote a wide range of deployment of DNSSEC, so we have prepared these kind of things. We are trying to even resort to step-by-step from second half of 2012 by majoring impact to end users and ISPs.

For measuring and analyzing significant impact of DNSSEC, we are now developing CNAS. It is some kind of monitoring system. Some vendors provided this kind of tool but we developed suitable for our system. We expect that DNSSEC is used before detecting end donor key about DNS and DNSSEC and detecting any configuration error from DNSSEC adopted domain under .KR domain name. One other very important thing I think is by this point by [PGRIs] DNSSEC it makes people understand that [virtual] safety can insured when they enjoy internet. So we can show the graph and something and what is going to be secured, sort of information we provide.

In conclusion, we are trying to do loading during that initial stage for each domestic stakeholder, it is important. So sharing our infrastructure and [listening from] DNS operators providers and providing some training program. Recognizing our new stakeholders that we had missed before is one of the challenges I think. For example we now concentrate on web browser things, but every application enabling internet is kind of a start we have to consider for DNSSEC.

We are trying to find out the best practice to promote DNNSEC domestically and this year we announced our contact point in financial sector and government sector. We will continue to make effort with our registrar for keeping our value to end user as a new DNSSEC service and we are trying to move forward fully structured and fully functional DNNSEC environment with every stakeholder in Korea. Thank you.

[Applause]

Luis Diego Espinoza: Very good. I'd like to open the session for questions from the public. But before that, I'd like to ask to Frederico about these, how is this rooted, these (inaudible) signing domains – it's near 200,000 domains? There's many registrants there or is this a few infrastructure companies, like registrars that sign on?

Frederico Neves: Well, there is probably 210,000 registrants because it's completely spread out. It is not a single company doing that.

Luis Diego Espinoza: That is great.

Frederico Neves: It's because basically end-users actually don't know that there is DNSSEC signed.

Luis Diego Espinoza: Okay, any questions? Yes?

Dan York: Dan York. Question about your DNS [Shim], which sounds very interesting. What have you done to… I guess how applicable is it to… Will it work for any of the registries, I guess? Who do you see as the consumers of this and what do they need to have it work?

Frederico Neves: It started that you’re hosting providers, especially in that scenario that I pictured during in my presentation, large amount of zones; small ones, small about of records. I know that some vendors currently have alternatives with templates on, something like, that for this kind of scenario, but to me quite frankly, I think that most of the hosting providers at least in the Brazilian market use database baked-in backend provisioning systems, mainly Power DNS and with Power DNSSEC in place, I would go for Power DNSSEC and not our solution. We have XML interface for the provisioning system of the customer. It could be a little bit more challenging to integrate, but it’s fully documented. We are using because at the time we’re the only option.

Dan York: I think it’s a great thing because certainly if we can get the automatic signing happening of domains, then it completely removes some of the barriers that are out there right now for people to get their domains going. So I commend you on that and thanks for making it open.

Julie Hedlund: I should note that we do have somebody looking at the mics right now. None of the mics on the table seem to be working, so we’ll run around with a handheld until we this settled. So continue and we’ll hand mics to people.

Luis Diego Espinoza: Okay, I have a question back there.

Christian [Hessleman]: Hi. I’m [Christian Hessleman] from .NL. I’m interested in the visual aspect of DNSSEC. I noticed that .BR says that they totally hide it from their end users, whereas .MX is developing this plug-in. I was kind of wondering what the rationale behind the plug-in is or behind not showing it to end users at all?

Frederico Neves: Actually both are complimentary, but the point of view of the end user, actually normally end user not even know what is an A-record is, so why do I…this should be their concern to how do I sign my zone or what's the size of the key? For the most of the cases, this is not an issue so we try to keep this as hidden as possible for the end user. But in the sense of, like our deployment strategy to push this to safe havens and areas of high security for the end user, an effort like the one that .MX is taking - and others - to pinpoint to the end user that is actually signed and secured is actually needed. But the major gain in this scenario is actually the mindset of the user - that you actually need to do marketing or something in this area because the user will actually… they should leverage these advantages from this deployment. You need actually to have a mindset in the user. Like, okay, I'm accessing a website below b.br so I know that this is safe. Anyway, I think to answer your question directly, I think they are complimentary.

Luis Diego Espinoza: I have a comment about that because I think the end user or the user must have some signs, some sign from somewhere. For example the people in the past learn how to identify the SSL lock on the browser and some people started looking then. At some point I think it's a good idea to show something to the end user.

By example, if you use some technique of hacking and change the DNS server for that person and that DNS server is not validating anymore DNSSEC, it could be an issue because the end user maybe don't have the knowledge to identify something wrong. I will let… you want to refer something about your plug in?

Male: Not our plug in, but in general somehow reinforcing what you just said - the user needs something to look at. We started looking at the HTTPS or the address bar, then we painted it green and those are hints for the user that the site is secure. He can be confident that their information isn't going to be stolen, but we want to educate or make the end user to learn and use and look for DNSSEC sign in site and prefer it over the ones that are not signed. We should give them something to look at. That's our position.

Male: In addition it might also have some business value because from a registrar perspective, you may want to offer some added value to your customers and this means that you have to somehow make that visible.

Male: Yes, yes.

Luis Diego Espinoza: I have another question back there, Julie, thank you.

Hossam: Yes, it's Hossam from Egypt. Actually, I have two questions regarding two DNSSEC. The first question regarding two DNSSEC, if it's utilizing these people to call the [port] number, this is the first question. The second question at implementing DNSSEC as a central request over the internet, is a number of requests over the net IP addresses. To compare the two – the normal DNSSEC – it would be the same or it will generate more traffic over the internet to resolve [DS] identification?

Julie Hedlund: Did you catch that or-

Male: I didn’t hear what…

Julie Hedlund: Could you repeat, please, a little slower too?

Hossam: Yeah, I have two questions. Number one, related to TCP of DNSSEC (inaudible), either TCP or UDP protocol. What’s the port number? Is it 53 or another port number? This is question number one. Question number two, related to the number of coded requests generated by the DNSSEC to resolve the IP address; it will be the same, like DNS or it will be generated more [thoroughly per request] over the internet to resolve that same IP address?

Frederico Neves: My opinion on this, the DNS protocol is the less consumed protocol in the web. Then about the bandwidth it uses, I think it’s not a huge problem and will not be a huge problem in the future because the bandwidth increasing constantly. Then about the number of queries on DNSSEC could be not an issue in the future, but if some of the panel have comments about that.

Male: I will first address your first question. It’s the same ports, Port 53. There is no different port. You only have some signaling mechanism necessary, but something that is widely deployed these days. And regarding the query rate, the amount of extra queries that actually we see - it’s marginal. Regarding bandwidth, depending on the [collectiveness] of your zone, you could have something a little bit bigger. But normally for end users, institutionally as somebody said, you will not see great increases, not an issue.

[Sergio Sy]: Hi, [Sergio Sy] for the Accelerance Corporation. This is more a comment than a question with regards to whether an end user should see or not see whether it’s

DNSSEC-enabled. If you've been involved in DNSSEC for a long time, you get the familiar thing is nobody asking for it. ISPs are saying my clients are not asking for it, that's because they don't know anything about it. If you're going to generate the market in, they don't need to know the technology but they need to have some kind of indication as to whether they're more secure or less secure to today's standards. That will drive the request for that technology which will make the ISPs get involved in it. And very large companies are saying, "Well, my cash register still ticks every day, I don't need to spend any more money on it and my business continues." So until the end user actually stops doing business with some online processors that are not DNSSEC enabled we won't get there. My vote is to show it to the end user.

Rick Lamb: Hi, this is Rick Lamb, ICANN. I was wondering - it seems like a few of you have already identified that in order for DNSSEC to work there has got to be a full chain of trust through the ISP. I was wondering what each one of you might say about your respective markets about the take up rate or the support by the ISPs in each one of your regions for DNSSEC, turning validation on specifically.

In the U.S. we have Comcast, who has done a wonderful job, but it's still without completing this whole chain of trust, DNSSEC is great but it doesn't get anywhere. I was really curious to find out from Brazil and from Korea and from Mexico because I know each one of you seems to have thought about this in some ways - what, if any, information you have or knowledge you have about what the ISPs think.

Male: We do have some large ISPs - not as large as Comcast - in Brazil but that are already providing validation for their customers. My take on that is that they are really important players in the market, but as long as they don't mess up with the DNS path, I'm seeing more end users' validation applications in the future. So my hope is that it's wonderful if they play well, but at least if they don't mess up with the DNS path, I'm okay.

Joonhyung Lim: In Korea it was a big resistance from ISPs, we faced also. The authorities - they have to invest something on their bunch of cache servers to improve their performance and certain things. I presented about that so we learning, we're training to have some open cache servers for supporting DNSSEC so we can show them it works very well and you can share our resource in its initial stage. That's our resolution and there is still big, big resistance in ISPs.

Male: I agree with your point of view because in my country ISPs - we think they are a very, very important part of the validation on the DNSSEC. But as I said in my presentation, they don't know about that. They are now concerned about IPv6 issues and if you talk about this kind of things now, it's not a market, it's not a sales part, it's not part of their business model, so it's not easy to make these things happen from an adoption perspective. I think that's the main part, we need to think about that because they are the main stakeholders in the DNSSEC chain, I think so.

Luis Diego Espinoza: Anyone else? Okay, I have a question from Adobe – Ross Mundy.

Russ Mundy: We had two questions from the Adobe chatroom. The first one was from Robert [Guerrera] and he was asking about the use of DNSSEC in social media context and email and Hotmail - other applications kinds of things - and would like to get a response from the panelists about what they think about the need to use DNSSEC in that realm.

Luis Diego Espinoza: Anyone want to refer about that? No? I think it's a short question. The short answer for that is websites, the DNSSEC solution will be helped by DNSSEC anyway. But, for the email, email depends completely on DNS and DNSSEC will help a lot with validation.

Russ Mundy: Just to jump ahead a little bit in our panel structure here, we've got a panel later on about reputation protection that gets into that area, not so much as a social site per se but an application use of DNSSEC and we've got a couple folks that will talk about that. I think that will be related to it.

Now the second question that was from Andre [Hess] I believe, and it dealt with, I believe the question was when trying to buy a domain from a registrar, he's not has success at finding a registrar that would sell him a domain that is DNSSEC enabled. So he can buy a domain, but can't get in from the registrar as DNSSEC enabled. Thoughts and comments from the panel?

Male: I would give our perspective, but it's kind of (inaudible) as one because of our situation that is a little bit different from the others. As we still provide services directly to the customers, we started the registry/registrar model in 2006 and currently we have 25% of the market in the hands of the registrars, but 75% of the market is still directly with us.

In our case we are a kind of lower bar in the market, so if we provide DNSSEC interface it's difficult for the registrars to not provide. If they don't provide, it's not a problem because we can fill this gap. But in situations when you have a completely two-layers market with registrars this is actually a challenge having across the board same service level from each of the registrars, especially in a situation where you have transfers. This is an issue, I think. Some registries have dealt in different ways. Probably people from .org and maybe .sc could talk a little bit about it later.

Male: Yeah, complimenting Frederica's telling about that, we have the same model as a registrant model, so different kind of registrars provide DNSSEC solutions as value service, but you cannot guarantee when you have a registrar or registrant to transfer to another registrar, it's not easy because the new registrar doesn't offer the service for the user, for the final user. It's not easy to manage that kind of thing.

Russ Mundy: I have a question from [Bob].

Bob: It's a response to that, Russ, and Richard Lamb isn't going to mention it, but I'll mention his work that he's been doing at ICANN. He's put up a website on ICAAN's site, and Richard is here, I'm looking over at him there. He's been maintaining a list of registrars that do support DNSSEC, so to that person that's asking that, there is a link. I don't know how to get you the link easily but it's up on there and I just tweeted it out as well. It's a list of registrars that are there. I know Richard is also looking for more, to add registrars there to the list who support that. Basically it's registrars who support adding DNS records or doing hosting signing.

Male: You are referring to the deployment 360 in the internet society site so you can just browse to www.isoc.org and you can see that on the deploy 360 project.

Russ Mundy: Perfect, and I'm about to talk about that. It's a perfect-lead in and I thank you for saying that. But also over on the ICANN site, Richard has been maintaining this list which is good.

Male: I would like to add just something, in the past it was really difficult to get a registrar that provided these services, especially in the gTLD market, but after one of the big guys made an announcement, actually in one of these meetings, we have probably the biggest registrars in the world that is providing this service – GoDaddy - so this is not actually difficult to get these days.

