HELSINKI – DNSSEC Workshop
Monday, June 27, 2016 – 09:15 to 13:30 EEST
ICANN56 | Helsinki, Finland

DAN YORK: …a little bit. We had, I know, no coffee, nothing.

[SPEAKER OFF MICROPHONE]

Yeah. Ohh, yes, we're in a room full of geeks. Yes, okay. Good morning. I'm Dan York. As many of you know, and were here for a day of the DNSSEC workshop and Tech Day combined in one, as part of this new format. I'm delighted to see this many people. We were seriously concerned about whether we would be talking to ourselves today.

But it's good to see, we kind of are, okay, but there is more people here. There is other folks. It's good. Okay. Before we begin, we have a couple of little logistical things. All of you will see the things here, what we're talking about today, you also need to have one of these. All right? If you want to have lunch today. We have only so many slots. There are ushers who will not let you in if you don't have one of these.

We kind of spread them around, so if there is not one right with you, grab the other part, hold on to it, do whatever you want to

do with it, put it away, but you need to have this ticket to get in there. And when it gets closer, Julie will explain how to get there, because she and Kathy…

[SPEAKER OFF MICROPHONE]

Yes, but they've walked it. They have stuff to tell us about what we should really know. Which elevator door to get into and not, and those kinds of things. Okay. Slides and audio stream are at this link. Okay.

If you're in the room you probably don't need that, but we do have remote participants. We have a number of people on there. So when you are speaking, please do state your name, etc., because we do have people who are on remote, can see what's on the camera. All right. It's aimed at you guys. There we are.

So this is the program committee that's brought people together. I would like, the folks who are on this list, could you stand? Jacques? Mark? A couple of people who are here, Russ? Okay, Andre? Okay. So these are the folks who have been helping put this program together. We meet weekly on a call. And so if you want to thank them, or blame them, you can.

And also if you would like, if you've got an idea for next time in Hyderabad, talk to one of the folks who are here too. We'd like

to do a little bit more about that. We'd like to thank our four sponsors that are here. And I saw, we have Jacques again, from dot CA, and I saw Cristian. Cristian? There he is, from SIDN. And [inaudible], anybody from [inaudible] in here? No, okay.

Anybody from Affilias? Yeah, Jim. Right back there. Thank you Jim. So we'd like to thank these four companies who have come together to offer sponsorship. They're sponsoring the lunch, and this time, they're also sponsoring the implementers' gathering.

[APPLAUSE]

So, speaking of that, no. That wasn't it. That would be tomorrow night, and if you don't know, it's at a nearby restaurant. If you don't know about the information about how to get there, talk to us, and we can tell you where to go. Julie is about to say something.

JULIE HEDLUND: I'll just note that is a limited space thing. So we've got a few slots left, if you haven't RSVP'd, please do send me an email, and so I can send you the information of where it is. But just, we wouldn't be able to accommodate everybody in this room, just so you know. Thank you.

DAN YORK: Thank you Julie for pointing us back to the budgetary track, since we have a limited budget to pay for that. Anyway, we want to thank our… And I had to do that because the cameras synch to the nearest microphone, that's why I did that. Okay.

This is a project of the Security and Stability Advisory Committee. A number of the members are throughout here, also with the assistance of the Internet Society, the [Deploy 360?] Program. And you've seen the program that we have. We are going to… I'm going to do my normal discussion of the counts and things. And then you can see next we've got Dr. Matthäus Wander, who is right over there, yes.

Okay. He's going to talk to us about some of the measurements he has done around DNSSEC adoption. And then we've got Geoff to talk about, back in the back there, to talk about his ongoing measurements of validation side. Then we've got a panel that Russ here will be monitoring, which is going to be talking about different challenges to DNSSEC deployment, ways people have dealt with that, that kind of thing. And then we've got a, Matt Larson is here, yes, there is Matt, to talk about, and Duane, who is sitting next to him over there, are going to talk about the key signing key, the KSK rollover process and where we are with that.

And then Andre, Suri and I will come up and talk a bit about encryption agility, and the migration to new encryption algorithms. And then Russ and I will wrap this up, and then Roy… Is Roy here? He will be here, okay. Roy will take us through the great DNS and DNSSEC quiz. How many people are at their first DNSSEC workshop?

Okay. Cool. Welcome. Welcome to this. You'll…

[SPEAKER OFF MICROPHONE]

No, their first, not the first. Their first. Okay, you'll get to experience the great DNS DNSSEC quiz. Now one thing you will notice that is missing from this schedule is a break, but if you'll notice the new schedule that ICANN has, there is part one and part two. We had to do that because we were mandated that we should respect the break as part of the schedule to that. Then we went ahead as a program committee and ignored that entirely and just ran anyway.

So you are invited… We don't expect you to sit here the entire time without caffeine or other types of things, so you are certainly invited to get up, during the break time, or other times, and get something when it's out there. So you are welcome to do that, we will not be offended. Go right ahead.

Okay, so I want to talk a bit about the deployment that we've seen, the rates that we're seeing around this. And this is one map that Geoff Huston's team produces, showing the level of validation that is occurring globally. And when Geoff comes up, he can maybe explain the dips, but we know it's the measuring mechanism he uses with the add mechanisms, etc.

But basically what we're seeing is, overall around 14% validation happening globally right now, according to Geoff's measurement. And he'll talk more about that in a few. Another… When we look at the regions that are here, you can see the different areas of the world that have more validation than others, and some of those might be surprising if you look at some of the, where they are. You'll notice that other column, it says, use Google's PDNS, public DNS, that's the 8.8.8 and associated IPv6 addresses and such.

And we put that column on there because if there is a higher percentage of that, that means many of the countries, many of the areas, are doing validation through Google's services. If there is a lower percentage, such as North America and Northern Europe, that means that more of the ISPs are doing the validation themselves in that space.

So interesting stats there. This was the Google, or this was the European one, since we're coming to Europe, that I put up here.

You can see some of the places like Farrell Islands, 91% validation. So there is DNSSEC validation happening in different parts of the space, near Sweden, right next door, at 77%. Norway, 62%. So it's great to see this growth as we've seen over time of DNSSEC validation happening out there in many ways.

Switching to the signing side, this is Rick Lamb's report showing the DNSSEC deployment of domains, and that big, huge, hockey stick like thing is, of course, because of all of the new gTLDs that we're seeing there.

But, you know, a very high percentage of that. Rick has started tracking, and this goes, this is for the TLDs for which he can get statistics, he is showing the percentages of, or the number of signed domains and the percentages, and you'll notice that of the ones he's tracking, we have dot NL, is up on the top there with the largest number of signed domains, followed by Brazil, com, etc., and going on down that list.

So we're seeing some, you know, continued good deployment on the signing side. This is the second level domains. And Matti is going to talk a bit more about that in a few, when he comes up here. I was also going to point out, on the new gTLD slides, and I don't know how many of you are aware there is a site called NTLD stats dot com, and they have a page specifically on DNSSEC, which shows the number of domains that are there,

and the [piece?] that are there, but if you look at some of the new gTLDs and where the signing is happening, [O-V-H?] is…

Anybody have an [O-V-H] domain here? Okay. Yes, it's a domain that was setup and they do the hosting, they do the signing, they do all sorts of things on there, and they have that. But then one that I thought was interesting was number eight here, dot bank, what's interesting about that one is 100% of the domains are signed because their business model is actually includes the fact that when you get a dot bank domain, they automatically do the signing and that's all part of that.

So it's interesting just to see, we're seeing a couple of these newer domains that are embracing this. Dot insurance is doing the same kind of thing as well. Moving into our maps, and looking into our country pictures, and some things that have changed since we were last together in Marrakech, this is our big view of the world in terms of where the ccTLDs are signed, and I'll come into a little particular issue with this when we talk about the Middle East.

The maps are showing, this is the two letter ccTLDs that are shown here, and which are signed. And so right now, you see a lot of the coverage. Obviously, Africa is still a little bit, needs to be filled-in in some parts of that, but let's take a look at this.

Africa, again, we've had a couple since the last time. One was Morocco signed their dot MA, and Madagascar signed dot MG.

So and we know from some of the workshops that are happening that there is still work in various parts to fill-in that map and get more of those ccTLDs signed as well. On Asia-Pacific, we had a couple of interesting ones. Syria signed their dot SY. And that's now active. And Saudi Arabia signed their IDN. And so you'll notice, though, that they're still yellow in the map there, they're in the announced state, which means we know they're interested in that, and that's because they haven't actually signed dot SA.

And I was having a discussion with the folks there, sorry, my system is set for the two-letter country codes, and maybe if I had somebody, any Python developers want to help me work on this, we can maybe look at how to tweak the maps to also incorporate IDNs. But I don't have the cycles yet to do that, but anyway, we should note that Saudi Arabia is on this path where they have signed their IDN, and they are looking to sign dot SA, they hope by the end of the year.

Moving on, on Europe, we had Romania come in with dot RO, in the past few months there. And in Latin America, picture is as in Marrakech, and so is North America, which, anyway. These maps are available. You can get them off the Internet Society's

[Deploy 360] site, and you can sign-up and get them every Monday morning. They get shipped out automatically.

We have an event calendar which we haven't been populating as much, but we're trying to maintain that on the DNSSEC deployment site, if you've got a DNSSEC site ordain, or DNS security event you'd like us to list, please let me know. I'll be glad to do that. I also point out that… Who is going to be at the ITF in Berlin? Okay, a good number of folks here. Well, if you want to come a couple of days early, and you want to be part of the Hack-a-thon that's on the Saturday and Sunday, there is a group of us who will be working on DNS, DNS security, DNS privacy tools, etc.

And the past couple of sessions, we've had some good work there, working on doing things with TLS and some other different pieces that are a part of that. And we have a DNSSEC history project. I'm still looking for volunteers to help me collate this and put this into a form that's more readable, and work on that. I would love to have any volunteers with that. And my final slide is to mention that, just this past week, anybody see the Global Commission on Internet Governance's One Internet Report?

Okay, a few people nodding. This is a work… The Global Commission on Internet Governance was created two years ago

in 2014, and has a whole, about, 29 different people from around the world, chaired by Sweden's former Prime Minister, Carl Bildt. And has been doing, producing this whole series of reports.

I think, actually, Patrik, you had a report come out from them, right? Patrik had a report come out and was involved in that and things, and they put together this final document, because the Commission only went for two years. It's done now. It ended its tenure as an entity. And they put out this report on basically what their view is, this collection of people, experts in the field, and others, around what we need to do for the internet, and internet governance, internet policy, all of those kinds of things.

And I wanted to point out that among the many recommendations. They did specifically call out DNSSEC, and say, DNSSEC offers significant improvements to the current security, even though it is currently being deployed. It's not happening quickly enough. We all agree. Accelerating its adoption should be considered a high priority by DNS and network operators. It's essential that the internet technical community's ongoing promotion efforts, continues to support operators with [the one?] of DNSSEC through the promotion of capacity building programs, best practices, and guidelines.

So I just thought that was great the GSIG recommended that DNSSEC was something that the governments of the world and others should be paying attention to and working on. So, kudos to that, and with that, I am going to wrap my stuff and just say, any questions before we begin?

Okay, for speakers, Russ Mundy is sitting right here, and he will be operating his little clock, which you can see right here, which will show you how much time you have left. So we are endeavoring to keep on time. And let it be noted that I was one minute and 53 seconds early.

[LAUGHTER AND APPLAUSE]

Do you want the microphone, or do you want to…?

[SPEAKER OFF MICROPHONE]

UNKNOWN SPEAKER: It's up to you.

[SPEAKER OFF MICROPHONE]

MATTHÄUS WANDER: All right. Good morning everyone. My name is Matthäus Wander. I'm from the University of Duisburg-Essen in Germany, and today I would like to present some measurements and analysis about DNSSEC deployment on the service side. So how

many signed domain names do we have? All right, so actually we have three different studies here. The first one will be DNSSEC signing at the top-level domains.

Second, it will be a quantification of all second level domains, registered domains, by end users, by organizations, and this will be a total number, so this is a complete quantification. And spoiler alert, the number is over 5 million domains. And then we will look into some parameters, algorithms, key length of part of these domains, of 3.4 million domains. And I have to say that, data sets that we're talking about today are only slightly updated from 2015. However, I have run an update in the last week, to present you the most recent numbers on DNSSEC algorithms so that we can see how many elliptic curves, signing [inaudible] are being used.

All right. So first, let's talk about the top level domains. So next slide please. The measurement that we're using here is, we're downloading the root zone file from IANA daily, and we're probing the top level domain service daily for DNS key record and for some other records. And [inaudible] you're seeing observation over two years, from 2013 to 2015. All right, so you've seen figures similar to this.

As you can see, the total number of DNSSEC domains has increased, as has the total number of domains at all, due to the

new gTLD deployment. And as you can see, there is still a gap between signed domains and total domains, but this gap has been getting smaller and smaller.

All right, so let's take a look at what algorithms are being used by top level domains, and all top level domains are using RSA as signing algorithm. All of them are using separate key signing keys, and zone signing keys, which is no surprise. And if we take a look at the key length that are being used, the most frequently used RSA length, but length, for the key signing key is 2,000 bit, 2,048 bit. And the most frequently used size for the zone signing key is 1024. And there is a small cluster, well not quite small, it's a large cluster of zone signing keys with 1280 bit, which most of them can be attributed to [inaudible] registry services, which is an infrastructure provider for new [general?] top level domains.

Okay. So, now that we know 1024 bit is the most commonly used zone signing key size, now the interesting question is how often are they replaced? This is enough, and how often are the keys rolled over. I would like to present this data in two different groups. So here on the life side, you see those top level domains that have been signed for the whole time.

So these are the well-established domains that have existed for a long period of time, that have been signed for the whole two years. And we can assume that they have a stable operation,

reliable operation, they know what they are doing, and they are not changing their parameters daily, probably. And as you can see here, on the X-axis, the X-axis says the interval of key rollover procedures. It's in days.

And the blue line here says that about one-third of those top level domains, of 94 top-level domains that have been signed for the whole two years, are switching keys every 30 days, and most are switching keys after 90 or 100 days, so let's say three to four months. And almost all of them are actually replacing the zone signing key at one period, at one point in time.

There is a very small gap. You can see the blue line ends here. It does not go to the upper end. So a few top level domains haven't changed the zone signing key at all. These are the exception. However, if you look at the red line, you can see the key signing keys replaced by some top level domains once a year. By some top level domains, it has been replaced in an interval of two years, and this is what we can say from our observation of looking at the two-year period. And about half of the top level domains did not replace the key signing key at all, which could mean that they haven't done it yet at all, or it could mean that we haven't seen it in our two-year observation period.

If we go to the right figure, here we see those top level domains which have been signed for only part of the two years, because they started signing within these two years, or they existed for only a partial, well, only part of the two-year observation period, because most of them are the new generic top level domains.

So what you can see here is, those that are replacing the zone signing key, are doing it after 30 days, after 90 days, of the 120 days. So this is the usual replacement period, and about half of them did not replace a zone signing key at all. And if we take a look at the red line, the key signing key, about 90% have not replaced the key signing key at all. However, this could simply mean that the DNSSEC operation hasn't matured yet, that it hasn't existed for a long enough time.

So if the observation continues here, and if I present an update on the analysis, the figure might look a bit better. So yeah, we will have to look at this in the future. All right, let's take a look at the RSA public exponent, it's one of the vital parameters that you can choose, a part from the key length for the signing procedure. And the choice of the public exponent, the E-parameter, determines mainly the verification performance. The usual guideline is use a small value, and use a value with a low [inaudible], so use the value which has a low number of once in the binary representation.

And as you can see here, the most frequently used public exponent of this, two to the power of 16 plus one, there are some other numbers, Verisign uses, for example, the value of three, and there is also two to the power of 32 plus one, but all of these choices are fine. They are safe, they are fast, there is nothing wrong with them. So there is no big surprise in here.

Okay, so now let's take a look at the second level domains. First of all, let's count how many second level domains we have that are assigned. And the method that we're using here is zone enumeration, NSEC zone enumeration, which is quite easy, and NSEC 3 zone enumeration, which is a bit more difficult, but also possible. And we will be querying top level domain service, or top level domains. And we will include a few second level domains, which are well, let's say, part of a top level domain registry.

Like for example, [inaudible] or CO UK, we will apply zone enumeration on these as well and aggregate them under the respective top level domain. Okay, so the zone enumeration takes about three or four days. Can be run in parallel on all of those top level domains, and after it has completed, it yields 8 million NSEC records from 100 top level domains that are using the regular NSEC denial of existence, and yields 7.5 million NSEC three records with hash values from the NSEC three, of 540 top

level domains, which are using NSEC three hashed denial of existence.

