PRAGUE – DNSSEC for Everybody
Monday, June 25, 2012 – 16:00 to 17:30
ICANN - Prague, Czech Republic

Julie Hedlund: Welcome everyone to DNSSEC for Everybody, A Beginners Guide. MY name is Julie Hedlund and we are going to start this session is about five minutes. So please come in, take a seat, get prepared to join us to ask questions and get excited about DNSSEC. We've got really a nice program for you, so anyway in about five minutes we'll get going, and welcome. Yes, please do come up and join a little bit closer we promise we won't bite you, much.

[background conversation]

Julie Hedlund: Welcome everyone to DNSSEC for Everybody, A Beginners Guide. I think we are about ready to get started. I urge everyone to come up close, because we like you and we want to engage you. My name is Julie Hedlund and I will just take a moment to introduce our participants and standing behind me in the striped shirt is Simon McCalla from Nominet UK. And next to him with the Joe User t-shirt is Norm Ritchie from ISC. And over across from me we have Roy Arends also from Nominet. And next to Roy we have Russ Mundy from Sparta, a Parsons Company and we also have Matt Larsen from VeriSign and assisting me in this is Janice in the blue shirt and she's doing the Adobe Connect Room.

This session is being recorded and there will also be a transcript. And please also feel free to join the Adobe Connect Room and right now I will turn it over to Simon.

Simon McCalla: Thank you Julie. First I just want to say welcome everybody, thank you for coming along to what is the sixth time we've run this session now at ICANN and I just want to say hi and welcome to our four participants, to Hans, Jean Paul, Juan Manuel and [Wes] as well. Welcome to you guys as well for joining us.

So what's this session about? Well, it's the day and it's been a long day I'm sure for many of you so what we're trying to do is have a little bit of a lighthearted look at DNSSEC. When I first joined this community and when I first started coming to ICANN I heard about this thing called DNSSEC and when Roy tried to explain it to me I was like, I scratched my head and it sounded really, really complicated and it took him a few goes at explaining it to me.

And I said wouldn't it be a really good idea if we did a session where we try to demystify some of the stuff you hear about DNSSEC. It seems really complicated, it's got lots of complicated acronyms, but actually I'm sure we can tell it in a way that makes it easy to understand. And that's where this session came from. I hope you'll enjoy the session in the next hour. If you look on your seats there's a bit of a handout here that just briefly explains who all of my co-conspirators in the session are. Also on the back there's some really, really useful resources. So if nothing else, if you go away with nothing else but you just want to sit and have a look at some resources for DNSSEC, it's on the back of the sheet there, some very useful tools, technologies, sites and so forth.

So it's a really informal session. Please do feel free to interrupt us, stop us, ask questions, shout at us, you may want to throw things at us that is all fine, please do take part in the session. So without any sort of further ado, let's kick off. I'm sure some of you have heard about DNSSEC. You've heard a little bit about it. You'll heard about some of the myths about where it was created and you'll have heard about people talking about the ITF and they'll talk about [Wid Difi] and all sorts of stuff like that. Well most of that's a complete lie.

DNSSEC was actually created thousands of years ago, and I'm going to explain just a little bit about its genesis. Okay, in actual fact DNSSEC was created in 5000 BC on the edge of the Grand Canyon. So here we have Ugwina and she lives right on the edge of the Grand Canyon and she looks out across that fantastic view. On the other side of the Grand Canyon is her friend, I say friend, Og. He lives in a cave and he looks across and he sees the beautiful Ugwina on the other side.

The problem they have is it's a really long way down and it's a long way around and they don't really get to talk much, which is kind of a problem when you've got a bit of a thing going on. So on one of their very rare visits they sit together and they're sitting around the campfire chewing the cud and then they notice the smoke that's coming out of Og's fire and they have an idea. And soon they're using the smoke to chat and suddenly their relationship starts to blossom, if you know what I mean.

So they're chatting away using the smoke and life is good on the Grand Canyon. Unfortunately until a chap calls Kaminski moves in next door. And he's a mischievous guy and he quite likes Ugwina too. So he starts sending her rather flattering smoke signals. So poor Ugwina, she's usually confused, she doesn't know who it is that's trying to chat her up. So she's a sensible girl, sets off down the Grand Canyon to try and go sort out this mess. She gets to the other side, you can see she's not very happy, and she decides to consult the village elders.

And there's a caveman called Diffie and he's sitting there and he thinks he may have a cunning idea. So he jumps up and in a flash he runs off into Og's cave. They're like "what on earth is going on," but he knows right at the back of Og's cave is this pile of blue sand and you can only find this blue sand in the back of Og's cave. So he comes out grabs a handful and throws it on the fire and the smoke and the fire turns into this incredible blue.

And now Ugwina and Og are sorted. They can chat away and she knows only to trust the blue smoke and not the gray smoke. And that is pretty much it when it comes to DNSSEC, so don't let anyone tell you it's really, really complicated. All you've got to do is remember the blue smoke. DNSSEC is all about making sure the message that you're sending is being received intact, and that's exactly what the blue smoke here is representing.