Luis Diego Espinoza: Okay, any other questions for the panel? Okay, I want to talk about a little bit, ask to some members of the panel about the, I feel that there is some concern about how to enforce the validation. I want to ask you if you have some thoughts about what should be the way to provide this enforce of the validation. We are seeing on the market, on the internet the .tc plug in for Firefox and Chrome DNSSEC validator and now My DNSSEC from Mexico is running on Windows Explorer, but any of you have thinking about this validation to be at operating system level by example or any other strategy to enforce this DNSSEC validation?

Male: I think the key part of this is ISP's part. I think they have very strong infrastructure for any cache, for caching and I think that they have infrastructure to make the DNSSEC validation. It's not a very difficult part for making these kind of things more adaptable in the adoption part.

Luis Diego Espinoza: I want to explain a little bit more my question; it's about the end user. What the end user sees, so Frederico talked about it's more like transparent for the end user and we can think about the, we need to show some kind of key or lock on the screen or red or something like that to the end user to provide some information. At the end of these, any security system should be secure from one extreme to another extreme. It's a good idea to think about the computer of the end user is more like my question.

Male: I think, you know, Windows 2008 has DNSSEC features, so I think in Windows 8 there is going to be DNSSEC plug-ins inside, I think. That's not a difficult issue for the operating systems in the near future, but I don't know the forecast.

Deimon Tencio: With respect to Windows 2008, I was making some research and in terms of policy regarding Windows, you may apply Windows DNSSEC - it's almost mandatory. So any query from the operating system has to include DNSSEC, otherwise they will not work. At least as far as my research, when the operating system does the validation, in this case it will be an internal DNSSEC, that's at corporate level. I haven't seen whether it's done through, whether it's used in DNS queries over the internet.

Male: Unfortunately (inaudible) security information over DNS, I think we still need to push further for more contents signed. From the point of view of applications in the validation, and especially for highly secure situations, to be quite frank, as we don't have the way of securing the first mile, at least only easy way besides 60 and TC that is a little bit difficult to deploy, I still have, at least in my mind, I think it's - and especially from an applications point of view - should do the validation on the application.

So that's why I said that I hope that the ISP doesn't mess with the path. And I don't think that this end user validator will be a complete caching server, just a validator. It will leverage the cache from the ISP, but it will do the validation at the application level, especially if you want to defend from hosting bugs that actually deal with host TXT infections and things like that.

Male: Personally I do believe that DNSSEC supporting (inaudible) server is the solution. I think it's better than the software for programming things. So programming has to respond to so many variants of OSN application things. I think at the first stage of the DNSSEC for deployment it is reasonable for [hosting] the cache DNS servers. That's what I think.

Rick Lamb: Thank you, Rick Lamb, ICANN again. I love Frederica's idea and I really think these are complimentary, both of these approaches. I think both caching servers and ISP adoption or support for validation is good as well as this. I think a subtle distinction that is rather new I think, that we do just the validation on the end machines. I think that makes a lot of sense because that takes care of the whole end to end model and I think it's critical. I'd love to find ways to raise awareness on this because I think that subtly is sometimes lost. But I think they're both complimentary. I don't think one precludes the other at all.

Russ Mundy: This is Russ Mundy. One of the things that we have seen in years of dealing with various ways and types and places of doing validation, is that there is almost no wrong place to do validation. There may be some places that are better than other places for certain situations and one of the things, I talked about DNS check earlier, they have done. DNSSEC runs on this device. DNSSEC runs on this device. DNSSEC runs on this device. It doesn't take a huge, massive, powerful machinery to run DNSSEC anymore. So you need to examine what makes sense for the situation in which you're dealing with. Whether it's customer needs, whether it's ability to use software, whether it's a business structure and enterprise structure, there are lots of good places do to validation.

Luis Diego Espinoza: I have a last question for Deimon, he's from Bank. I'd like to know if this immense world of malwares, virus attacks, what could be, how could be helpful DNSSEC in all the security issues you have in the bank? How many of these possible issues about security could be helped by using DNSSEC or do you need to always compliment with other technologies?

Deimon Tencio: I believe that in this portion, many of the issues of attacks here, if they're sorted out with DNSSEC, they are, but well implemented. We were talking about how far you have to show the end user about the validation of DNSSEC. Should this be part of the application or of the OS? I think it should be in both. Why is that? Because attacks to OS is the first thing that they do. What do I mean?

If the application were the only validation, it is very easy for hackers to try and to receive the plug in where is controlling in our explorers and fake it. So the OS natively would need to validate that query in DNSSEC as a mandatory requirement. So at the beginning when I was talking, I was telling you that it is important for companies such as Microsoft, Apple and others to include in their OS DNSSEC as a way to validate in the OS as a baseline.

In this case there will be many issues sorted out as to internet attacks. If we make use of the signature of DNSSEC, the security mechanisms would be put in place in security systems, in email servers, *etc* from the OS. So services would be safe from the very beginning. Example - today many companies have proxy servers for browsing. In major companies this is the approach. If DNSSEC is validated, we can rest assured that all customers behind the proxy will send their query to the right destination address. So I think it is important for the validation of DNSSEC to be in the OS, and so those applications that are believed to make a question to main resolutions should be also set up. I don't know whether I have responded to your question or not.

Luis Diego Espinoza: Yeah. I would also like to know what is the share of things currently in place in the internet world as to phishing and attacks requires something else than the DNSSEC and what else could be required. Would you please expand on that so I can pinpoint your question? DNSSEC is a tool, a supplement for security but from the standpoint of the bank, there are many other things that need to be considered apart from DNSSEC. You could think that DNSSEC is a very important contribution or regular contribution or without any contribution as to the challenges of a bank in the internet banking and which context would it be?

It is a good contribution for bank security. The most common attack that I explained is phishing. It takes the user to affect sides so as to gather information. This is used for validation of the user in the transaction of the environmental bank. There is practically no other way to commend some of this account if you don't capture information of the client [for] the user and the password and in this case the information used, as there are multiple factors like token key, account. So all of this is information used by the hacker to enter bank accounts. How is that achieved? One, by installing applications into the computers that capture information or by using phishing.

If DNSSEC on the client's side let us validate the side we're at, we will be able to know we are on a site used for phishing and when I am not. If the client is clearly shown that the site he or she is getting in is risky, they will not include their information or see their credentials exposed to log into the bank. But if this validation is done and the user relies on the fact that the user is a safe side, he or she will introduce the information. In this case we would be highly reducing any intended miscapture of data.

Male: Do you plan that My DNSSEC will be available for the community or will be a product? What would be that?

Roger Castillo: At this moment it's an experiment; it's a BETA version. I'm sure it could be a very helpful tool for the public. I can be somehow sure that it will be available. I can't tell you when, but I think it will be. Having a little bit of what the engineer said, I think DNSSEC tools and everything has to be complimented by education. The most clear example I can think of now is, for example, the .B.Br zone in Brazil, it's safe haven because all the domain names there has to be signed. The end user needs to know that because he needs to be aware that when he visits a .B.BR bank site and he needs to look for the DNSSEC okay valid indicator to be sure that it's not a phishing site for example. Or maybe the operative system of the proxy server wouldn't let him at all visit that site. It is not currently signed, but that's because, well, that's why I think education is very important for DNSSEC to be adopted.

Luis Diego Espinoza: Any other questions? The last question, maybe. Yes?

Male: One question that I have in terms of the browser plug-in is whether not it is validating all of the links on all of the DNS on the page, or is it just the URL bar? Because many website have links that go off elsewhere and they can also be hijacked. I was curious if the plug-in did every name lookup on the page or just the one at the top.

Male: Just the one at the top. The plug-in will validate it when you click on the link.

Male: Okay, thank you.

Luis Diego Espinoza: I think this panel was very productive in terms of we have many input about what is happening in browsing, for example, what is happening in Mexico and what the development of this group of DNSSEC users in Colombia is great and what is happening in Korea about the implementation with DNSSEC. We have an idea right now about what is happening in these [stages] about implementation and I feel there are some common concerns or common thoughts about this. It is a work in progress. It has many things to do and I feel that the enforcement of some of these technologies could be needed in some point. I want to thank you all for participating in this panel. We are on time right? Thank you.

Julie Hedlund: Thank you very much, Luis Diego Espinoza, for running the panel so well and all of your excellent questions and for keeping us right on time. At this point we're going to ask the panelists to step down and we're going to turn the floor over to Dan York and I'll get his slides up while we're doing the transition here. Now please go ahead, I just want to introduce Dan York. He is the senior content strategist at the Internet Society, ISOC and I'll turn it over to you, Dan.

I just want to introduce Dan York; he's a senior content strategist at the Internet Society ISOC and I'll turn it over to you, Dan.

Dan York: Alright, thanks Julie. Since I'm a panel of one, I decided to stand up here and give you a little bit more dynamic, I mean, somebody up here in front of you rather than just sitting at a table. As Julie said, my name is Dan York. I work for the Internet Society. How many of you have seen the Deploy 360 program that was briefly mentioned? Alright, a few people here, a couple folks. The Deploy 360 program is a new program that was started by the Internet Society about two and a half months ago, we brought it online. I join ISOC in last September.

The project was created to look at how we could accelerate the adoption of IPv6 and DNSSEC primarily by looking at how can we find the resources that are out there and the content that is available that can make it easier for people to go and deploy these technologies - what's out there – and finding content that's there and creating new content.

What I want to talk about today is a bit about what we found as we were developing the DNSSEC side of the site and looking at what were the major pain points for users - domain name holders, the people who are registrants - what were the pain points for operators, for infrastructure providers, for developers, for enterprises? What were the pain points and how could we take them away.

It was interesting to look at where we are because as the charts have shown, we've seen a great amount of growth in DNSSEC and it's actually quite easy to go and now sign domains and get them out there, but there is a good bit of work still to do and I'm going to talk a bit about that. Our site has been primarily focused not so much the "why" of DNNSEC but on "how" and how you get to doing that.

The first one was a question the panel echoed very well this morning which is what is the user experience? If I'm just a user and I'm going to be starting to work with DNSSEC, what is the experience that I should have? We talked about icons. you can see on the slide here is the, I'm using the plug-ins and Chrome and Firefox from the cz.nic folks. Is that the right user experience that we should have? Should we have - there is a good question, I think the gentleman from the Netherlands raised that back here too, what should the experience be? Should we show somebody an icon or will this just overload the user experience and be yet one more thing for them to ignore or click through? Should it be just the experience we get back with the site failed?

We saw that, that's the other approach is just give back a server fail and you don't get the response. We saw that as Jason Livingood will be talking about in his Comcast experience a little bit later, you know, we had the challenge with Nasa.gov had the keep issue there, all of the folks on the Comcast side were suddenly getting back a DNS error. They couldn't get to the site, but yet if they took out their mobile phone they could go to that site. They saw it was working so of course what they did is they jumped on Twitter and blamed Comcast. That was natural, right? They had no indication that it was some other larger issue. So the question comes in is from a user experience point of view, is there a way we can send back another DNS error that would say that the browser could indicate that the issue, the reason why the site is not visible is because there is a DNSSEC failure.

What's the user experience? Certainly something that we need to be thinking about in terms of how DNSSEC is really out there in large scale deployment. I don't have an exact answer because in truth, I like the little key icon, but I'm a DNSSEC enthusiast. I like doing this. Would my wife care? No, this would just be clutter on her browser. If we pop up warnings like we do with SSL, how many people click through the SSL warnings that they get on their browser? Be honest, come on, more honesty here. Right, most folks just go "click, click, click, sure, yeah whatever, I'm secure." If we do the same thing with DNSSEC, what are the odds they're going to do the same thing, right? Yeah, same kind of issue we're going to see there. So we have to think about what that is. Next slide, please.

The other question that we had is the DNSSEC validating resolvers. If you've got domains that are signed, you've got applications that might use them, who is doing that resolution? We talked here about should that live at the end user site, should it live, and by end user I mean somebody who is using a laptop right here. So somebody who is right there. Should it live in the ISP infrastructure? You know as Comcast rolled out its DNSSEC validating resolvers, instantly all of those customers now have DNSSEC validation protecting them. It's just baked right in the infrastructure. Sweden - I've had multiple people now telling me that all ISPs or almost all ISPS in Sweden do the validation of DNSSEC right there, so there is nothing that the end user has to do.