As you can see here, the NSEC three record count is lower than the NSEC count, although more top level domains are using NSEC three, which is simply because they're using the NSEC three out feature, which means less records are created, thus we have few NSEC three records and NSEC records. NSEC three zone enumeration requires a bit of computation power in order to, well, compute on the client's side which query you would want to execute next, and then to send it to the server. And it requires computation time, however, as CPU, let's say a quad core CPU machine, sufficient to retrieve most NSEC three hash values.

So you would get about 99, more than 99% of NSEC three records, with one machine, with a CPU, but if you want a complete NSEC three chain for those top level domains which have large zones, which have let's say more than 100,000 domain names, then a CPU will take a very long time. So this is a point where we switch to a GPU or graphic cards, which offers more computation power, to close the few gaps so to get complete NSEC three chain.

All right, so here is the statistics about the NSEC and NSEC three records that we have counted, and the record includes a type

information, so we know how many secure delegations, or how many DS records do we have. And as you can see here, the Dutch top level domain, dot NL, has most DS records, 2.2 million, and then we have number two, the Brazilian, and the Czech top level domain name.

We have dot COM and dot SE. And what is interesting here is that out of those top five with DS records, with secure delegations, four of them, those country codes top level domains, have provided some kind of incentive in order to activate DNSSEC, so that the registrars who will be using DNSSEC, and it looks that these initiatives have been successful, and they actually led to, well, quite high, or quite large, deployment numbers.

I don't know whether dot COM has provided some kind of incentive, but it's safe to assume those, these incentives provided by country code top level domains, have fueled the deployment at the dot COM top level domain as well. So on the next slide, here with an explanation of the, what we actually see here in the numbers. We have a total number of securely delegated registered domains, so people have registered those domains and have activated DNSSEC, and the total numbers here, 5.1 million.

And then we have a few, not only a few, but one million, almost one million, address records, so we can see that there are A records, quad A records, and a few C name and [inaudible] records in top level domain zones, which is not what you usually would expect, but yeah, it exists as well.

We have some NSEC three records with an empty type field, I will explain it on the next slide, and we have, well, other records which are not of interest to you. Okay, so why do we have these many address records and NSEC three records with an empty type field? Some top level domains allow to put address records, that's part of the operation. For example, the dot DE top level domain allows us to put delegations, secure delegation into the zone, but under certain conditions, you're also allowed to put address records directly into the TLD zone.

So this is why you can, for example, put WWW dot example DE into the zone, and if you put WWW dot example DE into the TLD zone, then NSEC three would [inaudible] that there will be also a NSEC three record for example DE, which will have an empty type field, which will be for an empty [inaudible]. This is how NSEC three works, denied of existence requires that each empty non-terminal will have its own NSEC three record.

So this is why we have address records and empty records. And if we go to the next slide, we can see here dot ORG has also a few

address records and NSEC three records with an empty type information, and I'm not aware that dot ORG allows to put address records directly into the zone, however, dot ORG seems to, it seems that it does not force the removal of [blue?] records after a delegation has been removed.

So if you have a delegation, and if you put [blue] records into the TLD zone, then the [blue] records is not authoritative, it will not be signed. However, if the delegation is removed, then the formal [blue] record will become authoritative, and it will be signed. So this is why there can be records like NS1 dot example dot ORG, which will be an authoritative record after the delegation has been removed, when there is no longer a delegation.

And if there is an address record, as one example of dot ORG, then it will be also a record with an empty type field, so there will also be record for example dot ORG, which is again, because NSEC three denial of existence requires these [inaudible] records.

[SPEAKER OFF MICROPHONE]

I'm not sure about this. I will have to look at the complete statistics. Oh, we had a question. Maybe you can…

DAN YORK: Yeah, so just to let people know. If you are going to ask a question, which is awesome, we encourage questions, please do come to the microphone and speak, because we do have people listening remotely.

MATTHÄUS WANDER: Okay, so let's move on to the next slide. So now that we've quantified second level domains, now that we know how many second level domains are, let's take a look at their parameters. So the measurement method that we're using here is, first we need to know the clear text domain names. We have now counted NSEC three records, but these include only hash values, but now we need the clear text domain name, so that we can send queries for DS records for DNS key records.

And in order to do that, we need to, well, reverse those hash values to clear text name, so we need to employ hash breaking techniques, and this requires a lot of computation power. And in order to do this efficiently, we need to use GPUs. We can use CPUs, but we will go get only very few results from it, so we're using GPUs in order to do this.

And the numbers that we're getting is from the 7.5 million hash values that we acquired. We can reverse 4.6 million hash values, in about three weeks of GPU computing, with four graphic cards. So four consumer graphic cards are sufficient to break 60% of

the hash value with little effort. And I don't want to go into the detail, how this hash breaking techniques works, however, there are different methods. [One possibility is to use] brute force each and every mark of chain based attacks, but a dictionary based attack is the most efficient one.

Okay, so after we have broken part of the domain names, and that we also know the NSEC records, there are also clear text names in it, we're now sending queries for DS records for DNS key records, and out of those 5.1 million DNSSEC signed domain names, we get a response from 3.4 million domains. So this is, these are the [inaudible] that we know. And we're sending DNS key queries, and we're looking at the algorithms that have been used. And what we can see here, first of all, zero domains are using RSA with MD5 as hashing algorithm, which is good because it's deprecated and insecure. And what we can see is a few domains use DSA, but the number is not very large.

But the most frequently used algorithm is one of the RSA variance. More than 99% of domains are using RSA assigning algorithm. And in 2015, this is again a slightly outdated number, we have seen that a few appearances of elliptic curve signing algorithms, either the Russian ghosts standard, or the [inaudible] standard.

And on the next slide, we have update from last week. I've re-queried those 3.4 million domain names, and I got a response from 2.6 million, so not all domains are responding anymore, which is while domains are appearing, they are being added and removed. So the name space is always changing. So not all domains exist at this point. This is, well, I would say, expected.

However, 2.6 million are still existing and have responded. And what we can see is that DSA number are declining. RSA is still the most frequently used algorithm, and easy DSA numbers are growing. The number is not huge, but keep in mind, and this is the number of domains that have switched from one of, well either DSA or RSA to [easy] DSA, so this, these are not newly signed domains.

This is a number that I cannot give to you today. Okay, so let's take a look at RSTA length being used at second level domains. First of all, we can see that a few thousand domains are using 512 bit RSA keys, which is definitely [inaudible] doesn't offer any reasonable security over unsigned domains. 512 bit can be broken on one machine, within three weeks, and if you invest some computing power [inaudible] NC2, you can break it within a few hours, if you invest some few hundred dollars.

So the most frequently used size for the key signing keys, like with the top level domains, 2,000 bit. The most frequently used

size for the zone signing key, like with the top level domains, is 1024 bit. And I haven't included the 2016 numbers here, but the numbers are slightly shifting to longer keys, but there is no major change here. So the keys are getting slightly longer, but 1024 bit is still the most frequently used size for the zone signing key.

Okay now let's take a look at the RSA public exponent. Here we see a bit more diversity at the top level domains. First of all, two to the power of 16 plus one is as well, the most frequently used RSA public exponent. But we see numbers that are close to the power of 16 plus one, but not exactly. And this looks like there have been some occurrences of a type, also people maybe manually entered, or tried to enter, 65,537, but they made a typo, and this is, well maybe, a strange or funny, but this shouldn't be really a problem.

The verification performance will be slightly lower, but probably within a [inaudible] range, so nobody will notice. And there is no security issue with this, as long as the RSA algorithm is implemented correctly. If the RSA algorithms is implemented correctly, and the basic RSA properties are met, and then you can use different exponent. This shouldn't be a security problem.

Okay, so we have seen few domain names, a few domains have been using DSA, let's take a look at the key lengths here. And the maximum key length, which is specified for DSA in DNSSEC is 1024 bit, and this is also the most frequently used size for the key signing key and the zone signing key.

So you cannot use a longer key because it is not specified. However, please not that 1024 bit DSA key is, does not have the same size in your DNSSEC response on the wire, like 1024 bit RSA. This is because these algorithms work in a different way, and a DSA requires additional parameters. So the 1024 bit is [inaudible], but there are additional parameters. So the response will be about three times as large.

And as DNSSEC is quite sensitive to the message size, DSA may not be the right choice here, compared to well, other algorithms. Okay, let's try to validate those domains. We have 3.4 million domain names, and we are trying to validate the DNS key records, and what we can say is that 99% validate successfully, but we can also see that 0.6% fail to validate in 2015.

And in 2016, numbers got slightly worse. Now 1.3% are failing validation, so which would be in absolute numbers, 20,000 and 30,000 domain names. And the most frequent error that we have seen is that when we're querying for a DNS key record set,

we do get a response, but the response does not include any DNS key record.

So there is a DS record, it indicates this domain name as signed, this domain is signed. It should be signed, but we don't get a DNS key response or… That's not true. We get a DNS key response, but without a DNS key from the DNS service. So there is a dangling DNS record, and the validation will fail.

Then another error that we've seen is that there is a DNS key in some instances, but it's not the right DNS key. So probably there was a rollover and it hasn't been updated, or some other configuration error. And we have also seen that signatures have expired, so this will also result in a validation error. And this type of [fault?] has actually gotten better, so in 2016, there were less expired signatures, so maybe automation of the signing has worked on maybe, I don't know, signing operations got better, and whatever the reason is.

Okay, so here are a few recommendations. First of all, deprecate DSA. It's using large DNS key records, specified up to only 10, 24 bit, which is, which may be sufficient for now, but it won't be sufficient in the next year or so. It's better switched to RSA or ESDA, this would be a better choice in my opinion.

If you are using RSA, use keys with at least 2,000 bit key length, and this is a general consensus that a 10, 24 bit has not been

broken yet, so it's considered safe for now, but it's not, secure for now, but it's not considered secure for the next few years. So if you're continuing to use RSA in the next few years, you should update too long a key. So let's say 1500 bit or 2,000 bit.

These are recommendations which have been made by [inaudible] or by BSI, or in academic literature. If you are stuck with 10, 24 bit for operational reasons, replace the key every few weeks, if you can. This is what most TLD operators are doing, or what many TLD operators are doing. I don't know whether second level domain operators are doing this number, which I do not have here.

Consider using ECDSA, 256 bit should be enough. This offers security level comparable to RSA with 3,000 bit. So ECDSA has short message sizes, and has good security level, so it's a wise choice for an algorithm. And consider if you can use a combined signing key instead of a separate key signing, key zone signing key.

If you are TLD operator, this is not an option for you. You are probably using hardware security models, and you need to use those separate keys, but if you're signing on one machine, and both of your KSK and your [inaudible] are on the same machine anyway, you probably don't have any advantage from doing this. So in this case, you can use a combined signing key, which

serves the same purpose as both the KSK and the [inaudible] and you will save a bit on the message size.

So you can increase your RSA key length, for example. Okay, so let's conclude. We have seen there are more than 5 million domains that are using DNSSEC. Around 1% of them have shown validation errors. We've seen that RSAs are dominant signing algorithm. A few domains have switched to ECDSA, but what I do not know is how many newly signed domains are using ECDSA, or another elliptic curve [inaudible].

This is… In order to do this, I would need to rerun the zone enumeration, and this is a number which I can maybe provide to you in a few weeks. Thank you so much.

[APPLAUSE]

DAN YORK: Thank you, Matthäus. And I knew the question line was going to start, because I remember the comments you had in there were just like baked for the folks who are here. So go ahead, Robert, shoot.

ROBERT: Hi, I'm Robert from PCH. Have a question about one of your earlier slides, says how often people, KSK rollover. It seems that

many of the new gTLDs that came into the root zone, immediately after getting into the root zone, they would actually roll the key. And it would be interesting to see if anyone, just after the initial key rollover, if they actually did something, because I think they probably came into the root with a test…

MATTHÄUS WANDER: With a test key, yeah.

ROBERT: …with a test key, and because ICANN wasn't really clear into how to get into the root. And suddenly they would email these gTLD registrants saying, "Hey, you live to go… You're set to go live tomorrow." And people were kind of panicking a little bit. So I think many did the PDT test, pre-delegation tests, with actually software keys, and then they got into the root, and then they switched. That's my guess.

MATTHÄUS WANDER: That's an interesting point. I would have to look into that. Thank you.

SHANE [KIRK]: Hi, Shane [Kirk]. Could you go back one slide maybe? To the recommendations? Yeah.

[SPEAKER OFF MICROPHONE]

What's that?

[SPEAKER OFF MICROPHONE]

[Inaudible]? Yeah, actually that was my question. Consider using a combined key. So I probably didn't really understand it, because it seems like… I mean, the whole reason why we have the KSK model, ZSK model, is to make administration easier. So if you're using a combined key, then don't you have to update your DS record every time you change your key?

MATTHÄUS WANDER: That is true. That can be a disadvantage, you're right on this point. However, if you can automate the DS update, then this shouldn't be a problem for you. And there are algorithms or methods to simplify this update.

UNKNOWN SPEAKER: Okay. I know there is some work going on at the IETF right now to try and automate that, and guess if you are happy with your registrar and are comfortable doing some scripting, then it can be made to work.

MATTHÄUS WANDER: Okay, so let's say it's maybe not the best choice for everyone.

UNKNOWN SPEAKER: Okay, fair enough, yeah.

DUANE WESSELS: Hi. Duane Wessels from Verisign. You talked about zone enumeration. Did you enumerate all of the zones? Or did you get the zone files from some places?

MATTHÄUS WANDER: We enumerated all top level domains.

DUANE WESSELS: Okay. Is there a reason you didn't get the zone files from the ones where they were available?

MATTHÄUS WANDER: Well, zone enumeration works fine. So… [LAUGHTER]

DUANE WESSELS: Okay. Well, the reason I asked is because, like for dot COM and dot NET, I get different numbers than you showed.

MATTHÄUS WANDER: Maybe this is because numbers are from 2015. I'm not sure about this, but it should be a good idea to compare these numbers, if you write me an email.

DUANE WESSELS: Okay. Can I ask one more? Did you…? Do you see any evidence of like more than one algorithm used by TLDs or second level domains?

MATTHÄUS WANDER: Not by TLDs, by second level domains, I haven't looked into this specifically. But I guess this could probably be happening. I should look into this. Thank you.

DAN YORK: Opportunity for future research, there you go. Andre.

ANDRE: Andre [inaudible]… Why 2K RSA keys? Why did you pick the [inaudible] bits?

MATTHÄUS WANDER: Why to use 2K RSA keys?

DAN YORK: In your recommendations.

ANDRE: In your recommendations. Why not something in between?

MATTHÄUS WANDER: Well, there is a recommendation [inaudible] which uses 2,048 bit [CROSSTALK]…

ANDRE: …for long-term signatures.

MATTHÄUS WANDER: That is true. All right. That's true. So if you're replacing your key very often, you can use a lower number, will be still secure. However, this recommendation here, this is not specifically for TLD operators, which are changing the key regularly before, let's say, the general audience. And second level domain operators might not want to roll the key every few weeks.

ANDRE: Yeah. Well, it's my recommendation, don't use 2K keys because they are too big, just switch to ECDSA.

MATTHÄUS WANDER: Yeah, that's a good recommendation.

DAN YORK: All right, we like that. I'm going to cap the question queue, because we're running out of time there. But go ahead Edward.

EDWARD: Edward…

DAN YORK: [Inaudible] ask another one if you want to.

EDWARD: Edward [inaudible] from dot NA. Since I know you didn't ask me for permission to do this, how many laws have you broken?

MATTHÄUS WANDER: I got a similar question two or three years ago when I introduced NSEC three zone enumeration tool. And I know that some people are not happy about this, and I actually was [inaudible] when I started this research, and I emailed one of the SIDN labs employees. And he said, "Well, continue doing if you know that you're not doing any harm. And if you feel that something might go wrong, ask us first."

And I don't know how many laws I have broken, but I haven't caused any disruptions. So this is what makes me happy about this.

[SPEAKER OFF MICROPHONE]

I don't think there is a law about root zone enumeration, there probably is a civil case.

DAN YORK: Not yet anyway.

[SPEAKER OFF MICROPHONE]

MATTHÄUS WANDER: All right.

MARK: Mark, from Microsoft. I have a comment and a question. The first comment is, the first speaker mentioned that they were not looking at IDNs in the ccTLDs or otherwise, please look at IDNs.