So that's about as complicated as it's going to get today when we explain DNSSEC. There is a little bit more to it and so I'll hand over to Roy Arends who will take you through that in a little bit more detail.

Roy Arends: Thank you Simon, can I use that as well thank you. So I'm going to talk to you about DNS and DNSSEC and I'll give you an overview of what DNS does and how DNSSEC works. Basically DNS or the domain name system is a way to translate a name into a resource, and it can be an IP address or text records, it can be anything. If you look at a domain name it consists of a bunch of labels separated by dots. And these bunch of labels form a path from right to left, you go, for instance, on the screen behind me from the root to com, from com to bigbank.com and this is what we call delegation of authority.

So, that name space gets to be traversed by a thing called a resolver. A resolver is a box, a piece of software sitting at your ISP or at the company that you work for that resolves this name space on your behalf. And these systems know where the root zone are, it doesn't know where anything else is, it knows where the root zone is. And the moment it hits the root zone with a question the root is then able to delegate the resolver to the next level and so on and so on. This continues until the question has been answered.

Now to put this in line with Simon's presentation, this slide where Ugwina talks to Og, Ugwina is in fact the resolver and Og is the server that hosts the domain name. And Ugwina is actually a very, very modern woman; she has many relationships. Not just with Og but all kinds of Og's. So in order to visualize this concept better, we devised a little play and I would like to ask my friends to join me and we're not going to enact how a resolver, on behalf of Joe User, traverses from the root all the way to bigbank.com.

Okay Joe if I may invite you over to my left. Joe would like to do something.

Norm Ritchie: Hi, I'm Joe User. I'm going to do something very typical that everyone does, I'm going to do some online banking. So I sit down at my computer and I want to go to bigbank.com. So I type it in – www.bigbank.com – and hand it over to my ISP.

Roy Arends: Thank you Joe. Joe wants to go to www.bigbank.com, I don't know where that is but I do know where the root zone is, so I'll ask the root first. "Root, do you have the address for www.bigbank.com?

Simon McCalla: Hi Mr. ISP, I'm sorry, I don't have that address, but I do know where .com is and that's at 1.1.1.1.

Roy Arends: Perfect. So know I know the next level, com. So I go to the server, 1.1.1.1, and I ask the same question, "do you know where www.bigbank.com is?"

Russ Mundy: I don't know that but I can tell you that bigbank.com's name server is at 2.2.2.2

Roy Arends: Brilliant, thank you. Hello 2.2.2.2, I would like to have the address for www.bigbank.com.

Male: I can give you that information if I turn it right side up. The address for www.bigbank.com is 2.2.2.3.

Roy Arends: Perfect, thank you. And now I have the address or www.bigbank.com and I can give this to Joe User.

Norm Ritchie: Thank you. Now that my computer knows the address of bigbank.com I can go off and do my banking.

Roy Arends: Thank you. And that's really how it works. Forget ISC forget all these authorative name servers, we have people walking around with pages. So thanks, I'll need you back in a minute. So if I can just continue with the rest of the story, thank you. To make things a little bit more efficient, I'm not going to do this as a resolver every time. What I'm going to do is every time I get a piece of information I store it locally in a thing called cache. This thing has been devised over 20 years ago and when it was devised it had no security in place.

It all goes over UDP and UDP is a transport mechanism that is basically the little brother of TCP. You can compare TCP with the telephone system on a high level. I call you up, you answer the phone, you say "hello." I say "who is this," you say "this is me and me." "Okay this is me and me" and we have kind of a handshake. That handshake that I just described doesn't happen with UDP and DNS is mostly used on the UDP. UDP is basically like sending a postcard. I want to send you some information, I put your address on a postcard. I dump it somewhere and I never look back.

And eventually, hopefully you're friendly enough to send me a postcard back with the information that I wanted from you. This is kind of how the DNS over UDP works. The problem there is there is no security. Anyone can write anyone else's name on a postcard and send me that information. So this is called address spoofing. Even worse that information I know cache as I just described, so now this cache is poisoned. So these two fundamental problems we would like to solve with DNSSEC.

And just to put it back in Simon's presentation, we have Ugwina. She can't make a difference between Og #1 and Og #2 because there's no way to distinguish between the two smoke signals. So let's introduce my friends again and let's enact how this cache poisoning stuff actually works.

So again we have my good friend Joe User, I'm acting again as the resolver at the ISP for Joe User, so Joe.

Norm Ritchie: Once again, some more banking to do. So I'm going to pay some more bills. I want to go to my bank at www.bigbank.com.

Roy Arends: And I'm going to start from scratch, I don't know where anything is. I do know where the root servers are. The root servers are 0.0.0.0. Hello root server, I would like to have the address for www.bigbank.com.

Simon McCalla: Hi Mr. ISP. I'm afraid I can't tell you where www.bigbank.com is. But I do know where .com's name servers are; they're at 1.1.1.1.