As the gentleman here was talking about, it would be great is ISPs would at least pass the DNS information back to the end user's system so the end user could do something with it if they wanted to. If we have applications that will consume it, can they get there? We have to look at how do we do this. Again, what's the experience? Should it just be baked into the infrastructure or should it be something that somebody chooses? The thing I have on the screenshot here is from the cz.nic plug-in where you can choose if you don't have ready access to an ISP DNS validating resolver, you can choose what you want to use.

Do you want to use cz.nic's validating resolvers or [OARC's] or in my case I run—has anybody seen DNSSEC Trigger? THE DNL lab's folks did a nice job with that packaging unbound making it so you can just install it on your laptop and you can have a local DNSSEC validating resolver on your own local system. I'm running that on my system and it works quite well for that, but again, we're not necessarily going to get the average user to go and install that on their system. It needs to be something that as the gentleman was talking about, it needs to be baked into the operating system at the lower level or something like that. So, that’s one question. How do we get more DNSSEC validating resolvers out there and where do we do it - at the ISP level; at the local level? How does that go?

The other part is how do we get developers using DNSSEC? The good news here is there’s a whole lot of libraries. We were, I was presently surprised when I was building out this page of our Deploy 360 site, looking at the number of different libraries out there in a variety of languages in C, Java, Pearl, Python, Go, Erlang, all sorts of different libraries out there that had DNSSEC in it. So if people are interested, if developers want to do this, if they know what is involved, they want to work with that, there are libraries out there. We need of course more. We need to have it baked into some of the more just basic libraries that are there. We need to make sure that some of these support the pieces, but at least the good news, is there are libraries out there. And we need to encourage developers to look for those libraries, look at how they can use it and get it working in that regard.

The other piece, as I mentioned earlier, I’m an end user. I hear about this DNSSEC thing, I want to sign my domain. Where do I go? The good news is that since the time that I made this screenshot to send it into ICANN, Richard updated his site and there are a few more on here, like now there are two registrars that will let me go and sign .com names. This is good, we’re moving up. We’re getting there. We need more of these. We need this list to be so long that Richard stops maintaining it because it’s just a *de facto* thing that registrars will go and just let you have DNSSEC signing. I love the fact that in .br you’re auto signing all of the domains. [Binaro] over in Sweden is just doing that. You register a domain with [Binaro] and boom, it’s just all automatically signed. There’s some of those who are just doing it, but we need to make this list a lot longer.

I would also say again, I’ll put in a pitch, if you know of registrars who are supporting it please contact, go to this page at ICANN, there is an address on there. Or if you’re here in the room today, Richard Lamb is right there. You want to hold your hand up, Richard? Right there, go bug Richard. Let him know and he can add you to this list. But this is a key thing to help other registrars see what is there. A key point is once you've found a registrar, I want to go back again, what's the user experience? It varies widely.

Now GoDaddy actually has one of the best implementations I've seen in looking at the various different registrars in terms of DNSSEC because all it is if you buy their premium DNSSEC, which is a few dollars more a month for five domains, you get this little on/off switch. It says there "Enable on or off" you click "on" and you enter the email address to which you want reminders whenever they roll a key. Boom, you're done. Your domain is signed, it's all up and good and everything else. Now of course this is not as good as the automatic signing of it but if you don't have automatic signing of it, this is a nice step. Click it once, go and do it here.

Dyn DNS, they have on their managed hosting side, they have here again it's just a simple thing to say, "Do you want to go and add DNSSEC? How often do you want the key to expire? What size do you want it? And email me when there is an issue." Again, very simple end user experience. Dyn though is a perfect illustration of one of the challenges we have in the registrar space which is that we use the term "domain name registrar" kind of loosely. We talk about it as a place where you go and registrar a domain. But in fact there is a registrar function and there is a DNS hosting function and the two are distinct and we, in our terminology, we're kind of a little sloppy with that. We talk about a registrar doing all of this. But in fact, and even on Richard's list, many of those registrars support the registrar function which is they will take your DS record and they'll bring it up the parent domain, the top level domain. They'll do that for you but they will not do automatic hosting, automatic signing of your domain. You need to use somebody else or roll your own records to go and do that.

I would put out this plea to us as a community - we need to start being careful about that distinction between the registrar function of dealing with DS records and the hosting, signing function that a DNS hosting provider will do. Like Dyn DNS, they have their DynECT service which is fantastic. They also have a DNS registrar, DynDNS. But if I want to register a domain and have it fully signed and can register it here, sign it here, I manually have to copy and paste the record from the hosting web interface over to the registrar interface and I'm not just picking on Dyn. A lot of other registrars are doing that same kind of thing. There is a disconnect there between those. We need to make is simpler. Let's go on to another one.

Right here, Russ was talking about this issue; complexity of modern websites. We website is no longer a single HTML page; it's a lot of other stuff. It's JQuery libraries; it's pulling in components from here; it's dynamically loading stuff off of different pieces. There's a lot of different parts to a website and for true validation that the site is secure, we do have to look at how do we validate more than just simply that single URL that we loaded at the beginning - how do we validate all of the pieces that are part of that? Beyond just the validation, the other thing is just from a component-wise. How many people here maintain their own web servers? I've got a couple of people. How many people have them hosted at a web hosting provider? How many people have them off in a cloud provider somewhere - Wordpress.com or Type Pad, one of those? Right, okay.

A lot of people, especially smaller businesses, smaller entities will use domain names which will then go and use a C name record to go out to another site. What happens with a C name in DNSSEC? You run down the chain of trust, you get down there, you validate all of the domain name, you hit the C name, it points out to another domain name. Now you have to go off and run down the DNS chain of trust on that other domain name. You need that hosting provider to be fully DNSSEC signed in order for your domain to fully be signed. There is complexity there - C names. How many people use content delivery network, CDNs? Context distribution networks, several of you. Several of you operate CDNs. Okay, CDNs are a great way for companies, content providers to make their context accessible to everybody in a large scale form, but the CDNs also need to support DNSSEC in there. So those are some pieces that we need kind of need to look at there.

Let's go on to the next slide, the other general feature that a number of people mentioned is there is not a lot of awareness of DNSSEC in general - we have to ramp that up. There is a lot of good content out there. The good news, I think, is that what I found in working on the program with ISOC is there is a lot of great content - some really good tutorials, really good white papers, we need more but there is great stuff out there. We just have to get the word out there, let people know. That's part of what we're looking at. And to that end, let's put up the last slide.

I'll just mention because I'm certainly tight on time here too, the program I talked about is the Internet Society Deploy360 program. It's www.InternetSociety.org/deploy360. Part of our goal is to put up case studies, tutorials, how-to documents, and so one of my reasons for being here is to say to you all, I want your content. I want to be able to point to material you have. I want your help. If you've got some great case studies or something we're looking at now in terms of people who are rolling out DNSSEC, both at a registry level, registrar level, and enterprise level - people who are doing that - I would love to talk to you because we would like to get some good case studies up there that talk about what's involved, whether you're an application developer or an enterprise, whatever, please come and contact me or look at it there.

We're also looking to do more video content, more pieces and so that is what our site is. We're aiming to be a repository of DNSSEC info to help accelerate the deployment of DNSSEC and we'd love to help you. I think that's my time and all I'll say here. If there are any questions, I'll be glad to entertain you.

Male: Excellent, Dan, thank you. Let's give Dan a round of applause. Don't go away, I want you to take questions, see if we have some. Any questions?

Russ Mundy: You made a comment about websites becoming more complex, but let's say the managing of the DNSSEC infrastructure is also more complex. Managing a DNSSEC infrastructure is also more complex, so perhaps the program should also pay some attention on how to operate a DNSSEC infrastructure if you're a registrar for example.

Dan York: Perfect, the question was basically how could our program help registrars understand the process. Absolutely, one of my actions coming out of here is to look at how can we add content for registrars and point to the folks, in some cases programs like DNS Shim, some of the stuff with Open DNSSEC, some of the folks who are doing some good work to automate that. Your suggestions would be helpful too. For those of you who have found solutions that work really well for you, I'd love to hear about them so I can help write that, help create some material to pass the word along to other people as well. Other questions, comment?

I'd also like to just recognize Russ here for the work that the DNSSEC tool initiative has been doing a project for a while. They're really come up with some great tools. They are certainly ones and if you're looking for other things too, is anyone from NLNet Labs here? The NLNet Lab folks have some great stuff and the cz.nic guys have been doing some great work too. Alright, thank you very much.

Russ Mundy: Thank you very much, Dan, and if we could have our next panel make their way up we'll get started with that very shortly.

Our next panel, for those that are watching the agenda here, is the operational best practices and lessons from the trenches. We're very privileged to have some of the deeply experienced long-time participating in the DNSSEC deployment activity folks here with us. Most, I won't say most, a lot of people have now forgotten that .se was the first TLD to be signed and so certainly from that distinctive point they have the privilege of being able to give us a great deal of insight. So, Staffan, you're first, please go ahead.

Staffan Hagnell: Thank you, my name is Staffan Hagnell. I was responsible when we introduced this DNSSEC service a couple years ago. Today I'm working with research and development and a lot of work with identity figuration but still I can't leave this DNSSEC stuff because it's very interesting. Today some information about our marketing campaign for DNSSEC. What you need a marketing campaign for DNSSEC - that's what I tried to explain and our conclusions and how we should go forward with this.

So just give a short background on major milestones for us, which are sort of important for this campaign. We signed a couple years ago in 2005. We had users start using DNSSEC in 2006. We call them friendly users because we had no support, nothing so it was very skilled users using DNSSEC. We started a commercial launch of DNSSEC and we said that we shall give support to our DNSSEC users, but we didn't have any tools for management. We had to handle everything manually. Because of that we said maybe this is very popular, we will have a lot of customers. We will have problems because we can't handle large volumes manually.

We actually charged more for DNSSEC in the beginning just to avoid the big demand. But the big demand didn't happen. We got a couple dozen DNSSEC when we opened up this service, but not so much more. We implemented tools so we could handle this automatically and we took away the extra charges for DNSSEC at that time.

A major milestone for us was also that we changed our business model. We went into something more normal, registrar model, in 2009. Before that everyone was customer directly to .se, but that meant we opened up the EPP interface. One very important thing was that we, at that time, made it mandatory for all the registrars that they should be able to remove DS records.

This is because of transfers, the problems that could happen with transfers when you transfer from one registrar supporting DNSSEC to a registrar that doesn't support DNSSEC. So we said that everybody should at least be able to remove those DS records because we think it's the importing registrar who will actually have to deal with it and they should at least be able to take away DNSSEC. As I mentioned before, we needed some tool and we started this open DNSSEC development.

In the same time we've been working with high-end customers. We have tried to get government and others interested in DNSSEC and it's been a long job but I think we have been successful. The governments are actually providing money, funding for local governments and others now to implement DNSSEC. We were very lucky with resolve operators which from the very beginning started to support DNSSEC so we haven't put in so much effort in that lately. We have also, just to inform the local community, given out a yearly health check report which is basically health for the DNS and DNSSEC on all the domains, major domains. That's a good thing just to make some focus on how well this is implemented within the community. It's been a good tool for the high end customers to actually make them achieve DNSSEC.

Now a couple years later we still had problems with low number of signed domains. Once we were out speaking to registrars we always get a positive response, they say "This DNSSEC stuff is great. We should implement it any day now." But they never did actually because there was no money in it. The technical people, it wasn't priority enough to implement DNSSEC. So we have to do something with that.

How do you solve the problem? Well, throw money on the problem. That's one way to do it. How much money? Well, we started in 2010 and said that everybody has got a signed domain when the year ends should get two out of 80 crowns discount - that is 2½% discount - on the domain price. What happened? Nothing.

If you see the figures from 2010, 2011, we had 4,000 domains and in that pace it would have taken 1,000 years to get a fully penetrated DNSSEC. We increased the amount of money said "Okay, this year you will get four out of 80 crowns - that is 5% discount on the domain name price - for all your domains signed at the year end. What happened? Well, it wasn't much until the year almost ended. As you can see month 11, November, nothing. As you can see New Year's Eve a lot of things happened. From this curve you can see something strange happened. First a little bump, that's a major learning that this was one of the registrars who started to sign. The ambition was to sign quite many, I think 50,000 something, but they have to stop signing because there was a bug. The bug had been there before, but now when we started to have real numbers it started to notice.