MATTHÄUS WANDER: IDNs have been included here. I've included all top level domains. However, the IDN numbers are lower, so they're at the bottom of the list.

MARK: Yeah. I am very interested in universal acceptance, so IDNs is of particular interest to me. Also, the question, I don't know if you have… If this is…? Is this the first time you've done this or the second? I was very surprised to see how much [inaudible] was still being used, and I was wondering if there were a trend towards deprecating that? And I was wondering if you could make that part of your recommendations to use [inaudible]?

MATTHÄUS WANDER: This was the first time that I've made this study to this extent. It is a complete quantification. However, I can compare the 2015, 2016 numbers. I think, we haven't seen a shift from [inaudible] 156, but yeah, this could be one of the recommendations. Yes. Thank you.

DAN YORK: Thank you, Matthäus for this research. Thank you. Give Matthäus a round of applause.

[APPLAUSE]

Mark, just to clarify to you. We actually track all of the IDNs in our database, but in the maps, right now, they just go on ccTLDs. So they only change color based on that. So to give us another

perspective on some of these measurements, and for those who are new to DNSSEC workshop, part of what we like to do is look at some of these measurements, and we have different mechanisms and methods for that, and so Geoff.

GEOFF HUSTON: Thanks Dan, and good morning all. My name is Geoff Huston, I work with APNIC. And I'm going to give you a very quick rundown of the other side of the coin. There are folk who sign their domain names with DNSSEC, and you've seen how many and what algorithms they use, but of course, folk need to use it to validate. And so what I'm trying to look at is, how many people will validate a signed name?

So this is a quick review of where we are with that. Next. So, I'm actually doing a particular experiment, and I used Google Ads to do this. Why? Because for this kind of broad based measurement, the ad network is amazingly good. They actually try and give me fresh eyeballs every single time, as long as you don't click on it, it's really, really cheap.

For a little over $100 a day, we get around 10 million experiments a day, because inside the ad, you can put HTML 5. You can put in active scripting. So you don't need to click. As soon as the ad gets impressed in your browser, be it on a mobile or on a laptop, or whatever, the HTML 5 will run. And what it

does is it gives you three very simple tests. Get these three URLs. The URLs are unique, absolutely unique. They include timestamp, they include a bunch of stuff inside the domain name part of this. So in [inaudible] won't help you. Doesn't help. This is designed to defeat all [inaudible].

One of the names is correctly signed. So it has got full DNSSEC, the lot. And I've actually done a little bit of a trick, so that it looks like there is an infinite number of signed, delegated domains to make all of this work. So I'm using a sort of [inaudible] resolver, thank you Ray [Bellus?], that actually generates signed sub-domains on the fly.

The second one is badly signed. So that if you go there, you're not really following validation, are you? Because you're never meant to go there, it's badly signed. And the third one is not signed at all, which is the control. In this particular experiment, I'm using [inaudible] one. I have reported, and I reported at the last meeting on ECDSA, and I'll share the results again now, it hasn't changed much.

And what I'm looking at is, how many users will do this? Because actually there is a difference between resolvers and users. The ad goes to the user's browser, I'm counting users by browser. Looking at resolvers is much more complicated, because of resolver farms, passing around queries, resolvers are

difficult. So I'm not measuring resolvers, and I'm not measuring signed domains, that's a different problem. Next.

So this is, you know, a standard map of the world. The light of the color, the more [inaudible] elevation I see with the users in that country. This is a percent, basically, of users in that country that receive the ad. So Iceland, Sweden, and Norway, you know, a little pocket of green. Next. And that's where we see the most validation by user communities. There is an impact of Google's public DNS. And Google's public DNS has been actively pushed in areas of what looks to be sub-Saharan Africa and across Southwest Asia, is where you see most of it. So those high numbers there are largely as a result of ISPs actually using Google.

I have no idea about Papua New Guinea. Absolutely none. Little pocket of green down there. Next. So this is the picture you saw before. Those dips down that you're worried about, when I say I do delegated sub-domains that are signed on the fly, I do most of the time. But sometimes, the delegated signing code sort of gets stuck on a date and the date expires, and it takes a day or two to go, oops, and fix the thing. So, as you see, it's sort of a 30 day interval, and sometimes we jump a bit late. That's why it dips a bit.

So next. What you actually see is, oddly enough, a momentum of DNSSEC adoption has largely topped off. That globally, you know, between 14 and 15% now, and that hasn't really changed an awful lot since the start of 2015. Next. So what's going on? Now, there are some folk who have had this switched on forever, and almost every single ISP in Sweden has it turned on.

So no matter where you look in Sweden, they're doing DNSSEC validation for their users. If you are in Comcast and you let Comcast do your DNS for you, it's validating. And there are an awful lot of Comcast users on this planet, you know. If you are in Estonia, that way? [LAUGHTER]

Two-thirds of you right down there, are doing validation, and have been for an awful lot of time. And Romania, which recently signed dot RO, actually turned on validation back at the early part of 2015. So these are a kind of incumbents. There are more than this, but that's kind of the folk who have been doing it for some time. Next.

And these are the folk who just turned it on. If you notice, Brazil changed color, and the reason why, is that one provider, [Clair-O], turned it on. Now [Clair-O] is big. So then when [Clair-O] turned it on, you actually saw a large amount of users in Brazil actually then started doing DNSSEC validation. Iceland is green

largely because Ice Net turned it on start of the year. And you can see the results. Obvious, you know, that it's working.

And interestingly, the Farrell Islands, which is almost the clean sweep of the Scandinavian countries, the Farrell Islands, again, turned it on earlier this year, and 90% of the sheep and the people on the Farrell Islands all do DNSSEC validation.

In Australia, we're keenly interested in New Zealand, obviously, the poor cousins to the east. And fascinatingly, the bastards have ratted on us, and now about half of the users in New Zealand are now doing DNSSEC validation, which is not the case in Australia. So while the numbers are steady globally, there are still folk who actually are turning it on.

And you can see, as they turn it on, some cases, like [Clair-O], they do bring a few million users with them. Other cases, like the Farrell Islands or Iceland, it's a smaller population. Next. So what about here? That's not my measurement. In Finland, you actually turned it off in July last year, and turned it back on again later in the year, and almost none of you use Google in Finland, if there are any Finnish here.

Very few folk in Finland use Google. These are actually the service providers actually doing DNSSEC validation. Currently sitting at around, if I can see that right, 30, 40%. No, 20, 30%. Next. So we know who you are. So if you're using [inaudible],

you're validating. If you're using [inaudible] Networks, [inaudible], what does [inaudible] mean? Something.

[SPEAKER OFF MICROPHONE]

Yeah, right, okay, thank you. Thank you Finns. If you're using [Nebulas], you will probably be using a validating resolver. If you're using DNA, like my phone, wherever my phone has got to, no. Or [inaudible]. If you look over on the right, that's the sample count. And within a country, Google tends to smear the ads relatively evenly. So my guess is, in this country, there are three biggies, DNA, [Alyssa], and [inaudible], and then a fourth, a [U-Net], which is kind of there, about half of the size of the others.

And the rest are kind of small. So one of those big four is validating, the others aren't. Someone should do something. Yes? Okay, good. Next. The bigger picture around here. Google has done most of its work with public DNS in Africa, so this, the numbers in Africa, and in parts of Asia, largely reflect that concentration where Google has evidently concentrated their efforts.

Anyone else using [all eights?] is basically doing so almost, I think, accidently. Yes, they can, but there is no great focus. In North America, the momentum is stronger behind Comcast decision. Interestingly, the other big providers haven't taken it

up, which is surprising but, you know, sometimes folk look at their competitors and emulate it, sometimes they proudly just ignore it. Don't know why.

Where I've seen trends that I haven't actually noted, as well as Iceland and New Zealand, bastards, Norway has actually moved, and Nepal has been recent ones that have taken this up as well. Next. The first thing I should mention though is just a brief sideline, it's not in the slides about ECDSA. As we try and increase the key links, we run into larger responses.

As we run into larger responses, we're going to run into a problem with UDP and v6. Once the response rate gets above 1280, and you're using a MPU of 1280 in your server, you're going to run into an enormous problem, because once you start using extended headers for fragmented packets, you can confidently expect a drop rate of 30%. Not of the frag, of the leading part of the packet. So big packets in the DNS, particularly with v6 which is where you're definitely heading, do not go well together.

And so ECDSA, you really should be looking at. And you really should be looking at whether you're doing an up to date resolver library. So if you're running a recursive resolver for your users, check out whether you support ECDSA. If not, it's likely you're running a really, really old software set, that's bad for two reasons.

Really, really old software has its bugs, and that's really, really bad. And secondly, you really should be running ECDSA and v6. So, do something. Back to what I've said here. If you actually are running an authoritative name server, what you actually see is not 14% of folk validating. That's not what you see.

What you typically will see is that almost everyone, 80% of all of the queries you get, are going to have to have [inaudible] zero and DNSSEC okay. So if you've got a name that's signed, you will be serving those credentials, for eight out of 10 of those queries, which is amazing.

However, only one quarter will follow it up with a request for either the DNS key, or the DS record. So any one quarter of them, will actually start to perform validation. That's still more than 14%. That's 25%. But, a whole bunch of you, including ISPs as well as users, have set up a second resolver. And if you don't like serve fail, you go to the other one. And about half of the folk who validate, go to a non-validating resolver as their secondary resolver.

Why did we do NSEC three? To stop zone enumeration. Yeah, that worked well. Why do we have secondary resolvers? So that we don't believe DNSSEC validation. Yeah, that worked equally well. If you're going to have a secondary to a validating resolver, make that one validate too, right? Because half of you don't.

So that leaves us with that 14 to 15% of folk, that when they get back server fail, believe it, and even if they have a second resolver, still believe it. Serve fail, in this context, a badly signed name, is a badly signed name. So that's kind of the area. There is rich picking. If you are an authoritative name server, it looks like the world is validating actually already. Everyone is picking up credentials.

It's just the resolvers aren't following up, and maybe they should. Next. So that's where the reports are, world maps, stats, all kinds of cute things. There is a whole bunch of v6 stuff there as well, if you kind of look behind that URL a bit, and in particular, some new reports that I've put up as to who is dropping v6 on the floor, if you're interested. So any questions?

UNKNOWN SPEAKER: So we'll turn things over to questions, and be sure to state your name please. And I see that there is Dan York. Thank you.

DAN YORK: Dan York. Thank you. So, Geoff, these are great. I love your trend lines. It's always good. One question I had for you, on your mechanism, you know, there is an increasingly amount of use of ad blocking software. I use it myself on all of my things on that…

GEOFF HUSTON: Evil, evil, evil person.

DAN YORK: Well, so my question is, are you seeing…? Do you have any way of measuring that impact, or seeing…? Are you seeing a decline in sample size? I mean, it's a big debate within the publication industry right now. The media industry around the use of ad blocking. I'm just curious.

GEOFF HUSTON: Well, right now, sort of we put up a budget, it's called CPM, it's clicks per million or something, and we put up, I think, 150 budget, and it delivers approximately 11 million ads a day. We exhaustively analyze what we're doing, and how we're doing it, and how the ad machinery works. But what we don't know, and it's really, really hard to know, is, what's the live population out there that isn't getting ads?

It's one of those huge unknowns in all of this industry that we can sort of dimly guess at some of these numbers. What we do know, and we do analyze, is the source address of the folk that actually get the ad. So this is why we get this constant evidence that Google's pool of potential ad folk, is very, very big. It's certainly up in the low billions, you know, easily.

We're constantly at 11 million a day to seeing new addresses. To what extent we see blocking? Really, really hard to tell because if the ad gets blocked, the HTML 5 doesn't run. If the HTML 5 doesn't run, you don't talk to me. If you don't talk to me, you don't exist, Dan. All right? It's as simple as that.

DAN YORK: Yeah, no, it's interesting. Anyway, thank you for the ongoing reports. It will be interesting to see how this continues as ad blocking, because I know there is one provider, a mobile provider in the UK, who is now blocking all ads on their mobile networks for all of their providers. They're doing a new thing, so you might not see anything coming back from three, I think, in the UK.

GEOFF HUSTON: I'm seeing Sky Net like crazy. The only one that's sort of weird is anomalous is SKA Telecom in South Korea, extensively has a much higher market share than I'm seeing in ads.

DAN YORK: Yeah, anyway, good. Thank you for the continued work.

GEOFF HUSTON: Thank you.

UNKNOWN SPEAKER: Thank you very much.

[SPEAKER OFF MICROPHONE]

More questions, please.

MARK: Mark [inaudible] at IS. I have a question about fragmentation. Do you suggest that the size should be limited to 1280 to prevent fragmentation of UDP?

DAN YORK: If you're running UDP and v6, I would strongly urge you to set your NTU at 1500. If you're running TCP and v6, I would set your TCP MSS down to 1220, because the whole issue around the fragmentation handling of v6 is so shocking, you need to avoid it. If you run your UDP at 1280, and you've got responses of 14, 14 octets, I think Verisign are going to tell us in a few minutes, if you've got high response sizes, you know, drive straight into that problem with UDP.

And the problem is, because both leading and trailing frags get dropped, as if the server wasn't there. So you're getting at this whole query retransmit, time out disaster. So if you are running v6 on your recursive resolvers, look at how you can up your MTU

to 1500, but drop, kick your MSS for TCP low, because if you're running a high MSS for TCP, you've got the other problem of ICMP6 path too big.

Whoever said v6 was easy? Yeah, right.

[SPEAKER OFF MICROPHONE]

Thanks Martin. No, it's a little bit more complicated than we thought, and one size does not fit all is what we are learning. 30% packet drop rate is just horrendous, but that's what we're seeing out there with v6 large UDP packets.

UNKNOWN SPEAKER: [Inaudible] and [inaudible] actually [inaudible] on DNS, UDP, IPv6, and if you behave nice, that's what unbound bind are doing in default, you actually, as an application, you'll create the fragments at 1280. That's the recommended way of doing it. But it turns out that if you're not nice, and don't do the [obvious] thing and fragment, you have to get a much better [inaudible] using UDP v6.

But apparently a lot of networks do accept [inaudible] and 12 80 packets. So we are actually thinking about changing the software and being not nice.

GEOFF HUSTON: The underlying drop rate in v6, that I did the same experiment using ads and using large responses. The underlying drop rate between 1280 and 1500 and v6 is 3%. If you turn your MTU down to 1280, your drop rate immediately climbs up to 30%, oops.

UNKNOWN SPEAKER: Yes. And that's, I mean, as I said, since IPv6 [inaudible] in the application, not in the network, you know, unbound and bind are actually doing this nice, and so…

GEOFF HUSTON: I think the default configs are wrong for UDP, is what I'm saying.

UNKNOWN SPEAKER: Yeah, yeah, that's right.

GEOFF HUSTON: That's what you're saying too, right?

UNKNOWN SPEAKER: That's what I'm saying. We were really thinking about making the default not nice.

GEOFF HUSTON: Yeah.

SHANE [CURR]: Shane [Curr], Beijing Internet Institute. So, I have a question. I agree with your recommendations about UDP for fragmentation. It makes abundant sense. And hopefully you can convince all of the Australians that this is true. So, but I'm not sure I agree about the recommendation for lowering the TCP segment size.

My thinking is that, DNS is weird, but if we're using TCP, we're using the same thing the web browsers use, so surely if the web works at all in IPv6, we shouldn't have all of these ICMP blockage problems and things like that, right?

GEOFF HUSTON: Wrong.

SHANE [CURR]: So why does this not affect people on the [inaudible], and why does this not cause huge consternation of problems for the Googles, and the Facebooks, and the [CROSSTALK]…

GEOFF HUSTON: …eyeballs is your friend is the base answer to this, Shane, that all of, most of the world is actually ill-stacked equipped, and most of the world actually sets off the two horses down the

same race, and they're waiting for the first [inaudible] exchange to actually work. And so, in general, v4 saves your bacon when v6 dies, seems to be going on.

But in the DNS world, that's time, and it's time you don't want to spend resolving an ephemeral question. The fast you can get rid of the user, the better everyone else is. So for TCP, you will avoid that problem by starting with a MSS that's at 1220, you just avoid the problem.

And your payload is such, because you're going to stream, hopefully the guy is giving you a window, that allow you to stream multiple response here. The parts of the response that are big anyway. You're not losing time, what you are doing is avoiding the RTTs to measure, to repair the problem.