Roy Arends: Perfect, thank you. 1.1.1.1, allegedly you are .com and I would like to have the address for www.bigbank.com.

Russ Mundy: Well I don't have that address but I can tell you that bigbank.com's name server is at 2.2.2.2

Roy Arends: Perfect, thank you. I now go to bigbank.com. bigbank.com I would like to have the address for www.bigbank.com. Perfect, I just got the address for www.bigbank.com and the address is 6.6.6.6. Joe here is the information that you wanted, go ahead and do your banking.

Norm Ritchie: Thank you Mr. ISP. Now my computer knows which address to go to, it's 6.6.6.6, and I would go off an happily do my banking.

Roy Arends: Perfect. So we've just shown how spoofing works. The problem with cache poisoning is is that this information that I've got from allegedly the authoritative server for bigbank.com, I will store that in my cache and I will reuse that every time Joe, his family, his neighbors, he friends will go to www.bigbank.com. So thank you again I will try to explain how DNSSEC will solve this issue.

So now it gets a little bit more complex because DNSSEC introduces the concept of digital signatures. Digital signatures in DNSSEC ensure that the information received came from the proper source and has not been mangled with in transit. And it used to use public key signatures. Now who understands from a fairly high level how digital signatures work? Okay, I don't have enough hands so let me try to explain that.

Public key cryptography works with a public and private key, basically what we call a key pair. The public key, my public key, and I'm not acting as the resolver now, I basically have a zone, let's say bigbank.com and it has a public key. That public key I give to everyone and anyone can have that. And the private key, which is the counterpart of the public key, I store that somewhere safe where no one can touch it. Now if I want to sign something I will use this private key to sign the piece of information. That piece of information I then publish on the internet and that can then be verified by the public key tha ti just gave you.

The cool thing about this digital signatures is that they're digital and they're fairly small pieces of information. And just like it can store a text record or an address record or anything in the DNS, I can store these signatures in the DNS as well. So now if I've retrieved www.bigbank.com I get a signature with it which is just a blob of information and now I can verify this signature. There's one piece missing and that's the DNS key; that's the public key I just told you about. Since it's public and since anyone can have that and since it's also just a blob of digital information, I can put that in the DNS as well. So next to the information that is signed, plus the signature, I can now retrieve the digital key as well.

So I can do, now, the validation. There is one small piece missing, and I will go to that in a second, because if I resolve this stuff now, just like this text record or this address record can be spoofed, these signatures can be spoofed as well. Remember that we talked in the beginning that I know as an ISP where the root servers are, that's how I start out. I need basically to start with authority and in my case that's the root server. Now, if I also trust the root servers key, sorry the root zones key, that key can then be used to sign stuff below. As in sign the second level domain, sign the com domain.

So, now I can trust the DNS key from the com domain because it's been signed by the DNS key from the root domain. And to link that again with Simon's presentation, DNSSEC is the blue smoke that he talked about. With DNSSEC I can now discriminate between what's true and what's false. Okay I've explained already this part of the slide; we're going to enact the play again, but now with DNSSEC involved. Can I ask my friends to come up?

Now that I have my friends here, we have the root zone, the com zone, bigbank zone and what we first need to do is build the chain of trust. Just like you can traverse the name space by going from the root to com and as then delegated to bigbank.com, we can also build the chain of trust that way.  And basically we need to have the root sign the key of the com zone.

Simon McCalla: Here’s my key, thank you very much.

Roy Arends: Perfect.  And of course similarly between com and bigbank.com.

Russ Mundy: Here’s my key.

Male: Consider it signed.

Roy Arends: Perfect.  We’re almost there because I still need the key of the root zone.

Simon McCalla: Here you go, here’s my key.

Roy Arends: Thank you for that key.  That means that I can now validate stuff just like I can traverse this tree.  So let’s try to do this.

Norm Ritchie: More banking, more bills. Okay, here I go again. I'd like to go to www.bigbank.com.

Roy Arends: Perfect. I'm starting from scratch, nothing has been cached. So I go to the root zone and ask for www.bigbank.com.

Simon McCalla: Hi Mr. ISP. Afraid I don't know where www.bigbank.com is, but I do know where .com's name servers are and they are 1.1.1.1.

Roy Arends: Perfect. Since I have the key of the root zone, I can now actually validate that this information is correct, and it is correct. So now I can go to com. Hello com, I would like to have the address of www.bigbank.com.

Russ Mundy: 2.2.2.2, you look familiar so I'm giving you the short answer.

Roy Arends: Good. I also would like to have the key for .com.

Russ Mundy: You can have that too then.

Roy Arends: Perfect. Now I have the key for .com, I can validate that because I trust the root key, which assigns com's key, so now I can go to the next level to bigbank.com to ask for www.bigbank.com. Perfect, thank you. I now have the information for www.bigbank.com, 6.6.6.6 and let's just check if that's correct. No, that's not correct, the signature doesn't match because the person who gave me, or the entity – I'm not sure Julie – the person who gave me this information does obviously not have the private key for bigbank.com. And therefore I drop this information, this is incorrect. The DNS protocol works in certain ways. I probably have to ask again at some point and there we go.