The bug was in the Power DNS. It made something strange with C name records and resolvers started to crash because of that. That's a good lesson for others who are trying this experiment. It's a good thing to inform the community, to resolve operator that you will things happening now and so you don't need the reaction as we get. Some of them were a little bit upset because they weren't informed good enough about this. Once you start to make these kind of changes, it could get to the effect that bugs get visible in a way. They have to stop the deployment, and actually a lot of the resolve operators turn off the DNSSEC validation for a while. Some of them have not yet turned on DNSSEC operation, so we have to work with that. Some did really fast but some have not yet turned on [the resolver].

5% discount is definitely enough for getting things moving. This is the incentive needed. You can see some economy. From the [.s] perspective we think we get a better domain so we think it's worth having this. It's a bug, it should not be six out of 146 registrars. We got now 29 out of 146 registrars signed. Still not all of them, so there are some more work we have to do.

Our plan for this year is to increase to 350,000 out of 1.2 million domains, get them signed. And okay, let's increase the amount of money and let's do it twice a year now. Is this sensible to give a lower price for those who have DNSSEC?

Well, I think we will end up the other way around soon – that those that don't have DNSSEC will have a high price because we will see now that we get more and more registrars running DNSSEC and they will have a lower price and the other will have a higher price.

We will also make it mandatory for all registrars in our new registry/registrar agreement to be able to have not just removal of DS records, but also add change. We will not require everyone to actually provide DNSSEC service, but they should be able to do this technically anyway and then we see what the next step will be.

There was some discussion earlier about this transfer problem and the way we have handled it - I think, has been enough for so long - is that the importing registrar should be able to take away the DS records. What happens is that they not always recognize that they should do this. Now we will put in a new routine where each day we will check out the status of the domain and see if there are any inconsistencies in the domain and we will contact the registrar having problems and inform them that they should do something about this. I think that simple routine helped us a lot with the transfer problem. So that's pretty much it.

Russ Mundy: Great, thank you Staffan. We're going to hold the questions until the end as we did with the other panel, and is Jason next? Okay, Jason Livingood is the next speaker from Comcast. Jason, over to you.

Jason Livingood: I'm Jason Livingood. I'm from an ISP in the United States named Comcast. We began our deployment in 2008. This is quite an eye chart, I'm sure you can't see it very well there, but we started in 2008 right after the Kaminski vulnerability was announced and I think the essential bottom line here is if you have a big resolver network, it probably takes a little bit of time to prepare and test and so on. It's not something you just flip a switch on. As of right now we finished activating or deploying all of our DNSSEC in January of this year. We have validating resolvers protecting over 18 million customers and we've signed, as of today, over 6,000 of our domain names.

Lessons learned in testing in the early phase of our deployment - first is you need to assess whether - from a resolver standpoint - you need software upgrade. In most cases you probably will, although if you're current on your software release within a few months, you'll probably be okay. You should also look to see if your servers can handle the incremental CPU load. Depending upon your resolver and the volume of queries you get per second that peak, that might be maybe up to 10% additional CPU load, but it really depends upon the resolver software. You should really test this extensively and your software vendor should be able to optimize that over time.

Of course network equipment may need to be upgraded in some way. This was one thing that we found needing, to make sure that firewalls and load balancers and so on can handle both UDP and TCP traffic on Port 53 and handle larger DNS responses and fragmentation. It's important to not just look at the servers themselves, but any of the network equipment that traffic passes to or between the customer and the resolver.

And of course from a signing standpoint, authoritative infrastructure likely needs to be augmented. We heard some earlier people talking about this, with the used HSMs or have something embedded in your existing servers. Essentially zone signing can be resource incentive, especially if you have complex domains that have a lot of subzones.

Of course the best way to figure that out is essentially roll up your sleeves, go into the lab and try it out and see what happens, see what works. Try to validate it of course, eventually with production traffic. That's really helpful. One of those strategies is to potentially have one of your resolvers in, say, a load balancer pull and direct a small amount of traffic to it for some period of time and sort of do a bit of burst testing and see what the result is - that's a typical operational tool. And of course if you plan to do this around the same time that you're doing your IPv6 upgrade, it sort of works out from a cost standpoint. We timed both of these at the same time and it was easier to validate upgrading all of our load balancers and servers and so because it was for both purposes. It was sort of killing two birds with one stone.

Importantly look for operational processes that need to be adjusted. This can be troubleshooting processes that you need to follow or troubleshooting processes that you give to a customer care representative that might troubleshoot with a customer - customer frequently asked questions and so on. We also recommend adding a lot of new metrics or key performance indicators. So for example, the number of serve fails that you see, you can set thresholds. So if you suddenly see a spike in them, that probably means go investigate; something is going wrong. And serve fails as a percentage of all response codes, again when you see a change in this very suddenly, it probably indicates someone needs to investigate someone.

When, at some point, hopefully, someone like Google.com or Facebook.com or Netflix.com signs, you may want some temporary adhoc monitors just looking at them since so many of your customers access those domains so many times every day. If they can't access them, they probably pick up the phone and call you. And of course for signing, a number of people have pointed this out, make sure your registrar has an automated process for inserting DS records. It's not fun doing it manually.

Some more recent lessons, these would be at scale, different software vendors interpret ROCs differently. That's nothing abnormal. We had an interesting one where we had a CNAME at a zone apex that was pointing to another zone and it worked, we thought, because it worked before DNSSEC, but afterwards it didn't work so much with one of the main resolvers that we used, but it did work with a bunch of other ones.

What we would recommend is if you have a complex domain with lots of different zones, you might want to test it out with lots of different resolvers to make sure it doesn't have errors. This is probably one thing we learned - it's an opportunity when you have a complex domain that you know has been complex for ten years and you've always thought, "If the opportunity presents itself we should clean up this and try to organize it better." Maybe this is an opportunity to do it before you sign. So do some of your spring cleaning beforehand and simplify your authoritative zones.

We've also observed some interesting things from registries. One example is a very big one that has a premium service. Not you guys, I don't mean to look at you guys. But they have a premium service that automatically turns on DNSSEC signing. But if you downgrade from that service, which is a really cool feature - maybe this is the penalty if you downgrade - it basically causes a scenario where your DNS key and RRSIGS are deleted which is fine, but the DC record upstream is no So that kind of causes a problem for people that are validating. Of course, some recent stats on our authoritative servers for our 6,000 or so domains that are signed - we don't see a lot of DNSSEC-related queries as of yet, but given the state of validation that's not unsurprising.

One interesting stat, which is the last bullet - of the top 2,000 domains that customers query, we see about 1.75% are signed. What is interesting is that almost exactly, not exactly but very closely correlates with the percentage of domains that have AAAAs, so maybe other people are also doing this at the same time they're also doing v6.

I'll come back to the first bullet in a second. The most common issue we see are incorrectly signed zones, usually, almost 90% of the time or more, related to bad key rollovers. We've seen a lot of these for whatever reason in the .gov top level domain. I think perhaps that's due because they have a very good level of adoption, very high level of adoption and it's sort of natural. On the other hand, it keeps happening again and again and again for some domains, so we don't quite know why and we sincerely hope that they mature and improve their signing processes.

One of the things that we've done as a result of this is created something called a "negative trust anchor" or used something called a "negative trust anchor." I'm going to document this in an ITFID in a few weeks. I missed the cutoff for 00 drafts. When you do this, essentially what a negative trust anchor is, let's say that a domain in .gov fails to validate and you talk to that domain administrator and they say, "Yes, our domain is not having a security problem, but we have really mangled the signing. Will you please help us and turn off validation on our domain for a little while, while we fix this." A negative trust anchor allows you to do this by not validating a very specific domain name and it wouldn't affect anything above that. So if you chose not to validate example.com, that does not mean that you're not validating .com.

We put some controls around this so that it is not something that is automated. We require an engineer, DNS engineer to personally validate the failure to, in most cases, communicate with the domain administrator to understand what happens. This obviously does not scale. It's a temporary tactic. It can be helpful to try to avoid getting a lot of customers phoning you, and it probably will be something that is useful for the next year or two as processes start to mature in this area. Ultimately, of course, it is the responsibility of the domain owner to make sure they administer their domain correctly, just in the same way you would net expect a recursive server operator to fix a broken mx record or A-record, they also in the long term won't fix this.

That goes back to the first bullet, which I skipped, which is with any sort of new technology or new deployment, there will be issues here and you should go into it knowing that this will be the case and you should prepare in advance. So for example when you have a major domain have this problem and you wanted to put in negative trust anchor in place, everybody knew what to do. The scripts were in place on all the servers. It took a quick call to say "Go, do it now." And within a minute or two it was done, versus, "Wait, where is that script? Do I have to write it from scratch? Oh I have to get it to all of the servers and then I have to run it. Who is going to do that? Oh, I lost my secure ID file I've been…so on." So having all of that stuff well practiced and rehearsed, potentially even running it as a practice run a few times beforehand is something I would advise.

We had an interesting one, 18 January 2012 we had a validation failure of Nasa.gov and this was the first validation failure that a lot of our customers noticed and it came just days after we had finished fully deploying, validating resolvers everywhere. It also, in terms of the worst timing in the world, well I'll come back to this is a second. Looking at the failure, basically they did a key roll over which was fine. They created a new key and signed the domain with that key. They updated their DS record and the .gov domain, also good. But they did not double sign so basically you had a problem. Chain of trust was broken, we had a serve fail situation. You can see this is some screenshots from DNS Vis which is a tool we use regularly for figuring out what is going on. That failed; kind of a bummer.

How do customers react? I said bad timing. This happened, you guys might have heard of SOPA, so the day of protests on the web for SOPA when Wikipedia and other sites went dark, this happened on that day. So what was really awesome was that for a long time we at Comcast and I specifically was saying that SOPA caused problems, DNS blocking caused this problem with DNSSEC so we're trying to do the right thing and warn everybody about the dangers and ills of some of the effects of SOPA. On the day of protest this failure happens and immediately a bunch of customers conclude that we are unhappy about this day of protest so we're starting to block access to sites and we started with nasa.gov. I was like "wow." This is like a bizarro world that I just woke up in and truly it's a bad dream.

Customers really interpreted this failure as us blocking and even when it was explained to them that it was a DHSSEC validation failure, they still thought that in some way it was our fault, which was really quite, quite interesting. We found this both… there was a blogger that tracked NASA thing, NASA watch. He first reported it and then we had customers on our site saying that we've blocked access to this. And they said, "What are we - China or something?" And then a bunch of people went to Twitter and started tweeting about it. One of my frustrations with Twitter is there is not a way to correct information and as soon as somebody says something people start retweeting it and it sort of gets out of control very quickly. And then people from the news media start calling and wondering, "Hey are you really upset about the SOPA thing?" It's just bizarre.

Anyway, customers will tend to interpret validation failures as the ISP blocking a site potentially or as our DNS servers going down or failing. This is one reason, at least in the short-term, why we think a negative trust anchor is useful because quite frankly we don't like taking a lot of phone calls when other people do things wrong.

Some other measurement data, we've signed 6,000 domains. When I made this slide we had signed 5,000. These are from the VeriSign tracker of .edu, .net and .com DS records. Those big jumps in .net and .com were us signing most of our domain names. We were happy to have an early affect and it was actually kind of fun to see that. That's all I have. Thank you, I'm happy to take questions later on.

Russ Mundy: Thank you, Jason - that was most informative. I just can't resist adding to the NASA piece that at the time that this was going on, there was also a big solar event underway that my wife happened to be reading websites about. The websites were pointing to this problem again as a Comcast problem - not that they were doing anything bad, but that the solar flares had knocked the DNS servers off the air.

Jason Livingood: That was a good one because we did get one inquiry from, I think, someone internally who said "There are these coronal mass ejections and these solar flares, is it true they've taken down NASA or our DNS servers?" I'm like "No, just bad timing."

Russ Mundy: That's another illustration of how customers can badly interpret what's happening.

Jason Livingood: By the way, I should add we got so many queries that day because there were so many events going on like the solar flares and SOPA and this stuff. Because we had recently signed, we put together a white paper and you can find it on our DNSSEC website, which is www.dnssec.comcast.net, or if you just Google for "Comcast Nasa.gov validation failure" I'm sure you can find it.

The reason we wrote that whitepaper up is important. As one of the big resolvers implementers, we knew that we were going to continue to see this kind of thing. We had seen it for awhile and we thought that if there was no visibility in the community on signing practices that this would continue to be a problem. We wanted to create this as an example, put some scrutiny on it and get people focused so that as they started to sign their domains, they made sure that they had mature practices and that they were aware of this as an issue. Otherwise the worry is that people start to sign and then they have these problems and they say "Oh, it's a DNSSEC fundamental flaw and we shouldn't do stuff."