SHANE [CURR]: Sure. On the other hand, that makes a certain amount of sense, although if there is any problems with the v6, which you know, v6 networks tend to be crap, then have the eyeballs, all the logic there makes sense, in which case…

GEOFF HUSTON: Go to Italy, v6 is astonishingly fast compared to v4.

SHANE [CURR]: Okay. Well, interesting, thank you.

JULIE HEDLUND: And with that, I think we do have to cut off the questions, but please join me in thanking Geoff for a very informative presentation.

[APPLAUSE]

And now I'd like to ask the moderator, Russ, and the panelists to come up for our panel discussion on DNSSEC deployment challenges.

RUSS MUNDY: Thank you Julie. I think we've made our way up here, and we're going to just move right into it. Most of the people know me, I'm Russ Mundy. If you don't, well I guess this may be your first workshop. And if it is, I'm very glad about that. We're always happy to have newcomers here. So today's panel, and this is one of my favorite ones that we do something of this nature at almost every one of these workshops, and that's what are our challenges in DNSSEC?

And so we have a great cross-section of people here today. And I want to just go ahead and go down the list alphabetically. I think that's how we have the folks on here. So why don't we go

ahead and just start with Dani. Just jump right into it. Dan's going to run the clock, and I think we had 10 minutes a piece, was it? Eight. Eight minutes a piece, okay.

Because we do want to keep time for questions. Go ahead Dani.

DANI GRANT: Hi everyone. I'm Dani. I work at CloudFlare on DNS and registrar. Next slide. CloudFlare signs 56 billion DNS record sets live on the fly every day. And at this pace, we care a lot about computing costs. And one of the key ways we save compute is by lying in negative answers in DNSSEC. So I'll give brief background and then I'll show you exactly how we lie. Next slide.

So this is everything that goes into a negative answer. Next slide, next slide. SOA, next slide. The signature, next slide, NSEC, next slide, for previous and next name, next slide, the signature, next slide, next slide. Keep going. For the wild care, so the signature, okay. So next slide.

So that's six records, next slide. For IETF dot ORG, that's over 1,000 bytes. Next slide. And of course, there is a problem where you can continuously ask for the next name, next slide, and discover every name in the zone. Next slide.

So this is actually in the spec. This was considered a feature. Next slide, but it's a bad idea. Imagine you can get every name in the dot GOV zone, and you would discover every US government agency, including the secret ones. Next slide. But of course, there is NSEC three to the rescue. Next slide.

But NSEC three is a close but no cigar solution to the problem. Next slide. It actually gives you bigger answers, and now requires a third NSEC three and signature in the answer, and while it makes zone walking harder, it's still not impossible, as we saw, in Matthäus's talk. Next slide.

So to recap. There are two problems with negative answers. The first is that it requires the authoritative server to return the previous and next name. This is an extra lookup in every negative answer, and it enables zone walking. And the second are these giant answers just to negate the non-existence of something. Next slide.

Okay, so let's look at the first. The problem with previous and next name. So they're expensive, there is an extra lookup, and it leaks information about the zone. Next slide. So, something interesting about CloudFlare is, we actually do not have a zone file at all, which makes this lookup even more expensive for us.

We have a database with all of the DNS records, and so if we want to get the previous and next name, we have to go to the

database and ask it to do a sorted search. Next slide. So there is a solution to this previous and next name problem, it's RFC 4470, and it's called white lies. And white lies says, you can just make up the previous and next name.

And this helps. This is great. It solves the extra lookup, and it solves the zone walking problem, but it still requires two NSEC records to say one thing. Next slide. So we decided to take line to the fullest extent. Instead of white lies, we do black lies. Next slide. This is an example of CloudFlare's black lies. You'll notice two things.

The first is that the NSEC is returned directly on the missing name. so this means that we can return one NSEC record instead of two. Next slide. The second thing you'll notice is that we always return this generated value as the next name, and this saves us a database look up. Next slide.

This means we can just return one NSEC, these four records, next slide, and our answers are pretty small. Next slide. So we just don't rely on an ex-domain, we land on data too. Next slide. So no data, just background, returns one NSEC with all of the types that exist on the name. Next slide.

We think this is super inefficient. To do this, we would have to go and look up at all of the types that do exist, just to tell you that the one type you ask for does not exist. Next slide. But

remember, we like to lie, so what do we do? We set all of the types, just not the type that you asked for. So next slide. So we call this the DNS shotgun, when you ask for TXT, we say, "Yes, all the types exist, just not TXT." And then if you ask later for MX, we'll say, "All the types exist, even you know, TXT, just not MX."

You might be wondering how this might be standards compliant. You might be. There are three things. White lies already allows us to randomly generate the next name in NSEC. The second thing is that while because we set NSEC directly on the missing name, we do not need a second NSEC in the record, in the answer, and zone files are constantly changing.

And so setting many types in no data responses is feasible as well. We've also submitted our black lies as an internet draft, and so hopefully they'll just become the standard.

[SPEAKER OFF MICROPHONE]

RUSS MUNDY: Well Dani? That was impressive. Thank you. [APPLAUSE AND LAUGHTER]

I think I'd like to have us continue on, and then we'll keep the questions at the end. So if you have any questions as we go through, take a little note, write them down, and we'll jump into them afterwards. But I will take the moderator's prerogative

and say, have you been visited by the protocol police? [Laughter]

Guess not. Okay. I believe Ari-Matti, is that right? Okay. Good, please, go right ahead.

ARI-MATTI HUSA: All right. I have a different view on this. I represent FICORA, which is the registry in Finland. We do the FR domains, please next. Administer the domains. There are about 400,000 now, a little bit less. IDN, DNSSEC, and IPv6, of course. And the law is changing in September so there might be a little bit of those domains registered then.

And also a side note, that [inaudible] Island, dot AX, is not managed by us. They have their own registry. Next please. That's the infrastructure we are using. We have the domain database system in-house, and then we have the primary data [inaudible] and a bunch of secondary all over the world.

The website domain, dot FI, which is going to be [inaudible] for some reason that I don't really understand, is the place to register domains and manage them for the customers also. And at the moment, anybody can, any Finnish person or company can register their own domain directly from us.

We provide the website and web service interface also for registrars until September 2nd, and then the WHOIS is open data service. And from September the 5th, when the law changes, we have the EPP interface for registrars. Next please.

Okay, that's, well the same thing really, we're switching to registrar-registrar model for all domains in September. No longer open only for Finnish registrars, so you can register your domain name with dot FI if you wish, even from New Zealand. [LAUGHTER]

Also, at the moment, we require when you register a domain, you have to fully functioning DNS server, that's not going to be the case after September 5th. Okay, the plan was to, of course, reduce the number of contacts and end customers for us, but so far, it hasn't been a great success. So far we have about 2,000 registrars already, already registered. All the nerds, they must, you know, control their own domain, of course. Next please.

Okay, how about DNSSEC? The topic was, what are the challenges of the DNSSEC in Finland? I think the challenge is nobody is using it. Really. The root zone was signed in 2010, and support for sub-domains from late 2010, and so far, this number is from two or three weeks ago. We have 329 signed FI domain zone. That's 0.1% of the whole number.

In our neighbors, it's a bit better. Sweden has about half of their domains signed. So it has not been a marketing success, what can I say? And I don't know if it's too complicated, or just a failure to justify all of the trouble with rolling keys, and so forth, and having all of the trouble, for what?

And I think our question really is, how to motivate domain holders to use DNSSEC? Next please. That's the specification. We have all of this, of course, on our website, so nothing really fancy about this. Next please. And also this is the same thing really again, and they can add DS records for the [inaudible] zoned by themselves, from the web.

And after September, that will be managed by the registrars. Okay, next. Okay, the detail that we're using, [HSM?] module for signing, and the root server and signing functions are operated by CSCIT, Center for Science Limited, that's our contractor. Next.

Okay, now, I get caught on this two weeks ago. I stated that the biggest providers do offer the NSEC validation [inaudible], and as we just saw, only one of them, one of the three, does it. I actually tested this at home, and later when I thought about it, well, I was using my own resolver. Okay.

[LAUGHTER]

Yeah. But, the ISPs, it was really hard to find any information or statements from the web about DNSSEC and when they are going to support it, and when their resolvers are already supporting it or not. Next. That's it.

RUSS MUNDY: Thank you very much.

[APPLAUSE]

So I think we're doing really great staying on time here. So we should have good time for questions at the end. I think… See if I got it close, Mauricio? From Costa Rica. Did I skip Geoff? Oh I did skip Geoff. I went too far down my, yes. Geoff, you're up, thank you.

GEOFF HUSTON: Thanks Russ. Next slide. You know, when you sort of talk about deployment challenges, and I'm looking at this from this side of the validating resolver, there is no doubt that no one could ever say it's complicated. You know, if you're running by and then it seems at least 70 to 80% of the world run bind, inside your name the config file, you just simply say, DNSSEC validation, yes.

Now, if anyone thinks that's hard, take up fishing or something because it can't get any easier than that. Next. So, sort of why

don't folk turn it on, and you know, it is a fascinating question. It's all too hard, well that doesn't really work. It will take more time to resolve a name is potentially an issue, but quite frankly, that's what caching is all about. And if you didn't have caching, you wouldn't have a real time DNS, right?

So the most popular names, including the DNS key and DS records, all of that validation chain, will get cached. So when you actually look at the cost, the incremental cost to the user, when your recursive resolver actually does DNSSEC validation, most of the time it is remarkably hard to actually find what that cost is over and above not validating. It's basically extremely small.

Or block out names was invalid DNSSEC signatures. Now if you happen to work on the, if you will, the firewall side of a national name firewall, this is a really very bad thing, because once you started futzing with the DNS, if the domain name is signed, and you are synthesizing bad answers, as happens in a number of countries, then all of a sudden, that's not going to work anymore.

And if you're trying to do some stupid, clever trick of trying to synthesize v6 or v4 when you haven't got it, such as DNSSEC six, or DNSSEC six four dot Google dot com, that won't work. But is that necessarily a bad thing? Because what you're really after is,

if I want the DNS to be true to me, then the truth is what counts, not stupid synthetic tricks. So, I actually think that's not really an argument.

Next one I've heard, two few names assigned to make a difference. Well, maybe. But again, the issue is, if you don't validate, no one is going to sign. Once you start validating, the values of signing are going to become obvious. Attacks in the DNS are too rare to raise concerns. Structurally, a number of countries put attacks in the DNS on 24 hours a day, seven days a week.

Attacks in the DNS occur all of the time. Some by state actors, others by other forms of actors. But realistically, the DNS is one of those attack intensive areas, where the easiest way to implement some censorship policy, or anything else is, go whack it in the DNS. And so the DNS becomes this toy, this play thing, of institutionalized lying.

So, too many folk are now relying on lies in the DNS, and that's probably a bad thing to do, because the DNS is changing under your eyes. Go and look at DNS dot Google dot com as a small example of what is happening, as a result of all of all of this. We are now turning the DNS black. We're putting the DNS inside encrypted tunnels, whether it's on port, what is it? 433 or what is it? 5380 or something?

[SPEAKER OFF MICROPHONE]

Sorry?

[SPEAKER OFF MICROPHONE]

Port 853, and putting the DNS inside a TLS area. The more you play in the DNS, the more we're going to hide the DNS from you. And so, the issue is, don't do that. But the most compelling reason I'd like to actually put forward is the last reason, how many more headlines do you want in *The New York Times* about the putrid, rotting mess that is CA certificates? How much do you really want to rely on the security of this entire system by a bunch of fanciful bits that time after time, we see structural lying?

Why does Google no longer have CNIC in its set of trusted CAs? Because CNIC authorized some Egyptian mob to put up a certificate for start dot Google dot com, so that that mob could then come and spy on Egyptian users. The CA system has been abused and continues to get abused continuously.

We have an answer, the answer is [Dane]. Actually put the keys in the DNS, and protect the lock with DNSSEC. We know how to do it efficiently with stapling. We can do this quickly and we can do this effectively. We can get rid of the middle men industry of institutionalized lying.

If we did the whole lot in TLS, you would actually have something that is worthy of your trust. What you don't have, today, is anything remotely worthy of your trust. So DNSSEC is not the answer, it's part of a building block, but it's part of a building block of taking security of users, and the usage of the internet seriously.

With the CA system we currently have, and the DNS we currently have, it's just an open warfare of institutionalized lying, and it's not helping anyone. Next. So, having resolvers validate the answer and sending [inaudible] isn't enough either. Turning on a recursive resolver is fine, but quite frankly, if I can get between you and your recursive resolver, I can lie anyway. Next.

So let's raise it a little bit further. Your application should be paranoid. Get DNS is the obvious way to go. Have the application validate what it's trying to do, because the application should trust nothing. It shouldn't trust the platform. Apple might be lying to it, so might Android for all it knows. Your ISP might be lying.

Do your own validation. Secure the conversation. Don't run it in the open. Have a look at DNS dot Google dot COM and think about why they're doing this. There is a very, very good reason, it's all about you and your interests. Hiding your DNS stops folk intruding into it, and inserting lies. And quite frankly what we

need to do is reintroduce, because they tried it once in Chrome, and it should come back, reintroduce [Dane] inside the browser's part of the call.

I see dot DE has just done [Dane]. I saw an announcement last week, and all I can say is, that's a damn fine move, and the rest of you should be looking at this, because if you're taking security seriously, and want to tie keys against domain names, why not put the key in the DNS with the domain name you're looking at? And secure the lock with DNSSEC?

We have no better solution out there, then CAs that's just a remarkably stupid compromise, that put the money and the control in all of the wrong places. Is there a next? Is there another one? No, thought not. That's enough for the rant. Back to you Russ, thanks.

RUSS MUNDY: Thanks Geoff.

[APPLAUSE]

As always, interesting and stimulating discussion there, but I am sorry I skipped you. We'll make up for it in the question time, I'm sure. So next we have Mauricio from Costa Rica. And I do remember when we had the ICANN meeting in Costa Rica, it was an excellent meeting, and we had an excellent participation in

the DNSSEC workshop from the dot CR folks. So thank you for joining us again.

MAURICIO OVIEDO: Thank you very much Russ, and glad you enjoy the meeting. I will be held in the last LACNIC meeting, last week in September. So [inaudible] announce so you can also join us there. So, this is my first DNSSEC meeting with you here, so just wanted to provide an update of what we have so far. And hopefully, it will lead us to continuing to improve the DNSSEC system that we have.

So basically, we start with DNSSEC in 2012. We implemented it since then. We have continued to improve the system that we have. So we added full key ceremonies to the process. We also added the DS publication automation through the NIC dot CR website. And then we continue with some changes with NSEC three, and since 2012, [inaudible] associated to DS publication.

So, as one of the biggest changes, and this is what I wanted to share with you, is that since 2014, we changed the way that we were signing the domains. Basically we moved from the TPM system that we were using, to [inaudible] for key generation, and then we're also using server signing for using DNSSEC signed zone.

So right now, what we use, or what we do is to create 2048 bit keys, both for key signing keys and zone signing keys. Then twice a year, we have the full ceremonies. One is for the TLD. And then the second ceremony is for the second level domains. And then during this ceremony, what we use is the, of [inaudible] we use a modified version of the DVD that was published by Richard Lamb.

So it's open, it's free, and it's ready to use. So basically what we do is to create one key signing key. We use it just for one year. We roll the key signing key each year, and then at the same moment, we create five different zone signing keys. The time that we use them is around 2.5 months each. Then we have key bundles created at that moment.

So it's basically, each bundle will last 15 days, and we roll it every 10 days. When we have all of the necessary material to the ceremony, we transfer security to the server that's going to do the signing, and we also have [inaudible] scripts. Some of them were contributed by Richard Lamb as well, to automate the key bundle rollover process. So basically we have a very simple administration process.

We just do it once a year. We generate the whole material that would be used, and we do constant rollovers of all of the information. So, some of the benefits that we saw moving into

this system, the first one is that basically the key signing key never leaves this marker, so we create the key signing key on this marker with the same thing with the zone signing key.

We create the key bundle material, but the private part of the key signing key never leaves this marker. So once the ceremony, key ceremony is over, the key signing key is putting into the safe, and then it never touches the internet. Then it's very easy to replicate. We were thinking on something that our customers could use, and could be flexible enough so that they can come up with a solution that could provide high security, but at the same time, that could be combined with other options, for example, in-line signing.