Can I have the address for bigbank.com?

Russ Mundy: It is 2.2.2.3

Roy Arends: Perfect. And let me just check that. Perfect, that feels good. The address is correct and I now can, as an ISP, give this information back to Joe User.

Norm Ritchie: Thank you Mr. ISP. Thank you for the authenticated address of my big bank.

Roy Arends: Thank you, thank you guys and this is how DNSSEC really works. Before I give over to Russ Mundy for the next part of the presentation, I just want to t4ell you one more slight thing. All of the stuff that we've done, all of this play that we've done, in the real world, in DNS servers this actually happens after you press the key when you typed in a URL in the browser and before you see a page. So we're talking milliseconds here. This is really, really fast. Thank you.

Julie Hedlund: Excuse me, would you like to take questions now from eh remote participants or would you like to wait till later?

Russ Mundy: We can take some now. That would be fine.

Julie Hedlund: Okay, so Juan Manuel Rojas is asking "is it possible to implement DNSSEC in any web server with any name."

Russ Mundy: DNSSEC is designed so that it can…

Julie Hedlund: I'm sorry, he said with any "C" name and I'm not sure if that was a typo.

Russ Mundy: Ah, with a C name, okay. Yes, the DNSSEC works functionally with the C name portion of DNS. We won't get into deep technical details here. Let me put in a plug for Wednesday, the full day session. If you want more technical details, that's the place to come. But the short answer for that question is yes.

Simon McCalla: Russ as well just before Russ starts, we'll definitely have a question and answer session as well, at the end of Russ's section we'll have an open mic and feel free to ask whatever you want.

Russ Mundy: Okay so I have a number of slides here that I'll go through very quickly and not talk a great deal about all of the content on the slides. The reason they are so voluminous in terms of information is so you can go back afterwards, take a look, generate more questions, ask more questions here if needed, but I'll cover the information but cover it fairly quickly. And what I'm specifically going to talk about is implementation of DNSSEC. And DNS itself as you've noticed can be explained and illustrated in a very high level, abstract way and so can DNSSEC.

When you actually get down to doing DNS, there are normally a set or providers that actually operate the name servers that you saw creating the smoke online. The smoke is the questions and the answers to DNS. And when you have a large organization such as a registry or the name server that's providing name service as part of their business you usually have a large highly competent staff that does and knows how to do DNS. And those are the people that are going to probably best be the ones involved in the details of doing DNSSEC. And we'll get into various ways in which you can approach that.

VeriSign is obviously a company that is very concerned with DNS as a service and we know, I personally know that they have extremely competent DNS operators. Many other large organizations also do. So they are doing this service in-house. Internet based business that really are not DNS centric, for instance the web presence for an organization that is a nonprofit very likely would not operate their own DNS. It would probably be outsourced or provided by someone that's not part of the DNS.

All of the end users, like ourselves here, we depend on somebody else in almost all cases to provide DNS service for us. So it really depends on where you are, what you're doing in the DNS world. And this structure you see here is similar to the one that Roy showed earlier, only it's slightly larger. And the enterprise that I'm showing in the far right hand side of the screen is Hewlett Packard, so that's hp.com and they have for years operated a very large complex name service and they do, for the most part operate their own name servers.

Cnn.com, honestly I don't know if they operate their own name servers or lot, but they operate a very big operation when it comes to DNS. So if you think about what happens when you are operating your own name server then you have a staff that knows about DNS and chances are that's the same staff that you'll want to use to do DNSSEC. If you've outsourced it to somebody, then you want to make sure that those people you've outsourced your DNS operation to understand and know DNSSEC before you ask them to go forward to do DNSSEC with you.

Because if they aren't capable of doing it then that's where it gets a little more complicated when you've outsourced your name service. So when you look at the whole of a zone, what happens to a name in a zone, the content, the www.x.com or the any other name that you have in has to go from the far left side where someone says "I'm going to put this name into a zone," until somebody on the far right hand side, like Joe User asks for www.bigbank.com.

And so you can see that there's a lot of functions in between that are involved in touching a name as it goes through the name service. And so everyone that is doing DNS now, whether you're going to do DNSSEC or not, needs to ask yourself these two questions: "Do I know where I get a DNS name from?" if you're in an enterprise you probably get a name within an enterprise from someone else in the enterprise as opposed to a registrar where if you're going to put up a new website and you want a presence on .com or .net or .org or a country code TLD you'd likely go to a registrar function.

So you need to know where you're getting your name from because they are the ones that are not the authority for the next higher zone that you will be using that name in. The next really critical question then is "Who operates my name service?" I may operate it. I operate some name servers. Other people operate some name servers and there's lot of name server operators around the internet. And so you as a holder and a user of names, if you're going to do something with DNSSEC you need to know who operates your name servers.