Russ Mundy: Great, thanks. Next on the panel is Ed Lewis with Neustar. Ed, I'm not sure, he may be proud of this, he may have wanted to forget it, but he is the person that I believe did the very first DNSSEC validating resolver many, many years ago. Some of his code is still around in some of the (inaudible) out there. He has been a very longtime, very engaged supporter of DNSSEC in all aspects and is now bringing us some interesting observations of things he has seen out in the world now that DNSSEC is out there.

Ed Lewis: Thanks, Russ. I would say, also tailing on the Nasa.gov incident. I wrote a note to Jason and some other people at Comcast afterwards saying that we've known for a long, long time that someday someone would make a mistake like was made in key roll and the ISPs would pay for it. But I said the thing we didn't count one was social media. I think that's an interesting topic we have to go into now, how to make DNSSEC not make people look bad when they didn't do the bad thing. I'll go into what I'm doing on the next slide.

To give you some background, I've been doing a survey and there is a presentation at Apricot I gave two weeks ago, if you want, I would encourage people to look at that presentation to get more of what I did because I think anytime we do a survey it should be explained—what was I counting? How was I counting and so. To keep this short I'm not going to go into the detail of that.

I should start it out with the reason for this survey is at Neustar we've signed a few TLDs already. We have a couple TLDs running and we're bringing a managed DNS service, LB DNSSEC. We were asked or I was asked, with all of the parameters in DNSSEC, what should we set ours to be? What is going to be our initial set of parameters? What are we going to let customers change to have more flexibility? Because we do cater to customers that do want to change their bits. They don't want to see things hidden from them.

Of the top of my head I said, "I know a lot of how we do these things, here is how I would do it." But to kind of back up my assertions I decided it was good to actually do a real observation of what is going on in the internet, actually doing kind of an astronomical type survey where I would just take data and start seeing if the data meets what I think it should be. That's what the survey is about.

The first thing I have going on here is about the adoption rate. I'm not really trying to measure adoption because TLDs are special people. Currently today there are 80 signed zones. I turned in the slides a few weeks ago. 80 signed zones counts the root zones and all of the TLDs from that, but not counting the 11 test zones. It's good to compare surveys. Some of the surveys will say their numbers are up higher by 11 zones. I just don't include zones that are test only. I really want the operational impact on his.

The purpose of my survey really was not to find the adoption rate and to get an idea of this. I should actually add to that because I have some time, of the 80 zones signed today, 74 of them have DS records, which is a pretty good number, very close. Generally that means that some TLDs have just signed and haven't really gotten to link it up to the root point. They're kind of testing so that's good. Also, actually I'll go through the next part. What I was after is what are the most common choices? I've put down on the slide the most common choices. This doesn't mean these are the best choices to make, but if you look at the TLDs this is what is most commonly done. In some cases it's what I call "a small majority" of zones do it this way.

A lot of people are using, if you're starting off today, RSA-SHA-256 is the algorithm to go out and run with. That's actually recommended in the RFCs and RSA-SHA-1 is more popular but, if you look at the trend you can see obviously 256 is coming on and the reason for that is RSA-SHA-1 was defined a long time ago; RSA-SHA-256 wasn't, and so the older zones haven't converted yet.

The next line is kind of interesting. - the size of the keys, one k, zsks, two ks ksk, this number—these recommendations actually appear in ROC 4641 which is probably the most definitive document on how I should go about doing DNSSEC and that document should explain a bit too. It's six years old and it has recommendations in it saying for the next five years these would be good numbers. The document itself is not trying to be authoritative. It says that very much and its recommendations have all kind of expired, which is kind of an interesting thing that we don't really have a good document saying for 2012 and on, what should we be doing?

Looking at what TLDs do, they do stick to these two numbers and of the 80 that are signed, 72 follow exactly those two numbers. I think that says a lot about the commonality. After that how many keys do you publish? Because size is an issue but we also do rollovers, we [reverse]. Most do one zsk, one ksk at a time. Most TLDS are doing NSEC3 because they are afraid of the privacy or they want the scaling ability that is a sub feature of NSEC3. One iteration and the salts are usually about four bites long. There is a recommendation somewhere to change it every time you sign the zone but some TLDs don't even bother changing it at all. It's kind of been a way, that's a frequency that's really required.

In general DS records appear in the root zone about three weeks after a TLD signs. That's a rough number. It varies all over the place. Some TLDs have never put the DS record in. One TLD actually came up day one, brand new TLD signed and DSed right away. They went right for the whole thing. They had no legacy to support so it went okay.

Now the work that I'm doing, it's not a discovery. I'm not looking at the TLD operation and trying to see what is going on there. There has been a lot of conventional wisdom built up about how to do DNSSEC from people who have work shopped this for years. One thing of .se's credit, their first workshop on DNSSEC was 1999. They did a couple in 99/2000 era. And DNSSEC was actually changed a few times but a number of people have been playing with DNSSEC in workshops for a very long time formulating the ideas that ultimately went into 4641, the RFC on that.

Taking a point where we kind of renew what we…I kind of knew what I was going to find. That's what I'm saying here. When you do that you have these ideas and I want to confirm them. At the end of it I thought two minds on this. One, it was unfortunate that there were no surprises. In other words, all of the work we did in workshops was feeding today's operational experience. No one is really experimenting because we really don't know what is the best size key. There is a lot of theory, but there is no tested practice. No one has seen an attack overrun DNSSEC or under run DNSSEC. We can't say that this size key worked, this size key didn't work. It's all kind of what we think.

On the other hand, fortunately there were a few surprises because that means the TLDs are not taking this lightly. They're going in with a very steady hand and saying, "This is the conservative approach. We're going to go this way." We're all kind of going the same way which means all of the TLDs are operating pretty much at the same level of performance. If you put more security out there you tend to slow down other performance. Security will take time to check everything out.

What is significant in this? The TLD adoption rate, I see here, is about 25% but that's very high compared to the rest of the world. Look at some of the numbers that are out there, TLDs some are 15% some are down less than 1%. The TLDs are very well DNSSEC-engineered overall. These are people knowing what they're doing, especially the ones who have signed their zones. They really know what they're doing.

Are the choices that I had on the previous slide the way to go? Not necessarily, it may not be the best for every signed zone out, there but it is a working example so you can pick how you want to go forward. Do you want to try and do what is exactly right for your organization or do you want to take what seems to be working for somebody else? I'm laying this out there as example to anybody to say you copy this, you may not want to copy this but these are numbers that are actually seen out there in the wild.

You can run DNS many different ways. I know people run DNS many different ways. I look at other things for other purposes. It's a strength of the DNS. The reason why it's so big is that you don't have to do things the same way as everyone else. We let things vary. Delegation really means it's up to you to do what you want down below. You have your choices and you may vary from what is said on the first slide, and I recommend that you do vary if you really need to, but that is an example where we are.

With this set of slides, what I'm trying to do is -when you do a survey, I see how a lot of people do operations and sometimes you say, "This is kind of a curious choice." I'm staying away from naming names. I never mention names of anything in these presentations. I really don't want to point out to somebody like "Hey, you're screwing up," because generally they're not screwing up. They're just doing something for a different requirement. But it's interesting to me to find out what was the rationale. Why did someone choose to make a certain number that big or that small or why does someone make a change every day where someone else makes a change every month or three months? I'm kind of curious of that. And sometimes it actually will feed back as I'm sure some of the operators may not be aware that their choices are using more resources than they really need to for DNSSEC.

DNSSEC can be pretty efficiently run, but if you change some of the parameters and use the wrong size keys, the wrong size number of iterations or you do something every day you should do every day, there is a big impact on data flow and I see this as some of the backend operations that we do. There are a lot of times where I like to talk, some people say, “Maybe if you tune back this number you will be just as secure.” But of course we don’t know what that really is, but you’ll be taking a lot less of a hit in performance in running the system and therefore DNSSEC will actually look better when you start using it. And so my desire here is to see DNSSEC work efficiently and to make sure that at least in the TLD areas we know what we’re doing and leading example for the rest of the DNS, at least a good working example. That’s my comments.

Russ Mundy: Thank you, Ed. Let me ask we give a round of applause to our panel for their fine presentations. Now is the fun part, we heard what they do. Now it’s your chance to ask them what you want to know about what they’ve done or what they’re thinking about or what the problems are. If there aren’t too - oh, Dan is right, first we have some questions up there too. Go ahead, Dan.

Dan York: I was just going to ask—first of all, Jason, I’d like to commend you on the, you and your team, on the technical analysis you did of the Nasa.gov. The whole issue there, that was wonderful and it really was a good, I think, a good learning experience or a document to help all of us with that. So thank you and I hope that many others will use that as an example if they have those issues while we’re all still in this learning phase. Ed, I have a question, do you have a site where you have your survey results or more info about this?

Ed Lewis: Kind of, right now the slides I presented at APRICOT is the best set, as of today I don't know that APRICOT has moved their site into archive mode, especially when I put these slides out there, I couldn't have put a URL out because I hadn't even give the talk yet there. But I would go to APRICOT 2012, look through their agenda, their program that they had. There is a DNS thing on March 1st and there is a video of their presentation. That's the best recording of anything there.

I consider this to be a live work item, so I try to update every so often and I will probably do that again - I can do this at the 1st of the month just to make everything kind of even. At some point I'm going to have another version of this so I'll try to figure out how I'm going to post this somewhere to be a thing you can reference. I would caution too that you have to really see how I'm doing a survey to interpret numbers.

Dan York; Sure, I appreciate that. It's interesting data, thank you for doing it.

Male: Real quick since you mentioned the nasa.gov thing. I wanted to make sure, while we certainly singled out the nasa.gov failure, that is not at all unique. We didn't do it to sort of say, "Hey, nasa.gov, they're not doing the right thing." They just made a mistake and they've learned from it, which I think is good and healthy, but it was just like the right opportunity with all of this stuff coming together to bring some visibility to it. I would say that we see those regularly so it is not a unique event.

Warren Kumari: Hi, I'm Warren Kumari; Google. The way I see it, there is sort of a problem with DNSSEC deployment and that is the folk who actually go ahead and do the right thing and deploy validation are the ones who see the initial set of issues. During the nasa.gov incident there was a number of things showing up on Twitter suggesting people change their name service somewhere else. I just wanted to congratulate and thank Comcast for getting this done and sticking with it. And now the actual question part - we seem to see a number of validation issues with .gov sites do you have any sort of advice for folk doing that and how to minimize this? And also, when are you going to publish the negative trust anchor stuff because that would be very useful?

Jason Livingood:

I'll answer the last one first. The negative trust anchor document is basically ready to go and I missed the window to get a 00 draft in unfortunately, by like a day. As soon as that opens back up, which I think is in a week and a half or so at the ITF meeting, it will publish and we'll ask for lots of comment on it. Mostly we're just documenting a practice, but it's helpful to document.

In terms of the effects, it is unfortunate as an ISP that operates a validating resolver, you sort of get a little bit of the cost of failures in some other part of the ecosystem. But to be honest, it's a little frustrating certainly, but it's not all that different from other failures that you have so if someone has a route that fails or goes down and somebody can't get to a website, they still will think it's a problem with their access ISP and call us. That's not atypical. It's a higher visibility one, at least now, and I think it will improve over time, I think.

The other that thing that I think makes it easier to absorb any incremental customer care volume and so on is that the objective here is to make a more secure internet experience in the long term, and we understand that's one of those things that sometimes there's a short-term cost to that, a short term annoyance or something, but in the long-term the benefits far outweigh that. You've got to play the long game on this one.

Russ Mundy:

I have a few questions up here on the screen and I'd like to focus on the third one. What would be the three most important things that you would recommend to DNSSEC deployers pay particular attention to it now that you've gone through a lot of this yourselves to help those behind you get it right? Staffan, could you go first?

Staffan Hagnell: Yeah, my prime recommendation would be to have a good cooperation between the resolver operator, the local internet community actually. We've been having that and that's been very helpful. When things happen like this roll out and things start to work out strange because of bugs and other things, it's really important to have that tight team among the ISPs and registrars and so on. So have a good connection with all of them and make regular contacts and so on with them.

Jason Livingood: I would say two things. One, make sure that you do a lot of testing, so both in a lab and some early testing in your production network so that you know what to expect. Two - maybe it's three things - two, make sure you have good metrics, so a good way to measure health or sickness, things going well, things not going well on an automated basis so it's not just "Well, it's going okay because no one has called us." You should have good measurements.