So, the important thing that we consider is that basically we're looking for a cost effective solution. In this case, when we implemented it, we didn't have to buy anything, other than these markers, which are very cheap. And then what we use is the existing infrastructure that we have. One way is to use the servers themselves. You can also [inaudible] where [inaudible] in almost everything. So this also come up with the fault [inaudible] system, and with this markers, depending on the one that you use, is very, very easy to create backups.

So in case you have any problem, you will have the system ready to respond in the end. So the last point is that we also saw a

very high increase in efficiency. This pick was quite good. With the previous system, it was taking around 10 minutes to sign everything, and now it turned down just a couple of seconds. And finally, some challenges that we have seen during this process is that sometimes when you think on implementing DNSSEC, probably you can think on money.

Would it cost a lot? Would it be very difficult to handle? Not necessarily the case. In our case, it wasn't like that, and with the option that we have right now, it was very, very cheap to implement it in a secure way. Then another challenge we have identify is that we speak about DNSSEC on different places, conferences in some talks in universities. We have done DNSSEC workshops, in fact, the whole point of changing DNSSEC process that we were using was a result of a workshop that was held in Costa Rica, along with ICANN, and [inaudible] resource center.

So we have done a lot of work on teaching people about DNSSEC. However, still we have less than 1% of domains signed. So I think that's the constant of most of the registries, and definitely there is something else that we should be looking at, and that we should be doing. Probably lack of technical knowledge about DNSSEC, could be a reason, but still, not everyone should know about DNSSEC.

So if we would like to see more domains signed, I think we should provide more options for people that it's not that technical to get into DNSSEC, but it's still use technical resources. So something we are thinking is to include within our system, our way, so the people can configure their zones, and to be automatically signed by DNSSEC.

So this way, they can have DNSSEC without getting to know the protocol itself. And then, last point, is that probably things will continue to change at the beginning, signing with DNSSEC was a very manual thing. Now we are getting to see more and more tools that automate the process and make it much more easier, in-line signing, and other options.

So probably things will continue to get better, the faster way that we have seen, but at least, from the dot CR, what we are trying to do is to look for different options so that we can add more people. That's just a very quick update, and thank you very much.

RUSS MUNDY: Thank you.

[APPLAUSE]

Well, that was interesting. Very good progress report from when we had the ICANN meeting, thank you. Last on our panel

presenters is Nick Shorey, and so we'll turn right over to Nick. Go ahead.

NICK SHOREY: Thank you very much. My name is Nick. I am from the UK government, and I sit on the GAC, who are in session now on some other bits and pieces. Just before I sort of start and launch into a brief chat, can I just get a show of hands, I don't know many of your faces. Who here is from the GNSO community? If you can just stick your hand up.

Okay, great. And who here is sort of numbers community? As well? Okay. Who here is from the GAC? Just me, okay. Right. That's really helpful. And SSAC people? Okay, the SSAC people, good. And ALAC? Anyone here from the press? No? Okay, great, so I can be quite liberal in my comments.

Right. So my name is Nick. I work for the UK government and I'm on the GAC. Prior to that, I used to be a cybercrime investigator. So I used to see the kind of, the end results of some of the small incidents or big incidents when attacks are made against the DNS. I'm here today not as DNSSEC expert, that is the one thing I can concretely say I'm the dumbest person on this panel.

But I'm here as someone who recognizes that this is quite important, and I think from a sort of, from that sort of high level concepts from government, in improving the security of the global addressing system, is a priority for all of those who support the continued evolution of this multistakeholder approach to internet governance.

When things go wrong with the internet, when people can't get access to certain services, when they see attacks, they get their machines infected, they lose trust. And people have alluded to that word before. And they lose trust, and when they lose trust, they ask questions. Why isn't this working for me? And they start to look towards certain answers.

And governments as well. If they sort of don't necessarily understand sort of the underlying principle of why something might happen, they will ask questions of the organizational structure. How did this…? How is this allowed to happen? How can we change the structure to make sure this can't happen again? Those are the sort of kind of questions that people can ask, but then the technical people be like, oh no. it's because you just didn't deploy the DNSSEC.

But people sort of immediately jump and ask these big questions. So I'm coming in here, joining the GAC. I've been on there for a year, and I'm sort of starting to sort of hear all of

these things and talk to people. So my interest here is less around the sort of technical [inaudible] of something because I don't understand that detail. I'm doing my best to learn.

But for me, it's quite interesting to hear what Mauricio was just speaking about in terms of the capacity building work that he's been doing running his workshops, and some of the challenges that they've faced with that, and some of the opportunities that they've identified as a result.

In the UK, I'm not going to speak in detail about [inaudible], there are much better people in the room who can do that, but they were one of the sort of early adopters of DNSSEC, and they've done a lot of work in this space. They've provided sign in services for years, and they've seen, you know, sort of a steady increase in their adoption.

I won't talk in detail about what they've done. But they've been very active, and I think that's been incredibly positive, certainly for the UK. There is an off-com report from back in 2011, that looked at this issue in quite some detail in the UK. And they cited a number of obstacles that they've identified through their studies. And I think one, which has already been picked up upon, really was around sort of the economic and commercial benefits or implications being sort of one of the barriers for this.

And the difficulty in quantifying, you know, where is the value in this? It's not something that we can necessarily see as, you know, as being able to make us loads of money. But there is a cost to deployment, and a cost to maintaining, and sort of updating resigning keys, etc. So that was one of, whether it was two or not, and we can debate that, that's one of the perceived barriers.

That lack of being able to sort of really quantify the benefits in economic and commercial terms of doing something. When I've had conversations with sort of other folks around this area as well, it's… What has been quite interesting to me, I remember I met some people at RIPE, and they told me they operate a business where they buy an old kit from sort of the US and the sort of UK and Europe, and they sell that old kit, that old hardware, you know, sort of at a knocked down price, to sort of develop in states. And on the one hand, that's great. That allows maybe people to get online, to afford that kit that they don't have, but I can imagine on the other hand, there are probably some security flaws, or it's sort of outdated firmware, and hardware, and software, which may impact the ability to properly deploy sort of not just DNSSEC, but ways of other security protocols.

And there is a risk that we're just kind of making the same mistakes again, as we're trying to push versus sustainable

development. And that, to me, seems just a missed opportunity. Yeah, so there are those kinds of issues, and then there is also the government ones. So there is me. I'm here, I don't know a huge amount about this, but I'm on the GAC.

But I don't do, in my department, the direct policy engagement with my ISPs, that's another team that do that. And so they have less, they're not engaged directly here at ICANN. Again, they've got sort of limited understanding. It would probably be fair to say around sort of the technical detail of some of these issues, they're looking at this from a high level policy perspective.

So it seems to me, one of the real challenges is how we better engage with governments, because governments have access to, you know, at a senior level, to you know, the ISPs, the registries, registrars. If you guys are having trouble getting resources, or the other people having trouble getting resources, governments have that kind of that way in at the high level. And they have, maybe if they don't sort of have all the regulatory power, or choose not to exert that, they've got that influence. They've got, they're meeting the senior folks, and they might be able to push this. Sort of do a bit of better engagement with government, draw out the core messages, what does this really mean for you in that big picture term of doing this small thing? What's the big picture thing?

And I don't get the sense that that's necessarily happening, and I would cite my case evidence is the lack of government people in this room. I don't know if you guys agree. And I think, yeah, there is more that we can do maybe around this sort of outreach coordinated, capacity building stuff, people sort of often seem to talk about sort of the key-less simplistic solution, which is just going to make it really easy for the end user to sign their zone, and sort of automate it without sort of having to get down into the deep technical detail that they don't necessarily understand.

So I'm here to maybe offer a little bit of a perspective, if I can, from a government place, but I'm also here to listen. And for me, I think, that's the key thing, and hopefully take your messages back around some of these bigger challenges, not necessarily just in the technical detail, but some of the broader capacity building challenges back to the governments later during the week. Thank you.

RUSS MUNDY: Thank you, Nick.

[APPLAUSE]

Appreciate that, Nick, and it's always good to get an additional perspective on how we're having challenges that have to get met here. And I think we have some people coming to the mic,

which is great, but let me kick off the question session to Mauricio. We had, at the CR meeting, we had a bank, and I forget which bank it was in Costa Rica, they announced that they were going to use DNSSEC as part of their security mechanisms.

Could you make any comment on whether or not they're continuing to do that? And has it spread or not gone anywhere? Especially with the small percentage that you were talking about.

MAURICIO OVIEDO: Sure. This is the Costa Rica National Bank. And yeah, indeed, they signed their domains, and have kept DNSSEC since then, since 2012. So they continue with signing, and we continue to support them, but still, the main problem is that the number doesn't increase fast, right? So we are having conversations with the government institution that regulates or that handles the economic part of the banks itself, so they can see the benefit of having DNSSEC within the financial institutions.

So it's one of the efforts that we are doing. They still have DNSSEC, yeah.

RUSS MUNDY: Good, thanks. Eberhart.

EBERHART: Okay. The point, I like smart [cards?]. I play with smart [cards], and the point in Costa Rica is, that particular bank uses a similar smart [card] as the same reader for their own security features to do your internet banking. So if you use them, you can use exactly this combination to do DNSSEC.

Now I wanted to address Nick a little bit. I come from a developing country, [inaudible], and we have a more cynical approach on this outdated hardware. It's digital landfill. It's cheaper to send this to [inaudible] so that we then get to do something then to dispose of it, environmentally friendly, under environment legislation in Europe or in America.

Never mind what is even upsetting then is that, an amount of money is assigned to the value of this, and that is then sort of deducted from the development budget that has been given to each developing country. I was personally involved in having to figure out how to restore services to a school when their manager left, outdated hardware, running some form of old version of Red Hat, and it was just a total, total mess.

And eventually, even our government figured out that it was cheaper in the long run, and more efficient to turn [inaudible] for proper hardware, and not rely on this crap that is being sent in a purely arrogant manner, that we have to be grateful for having

to dispose of this, despite our Constitution having a provision for being environment friendly.

I'm not criticizing you in anyway, I fully appreciate that you mentioned it and that you were critical about it, but I just wanted to reinforce the point, this is something that we really cannot accept.

NICK SHOREY: If you sort of hang on for a sec. If I can ask a question back to you, and you know, how much…? You know, to what extent is to say are you seeing this as being a real issue, in sort of, you know, the broader term of Africa then? I don't know what the statistics around the amounts of kits that is being shipped and how much of the budget, as you say, is being carved off for this.

Can you give me any indication of the extent of the issue?

EBERHART: I don't know. It came to my personal attention. I'm a gynecologist by profession. When in one hospital, the trolleys to bring patients to the operating theater were replaced by Finland as a donation in fact, and I don't… They just don't last as long as the things there that we had for the last 30 years. It takes two years and they're broken.

I don't know. But in poorer countries, now maybe it's on the middle economic level, it's not really a poor country, we have a big split on the [inaudible] between the haves and have not. I live a very sheltered life with several cars, several houses, can fly business class if I want to. But the poor people in our country are very poor.

Fortunately our government has decided that a few times, we don't want this anymore because these things don't last, and I'm not criticizing Finland for making a donation, I'm just, that's how it came to public attention because the trolleys, after one or two years, they were just, it just did not take the stress of how we do things.

And given outdated equipment to schools, it's unmaintainable. And then we are expected to be thankful that we get something, not from your presentation, but that's the usual. And what's really upsetting, money that could actually be used for something is then sort of artificially debited from the… We give you [inaudible]… We give you 25,000 bucks worth of equipment, and the rest was just paper money. That's really upsetting.

I'm not saying we should get more money, or we should get any money, but we should not get crap, and then be expected to be thankful for it. That's the point I wanted to make, and I fully

appreciate what you're saying. This is sort of coming through to reasonable development agencies, UK, [inaudible], we see this all of the time.

If a project is American, we find Jeeps, if it's German, it's the same people driving [inaudible]. If it's the Japanese, they drive Toyotas. It's always the same. The money, basically we get so and so, but the money gets basically back to the country of which the concerns are coming from and so on. That's not really DNSSEC, but it's development, but since you raised the point, I'm very grateful and stand here and have about five minutes longer than your presentation was.

[LAUGHTER]

RUSS MUNDY: Thanks Eberhard. Let's go on to the next question please.

MARK: Mark [inaudible]. One thing that surprised me a bit was that black lies should not become a standard of the internet. That's a different point. A question to Geoff, have you tried talking to the ISC and/or Linux distributors to make validation a default?

GEOFF HUSTON: Certainly ISC and I have a continuous conversation, and there are probably some ISC folk either in the room or close by. I've worked with them a fair deal on what the default choices are and why, and certainly the currently conversation is actually about a set [inaudible] option that sits inside the ISC code, that as soon as it runs v6, it draws it down to 1280.

And I suppose my point is, if you're running UDP, that's actually the wrong thing to do in my view. There is too much other stuff out there that doesn't like it. The other part of the conversation is actually about, if I stand up a resolver in both four and six, what should a validating resolver do against that service or an authoritative name server?

Currently, even though about half the world's resolvers will do v6, less than 5% prefer to use v6. Now, as long as we've got this idea that the dual stack world will last forever, bullshit, you're okay. But at some point, that's going to be a lie. At some point, you've got to confront the truth that the internet is going to have to run on v6 and v6 alone, probably in your lifetime, probably in mine.

So this stuff needs to work. Now, the thing about DNSSEC and the way this works is DNSSEC inflates the answer. There is no getting around that. And what we've found, and actually the question back to Dani, how did you do that on the fly? They use

DCC. In other words, they're using elliptical curves to get it back down again, because we've really got a problem with deep packets and UDP, and quite frankly, in v6, there is no satisfactory answer.

And the trick is, how can we have adequate security? Keep all of the responses under 1280? And make this damn thing fly on six? If you can get those three going, we're doing brilliantly. But I suspect elliptical curve in DNSSEC go together is part of the answer.

MARK: So at the end of the day, it's not as simple as turning it on?

GEOFF HUSTON: Nothing is ever that simple, no.

RUSS MUNDY: Next, we have a question from the chat room that Julie will read for us. Thank you Julie.

JULIE HEDLUND: Thank you Russ. This is Julie Hedlund. So there is a question in the chat from Peter Van Dyke from Power DNS, and the question is for Ari-Matti from FICORA. He asks, "Will you be dropping the requirement for authoritative to respond to RR Sig queries?

Right now, this is preventing CloudFlare customers and power DNS users from using DNSSEC in dot FI at all."

ARI-MATTI HUSA: Actually I don't know an answer to that question, but we are relaxing the requirements for the name servers. But I have no answer to that specific question, no.

RUSS MUNDY: Okay, thanks Ari. Dan, we need to move quickly because we're about out of time here. Go ahead.

DAN YORK: Okay, well then, I'll just say too for Finland, we do have to acknowledge that when you guys signed dot FI, that was the first time I had ever seen anybody Tweet out pictures of a cake, celebrating the signing. That was something that warrants there. And Mauricio, thanks for coming back and talking about Costa Rica.

Nick, I just want to say, I think you'll find everybody here, we're very interested in talking and working with governments, in working with folks around that, because we have had that as one of the discussions. And some, we've had in different venues

and different places. We've discussions around… How do we work with it? How do we do it?

So all of us here would love to talk to you more about that in some way shape or form. My question for Dani was, you mentioned the black lies work with, doing that within IETF. Where is that within the IETF process? I saw a draft is up in DNS op or something?

DANI GRANT: Yeah, the draft is up. It's like so early, early days.

DAN YORK: Okay. So it will probably be in DNS operations, I assume is where it would be. Okay. We'll look for it there.

RUSS MUNDY: John, go ahead please.

JOHN LEVENE: I will attempt to be concise. I'm John [Levine]. I always ask the same questions, so I'm going to ask it again. I have a tiny DNS system where I have 250 zones and they're all signed locally, but only half of them are actually signed because I can only get the DS records into half of the upstream servers, for which I am either the registrant or I am a registrar reseller.

For the rest of them, they delegate the DNS to me, but since I'm not the customer, and I'm not the registrar, there is no way for me to tell the up level zone, like here is your DS, so for anybody who is a registry or registrar, I can't be the only person with this problem. What are you going to do about it?

RUSS MUNDY: Anyone on the panel want to…? Go ahead Geoff.

JOHN LEVENE: …maintain DS, which is fine if you already have a DS.

GEOFF HUSTON: One of the other options that is being kicked around inside the internet and the IETF drafts, is to see the DS record and similar. Because you are the delegated domain and you control that, you can place, this is the candidate DS record parent, please come and look at me and drag it back up again, because you're not alone in having this problem. And the thing is, [inaudible] put in S records, in the parent to say, it's you, the reason they're not allowing DS is some kind of stuff out there that we can't fix.