So here's an example of the flow that I talked about earlier. So I have a zone already in place, it has an authoritative name server. If I want to add a www.whatever to that zone I have to put it in. So I put it in the authoritative name server, that blue box in the center of the screen.

And then when someone makes a query, Joe User wants to know where www.bigbank.com is, his query comes in the recursive  server who you saw in the person of Roy Arends as the ISP in that instance, will ask the question of the authoritative name server and get the answer.

Again, another illustration of how it works.  But it's a little more complicated than that when you look at the real world; how many name servers there are, how many places that you can go.  So the way that the bits actually flow around is a bit more sophisticated but just the thing to remember is the simplistic approach but there's a lot of things behind the scenes that are going on that you don't know about.

And so in this case www.cnn.com, you think oh well that's just one name lookup.  That would not be correct.  There's that many lookups that occur when you go to fill that webpage.  So each one of those happens in real time more or less as you're sitting there typing it in. And when you do DNSSEC all those names are validated.  And that's the cnn.com today, it's even bigger then we made the first picture.  So it continues to grow.  And the thing to remember that's probably most important about DNS is it's the information that matters.

If you remember when our player of Dr. Evil, our friend Julie, came jumping in and substituted information, that was hijack.  So it's the actual zone content that matters and the reason you do DNSSEC is so that you can assure the correctness of that zone content.  That's the whole purpose of DNSSEC.  And so when you actually add DNSSEC to a zone that's what you're doing, you're validating the zone content. You're providing the mechanisms for end users to validate it.  And if end users happen to not validate it, if they're not doing DNSSEC, they don't lose anything, it doesn't penalize them. But they can still be hijacked.

So even though you've signed your zone does not mean that every user of your zone content will be using DNSSEC to validate it. So the users, you've done all you can as a provider of a name, but for the users of the name, if they don't do validation they're still susceptible to hijacking. Now if you remember the triangle earlier from how name service involves many pieces for an individual zone, you can see only part way through the zone is where DNSSEC actually works.

So some of the things, like when I go to hand my information into the operator of the name server, if I don't do it properly there, invalid information can sneak into the zone and it will be signed. But provided that you get the right information into the zone DNSSEC will make sure that users can validate that information. So when you're doing DNSSEC you really want to take more or less the same approach that you're doing with DNS. However you're doing DNS today. So the end result of really what you want to get, and what you saw in the play earlier, is you want to get your DNSSEC signed zone into the authoritative name server. And that's shown there by the little box "signing zone data."

And then when the validating recursive name server asks the question, in this case it was Roy – here's my friend Roy – the ISP was validating the information. And so you know you get information out of the system and to that last point for validation. And the validation can occur at the end user also, but the most common thing initially will be for ISPs and others to do validation. And so if today, when running your name service, if you are a large operation who is operating your name server today, you will probably want to have those same folks be the key people in doing your actual implementation.

Now sometimes you've got a whole lot of pieces that make up your name server functionality. Sometimes you're using a product that's provided by a single vendor but you still have your own people operating it. And sometimes you're looking at using other mechanisms, such as an external signing service. There are several of these that are available from our folks that you saw in the play, the companies that they're associated with do offer DNSSEC signing services. So you can turn to external activities, such as VeriSign or Nominet and they will sign your zone data and hand it back to you.

And then if your name servers are capable of serving it in proper versions you have done DNSSEC and your zone is signed and you don't have to change your system other than making sure that your name servers are capable of properly serving DNSSEC. Now if you do a combination of creating and running your own name servers, using some products, using some external services you may have different combinations of all these things. You may do some outsource. You may use single product and then look at it and meld it all together to create your signed zone.

Now, when you – oh this is showing me both sides isn't it. I see. That's why I'm getting confused. I have the large one on one side and the Adobe Room one on the other side. So as you are using an external provider for your DNS functions, if your external provider is not ready to DNSSEC, whether that external provider is a product vendor and you're operating the name service but you're using their product. Turn specifically to that product vendor, find out when that product vendor is going to support DNSSEC. Ask them directly.

Because product vendors that aren't implementing DNSSEC in their products, one of the biggest things that we hear from people on the product side is "we don't get requests from our customers." You're the customers. Ask for it if you need it. You could also look at adding some things on and doing the external signing service and using some open source combination. So there's ways you can still do it, but if you're using the single products provider or an external name service provider where they're doing all of your name service ask them when they'll be providing DNSSEC. And again, having the external people that are providing services and products that do not do DNSSEC today, the most important thing that you can do is press on them to do it, or even consider changing how you're doing DNS service to use mechanisms that do support DNNSEC.

And in the case of product providers that's probably their biggest incentive. They don't like to lose customers. And whether it's a service provider, whether it's a product provider, if they're going to lose a customer they don't like that. So that's a very, very quick run through of how you can go about doing DNSSEC. And as you can see each and every time an activity starts to do DNS they decide how they're going to do it. And that's one of the great parts about DNS. It can be done very differently by very many organizations and so that's why it's really hard to say here is the answer for how you're doing DNSSEC.