And the third is do a really thorough analysis of all of the things that you think might fail and even in that process pull somebody in that might not be on the DNS team. Explain how DNSSEC works to them and DNS works if they don't know that and have them play some what-if scenarios. Sometimes they'll come up with ideas that you might not have thought of, that you just made some assumption.

So think about all of the things that might go wrong and then come up with plans for what you would do to mitigate that, so to reduce the risk of that occurring or to change some plans so it won't occur. And as I said with the validation failure that we see and negative trust anchors, have everything in place so that you're ready when a failure does occur. You should go in not hoping that something won't fail, but instead planning for when it does fail, what will you do? That's a very different operational mindset and it's an important one to keep in mind. Being prepared in that way will help you so that if that thing fails at two o'clock in the morning when half the team is on vacation or everyone is at a team barbecue and they've had a few drinks or something, that it's not everyone scrambling around at 2:00 AM in the morning trying to figure out, "What am I supposed to do? Where is the script?" It's all ready. They've practiced it. They know what to do. That's sort of an Operations 101 kind of thing at scale, but it's important to keep in mind.

Male: I'm considering how to answer the question by saying "DNSSEC is so easy. Don't you live and breathe DCNSSEC?" I think what Jason covered, a lot of the main points, one is—I'd say you start out with, setup your expectations. What do you think it's going to do? What is it going to look like at the end? That's the first thing as the developer, implementer or deployer of that service, where do you think it's going to go? The second thing is as you're trying to get to that point, constantly test, incrementally. Am I really getting where I'm going? But keep in mind too that incremental testing doesn't mean "Does this work?" Will it scale? There are two ways to that, you can implement something that will get you the right answer, but you may not realize until later that just won't handle the load later on. That's either machine load or human load.

And then finally, once you do go out there live, you have to have a lot of the safety belts to make sure things don't go bad. You have to be able to watch and I think, again, going back to nasa.gov, I think that's a really good case where it, what it shows is even if you are watching really well, you're going to get hit with problem reports faster than you could possibly look. If you knew in five minutes because were circling through all of the zones that are signed out to make sure they're all properly signed, someone in that five minutes is going to hit the one that is not working and you'll see an explosion in problem reports depending on sensitivity at that time.

I guess you also have to make sure that you go into this knowing it's a new venture. There is some risk in every technological improvement. On the other hand you have to remember it's necessary if you want to get security. A lot of the things that DNSSEC causes you pain, will cause pain in other ways. Like IPv6, any other use of DNS, anytime you try to increment the size of DNS messages and so on, it's a general problem. DNSSEC is just one of the things coming out to improve the internet and you're going to have to realize it is an improvement. It costs something to get there, but testing an monitoring are two big things.

Jason Livingood: Just to say one thing in reaction to what you said about incremental testing and so on. It's important for someone that say, just now or soon, is going to implement validation that that doesn't mean your work is done. Every day new TLDs are signing and new domains are signing. That will continue to grow and there will be a lot more of that. That means that the ecosystem and your understanding of how the system works, the organism of the network, is going to change and evolve very rapidly.

Male: May I clarify that we haven't had much problem since we began, but once you get into problems you really need to have the competence around to analyze them because there could be all strange kind of things. You must react pretty fast on the problem.

Russ Mundy: Any more questions from the audience? Warren, yes?

Warren Kumari: If I am an ISP, there is a reasonable amount of cost to deploy this - it's not huge but it's not zero. What's my incentive for doing this? Are users actually asking for it? Why am I spending any money at all?

Jason Livingood: I think that this touches on what is the security value add in general in ISP networks. I think it's important to understand that DNSSEC is one part of a larger security picture, if you will. There is not any one magic bullet that solves security. It's one thing of a number of tools that are in the toolbox so to speak. I think from an ISP's perspective the security landscape has changed and I don't want to say dramatically but it's changed meaningfully over the past few years and that's for a few reasons.

There are some effects that I point out which are important. One you have malware and bot networks and this affects more and more customers all of the time. You have things like the Kaminski bug come up and other things. And so it's important to look at security and work in every area that there is a new solution out and focus in these areas. But what all of this has cost in the minds of customers is a much higher awareness of security issues.

We really did not see that a few years ago. This was a relatively new thing where your average customer knows a bit more about security and in fact, importantly, asks about it when they're considering your service. ISPs routinely survey customers to see why did they buy service? And a few years ago it was speed, speed, speed, speed, speed and price. The last few years with the economic price it has been speed, speed, speed, price, price, and price, so maybe a little bit more price.

But in the last couple of years I think about half or so of customers are asking primarily about security first and what features, security features do you have and what things come with the service. ISPs do things like provide antivirus suites for many years and now they're more broadly defined as security suites. We have an add-on that does keyboard encryption to try and prevent key logging.

There are a whole bunch of things and this is part of it, so for example, our DNSSEC effort we created as part of a, we have a whole security program called "Constant Guard" and the engineers very deftly put DNSSEC as part of that so we could fly under the banner of this larger program. And so we explain it to customers and we explain it as part one slice of the pie, but it's a broad spectrum of security protections. And so I think that what I would recommend for ISPs and I think most are aware of this, your customers will be increasingly aware of security and you can make it a part of that because they're buying the service with that expectation in mind. And I think, at least in the United States, we're starting to get more pressure as a network operator to be more overtly focused on security.

I was just testifying in front of a congressional committee about cyber security because there are some bills that are going through our legislation, our lawmakers in Congress about this. There is a lot more visibility in general and it's just a part of the thing that you need to do.

Russ Mundy: Okay, well, let me ask one more – a nice round of applause for our panelists. We're going to give folks a ten-minute break to stretch legs a little bit since we are a little bit ahead of schedule. So ten minutes we will reconvene. Julie?

Julie Hedlund: Yeah, thanks everyone. Our friends at .CR have asked me to let you know that for the gala tonight you need tickets but they're free and they are available downstairs in this building. So if you want to use part of your break to run down and grab a ticket, you can do that. But to be sure to come back because we have a lot more program. At the end of the program at one o'clock you will be rewarded with lunch.

Russ Mundy: So restarting at approximately 11:34.

[break]

Julie Hedlund: Everyone we're going to start here momentarily with the next panel. Please take a seat and we'll get started. Thank you.

Simon McCalla: Good morning, folks. Thanks for coming back and thanks for joining us. My name is Simon McCalla from Nominet. We're going to spend the next half an hour, 45 minutes talking about how we might consider using DNSSEC to protect the reputation of your business. Often as a technical community we think about the hows and wherefores of how we implement DNSSEC and sometimes it's useful to look of it in terms of what the consumer might think of DNSSEC. Why a business might implement DNSSEC and what is has to gain from that. I'm thrilled to have two fantastic panelists with me today. Immediately to my right I have Bill Smith from PayPal, as you know has been very, very progressive with DNSSEC and we also have Cilliam Cuadra from Banco Nacional de Costa Rica. Welcome both of you. Without further adieu we shall kick off Cilliam and hand it over to you.

Cilliam Cuadra: I will do my presentation in Spanish so if anyone knows translation.

Julie Hedlund: Do we have our interpreters in the back? Yay, thank you.

Cilliam Cuadra: I would like to thank the committee for inviting the National Bank to cooperate with this. The reputation for the bank in the world is critical. It is the business as such, our business depends on the reputation that we can have and the different services we can offer our clients. The very existence of reputation for an organization is services makes customers or clients to come over to use our service and if we talk money, if we say that clients will invest their trust in our organization for their money reputation is critical. That is why for us DNSSEC implementation has a positive impact on a series of control elements that we implement in the light of the threats that we see.

What are the threats we see in Latin America? Basically most sophisticated banking malware. We used to see that phishing was just a simpler way to go. Now it is implemented through sophisticated malware working system files in just one activity or process it reactivates an attack with multiple targets, multiple countries involved and this is not as it use to be in the original phishing. At times of crisis they have becomes more creative and effective.

Effectiveness with companies is also associated to these groups. This is a real case in Latin America. We are getting some emails or information placed in high transit sites. For instance, the site of this malware is a site used by Latin America people and they were told that in order to activate something in the page they had to update Java. So the reputation of the bank goes beyond what we can get a hold of. In our world we need to have a tight rein so that when the client falls into any of this fake actions that they are prompted to do, not to have an impact when they get to our site. When the user say malware code to make a change in all of the Costa Rica and Chile banks mostly, including Yahoo, Hotmail accounts so that they can use an advantage that we have determined in the security world. People are using email accounts to store their passwords and bank accounts as well as bank statements.

Let’s see what is going on. When people receive the installer they feel it’s something normal and if we see how much we get from antivirus and security vendor stuff, just 20% can determine that the malware item is a major tool that requires some concern. As the malware is developed in Latin America for Latin America most vendors are pretty slow in determining that is malware has an implication on the rest of the world. They are mostly working in namely the US. A malware with an impact on the US bank would have a check in ours but in the case of Latin America we have managed to determine that it takes a week for security companies to determine that this is a malware piece. When the pages they design are just like ours. So the combinations they are using are quite effective.

What does that DNSSEC imply in our environment? We have looked at this for a long time. In 2008 we have the finest strategy to have a check on the number of aspects associated to security in our internet banking services especially in the reverse authentication area. It is a major check to define that our side is the official side. We have defined the DNSSEC strategy at our bank plus extended validation certificates as the means for the users from the stations to be able to determine that they actually were our site. What did we find in DNSSEC? We found some limitations in the fact that they user needs to get to know how it operates. For the user at that point in time it is not something intuitive so we have obtained a significant advantage with DNSSEC but we need to have a campaign in the future to make users aware of the meaning of this control and the advantages for the user to continue trusting in our reputation that we have nurtured for years in order to show that we implement state of the art controls.

The deployment up to now has had some impact in the technical world such as the people here but we have not achieved the fact that users interpret, think that this improves our reputation. So we will work on training. That will be the next goal. We already have a way to go forward and make customers aware. How do we believe DNSSEC will protect the reputation of our site? It will show clearly that the customer is at the bank's electronic services site. It will provide an extra way to guarantee that when they enter the site they entered the right place. And we will add an extra protection layer that Costa Rican authorities need to look into yet because there are legal issues and there are compliance issues. Compliance is very important for banking. We have to respond to our concept called objective responsibility and someone who operates a bank or trade electronic side is liable for this security in this site. It is very major thing for banking and we believe that DNSSEC will help us work with his and help improve the reputation with the authorities associated to the performance of our organization, validated with what clients can see.

We will also provide the possibility of preventing mass attacks. As the national bank is leaving this DNSSEC browsers we will get many other people, banks to follow and they will find an advantage in the protection of the reputation and they will follow suit. Finally it will let us continue in the pioneering place in implementing controls. This control as others we lead the path and this also is something that builds our reputation as a leader organization in security. Thank you.

Simon McCalla: Thank you, Cilliam that was fantastic. One quick question before we hand it over to Bill, how have you managed to gain awareness amongst your users of your site and how are they responding to that awareness campaign.

Cilliam Cuadra: Well, we are just beginning with our awareness raising campaign. The bank has deployed an interesting strategy in the social networks. We believe that we will have a significant impact as users join this campaign. We will use the social networks to give information to the clients so that they know how to do the checks and install the plug-ins and work with Chrome. We have been also working with a Monterey Institute people on DNSSEC so that clients or customers are told how to make this validation. We are going to present some instructions on our WebPages so that they can still trust us and we can take advantage of the technology that exists in Costa Rica.

Simon McCalla: Are you finding that this is giving Banco Nacional a competitive advantage over other banks?

Cilliam Cuadra: Well, we hope so. At present we represent a significant organization, a big organization so we have always tried to take advantage of every opportunity and we believe that we are doing that in this case.

Simon McCalla: Terrific, thank you very much. I'll hand it over now to Bill Smith from PayPal. Bill, over to you.

Bill Smith: Thank you, first I'd like to thank our hosts. This is a beautiful country and the people here are fabulous. I'm also pleased to be on the panel with Cilliam and Simon. Just like Banco Nacional we too are subject to a large number of threats and attacks. They ran from DDos attacks, phishing, spear phishing. Basically you name it, we see it. I'd also like to preface my comments by stating I am not a DNS expert. I am not a security expert. I happen to be in country and have been asked—this is not the first time—I'm being asked to present on our experience with DNSSEC.

Any errors or remissions in my remarks are mine and should not be attributed to the company or the people that provided them to me, the information to me. Our business, PayPal's business is based on trust. Without trust we have no business. It's also based on the internet, without the internet we have no business. We do not have a bricks and mortar fall back like many companies do. This trust has to go to the consumer. The consumers must trust us and to that end, to support that trust we internally employ a number of mechanisms to insure the security of both the information and all of the transactions.