JOHN LEVENE: Or it might not really be me, or something.

GEOFF HUSTON: Well like that, but I like the CS approach myself, that it's your zone, putting in the candidate record, and get the parent to periodically query and lift up the current value, that allows you to change keys, all of those things and then back under your control. So to my mind, it seemed like a nice answer. I don't know where it is in DNS, but it's in there somewhere.

JOHN LEVENE: There is a draft.

GEOFF HUSTON: Yeah, there is a draft.

DANI GRANT: We have the exact some problem. So we have all of these customer zones that we started sign, but because we're not the registrar for these zones, we can't send the DS ourselves. We need the customers to go to the registrars, to log in, to add the DS, and some of these registrars do not any have an interface for the DS. They need to be sent over email, or maybe they don't accept DS at all.

And so, we've published this draft, it's in DS [op]. And that's exactly the idea. We publish CDS, we ping the registrar, and they go and check DS and grab it from there.

UNKNOWN SPEAKER: Is that Oliver's draft or a different one?

DANI GRANT: It's Olivier's draft.

RUSS MUNDY: Jack can help. He's working on that space also, right down to your right.

DANI GRANT: As is Paul.

RUSS MUNDY: Okay. I think we've used a little bit more than our time here on the panel, but I want to thank again all of our presenters.

[APPLAUSE]

And please do continue to come join and participate. If you can't be in person, do it remotely, but we love to get this broad set of participation. Thanks folks, and next we'll move on to Matt Larson and Duane Wessels to talk about key rollover, key changing activities.

MATT LARSON: Good morning everyone. I'm Matt Larson, I'm VP of Research at ICANN, as of week four, week five now at this point. So happy to be here and talk to you about rolling the root zone KSK. As you can see from the agenda, Duane is also going to take, Duane from Verisign is going to talk about increasing the size of the root zone DSK, and I guess we're doing this alphabetically so I'm going first, even though chronologically, what Duane is going to talk about, is going to happen first.

So we're doing this in reverse chronological order. His presentation is also longer than mine, so this probably makes sense. Next slide. So, I look out and see all of the usual suspects so I'm going to go fast here because I don't want to tell you things you already know, but the root zone is complicated and unusual in more than one way. One of which is the way it's administered, and that's, there are multiple parties that are contributing to make the root zone happen.

ICANN is the IANA functions operator. From a DNSSEC perspective, it manages the KSK and has done so since we signed the root in June of 2010, July of 2010. June of 2010. And so the quarterly, we bring out the KSK and sign the new KSK because that rolls every quarter. Verisign is the root zone maintainer. They actually sign the root zone on a daily basis, twice daily basis.

They of course manage the ZSK. And the root zone DNS key is managed in these 10 day slots. So there is, every 10 days, there is a new set of signatures. And then let's go on to the next slide. So, as I said, the size of the root zone, ZSK, is increasing. That's what Duane will talk about in a moment, and that's happening first. But after that happens, we are changing, or rolling the root zone KSK. So these are separate activities, but what we call the root zone management partners, which is basically Verisign and ICANN, we're coordinating closely to make sure that all of this happened smoothly, and one of the things we're doing is not changing two things at once.

So that's why the ZSK is rolling first and then the KSK. So why change the KSK? The main reason is operational preparedness. As everybody knows, from DNSSEC perspective, there is no expiration dates on key material. You can use the same key as long as you like. There is certainly no weakness at this point, you know, I know from ICANN's perspective, we're very proud of how we manage the root zone key material, and you know, we have a real open process that we think that hopefully establishes a lot of trust in the community for how the key is maintained.

So, we don't have any concerns about the key either from a management standpoint, or from an algorithmic standpoint. But it is a bad cryptographic practice to have any key live

forever. So we do need to roll it at some point. In the DNSSEC practice statement for the root zone KSK operator, that describes how the key material is treated, it does talk about a five-year interval for the lifetime of that key. You know, five years or as circumstances allow.

So it's time to roll that key when we sign the root zone. Back in 2010, when I was wearing a Verisign hat instead of an ICANN hat, we always had the intent that the key wouldn't live forever, and that we picked five years as a reasonable timeframe based on the lifetime of some of the cryptographic hardware we were using to store the key.

So it's time to roll the key, and we'd rather do this under normal conditions rather than under abnormal conditions, if there was some kind of a compromise. So better to do it now, and do it in an orderly, controlled manner. I mean, there is a challenge of course, in that there are a lot of people involved.

Anybody who is doing DNSSEC validation has a copy of the root zone KSK, and they need to change that key. And unfortunately, there is no test environment that can cover all possibilities because of the number of people involved. So let's go on.

So here are some of the dates which we're just now starting to talk about publically. Ed Lewis, my colleague at ICANN, talked about these at [inaudible] 67 in Chicago a couple of weeks ago.

So as I say, this is the first time now, and the first, for these first recent weeks that we're talking about these dates. So in the key ceremony, a recorder, we have a key ceremony, as I said, where the KSK comes out, signs the zone signing key for the subsequent quarter.

So in Q4 of this year, the ceremonies typically happen in the middle of the month, so probably the exact day hasn't been set yet, but in November this year, we'll generate the new key signing key. And then in the first quarter of 2017, the KSK is what we're going to call operationally ready, and that's because we have two key management facilities or KMFs.

One in the US East Coast, and one on the US West Coast. So the current plan calls for the key to be generated in Q4 of this year, on the US East Coast. It will be securely moved to the US West Coast facility, and in that key ceremony, it will be imported into the hardware security modules there, and then at that point, that's what we're calling operationally ready, where we've got the key securely stored in all of the places that needs to be.

In terms of one this is actually visible in DNS, because those activities are, you know, they're just administrative activities that nobody can have any publically visibility to on a widespread scale. So in terms of things changing in DNS, that will be July 7,

2017, that's the actual date when you'll be able to see the new key in DNS.

It's actually going to be used to sign the DNS key or RSEP in the following quarter, on October 11, 2017. And then from a RFC 5011 standpoint, we're actually going to set the revoke and revoke the key in January 2018. So as you can see from the timescales here, this is going to be a drawn out, orderly process. The cadence of things for root zone key management happens on this quarterly cadence, because of the key center, you know, we're not trying to rush things, we're doing everything a quarter at a time.

And I should refer to the final blurb there, all of this is contingent on the ZSK size increase going smoothly first. So here is a timeline. The slides are available so you can examine this more closely, and look at all of the fine print. But these show the various phases. We've lettered the phases from phase 8 to actually goes off the slide, because there is some administrative things that happen at the end when the old key is actually destroyed.

But in terms of the phases that are probably the most interest, these are they. So this is kind of a recap of everything I've just said. Each phase is designed to take one calendar quarter, but as I'm about to talk about, we have plans for backing out and

falling back if necessary. So at any point in this process, well at almost any point, before we revoke the key anyway, we can decide to stay in the current phase, if there is any operational indication, we should do so.

Or we could even fall back. So if everything goes as planned, there will be a one-to-one correspondence between phases and quarters, but it is possible that a phase could last multiple quarters, or that we could, hopefully not, go from one phase back a previous phase. So as you can see here, I guess things to highlight, you can see some of the activities here in green, at the very bottom, highlights when some things, some visible changes happen, when we get some packet size increases, and when the rollover actually happens, and the revocation.

So you can see the way we design this process to happen back in 2010 when we signed the root to begin with, was that the ZSK rolls happen every quarter at the boundaries of the quarter, and then anything we need to do with a KSK happens in the middle of the quarter. So even within a quarter, we're never doing more than one thing at once. The ZSK roll happens independently of the KSK roll within a quarter.

All right, so as I said, we do have back out capability. We can stay at a current phase or roll back if we want, until we actually set the revoke bit on the key in the first quarter of 2018 at that

point, because of the way RFC 5011 works, we can't go back after that. That's the one point of return. And the way we're going to do this is that at each key ceremony, we will sign and generate multiple sets of signatures. So we'll have sort of a set of contingencies, you know, because it's such a big deal to have a key ceremony and get all of the trusted community representatives in place, and open the safes, and do everything.

We can't, if there are any issues, do one of those when the issue happens. We have to plan in advance for it, so that we have various sets of signatures ready for whatever contingency we envision. So there is going to be a lot of monitoring during each phase, you know, we're going to have near real time analysis of root server traffic. We're going to be, of course, watching mailing lists and social media for people reporting any issues.

You know, we're in the process of developing criteria that will trigger a fall back, and for all of this though, we're going to use our operational judgment. There is not going to be any absolute criteria, partly because it's hard to envision anything that could possibly happen. So it's going to be a combination of thinking in advance for what sort of things we could envision that would indicate problems, along with our operational good judgement when it's actually in progress to determine if it warrants any particular activity, like staying in a phase or falling back.

So, the timing for this is, you know, from right now until the end of this year, we're presenting the plan and going to accept feedback. And then once the new KSK is actually generated, we're going to be actually presenting the new KSK publicizing the new key, and then what we're encouraging everyone to do throughout this entire process is to follow RFC 5011. That's, at the risk of giving operational guidance, we're encouraging everyone to use 5011 if at all possible, because then all this just goes automatically and nobody has to do anything. It just happens.

As I've just said, 5011 will make this all happen automatically for you, otherwise obviously you will need to manually change the KSK October 11, 2017, that's the day when the new KSK actually starts signing the root zone. So that's the day by which, if you're doing anything manual, that's sort of the flag day you'll have to have the new KSK configured in your validators then.

In terms of testing, we've got two different kinds of testing environments that we're working on. One is targeted for software developers. This allows people who develop code that supports 5011 to test it. You know, one of the issues with 5011, not an issue, but I guess it's an issue from a testing standpoint, is that 5011 has this long ad hold on timer, it's called, it's a 30-day timer that you have to see a new key as a candidate trust anchor

before you finally take action and go yup, I believe that, I'll add it as a trust anchor.

And that's to avoid being potentially confused and being spoofed into believing a new trust anchor. You sort of have this paranoia, I'm going to wait 30 days before I really believe it. And that makes it hard to do testing because if you're going to test things exactly as they would be in an operational standpoint, that means waiting 30 days.

So a couple of different people have written test environments that do 5011, but on a much accelerated basis. So if you can change your 5011 software to reduce the ad hold on timer to a much shorter interval, then you could watch a trust anchor will happen, and test your 5011 software that way.

So Rick Lamb from ICANN and Warren [inaudible] from Google have each written separate test environments that do 5011 on a much more accelerated basis. So if you're a software developer, this is really more appropriate for you. You could test our RFC 5011 code and make sure that it can configure a particular key as a trust anchor, and roll it. At ICANN, we're going to be developing our real time, what we're calling a real time 5011 environment, that will actually do 5011 on a much slower basis, with a real 5011, or I should say a real 30-day 5011 hold on timer, so that somebody who is an operator could configure you know,

not the root zone trust anchor, but the idea is that in a production system, you could configure a trust anchor for a zone deep within DNS that wouldn't otherwise effect your operations, because it's a test zone that nobody is going to use.

But in your production systems, if you wanted, you could configure this zone's trust anchor, and then watch it roll on the actual 5011 long scale timeline. And then here is the obligatory information for how to contact us, and how to follow what's going on. So with that, I'll turn it over to Duane. Why don't we take questions for both of us at the end?

DUANE WESSELS: There will be no time for questions. I have like 40 slides.

MATT LARSON: That's why I wanted to go first.

DUANE WESSELS: Okay, so yeah, thank you Matt. As Matt said, I'll talk about the changes to the zone signing key, upcoming. Next slide please. That's just the outline so next. This says kind of some stuff Matt already said. This says that Verisign operates the zone signing key, and ICANN operates the key signing key, and it talks about what is it, it explains what is KSR, it's a key signing request. And

a SKR is a signed key response. These are actions that happen during ceremonies. Next.

So again, these slides are a little bit dated from before the time when ICANN and Verisign were presenting together. That's just to say that I'm really not talking about the KSK rollover, that's separate. So, this slide makes the point that the only thing that we're changing as part of the ZSK change is the length of the key.

All of the other parameters are going to stay the same. It's still going to be the same algorithm, it's going to be rolled at the same intervals and so on. Next please. So this is the schedule. Two of these things have already happened. Some testing has already taken place, and [inaudible] number 25 happened in May of this year where the two three ZSKs were signed, and that was important because, during that ceremony, they signed the very first larger key, which happens in the, it's the pre-published key.

It happens at the end of, right before Q4. Next please. This diagram shows the schedule for the ceremonies. It just sort of highlights the lead times and talks about what Matt said about how this is all driven around these quarterly ceremonies. And it explains our scheduling. Next please.

And this red circle highlights that pre-publish key that I was talking about. So that little dark blue bit that sticks out to the left there, that's the slot during which the 2048 bit key is pre-published at the end of September. All right, so let's go into some more details. Again, each, for CSK purposes, each quarter is divided into nine slots of 10 days each. Sometimes the ninth slot is a little bit longer because quarters have more than 90 days.

The R-SIG record changes on each slot. And at the end of each quarter, there is one slot which is reserved for the pre-publish and the start of the next quarter, one slot is reserved for post-publishing the old key. And this has been going on for years and years now, since the root zone was signed. And during those ninth and first slots, the size of the DNS key message goes up a little bit because of the pre and post-publish.

This diagram shows what a normal 1024 to 1024 rollover schedule looks like. Next slide please. And here it just highlights again, those slots, and when those responses increase in size. So this is the plan for increasing to 1024, from 1024 to 2048. That middle section is Q4 of 2016, and the green represents the 2048 bit as a yes K that will be introduced. Next please.

So the only thing that's a little bit different is during that quarter, we're going to extend the post-publish period for the old key to

give ourselves a little bit extra breathing room in case there are problems. And this is text for what I just said. Next please.

So let's talk a little bit about what it means to have a larger ZSK. This chart shows the size of signed DNS key responses, and sort of goes in order of how things will proceed timewise. So at the top we have, sort of the normal situation where there is the single ZSK, and the response size is 736 octets. When we do a 1024 to 1024 rollover, that goes up to 883. Then when we introduce the 2048 bit key, that response size goes up to just over 1,000, 1,011 bites.

During a period with a 1024, a 2048 bit ZSK with no roll, it will be 864. And then when we do a 2048 to 2048 roll, we're up to 1139. And then it will be the same for a KSK roll from 1024, or from 2048 to 2048.

However, during the times when we do a KSK roll and a ZSK roll together, it goes up to 1414 octets. And when the KSK is revoked, which will happen about a year and a half from now, it will be up to 1425 bytes. So that was just about the size of a DNS key responses, but we're also interested in, you know, the sizes of other responses too.

So to investigate that, we took some trace data and replayed it through name servers configured with various keys and signed in various ways. Next please. So in doing that simulation, we

replayed 10 minutes' worth of data, and looked at the responses that came back, including the size of the responses and whether or not they were truncated and fragmented and so on.

This work was done back in February, so all of this data was from around that time, replayed 37 million queries. The data was taken from A root, which was running at five sites listed there. So one of the first things we looked at was fragmentation. And as it turned out, there was almost no fragmentation. I think something like point zero, zero two percent, a very small number of responses had experienced fragmentation.

Next please. A lot of these were due to any queries, of which there were very few in this trace period. And there were some other types of queries actually, two that experienced fragmentation. But I can go into more details later on that. Truncation is a little bit different. Truncation happens when, you know, the responses can't fit in the advertised client buffer size. So here the green shows a case for a 1024 bit ZSK, and the far left shows the normal situation, with no roll over, and the darker green shows what it looks like during a ZSK roll.

So it goes from two and a half percent to about five and a half percent of DNS key responses get truncated. But it stays at that level for all of the other times when we have a 2048 bit ZSK, so it

will never get sort of above that level of five and a half percent. Next please.

So again, that was just DNS key responses. And here is the amount of truncation for responses overall. And in this case, it depends only on which, the size of the key that's being used for signing. So, when we're signing with a 1024 bit key, overall about half a percent of responses experience truncation. And when we switched it, 2048, they'll go up to almost 1.4%.

Something else that depends only on the size, of the key is for signing is the distribution for response sizes overall. So the red here shows the distribution for 1024 bit keys, and the blue for 2048. Yeah, you can go to the next one please. And lastly, something that's maybe more interesting to organizations that are operating root servers is the amount of bandwidth that they will be serving.

So this represents the bandwidth for essentially a single letter. Again, this data came from A root, and under today's situation, A root serves something like 250 megabits per second, but when we increase the ZSK size, it's going to go up to about 350 megabits per second.