In each case the individual DNS operation needs to be looked at and examined. There's lots of help out there available. It's on the sheet for where a lot of the tools are and a lot of the how-to's and so forth. And those of us that are here today on the panel, one of the main reasons we're here is to answer your questions. And so that's what we'd like to do at this point. We'd like to open it up for questions. It's not just me that's going to be answering. It's any one of the folks here, so feel free to ask directly individual or just general and we'll go for it.

Julie Hedlund: If I can I'll start with the remote. Ryan on remote is asking "what do you think the timeline for wide scale DNSSEC implementation looks like" and "what are the major road blocks."

Russ Mundy: Well that's a broad question and there are several segments of it. One of the segments involved is being able to get registrar support for signed zones. And the registrars, this is something that's important in this venue, we need to have more registrars that are actively supporting and facilitating DNSSEC. That's one of the road block, is registrars that don't support DNSSEC today. Another one of the areas that we definitely would like to see more support of is operating system, the actual OS vendors doing more DNSSEC support. There are some that do it today, but broad spread use is growing.

I can't really say what a timeline would be for wide spread use because if it's used just at the ISP level that's one area and that could be a number of years away. Large US ISP Comcast is doing DNSSEC throughout their network today every customer of Comcast is using a

DNSSEC validating browser.  We'd love to see more of that.  And so it is growing.  Back here we had, yes.

Male: My name is [Vladyslav Andrushchecnko], (Inaudible) Foundation. Thanks guys, girls for a great presentation, just one comment.  You said to go ask your service provider to use DNSSEC.  So if I tell that to my mother, go ask your service provider she'll probably ask me have you slept well, what are you talking about.  But if I give her a small program, a client, which is DNSSEC ready and then she's trying to use that and it doesn't work because the provider does not support it, then that's a legitimate question.  Where I'm trying to go is that we don't have good support on the client side yet, so I'm pretty sure that it will work on the service provider side, all of the chain, but if you don't have the client side DNSSEC it would not work with my mother.

Russ Mundy: So the answer is for your mother.  If it's not already in your schedule please include our session on Wednesday, which starts at 8:30 and you'll see some answers presented right in there, for instance doing a validation, DNSSEC validation on the home router.  And I believe it's called DNSSEC without humans, I think is what that presentation is for. And that is an effort to focus on the home router kind of interface so the only hijacking that can occur at that point if validation occurs there is within the house.

If the validation occurs at the ISP level, yes between where the ISP name servers fit and your mothers computer at home, you are still opened to attacks there. But ISP operations will argue that that's good enough and they operate securely. But you're right, there's not enough clients, Sparta does have a number of them. We have a fully capable web browser that will do DNSSEC. There's a number of plug-ins for validation.

What I was primarily talking about there in asking your service provider was focused at what I perceived to be most of the people at an ICANN meeting, and those that are interested in names in general and most often ownership and serving names. And so if you're an enterprise you have a name. if you're a name service provider you serve names for other people and that's where I was talking about ask your service provider. As we get more we'll have more end clients, but it's slow to the end client. Back in the back, can you come up to a mic so those online can hear you?

Male: (Inaudible), registrar. We did a quick scan for the people that we deal with DNS for. We register domains, we do DNS services, we do hosting, but sometimes we're only one of those three parts. The very quick scan showed that 87% of the DNS zones that we input from customer systems in order to serve out to the internet use wild cards, and that's not supported by DNSSEC. So implementing this is going to take 87% of our customers offline.

Roy Arends: I understand your concern but I think that you're incorrect in your assumption that DNSSEC does not support wild cards. DNSSEC definitely…

Male: But (Inaudible) explicitly says it doesn't support wild cards.

Roy Arends: No, Matt and I wrote this stuff. May, maybe you can help me out here, but the way I think we described it is yes it supports signing of wild cards, but that part of the protocol is a little bit more complex because we have to deal with those exceptions. But it definitely supports wild cards.

Male: So I can put a star in the zone and it will sign it and the A record will be validated by the client or the ISP or whatever?

Roy Arends: Well the way how it works is when you provision stuff and you for instance use your wild cards because you don't know what the question is that someone might ask, let's take foo.com. You have a wild card at foo.com and someone asks for alpha the foo.com. We can't anticipate alpha because that's not in the zone, that's why you have a wild card, so what is actually signed is the fact that foo.com exists and that there is a wild card for foo.com and a validator who validates all that.

Now it knows that this is a wild card expansion for that name. I don't know if that makes any sense, maybe this goes to quick. But if you have any concerns about it maybe you can I should just have a quick chat afterwards. Thank you.

Craig Schwartz: You commented earlier that one of the challenges is with registrar support of DNSSEC, can you say a little bit more about what that means for the nontechnical people in the room.