As a provider of the service on the internet we rely on the internet and all of the things sort of below our service level. That reliance takes the form of a trust of chain, sorry, chain of trust from source to destination. And also at all protocol levels and the services that we employ into providing our service, that goes from routing, DNS, HTTP, certificates, certificate authorities, the policies around them, etc.

With that as background I'd like to describe our experience with implementation, encourage you to begin implanting if you have not already. One of the things we had to look at when we began this is - how many domains do we have and how many do you have. We have, and I may have this wrong, the number 1,100 may in fact be 11,000. That could be an error in my transcription of a message that was sent to me or a missed zero when it was typed. I don't know but I didn't have time to look into that when I discussed this privately with a former member of PayPal. They said "You can't have only 11; it's got to be 11,000." Whatever the number is, it's large. If you're going to sign DNSSEC it's not one domain you're likely to sign. You're going to have to sign, in all likelihood, a large number if you are a large corporation.

We have about 50 of those that are actually active but as you all probably know, we end up, as do others, having a number of domains that come into our possession and we also have marketing creating what we consider, or what some of us consider, random new domains and there is no oversight with that. Some examples, you know gems, PayPal does stuffformoney.com, operation fruitcake, and there could be any number of them. In the foreground we determined that we needed a process.

We didn't really have one and that turns out to be somewhat, it's not impossible but it is somewhat difficult because we in the security space seem to be limiting marketing's ability to do things. They like to go do things fairly quickly. We tend to slow them down, is sort of how we sit it. Because we are so security aware at least there is a recognition within our company because we are transferring money even in the marketing departments, they need to employ some best practices there.

We're in the process of doing some moving, basically all of our parked domains to are registrar with redirects to some business sites. Basically one of the offload, some of our DNS, we didn't want to do with things like .Asia as an example, these are things you'll need to consider. These required internal process changes on our part, start all of the domains parked and no domain can change from the parked state until the live state unless there is some processes followed and the comment there is, right. Usually that happens but it doesn't always. After our clean up we changed our DNS infrastructure to move to dynamic zones, to add automation.

Automation is another thing I'll get to a little later. One of the primary motivators for some of what we were doing, prior to our DNSSEC implementation, was we were preparing for it. We knew we wanted to get to DNSSEC and we started moving some of our things away from the mechanism we had been employing.

Basically what went well for us, generally it was very smooth. We did a phase roll out. We left the critical domains, most important domains toward the end. That gave us operational experience along the way. If we made a mistake with an infrequently used domain or an entirely parked domain that wasn't a problem for us from a business perspective. It allowed the group making these changes to do things. Suggestions; plan your roll out. Some domains are in fact going to need to be done before others. We found that out. You can't just do these in an arbitrary order. Things that went less well, there is a lack of consistent or standard way to upload DS cues. There is no consistency between TLDs. Not all of them have implemented yet. Certainly as I understand it in the CC space. And then the DS key updates are entirely manual, which does not lend itself to be either flexible or scalable. When you have 10,000 domains if you have to update DS keys manually that is a significant effort.

The surprise we had was that everyone wants to use DS keys. And then what would we do differently? We might separate signing systems from the zone masters and do signing as a proxy in the middle but for us that wasn't an option at the time and now it is, so we might change that - something to think about. How long did this take us? It took us about eight months, roughly, give or take one month probably on either side. Again, pretty smooth, little drama, phase roll out was essential. Signing wasn't difficult, changing the DNS setup from static files to dynamic zone was somewhat more difficult. If that's something in your path, know that.

The other thing is we knew that DNSSEC was coming and we factored that into our infrastructure improvements way before we began the implementations. So as we were implementing our infrastructure along the way, knowing we were going to get the DNSSEC some decisions were taking that made that implementation easier. Are we done? For the most part we are done. We are doing some of the same work on our other areas but in terms of all forwards, we’re done. I’ll admit, I have no idea what that means but I was told it was important.

The future; for us the challenge now is key rotation. We’re setting it up and we’re starting to do it. This is not necessarily a security concern; it is more an operational concern. Will we have the people in place who know how to do this when we need to do it? If you don’t, the line there, if we do them rarely then nobody knows how to do it.” If you do them too frequently they’re all manual that’s very time consuming. We plan to rotate these keys about three times a year and in order to maintain operational efficiency we believe this is going to put a fair amount of stress on the DS key upload and hope that there may be enough upstream pain as a result of this to encourage a move towards a more automated process, which we think would be a good thing.

Conclusion, so basically this is not as hard as we might have thought. I suggest it might not be as hard as you thought. The sort of flip side of that is there were also times it was harder than we thought. Some things that we thought would be easy weren’t. There are going to be some surprises. You’re not going to think of everything. Planning is going to be essential. Start early; talk with your suppliers because we had to get others in basically our supply chain to begin doing things in order to support our requirements and requests. And so in essence - do it now, begin, don’t hold back. For us DNSSEC is a critical component because if a consumer believes they’re coming to our site through a DNS look up and they actually go someplace else, that’s a real problem because we will receive the blame, not whoever supplied the IP address or the actual site that they went to. It’s going to come at us and in order for us to maintain our reputation we will have to make good on much of what happened. Thank you.

Simon McCalla: Thanks Russ, that’s fantastic. A question for you, a lot of us in DNSSEC and awareness raising world were quite excited when we heard PayPal is going to sign and we were excited because we felt it would help raise awareness and it would raise awareness down at the end user level. This is taking DNSSEC away from the techies and the registries and turning it to something that was a real value being such a big brand. My question is how is that going? How is going in terms of raising that awareness with your customers?

Bill Simon: I doubt any or very few of our customers could spell "DNS" let alone DNSSEC. I'm not sure we're ever going to get much penetration into the consumer space in terms of a spec or implementation. For us we intend to approach the consumer more broadly. We participate in campaigns like "Know your browser" so update your browser on a regular basis, things like that. I doubt—I think very few of our customers actually are aware that we do DNSSEC. I would say our efforts on this in terms of outreach are to communities like this and others who have not begun to think about or are aware even that it's an option.

The technical people do know it but the business people do not. Similarly if we go to executives and talk about just the DNS generally, they have no idea what a registrar is, who theirs is and what they would do if there was an attack on their system. Frankly, it's mindboggling that people are, companies who rely so much on the internet are aware of it. So, don't think there are a lot but the people certainly in our supply chain and we do business with are aware of it. We make them aware of it. That, I think, is how we see the outreach going.

Simon McCalla: Something you just mentioned there actually, a nice lead in to my next question for both of you really, which is the flipside - how aware are the folk within your company? Is your Board, your senior manager, your chief exec are they aware of DNSSEC and do they understand its importance? Or is it something that is considered something for the techie guys?

Cilliam Cuadra: In our case we started based on the requests of Nic NICCR and we started working with management. We achieved a good level understanding at the technical level. We tried to talk about the advantages of DNSSEC with management but from their own perspective this is still difficult to grasp. They don't understand the benefit is for the user in full. So we had full support for implementation but from the point of view of governors I think we have made partial achievements. We still need to explain to management how this can improve the reputation of their bank vis-à-vis the eyes of the user. And how this can boost customers trust, we still have to work with management. We need to engage in this effort and we can do that provided that organizations like this one give importance to these kind of control measures that we are presenting today.

Bill Simon: We are fortunate in that because we are a money transfer agent, to pay particular attention to security up and down the line, risk management. As I stated at the outside our business relies on that we do that. So management, senior management is generally aware that it is an issue. Whether they are specifically aware of DNSSEC - probably not, though some may be. But they are aware if someone through the security groups come up to them and say "This is important." They believe it. We are fortunate there in that we have their ear and I would say that's something that would be, if your company isn't quite as security conscious, many on the internet are not as conscious as I would say some are.

That's not a bad thing. You have different business models and that's okay. But if you could find someone in management or senior management who understands the issues and basically is your ally I would suggest doing that because it may take getting someone at the top level to understand these issues. I would point to SOPA and PIPPA in the United States as examples where many executive members of congress had no idea that this legislation might impact security in any way shape or form. When it was pointed out to them even then it wasn't a major consideration. It took a groundswell, which I was very happy to see.

Simon McCalla: You're getting quite good at predicting my next question, you've kind of partially answered, which is great. My question was going to be, if there were folks out here in audience who were thinking about implementing DNSSEC and thinking, "How do I raise awareness within my own company and get people to support the necessary time and resources needed to implement DNSSEC?" What would be, either of you, what would be your sort of top tips to get them to do that?

Cilliam Cuadra: Tips for the organization and for the implementation of DNSSEC, of course, find the technical resources. It is extremely important to gain the technical knowledge. Although some rollouts seem to be highly successful on the technical side, for other organizations implementation of DNSSEC might not be so easy. So, my recommendation is to work well on planning. I think that there you have an essential issue. From the technical standpoint we made a lot of efforts and we also recommend that you partner with your providers, with your suppliers and those that work in the local organizations of the way their addresses and their domain names also help you with the transfers.

Although it is true that there is room for success, be ready because there is still some part that is not automated so you should consider all of the operational aspects that will have to be addressed. And that there are certain ceremonies and other elements involved in that regard have very specific schedules and time frames and they could have an impact on your schedule, on your timing. So be careful with that.

Something that is extremely important is an outstanding task for us and that is whenever you engage in this process try to address this issue as a business value added issue so that you can get more support. Everything can run more smoothly, your suppliers that are not yet involved can become engaged because they also see that this is something that has value to them and you have to have a well planned implementation and that is where the magic lies. That can issue a success.

Simon McCalla: Great, thank you. We have a few minutes. I just want to open up any questions from the floor to the panel that we have here. It sounds like we've got one from the chat room.

Russ Mundy: A question from the chat room, how long did it take the bank to prepare and plan and actually implement DNSSEC?

Cilliam Cuadra: Good question. We work with Costa Ricans in NIC. They did the offer and we sped up in our implementation with just working with domain - the main section of the main organization such as PayPal. We have many domains. We have more than 120 domains that will protect such as PayPal, we have that notion of protecting. Many of the brands that we believe can be used with some darker intent have. Our intentional implementation was the main transactional domain.

We work a lot with NIC specialists. They have a great level and it took one full week of planning and preparation and the implementation in the last week, one month per domain. If we had done this for all of them we believe it would have been much lengthier but the location and being small, the main organization in Costa Rica improves communication and supports that way of action. If Costa Rica people and the people allocated to .CR that's a good time to do it. General experience can help you achieve a similar term if you do it in the same thing.

Rick Lamb: The only question I had for both of you is this is wonderful work and so many people are looking for examples. Obviously this stuff is all done internally but do you foresee any time in the near future that you would be willing to share or have your engineers share an overall system diagram, maybe, of how you went about implementing your signing systems?

Bill Smith: We have talked about this internally Part of it is finding the time to actually do that and how would we do it. You can barely read probably but the slide says, “Not so confidential or proprietary.” We want people to know what we have done and our experience. It really is a matter of getting the cycles to do it. It took me, no fault of the people who needed to provide me the information, but it took me over a month to get the information that I got internally because they were so busy doing other things. Similarly, I was busy, my job is to attend these meetings and represent us. Absolutely we would like to do that and I’ll take that back inside and encourage us to do something.

Cilliam Cuadra: Same thing in our stand, we decided to work with this. The advantage with Costa Rica’s NIC is that it is a neutral organization so there can be trust. When we first started in this process it was like being the first one, you know, using some competitive value an advantage but we know that the financial system in Costa Rica will improve if we all get involved. From that stand point there is an opening to cooperate and to improve the system as a whole because of the system creates trust, we have trust as well.

Simon McCalla: We have time for one more question.

Male: I was interested whether PayPal or the bank have seen anybody else in your supply chain adopt DNS following your leadership? Anybody you interact with.

Bill Smith: Given that I don't operate in that area, I don't know. I know that in our "supply chain," the people we rely on for providing services. Yeah we had to wait in some cases until they actually began offering the services. In that sense yes, in terms of more horizontally, I just don't know.

Cilliam Cuadra: This is a recent implementation. We have just completed it. Yesterday we had other people interested in implementation, we are brought in together. In relation to the typical question as to how we do it, how we can continue and many of the questions are based on the fact of what is DNSSEC that is the question we get the most. But we believe that there is a long road to walk and many people will follow this DNSSEC path.

Simon McCalla: We've been here some time. We'll close the panel now. I just want to - can we please offer our thanks to both Bill and Cilliam for really useful presentations? Thank you, guys.