Okay, I've got like three minutes to get through the fallback plan, let's go. So, you know, while we fully expect this to proceed without incident, we're prepared for certain unforeseen

problems, and should it become necessary, we will fall back to a known good state, which will be a 1024 bit zone signing key. Next please.

So in order to make this happen, ICANN will sign two KSRs for us, at two of their ceremonies. I said one of those has already taken place, and the next one will take place in August. Briefly, criteria for fallen back will have to be something unforeseen and something that's very serious, and something that couldn't be solved by having, you know, a small number of recursive name servers temporarily disable validation.

So one of the first important milestones that we'll encounter is, at the start of slot nine in Q3 this year, that's like September 20th, I think, that's when that larger key first gets published in the zone, the pre-publish period. We'll be watching that closely. The next milestone will be the first day of slot one, Q4, something like 12 days later, that's when the zone begins to be signed with a larger key. And it will take a while, of course, for cached data to expire, so over the course of those days, we'll continue to watch that closely.

And then at the end of… Again, we have a three slot or about a 30-day post publish period for the old key, and that's our point of no return. When that key gets removed, then we're staying on the 2048 bit key. So this probably familiar looking diagram, you

know, shows sort of the two paths here. At the top, is the path of how we fully expect things to go, and the 1024 to 2048 bit transition. And the bottom shows are fall back option.

So if necessary, we have all the signed keys necessary to fallback to just a 1024 bit key. Next please. So again, we have the option to do this fallback in slot nine during the pre-publish period, and you know, this, if problems are going to happen, this would be my preference for them to happen here, because this is very easy to recover from. But we also have the option to do, next slide please, whoops.

I guess it's missing. But we also have an option to do the fall back in that slot one. If we have to do a fallback in slot nine, we just un-publish the new key and continue signing with the old key, and then there would be no ZSK roll for the next quarter. We would continue on with the older key. Next please. Here is the slide I was looking for.

So, this just diagram shows the fall back during slot one, and if, go ahead, next please. If we have to do a fallback here, we can revert to signing with the old key, and we can continue to publish the larger key for a while, depending on the nature and severity of the problem. And next. So the last thing I want to mention before we take questions is that, we have a sort of a

very simple tool, website, called Key Size Test dot Verisign Labs dot COM.

Next please. Which you can go to, and it will do some URL fetches to domains that are signed with larger keys, and tell you if they've all been successful. If you go there, you should see something that looks like this. If you don't, I'd be very interested to know and talk to you, and help you find out what's going on.

So that's the end of my talk, and we now have about two minutes for questions.

[APPLAUSE]

UNKNOWN SPEAKER: [Inaudible] Let's stay away from the technical stuff. As an irregular observer at the key signing ceremonies, East and West Coast, when you get to do the new CSK, sorry, KSK, what happens if a lot of people want to be an observer? That room is only so big. Has this one been…

UNKNOWN SPEAKER: You're looking at the wrong guy.

UNKNOWN SPEAKER: Yeah, I know that [LAUGHTER]. You get the drift.

DUANE WESSELS: Well, you're right. The room is only so big. We can have a limited number of observers. Everything about the ceremonies is public. You know, they're live streamed, there is an extensive record of what happened at the ceremony, it's all published. The idea is to be absolutely as transparent as possible, and we have the trusted community representatives that are there.

So our hope, as the new key, will be as with it has been all along, that you know, those are people who hopefully the community trusts, and there is more than one person there. The whole idea is that nothing can happen without multiple people being present, and also without there being a record of exactly what did happen.

UNKNOWN SPEAKER: Oh no, I'm an absolute fan of the process, and the extensive documentation, and commentary. I was just wondering, you know, if you've thought this one through, do we end up in a lottery situation? First come, first served?

DUANE WESSELS: Oh I see. What do you do if you want to be there as an observer?

UNKNOWN SPEAKER: And there is too many of us.

DUANE WESSELS: That is a…

UNKNOWN SPEAKER: You've had some pretty packed rooms in the past.

DUANE WESSELS: Yeah. I don't…

UNKNOWN SPEAKER: Who else wants to be there for this? We missed it five years ago. Am I really the only geek that, okay, Alan, all right. No [inaudible], I have no problem. That's, this is easy. I've got one-hour flight, he has at least 27 hours. So you know. Just something for you to think through amongst everything else.

UNKNOWN SPEAKER: During the first ceremony, there very first, wasn't there like an extra room that people could go in and sort of be close but not like be in the room?

DUANE WESSELS: We did, we literally had overfill seating with closed circuit cameras, and you could watch. But those of us…

[SPEAKER OFF MICROPHONE]

Yes, so those of us, there was a break. Those of us who were smart were not there for the first part. I just watched for the first part while they did all the gory setup, and then when we actually generated the key, that was when I went in, you know, after the bathroom break and everything. So there won't be as much setup, that was a one-time only event for getting everything all set up.

So yeah, I'm not sure how that will work for, we won't need to do that all again.

DAN YORK: Dan York. Just a quick thing. First Matt, congratulations on your new role here with ICANN. And second, thank you for publishing a schedule, so we can see, I mean, publically what the plan is as far as giving out there, I think that's important. So thank you for that.

DUANE WESSELS: You're welcome, and this is not the last time. You'll be seeing me and a lot of other people a lot between now and when this all happens. That's the idea.

DAN YORK: And I think that's, you know, in all of the comments we've had on this process, that's the important part, right? Because I think as communicating to people what the steps are and what the time is, because we don't know what that breakage might be, as we go to that, in that period of time out there. So I think, I'm glad you're out there doing that, that's definitely important.

JULIE HEDLUND: Any other questions for Duane or Matt?

Then please me in thanking both of you and thanks for coming.

[APPLAUSE]

Next, we have a discussion on DNSSEC encryption algorithms with Andre and Dan.

DAN YORK: Hello. I can use the clicker. All right. So, we heard conversations here earlier today about why it was important to sign with the elliptic curve algorithms. That's a great

presentation. That's awesome. Click to add title. We're going to click that to add a title.

So let me ask a question, how many people here have their DNSSEC…? Actually, let's ask this. How many people have their domains signed? All right, of course, in this group, we look at the percentage. Okay. High percentage. How many of you have it signed with an elliptic curve algorithm?

Okay, a few, a couple of people, and a number of which are suspiciously with CloudFlare. So, we've been having this conversation about why it's important, and here we go. Look, wow, cool.

Testing, all right.

Okay. So here we are, Andre and me. So we know, you know, algorithms are used for the signing side. They're in signatures, they are used for the DS record, and they're used for the validation side. We have a whole bunch of them, of which we see different conversations that most of them are not used. And we've got elliptic curve and we've got ECDSA, which is out now, and then we've got two others ones under development with this gentlemen being the author of the drafts that are being right there.

We talked about this in Marrakech. I'm not going to spend more time specifically around that. But we care about these because they're faster. We've heard this discussion earlier about they're smaller around the need for that as we go through that, and just in general, better cryptography, better security as we look at moving away from there.

The problem, of course, is there is many aspects to deploying these new algorithms. You've got to have them validated by the validators that are out there. You've got to have them in the signing side of things, this hosting operators, the registries, registrars, all of the folks involved have to play a part in this. And so it's a big, big thing. So we've been having these discussions. We started it back in Marrakech, we had a panel where we talked about this before. We went on to, there was a discussion at the DNS [inaudible] workshop in April in Buenos Aires. We had discussion in different working groups at IETF 95.

There was a RIPE session. And now we're here. And we're going to continue this drum beat to talk about it. We did capture some of this in a draft that's down there at the bottom, that I was reminded we needed to rev for the next IRTF with some of the feedback that were coming out of this discussion. But we have this discussion and so, we thought, given that we have all of this since last time, Andre and I, we talk a little bit about what we've

seen, and I'm looking to him in one part, to talk a little bit about what he sees in some of these things.

So Andre [inaudible] from [C NIC?].

ANDRE: Thanks Dan. As Dan has shown, we had the discussion in the Buenos Aries, DNS [inaudible], and it was, we the [inaudible] was composed of DNS vendors. And well, there was also some [inaudible] guys, then at the RIPE session we talked the [inaudible] DNS providers, DNS hosts. And what I am hearing from all of those people, and all the people from the audience, the problem is that the DNS is viewed as a basic infrastructure, and you don't touch the infrastructure because something will break.

And we need to change that. We need to change the perspective into people's eyes that the DNS is something that they need to take care, like on a regular basis, that it's not something you set up in the 80s and it's still running. And well, what we are looking for, and what we are talking about is how to change the perspective.

So if you have any other clever ideas, then what we've already heard, the RIPE session was quite productive and there was some suggestions to add this, to bundle this somehow together

with the HTTPS testing, because that's gaining traction now, and everybody has used [inaudible] Labs and [inaudible] used to test their websites, if they are correctly configured. And if you can somehow convince those guys that the DNSSEC should be part of this web test for web security, then that's part of winning the game.

DAN YORK: So that was part of what they discussed at the RIPE session was, how do we bundle that with that? So would that be something like when, if you were testing, you would go to the…? Well, I mean, we have sites like that now, that do some of that, right? Like, Internet dot NL, or some of those that have the test of DNSSEC along with it. But you're saying for applications? Or…?

ANDRE: Well, what I'm saying the people mostly care about their web servers. So if you can show them that their web server is not correctly configured, the DNS is not correctly configured as well, then it will gain some attention.

DAN YORK: How many people here have updated their DNS server recently? The recursive resolver? This is the wrong crowd to ask, of course, I know. So just curious. Okay. How many people have

not even thought about their DNS resolver since they put it installed in their network? How many people even know where their DNS resolver is?

Okay. On his laptop. Russ indicates yes. Okay, this is the wrong crowd to ask those questions. If we ask outside of this area, if we ask the rest of, okay [inaudible] is showing me he's got a DNS resolver on his smartphone. Okay. Yes, this is the wrong crowd. Okay?

But if we go… If you imagine we're going out there talking to the other people here at the ICANN meeting, how many of them do we think have probably updated their DNS software any time recently?

[SPEAKER OFF MICROPHONE]

DNS, what's that? Was the comment from the side over there. Yes, probably how many. Yes, Paul. It should be on. AV team, we need the mic on.

[SPEAKER OFF MICROPHONE]

PAUL: Hello? Okay. So sorry. I'm Paul [inaudible] at Red Hat. So one issue I'm personally running into, I'm the maintainer of some of the DNS software, is that especially with minor releases, for

instance, for our product, if you go from [inaudible] seven to 7.1, 7.2, 7.3, that there is a strong desire not to update anything. Those are sort of bug fixes and minor releases.

And DNS moves much faster, and I would really like to put those updates in, and I get a lot of pushback not to do that, in those minor releases. So what I would like people to do here, that do pay for [inaudible], everybody runs [Santos?] including me, but those who have a subscription to [inaudible], please file a bug, so that I can actually have, you know, some customer reports saying, "We need this update."

Because otherwise, these updates will slow down, and they will cost you your DNS server not to be updated whenever you type update on your OS.

ANDRE: Well Paul [inaudible] or there is an option by support and then fill the bug?

PAUL: That would be awesome too.

DAN YORK: Well, and this is the point, right? Like you said, Andre. DNS is one of those things that people are just thinking, it just runs. It's

not broken, don't fix it. Don't do anything to it, don't, it just works, right? So how do we help people understand that there is, that it can be changed, that it should be changed? Anybody out there?

UNKNOWN SPEAKER: Well my thought was to find some really nasty security bugs, and give them [catchy?] names. That's how it's done in HTTP, right?

DAN YORK: All right. So now we're looking for really nasty DNS security bugs that we can give cool names and logos to. Any takers out there? You know, you're actually, to be honest, there is an element of that, that did occur, that would be something that would be helpful. Other thoughts from folks out here? What do we do? How do we help move this along?

What else came out of the RIPE meeting that you saw?

ANDRE: Well, [inaudible] from IC was talking about cyber-insurance, that it might be, well, something to look into. But it's probably a US thing, so I don't even know what cyber-insurance is. Only the folks from Comcast have it. And the other thought was there is

something called PCI compliance. If you want to do online payments, so it might include the DNSSEC as well, perhaps.

But I don't know even how to do, approach those for.

DAN YORK: Well, we've actually talked to some folks around the PCI compliance side of things, in looking at some of the pieces there. But that really only helps on the DNSSEC side. But the question, this is this larger question of how do we get things updated, right? Because we're looking at… The last time, in Marrakech, we talked about any cycle to get, if we would like to move more and more to these new BC algorithms, etc.

You know, we're looking at a scale of years before they'll really be able to be out there widely deployed, because we have to get them out especially through the validation software, in getting that out into all of the validators that are happening out there. And that's a good, large amount of work with regard to that. Paul, you're standing at the mic.

PAUL: Paul again. So one of the big things that is keeping us on these old algorithms, is the fact that the most commonly used DNSSEC signing software doesn't provide for an algorithm rollover, like if you use open DNSSEC, you cannot roll to another algorithm. So

people cannot do easily roll, unless you're going to run two servers and two different versions of the zones, and then sort of manually merge them yourself.

So rollover, I think, is the thing that's keeping these old algorithms in the zones now. People are just stuck with it now.

DAN YORK: Good point. Shane.

SHANE [CURR]: Yeah, Shane [Curr], Beijing Internet Institute. Well, I hesitate to suggest that we discuss the whole problem of agility in general, which seems to be what you want to talk about. Because I think that's a big issue for protocols in general, for DNS in particular, as an old protocol that has a wide deployed base, and is [crusty?], and hard to work with, requires a certain amount of expertise and things like that.

So I think, that's an area that I've been particularly interested in recently, and I think there are things that the DNS standards community can do, and DNS engineering community to do. I think it's a real problem, and I think it can be solved. I have a really hard time finding where that work, and where that effort should start, and how it should move forward.

Maybe we can talk about this in another context. But I think, for me, it's a bit like looking at net neutrality, it's like the real problem is that there is areas in the world with fundamentally no competition, and you use net neutrality as a proxy for that. So likewise, we don't have an algorithm agility in DNS, but that's really a proxy for the larger problem of not having ability to change the protocol at all.

ANDRE: I very much agree with what Shane said. And we even talk about it, in more generally in the RIPE session, because there is new thing coming to DNS like cookies and stuff like that. And it also needs a softer upgrade on both sides. We need to find a way to upgrade DNS more frequently. And I think it was sort of suggested that it might be a time to start thinking about DNS two or something. [LAUGHTER]

UNKNOWN SPEAKER: DNS v6, what?

DAN YORK: And Shane you're right, look at us when we've been trying to push out ECDSA, and just finding that one of the biggest barriers was all of the darn web GUIs in all of the registrars around the world who didn't have ECDSA as a choice for a DS record. Okay, I

mean, you know, forgetting the whole just issue around the DS record in general, just you know, web GUIs.

So how do you go around and get all of the web GUIs to go and be updated to have one more item in their box? You know. This is a big agility question. How do we make this move to bring about a more secure DNSSEC and bring in these new algorithms, when it comes down to, you know, somebody is going to configure a web GUI somewhere? By a registrar who is not really even paying any attention to DNSSEC, and they're just doing it because ICANN said they had to, in some way, to do this kind of thing.

DANI GRANT: Dani from CloudFlare. Is this on? I have doubts. I can do that too. Okay. Cool. When we turned on DNSSEC, the biggest problem we had with using ECDSA was the support from registrars and registries. This came up in Marrakech, but there was no real resolution. What is the reason for registrars and for registries to do any validation on the algorithm number at all? Versus just accepting any arbitrary value that a user inputs?

DAN YORK: Do you want to have one of the registries who does that? We had a couple speak up at the event. Anyone want to talk about that?

So, okay. So the reason why, that was given to me in a number of cases by a number of different registrars and registries, was that they have support costs of broken records, and they have support costs when things, you know, when somebody puts in the wrong info and it breaks, and all of this, and then they call the registry, or they call somebody and they try and go and do this.

And so, in many cases, the registrars or registries are providing some kind of form validation on that, to protect themselves, basically, from having to do any of the extra support work. You know, they're trying to minimize their costs to make sure people aren't putting in bogus records. So that's what's been presented.

Now, if any other registrar or registry wants to come up here and say why they restrict the records instead of just taking everything, they can. Oh, and here comes Peter.