Russ Mundy: Right well today for whatever zone you may have, something in .com and when the .com registry elected to sign .com that's great because then they can participate and serve .com records for DNSSEC just like they serve name server records for DNSSEC. But no one deals directly with .com. VeriSign deals with .com through the registrar segment of the business structure here. And so just like today when you add a name server record, if you put up a new name server for your foo.com, then you have to add that information to .com. And that's done through your registrar.

And the registrar then talks to the registry. So DNSSEC has a DS record or a key record, they have both records. What gets published is the DS record for the zone. That information has to be passed from the holder of the zone through the registrar to the actual registry for the zone. So the registrar performs an important function of being able to pass that information to the registry. And a number of registrars do not have the ability to pass a DS or T record for DNSSEC to the registry like they can pass an NS record to the registry.

So that's what they need to have the support for, is the ability to support the passing of DNSSEC records specifically to the registry in question. Is that okay? Good.

Julie Hedlund: I have one from remote if I could slip it in. Robert [Gara] is asking we'll he's trying to tweet and I'm not sure we're up to tweeting at our sessions yet, but the question is how easy or not would it be for a key company such as Google Twitter and Facebook to DNSSEC enable their sites?

Russ Mundy: Okay. It really does depend on individual operations and I think Roy wants to jump in here.

Roy Arends: I think that's an excellent question. Remember for iPv6 we had this famous iPv6 day, I think we should have something similar with DNSSEC, have a DNSSEC day. And for organizations like Facebook, Twitter and all these large enterprises implementing and deploying DNSSEC is not complex, they understand the technology. The few of us who are here who have worked in the protocol have friends in the business and we know that they are aware of the technology.

One point that is often made to us is that these guys, the Facebook's the Twitter's of the world, they use something like large content provisioning networks. And that means that they like to tailor the response, the DNS response to the client who is asking for it. So they need to be a little bit more dynamic, but it doesn't mean it's impossible, they just need to do a little bit different work then the standard tools that are out there. But it's definitely possible.

I thank you for that question because I'm now trying to figure out how to get ISOC and basically the rest of the world to start with a DNSSEC day.

Russ Mundy: One area that Roy mentioned that I'd like to say a little bit more about is the content distribution networks, CDNs. And many of these large providers as Roy said do use these. One of the largest, [Akamai] is in the process of implementing DNSSEC and they do have it for some of their services but not all of their services. And again, having encouragement from customers for the need for it, so if any one of you all who are involved with [Akamai] or other content distribution, CDN providers, asking for and encouraging the providers to support this service is very helpful.

I mean I am by my work an evangelist for DNSSEC and so I say that, most people know that, but I'm not that much of a buyer. You folks are the ones that buy services and products from people and you are the important people to be asking for DNS services from people such as [Akamai] or [Efny] or something like that. Next question, yes please.

Male: By pure coincidence the Director of Internet Society Netherlands and I did just organize a world iPv6 day in the Netherlands and I'll gladly take it up and 666 is a good day for DNS spoofing as well.  So my question was we have a colorblind Ugwinda or whatever her name was, so everybody that's using a tablet here is basically vulnerable even if a zone is signed to DNS spoofing. And that's the most common emerging pattern, people with tablets, people with mobile devices, so why are we not pushing for this so aggressively that all these vendors do this. Because there is no reason for them not to do it, or is there?  My question is why aren't these, especially these mobile providers, on board with this.

Simon McCalla: I think the thing to remember here is the key step to this, and particularly if you're a tablet user and you're using it as your ISP, at the point at which you connect in and having a validating resolver at that point. So here if you're at ICANN you're connecting through an ISP, provided that ISP is validating you're tablet is safe for the bulk of that DNS journey.  It's just that tiny last piece as Russ mentioned, until you got it right in the tablet it's slightly different, but fundamentally where the man in the middle attack is going to happen is out there in that journey that we acted out there in front of you all until your tablet is protected.

The flip side is we are also starting to see DNSSEC being put onto tablets, I know Russ's group is already got some tools and software that will work on Smartphones and tablets and I've no doubt we'll start seeing it.  We know that Google is doing some really cool work with

[Cramer] at the moment and we're seeing DNSSEC stuff happening there. So I think it's only a matter of time, but I think the idea that it's got to be on your device to be protected is not right. Does that make sense?

Russ Mundy: So you'll definitely have more protection the closer you get it to you, but the ideal, which those of us in the DNSSEC world have been pushing for for a long time, is to have it done on the end device. But it does not have to be done there. Like Simon said that last mile, depending upon the technology, and if you're using cell phone technology believe me the cell phone providers are very careful and very precise in their technology between their towers and your end device. So your threat area in that link is honestly not that high in that link.

Male: But its' people using the free WiFi basically going to the Starbucks, to here to ICANN. I mean basically I can put up an ICANN network easily. And there's another of course layer of protection I might have the correct IP address, but if I don't get the certificate out of DNSSEC with [Dane] or another technology then I'm still hit because somebody else can stick in any other certificate signed by any other vague certificate authority.