[Applause]

Julie Hedlund: Thanks everyone and we're just switching slides. If I can ask Luis to come up we'll get sorted momentarily.

[background conversation]

Julie Hedlund: So while our slides are coming up I want to welcome Rick Lamb from ICANN and you've already heard if you've been in this workshop all day all of the various things he's been involved with. And of course Luis Diego Espinoza from .CR who kicked off our first session this morning and is now back to talk about, the two of them will talk about DNSSEC signer implementing hardware. Why don't I go ahead and turn it over to whoever would like to start. Okay, Luis.

Luis Diego Espinoza: Hello again. This time I want to talk about the hardware implementation we use for our signing process. Rick will be indeed with the dates about the technical things. I want to talk about how looks our system and how it fits the DNSSEC signature in this system. We have web based for customers, for registrants with development in Java. This site submit all the transactions of DNS transactions of all operations: add new domain, move domain, modify domain through using an EPP interface to another server that we use with running for it. And in this server we have a script that runs each hour, that generates the zones, all the zones we manage under CR. These zones are for different sectors by example, .CO .CR is for commercial, .FI, and .CR is for financial. This is one of the main focuses in this process of DNSSEC.

After we generate the zones, we verify the integrity and the completeness of the zone file and after that we push it on the DNS server that is a hidden server that publishes the masters and so on. What we do is place a DNS signer in the middle of the process. We generate the zone, verify the [zone] and pass this zone file to be signed. Then this DNSSEC signer provides the .signer files, verify again the completeness and everything that look apparently good. And then after reloading the system. What we use inside the DNSSEC signer, Rick will talk a little bit about.

Rick Lamb: Okay, this is a, you have it in PowerPoint, this is a moving slide. It's just PDF? Oh, the best laid plans. Okay, alright. I'll talk through this very quickly but first of all I'd like to say it was a pleasure and I was very, very impressed working with both Mario, who is in the audience, and Luis on this. So many times people try to do things and it's not until you all work together that you can actually make something good happen. I think this was really amazing. I was very, very happy with this. With that I'm going to jump into key management.

This is a picture of how the key management works. Basically the ZSK's are generated first. They're on the right hand side for you guys. So the ZSK's are generated first in a TPM. TPM is a trusted platform module. It's a chip that comes in the majority of laptops out there now and a lot of server machines as well. This is using cryptographic hardware that exists already and that's the key point in this. The ZSK's are generated on a machine with a TPM chip. The public half of those are transported across to an offline secure environment that actually both generates the KSK's and then signs those KSK's, signs the ZSK's with KSK's and pre generates DNS Key-R-sets for the next few months or year, what have you.

This mirrors very much what we do at the root. Not that that's any particular model to follow but this really does mirror the approach. And the advantage here is that the ZSK's are generated on one system and the KSK's are on a separate system and only public material, no private key material goes between the two sides. That's the advantage in this picture and I think that was actually Luis' idea to actually do the ZSK's this way.

Once these R sets, DS key - once the KSK has done its job those sets are transferred back to the online signer. Then on the online signer, I mean, unsigned zones come in. This is typical bump in the wire design - signs the zones with the ZSK and a sign zone comes out. Next slide please. A little about this, I've done a number of trainings and one of the problems is always the crypto part of the picture. Do we pay for a $20,000 box, the thing with the orange button on the bottom that we use at the root? Or do we buy that IBM card that's next to it or what have you? Or do we use smart cards?

This was really good. This is where I think we reignited. It just sounded wonderful. If we can make this TPM chip work, this crypto that comes on many platforms work, this would be great, substandard hardware. It's supported by actually an open source software package that IBM actually releases. It's not fast, that's kind of the draw back. It only does one RSA signature, one 1024 signature per second but if you look at the specification sheet for this chip, it should be able to do ten times more. I'm hoping somebody out there is really interested in taking advantage of this. The other key thing that is very important, it has a built in hardware random number generator.

I don't know if you guys have followed any of this but this has been the Achilles heel, the weak point in so many different implementation in security. I mean over the years it started with Netscape, earlier browsers having problems with it. And most recently, just a few weeks ago there was a paper by—well, referring to two very famous old sages in a cryptographic community, Ron [Rovest] and [Whit Diffy]. The title was "Ron was Wrong. Whit was Right" and it was basically a review of the SSL keys that were out on the net. They found some very undesirable percentage of those keys were based on bad random number generators. I think this is something we often forget about it. For you UNIX geeks, we just read off of [Dev Random] and we assume things are good.

Here is a way to try to solve that problem or at least cover your ass in some ways. I have the picture of the lava lamp next to there because there used to be something called lava rand which is a true random number generator where they had a camera end at a lava lamp and they would take the output of the lava, that picture and use that as a seed for a random number generator. Truly random. Enough ranting.

The final thing that was really nice about the design that .CR came up with in using this open source software is it uses something called PKCS 11 interface. This is a standard interface to HSMs so once you've done this exercise and used this free crypto chip that's built on the motherboards and you've used PKCS 11, the jump from there to something faster, bigger, whatever is a small one. I think that's important. Very quickly because this is kind of a geek group, I figured you guys would be interested. So how do I trust this? Why should I trust this system?

If you follow through like I did and go through all the source code and even contact the author, a guy named Kent Yoder, famous in the crypto area. The way the TPM chip works, it really, it's a small chip. It only has one key that it keeps track of in the chip, in the hardware and protects it. Everything else is encrypted with that. The term of art is wrapping but every other key that is generated is encrypted with that. So a majority of the keys are in encrypted form on your hard disk. Each level of this diagram - I'm not going to go into too much detail - is at some point tied to that key, the encryption key that's inside the TPM chip. When you first look at this - that's the package if you want to Google it - it's called "Trousers Open Crypto Key," you scratch your head and go, "Wait a second. All of the keys look like they're sitting on the hard disk. They can't be. They're encrypted form."

I ask you guys to convince yourself of this first but that's how it's laid out. Each key below the actual key in the TPM chip is encrypted with that key. And every time it's accessed all of the operations are done inside that TPM chip. There are some pros and cons to this. It's the slowest speed for the TPM chip. It's free, it's great but it's slow. I noticed that other people have tried to actually do this before and I think it wasn't until there was a really good, strong reason to do this that we were able to make this happen. I hope we can - I hope .CR is willing to publish some of their experiences at some point in the future.

This was designed for Windows mostly, windows operating systems so there is some difficulty in finding driver support but it's there. It's getting better and it's actually good to do. It took a little while to look at how the keys were stored and structured and understand. But the pros are, as far as I know this is something that just gets shipped with machines. So there is no import, export restrictions that you might run into if you were trying to drag this stuff through an airport and it's free. I think this has a lot of advantages.

I know you can't read this but I put it up there in case you guys want to download the presentation. These are the links to the key resources you need to make this stuff happen if you want to try it yourself. I also have a link to a DNSSEC practice [statement]. Approach me after this if you want more details on this. ICANN paid to do a translation and I understand there is not just one Spanish; there are multiple Spanish. If there is something more ICANN can do to help please let me know. We'll try to get other translations out here.

That's just the rest of those and I think - next slide? I think it goes back to you. There is one more, go to the next slide. Oh, you had pictures of, do you want to? Can we plug into it? Just plug it into one of these things. You can plug it into mine.

[background conversation]

Luis Diego Espinoza: I will describe a little bit this. You have two pictures, the things is, and it's not a big deal. It's a little illustrative. The thing is, we identify some small office in our building. We have a very small building. We are a few people. Identify some office and put cameras, security camera there recording and we close that door. We keep the door safe and we placed the desktop that we are using to offline TPM machine, offline inside this room and we keep safe the PC and [attacks] control and we keep recording every access to the computer. This is more like following some good ceremony procedures, good ceremony process.

The other picture is showing we are using tamper evidence to keep safe the USB flash drives where we move the [CS] keys. And we keep it safe because with that information we can reveal the keys in other TPM machine then this box is preserved and security safe in the bank one copy and one copy we keep in safe in our office. If something happen we can rebuild our keys from another PC with TPM.

The most important thing for me now is where do they sign? We know we can improve it. The most important thing for me now is if any here, any of the audience has managed a small ccTLD and especially in the region because we have very well relations with the region people, I want to implement some of these. We are very allowed to help. We are very allowed to easily and quickly develop or we have, we can share it easily. We will share it to all the process, our scripts soon. Keep in touch. You can send me an email. We can share things, by example, like TLD tech community. We can help a lot with that. This is the room and this is the back up of the keys. Thank you.

Julie Hedlund: Thank you very must Luis and also Rick. Let’s open things up for questions. Please go ahead, Roy.

Roy Arends: Thank you, Julie. Roy Arends; Nominet. Firstly, the design; I actually really, really like that you guys were able to use your TPM chip on the board somewhere and use to for cryptographic as a kind HSM. I was wondering are any of these chips actually fixed under the 40-2 validators or certificates?

Rick Lamb: Yes, some of them are, but you have to look very hard to find that information. A lot of the Dell machines have this and when you go to the higher end Dell machines they’re certified to TIPS level three, but again slow.

Roy Arends: If I may, can I ask another question? Thank you. As I understand it, the actual cryptographic key on the TPM has nothing to do with DNSSEC, it basically decrypts the keys that are on disk. Where does it store that key in memory or in memory of the TPM?

Rick Lamb: It’s call the SRK in TPM parlance but that master key is stored inside the TPM chip, in memory that is inside the TPM chip.

Roy Arends: That’s the cryptographic key, I’m talking about the [private] DNS Key that is used for DNSSEC signing. I know it’s encrypted on disk but will it be decrypted in memory?

Rick Lamb: Right, that’s all done - Roy is asking a very good question. The encrypted keys are kept on the hard disk. They are only unwrapped or decrypted within the TPM chip.

Roy Arends: That’s what I wanted to hear. Thank you.

Julie Hedlund: More questions? Does anybody know if there are any questions in the chat room? Let me see if I can switch to that.

Male: I would only comment that… I would just say I’m pleased to see this low cost solution out there and I would encourage you guys to keep doing it and document as much as you can about this so other people can use it. Thank you for doing this.

Simon McCalla: I have a great question - Simon McCalla from Nominet. What was really nice to see what the way you sort of scaled down some of the best practices that we’ve seen up at the root level. I wonder, for both of you, if there were some sort of top tips of the absolute must do’s. Rick, we’ve seen the process and the ceremony that you guys have went through quite rightly. When you scale these processes down what would your three top tips to the audience be about? These are the must do’s.

Luis Diego Espinoza: Yes, we are in the process to approve the DPS, DPS [roots]; how we manage the keys. The next key rollover will be in six months. We hope to have everything set to follow the key ceremony according with the DPS, approve it by our Council will approve it for the public and publish. We expect to do that in less than six months and after that start with the lower key end ceremony according with the recommendations of the root implementation.

Rick Lamb: And to fill in a little bit on that, most of the practices that we exercise in DNSSEC are barred from the certificate authority world. They have some very well defined things and the key elements from that, that are important in every one of these things is multi person control, i.e. no one person can get full access to the key and documentation such as a DPS. Say what you're going to do, publish what you're going to do, do what you're going to say and then prove it. That's it. Those two things cover the majority of the key aspects of any trusted DNSSEC deployment.

Julie Hedlund: I think I saw another question back there.

Male: I have one here concerning the capacity of the system that you build. If I understand this correctly you basically can handle an unlimited number of keys but you are only, the constraint is that you can only do one signature per second.

Luis Diego Espinoza: What we have right now is we have 14,000 domains and we have split eight sectors. Only we have our own domains. Nic.cr and Cr.cr and [BNO line fr.cr]; and the whole process from the sub generations until published to all the DNS now is happening in 14 minutes with our server right now. I notice if we have more power, CPU number power increases speed of the process. We run on this PC, its lowest than runs on the server, by example. Then probably we can increase a little bit the performance increasing the CPUs of the server but the point is what we have right now is enough. We're updating our zones each hour and we can have it in 15 minutes, it's okay. It's okay for us right now.

Obviously at the moment that server took more than one hour to sign. We need to find a different solution for that. Yes, for sure but we'll be safe for some time, I think.

Julie Hedlund: Any more questions? Then please join me in thanking Luis Diego Espinoza and Rick Lamb. This concludes our presentation and panels for today but we do have a little lunch in the back. I urge you to engage those who have participated today. They'll be around and any additional questions you have you can engage them over lunch. So please join me in thanking Luis Diego and Rick.

[End of Transcript]