PETER: Peter [inaudible]. I actually promised to stay in the back, but your comments was provocative enough to get me here. Mission

accomplished. So what we do is, independent of DNSSEC, we do certain checks on any delegation to maintain a high quality of the zone, and also to protect our own infrastructure. Adding DNSSEC to that means doing validation on the keys. So we need to understand the keys. We do understand ECDSA, actually we also understand [GOST]. I don't understand [GOST], but we accept the keys nonetheless.

The point here is, imagine that there was a massive influx of a new algorithm or anything that is related to DNSSEC, and there is a big mess up. I'm not really confident that that is actually beneficial to the future, to the ongoing deployment. So exercising a bit of care on multiple stages is probably a good thing to do. And so that, what we're doing, and I can only speak for [D NIC?] here, what we're doing is very much in line with what we've done before, and actually we're not really trying to restrict anybody, or restrict anybody's choices, it just took some time to deploy the software.

And that's… While doing that, some libraries were updated and so on and so forth. So it takes time. Taking time is something that's important here, and maybe while I stand here, my plea to the standardization community is, stop fiddling with the protocol.

UNKNOWN SPEAKER: [Inaudible] dot DK. I hope [inaudible], but as far as I understand you, only place we do validation on the keys is in the web interface, and is a very basic validation. Is it long enough? A to Z, zero to nine? Just because it's a web interface and people copy and paste and put things?

[SPEAKER OFF MICROPHONE]

Other than that, I don't think we do any validation on the keys.

[SPEAKER OFF MICROPHONE]

No, no, no, it's on the key, the hash itself, just to check. If you have this protocol, or this type, your hash needs to be this size, just because you copy and paste, just to help the user. Other than that, I don't think we have a lot of validation.

DAN YORK: Thank you for the… Go to the mic.

UNKNOWN SPEAKER: And no, we don't have [inaudible], I'm trying to work on that.

[SPEAKER OFF MICROPHONE]

DANI GRANT: Since you are not doing validation, has it caused you any problems? Like would you recommend this to other registries?

[SPEAKER OFF MICROPHONE]

UNKNOWN SPEAKER: Yes, we have about 1% signed domains, which is mostly one registrar. So the rest is, [inaudible] to know what they're doing. So no, we haven't seen any problem, because no one is using it.

DAN YORK: All right. Well, on that note, I want to say thank you to Andre for all the work he is continuing to do, and we will probably have more of these discussions at IETF 96 in Berlin, in the [kernel?] group or one of those, and we'll continue to have this. And I think, as a community, this is a question, this larger question of agility, but also how do we move to some of these more secure EC algorithms?

So thank you.

[APPLAUSE]

And with that, I think we need Russ up here as we enter into our final little bit before we the great DNS quiz. I did see Roy in the audience, so get ready to exercise your brains, or something.

Also, a reminder for folks who are new, you do need one of these to go to the lunch today. The ushers will… You need one of these that has this nice lunch on that side, there is a map on the

other. If you don't have one, the ushers won't let you in, and we thank again, these four people, the four companies that are on here. If you see them, say thank you, because they're buying lunch today.

All right. So with that… Oh, these should be around on the table. We kind of put them around in different places. There are some more up front, there are some others, there are some more in different places. So you can get one of those if you don't see them, we have a few more up here. We can get them to you.

So all right, this brings us to the conclusion of another DNSSEC workshop, and so let's go ahead with our slides here. Oh, I have the clicker, okay. I have the clicker. All right.

So basic steps that we encourage everyone to think about, or TLD operators to please sign your TLD. We want to fill in the rest of that map and get the rest of these. We ask people to accept DS records, work with the registrars. We also would like people to make statistics available.

This is something we talked about earlier. Some of these different efforts that are out there, we're just trying to track this and see how things go. We'd like help with that. Let's see. Russ, I'll give you, yeah.

RUSS MUNDY: Thanks Dan. Right, so almost everybody has a zone, or multiple zones. Some of you a gazillion zones. Or a billion maybe. But signing the zones is a critical step. So look at what you need to do to do that. Depending on where you are, you may need to work with your registrar. And registrars are doing more and more becoming available, but that's still, if you will, one of the weakest spots in the overall DNSSEC chain, is support from the registrar.

So work with and encourage a registrar to do what they need to do, so that your zones can actually get out there, get published, and again, statistics, statistics, we really want to learn more what's going on and be able to see more, collect more information.

DAN YORK: On the network service providers side, you saw Geoff Huston come up here and say that fact that if you can't turn on… What was it Geoff? If you think it's hard to turn on DNSSEC, you should take up fishing, I think is what I captured there. All right. So you know, yeah, it's a little bit more involved because you do now have to be prepared at least to answer potential questions when people can't get to sites that have issues with that, but that is a critical step around that, so we do ask, you know…

We want to see more of those registrars. Whoever is in Finland, let's talk to those other three large providers and see if we can get them to turn it on here. We need to figure out those spots where we can make those changes. And then, of course, sign your own zones in some way. So one of things that I think we got a bit of a flavor of, today, that on the panel, in particular, was a broad range of spectrum. So I think we heard a number of people saying various problems that they had.

I was thrilled that Nick was willing and able to join us and talk about things from the GAC and the government perspective, and I know sometimes people look at governments with suspicion, and sometimes they probably ought to. But they are a member of the community, and they have influence, access, and as Nick said, that they can get to people and encourage them. And that is something I think we may have heard a little bit more today than what we've not heard in the past.

And I'm not sure if Nick has left yet, but one of the things that I wanted to do, was ask him… Are you still here Nick? Ah, yeah. To please raise this within the GAC. And continue to raise the interest level. The US government has been a strong supporter, but beyond that, I don't know that there have been that many pushing from the government side.

So please help us do that, and if people from the GAC want to talk to anyone in this community, I think they'll find them very receptive. So, that was a little variant from what's in the slide this time, but I thought it was an important change, and a great input that we had this time.

DAN YORK: And on that note, we also want to encourage people to share what you're learning, and share it in the other sessions. The pieces that are there. Question? Yeah.

[SPEAKER OFF MICROPHONE]

UNKNOWN SPEAKER: …I'm from a Finnish small ISP, and we've been running a DNSSEC validating name server for about five years, because originally local ISPs didn't provide that service. And right now, I've been thinking about taking part in a system called [inaudible] DNS, which I'm hoping I'm going to get to talk to people here. So, talk to me afterwards if you are involved with this already.

DAN YORK: Did you hear that? Okay. Yes. Shane is one to talk to.

UNKNOWN SPEAKER: All right, thanks.

DAN YORK: All right. And so, and on that, I mean, please do, bring things that you're doing, bring projects, bring items. We'll have another one of these coming up at the next ICANN meeting. And I want to just, let's give a round of applause to everybody who was part of the presenters here today.

[APPLAUSE]

It does take a certain amount of courage to come up and stand up here and do this, and talk about what you're doing and what the kind of things are. So we greatly appreciate all of that today. I want to give a special thanks again to our four sponsors, Afilias, I see Jim in the back there. I see Jacques here for dot CA. I see Christian here for SIDN, he's somewhere.

Oh there he is, back there. Okay. And do we see anybody from [Dine?], no? Okay, Matt was with [Dine]. But we thank them all, and also do want to say too, we are looking for a fifth sponsor, if you're interested in doing that. It's a relatively inexpensive cost, but it just helps us ensure that we have the funding to be able to do these lunches and pieces like that.

Again, the support for this comes from the SSAC, as well as from the deploy 360 program part of the Internet Society. And these

are websites, if you have not been to them, we encourage you to go to them, and we have one last slide this time, which is to say, afterwards, when this meeting ends, we encourage you to stay connected, to be involved.

There is a mailing list for the, what we call the DNSSEC coordination effort, which you can go to and join. It's a public list, you're welcome to do that. We have a conference call on the first, using that old phone technology, I know, although we've been moving to zoom, we've been doing some things over it now, video.

On the first Thursday of each month, where we've talked about this and get a chance to talk, as a community, about where we're going with DNSSEC, and what we can do to advance it. So we encourage you to join those efforts, and also to get ready for Hyderabad for ICANN 57.

So I think with that, I also want to just say, thank you as well to the people who are sitting here quietly. Julie and Kathy who have both been our support in keeping this going, and organized, and everything else. So please, let's thank them.

[APPLAUSE]

RUSS MUNDY: And they're the ones that really make this happen, because it wouldn't happen without the help of Julie and Kathy.

DAN YORK: And so, with that, we want to bring up Mr. Arends for the great DNS and DNSSEC quiz. And for all of those who have never participated before… How many newbies do we have here in the room? Who have never done a DNS and DNSSEC quiz? Okay. Get prepared.

ROY ARENDS: Does this work? Can we make this work?

DAN YORK: Okay, what. is it turned on? The bottom?

[SPEAKER OFF MICROPHONE]

[CROSSTALK]

Okay, so here, one little detail. You know, I told you about this sheet of paper that was floating around? Okay, the other sheet that has the program on it, if you turn that over, Julie and Kathy were very clever, and on the backside is where you can put in the answers to the quiz that Roy is about to do.

So, and if you don't have one, grab some. There is a couple up here, you can grab one there. Couple of more in the front. This is an interactive participatory thing. So you need this sheet. Now, I'll leave it to you Roy.

ROY ARENDS: Great, thank you. Can I have the first slide please? So, as Dan said, use the back of the form to answer, to put your answers on. You can play in a group, you can play on your own. Put your name on the sheet as well. When we're done, give it to your neighbor so we can all check it, and we'll all play in an honest way.

And of course, if you're checking the form, and this guy or girl has all the answers correct, don't change the name into your own. At the end of this quiz, we'll go through all of the answers. Next slide please.

This is important. Sometimes more than one answer is correct. So sometimes all of the answers are correct. Or sometimes none of the answers are correct, and you have to figure this one out on your own. Point is scored for each correct answer, and I think there are 13 or 14 points to be scored in this quiz.

If you have a wrong answer, and a right answer, so if you ticked on two and one of them is correct, you lose all of the points basically for that question. Next slide.

Okay, so start with number one of the questions. I'm going to go through this pretty quickly so you don't have time to check this on the internet. Which of these top level domains do not deploy DNSSEC? Is it dot [Tel], dot ZA, dot arrow, or dot Moby?

Is it A, B, C, or D? Next question please. What is TPC in TPC dot [int] stand for? Is that A) Transition Policy Center; B) Technical Program Committee; C) Trans-Pacific Cable; or D) the phone company.

Okay. Question three. Which [int] domain does currently exist. Is it A) [inaudible] dot [int]… I happen to be a European living in England, for now, yeah. [Laughing] Oh, brilliant. B) IP6 dot [int]; C) Euro Fish dot [int]; or D) COT dot [int].

Next question please, thank you. This is an old one, you've seen this before. What does the [obit] stand for in a DNS query? Is it DNSSEC off? Is it DNSSEC on? Is it DNSSEC out? Or is it DNSSEC [inaudible]? I remember, one time I did this slide, a couple of quizzes ago, none of the answers were correct. And so you couldn't actually score a point for that. I thought I was cute, but I shoot myself in the foot.

Anyway. Number five please. How many bits wide is a TTL field of a DNS record? Is it A) 8; B) 16; C) 32; or D) 64? Next question please. What is SOA as in SOA records, stand for? Is it A) the source of authority; B) statement of authority; C) system of authority; or D) start of authority?

Next question. How are we doing for time? Great, okay, perfect. What does the CD stand for in a DNS query? This is an old one as well. Is it A) a compact disk; B) checking disabled; C) cryptographic device; or D) change directory?

Next one please. A simple one. What does KSK stand for? If you haven't paid attention today, then I don't know. Is it key signing key? Is it kill switch key? Is it key switch key? Or [inaudible]? I need to get rid of this question. This is getting old.

So this is slightly different then the questions we had, quizzes before, so how many different root server operators, as in organizations, not the individual folks, as in how many different root server organizations are there? Is it A) 12; B) 13; C) 24; or D) 26? And for the last question, number 10. Which country, as in which ccTLD, was the earliest to deploy DNSSEC? So not the first, but the earliest. Was it A) United Kingdom; B) Sweden; C) The Netherlands; or D) Germany.

Perfect. Thank you everyone. If you've… Make sure you've filled out your name on top of the form, and I would like to give it

to your neighbor. And if you're sitting by yourself, just turn the form 180 degrees clockwise. Sorry.

[LAUGHTER]

Oh by the way, the winner, just like every time, the winner gets a free lunch. [LAUGHTER]

You can use this, and also you get, what was it again? Oh yeah, eternal recognition. Right? Who remembers the last winner of the Marrakech quiz? I don't think anybody remembers that.

DAN YORK: Who did win in Marrakech? Do we remember?

[SPEAKER OFF MICROPHONE]

ROY ARENDS: Hey, there you go.

DAN YORK: Duane, were you saying it was you?

[SPEAKER OFF MICROPHONE]

[LAUGHTER]

ROY ARENDS: Okay. I think we're going to go back to question one.

[SPEAKER OFF MICROPHONE]

Oh yeah, no, I have the answers. I can't publish them on the… So, which of these top level domains do not deploy DNSSEC? Okay. I think none of these top level domains deploy DNSSEC. So if you have A, B, C, or D, you are correct. You can get four points if you've crossed off all of them.

Yes, this quiz also helps to shame top level domains. Okay. Next question please. What did TPC and TPC dot [int] stand for? This is D, the phone company. And if you're interested in a little bit of a backstory of that, come this afternoon to a presentation I happen to give on abuse in dot UG. [Inaudible] says a little bit about the phone company in there.

Next question. Sorry, this was answer D, the phone company. Question three, which [int] domain does exist currently? And the correct answer here is Euro Fish dot [int]. All of the others do not exist, currently. Question four, of course, the [inaudible] stands for DNSSEC [inaudible].

And five, how many bits wide is a TLD field of a DNS record? [Inaudible] Peter, how much?

[SPEAKER OFF MICROPHONE]

Yes.

[SPEAKER OFF MICROPHONE]

Perfect, yes, dear Peter, *danke*. So the answer to this is C, 32. I always do this when I forgot the answer myself. [LAUGHTER]

This is true, this is true. I know Peter knows it. So number six. What does SOA stand for? That's D, start of authority. Seven, what does the CD bit stand for in a DNS query? It is B, checking disabled. Number eight, what does KSK stand for? Key signing key.

If you have this wrong, you can bring your lunch form to me right now. Okay, number nine, how many different root server operators or organizations are there? The correct answer is 12. It is very signed. It operates A and to J, so that's why there are not 13. There are 13 root letters, there are 24 root server addresses, there are 12 organizations. So that the correct answer is A, 12.

And the last question, which country top level domain was earliest to deploy DNSSEC? And that is, of course, B, Sweden. The earliest of these four. That's not a country code, top level domain.

[SPEAKER OFF MICROPHONE]

It's…

RUSS MUNDY: One of the base rules of the DNSSEC quiz is the quiz giver is always right.

ROY ARENDS: Thank you. Okay, so with that, we're going to… If you can give the form back to your, to the original owner, you can check that by the name on the list. So who has…? Let's start with 15? Who has 15 points?

Good, because that would be impossible. So who has 14? 13? Anyone at 13? 12, anyone? 12 points? 11 points? Perfect, we've got a winner here. We've got 11 points.

[APPLAUSE]

Well done. And quickly, 10? Perfect. Oh, I see the DNS folks, yeah. Nine? Eight? Perfect. Seven? I do this to understand the distribution, right. Seriously, when I first give this quiz, it was ridiculously complicated. It was, what is the third bit in the DNS message stands for when the answer is signed? Something like that.

And no one had those correct. So I made it a little bit more wider, and I can see that in the distribution of the scoring.

Thank you everyone for participating. And I hope to see you the next DNSSEC quiz in Hyderabad.

DAN YORK: And thank you Roy for doing this.

[APPLAUSE]

And if anyone would like to help Roy with providing questions, he's always open to more questions. So if you would like to see a couple of those get out of the things, he would love to hear from you. And now, I want to turn it to Julie to give us info about lunch.

JULIE HEDLUND: Thanks Dan. Yeah, so lunch, if you don't have a lunch ticket, there are still a few of them around here. You will need it. And there should be an usher, or ushers out there to help you as well, but there is a map on the back of the ticket. The lunch is two levels up. It's in level two, we're on level zero. It's in the [inaudible] room. So if you go up the stairs, you can go up two flights of stairs, and there is also an elevator just to the right out of here.

And then the lunch is just sort of at the back, and of the [inaudible] room. So please go ahead. If you've got the ticket, you may have lunch. Enjoy.

[END OF TRANSCRIPTION]