Roy Arends: I just want to answer the previous part of your question. Why hasn't this been implemented yet in tablets, properly. Not as a patch but by the operating system developers. So what I think would be good is we as an ICANN community, as the ICANN community, and I'll try to do that in SSAC soon, there's an SSAC session on Tuesday. And our various friends here who can go to their own constituency, maybe ask the ICANN Board or the senior management of ICANN the company to write a letter to senior management of Microsoft and Apples of the world.

It is not unheard of, it has been done before. So doing it this time with DNSSEC as the focus we might actually get somewhere.

Russ Mundy: So let me speak a word about Microsoft. Microsoft actually has implemented DNSSEC. The way they do their last mile of DNSSEC is not exactly like those of us that are in the DNSSEC world would like to see them do it. But they've had DNSSEC since Window Server release. It's in Windows 8 Beta now. There operating system for their desktop and laptop is actually the operating system that's intended to go in their tablet line. So they are actually moving and from a major OS vendor, they've actually done more. Apple frankly has not been doing much of anything at all. Fedora in the Linux world is working very hard at incorporating DNSSEC.

So it is spotty and having it in operating systems is an objective that lots of people want to get to. But you aren't totally lost and completely out in nana land if you have your ISP doing it. Some of the demonstrations that I'll do possibly on Wednesday, I use a VPN back to my house and at my house, my service provider is Comcast and so I know I have DNSSEC. So that's how I do a lot of the things that I show people when we're at conferences. More questions? Back in the back could you come up to a mic so those online can hear you.

Male: Yes, why do you think that some large ccTLDs have still not used DNSSEC?

Russ Mundy: Well how about if I turn to my closest policy ccTLD person?

Simon McCalla: I think there's a number of reasons and I'm sure Roy is going to want to chip in as well. DNSSEC has been going through a long evolution and it's nearly what 10, 12 years old now since the protocol was first proposed. And so speaking from being a ccTLD we, depending on where you were in that process of involvement of the protocol is how early you tended to deploy it. So for example Nominet and VeriSign, we deployed a few years ago now, a couple of years ago. Some folks deployed even earlier than that.

So we had some really early adopters and we have some in the middle. There's a technology challenge because it depends on how advanced you are in your technology stack, if you like, as to when you would choose to implement. What we are seeing now is we're seeing at least what 65, 70 TLDs at least, the latest numbers – I'm sure Steve will say on Wednesday what the latest numbers are.

Russ Mundy: I think it's about 70 now, yeah.

Simon McCalla: It’s pretty significant number. And what we are seeing as the technology has matured and there is more information, these more sessions like this, we’re seeing more and more people getting involved with implementing DNSSEC. We’re seeing it put into appliances now making it even easier to deploy. So there’s one-click deployments of DNSSEC now. So we’re starting to see that acceleration, but there’s no easy reason – I can’t speak for every TLD and every ccTLD certainly, but Roy I’m sure you can.

Roy Arends: And when I look at the numbers, and not just ccTLDs but also gTLDs, I think that the largest cc’s and the largest g’s, largest by the amount of records in their zone, they have been signed. So com, net, org, info, de, uk and l, they have all been signed. By that we can probably state about 80% of the domain name space is DNSSEC enabled, as in the VeriSigns and the Nominets of the world, they can accept DNS records from the registrars. Thank you.

Russ Mundy: Let me just add that there’s at least one of the significant backend providers for particularly some of the, two, for the smaller ccTLDs that are offering either at an extremely reasonable or zero cost delta; I don’t know that much about the business aspects. And that’s the Afilias folks and the PCH folks. They operate a lot of the backends for the smaller ccTLDs. And the challenge in terms of getting those signed are getting the policy agreements in place. It’s not a technology question a lot of times. I mean it can be a technology question but it can also be a policy question.

And I know for instance even some of the Mongolia, .mn is a pretty small ccTLD, it's signed because Afilias just said we can proceed and do that. So there's a mix of reasons and now as Roy points out, the largest ones by count are signed and so working through the smaller ones. That's it.

Simon McCalla: Do we have any more questions at all, anything from the remote room. Okay so really just I first want to say thank you. Again, a quick plug for Wednesday session for those of you who would like to come along it's a full day of events talking about DNSSEC deployment. There's an update on how we're doing in this region, in Europe but also worldwide. We're looking at a number of topics, we've got engagement with ISPs. We're looking at DNSSEC on appliances. It's a really broad ranging workshop, it lasts most of the day. There's lunch included as well as some fun with DNSSEC, quiz with prizes; there's all sort of stuff that's going on in that event so please do come. Julie do you remember the location for it?

Julie Hedlund: Yes, it will be in Congress 1, so it will be right over here and it starts at 8:30 a.m. on Wednesday and it goes until 1:45. And like we said it includes lunch, it should be a very, very interesting set of presentations and panels so please do join us.

Russ Mundy: And thank you everyone for coming today and participating, good questions. Thank you very much.

[End of Transcript]