ICANN
Transcription
Next-Gen RDS PDP Working Group
Wednesday, 21 February 2018 at 06:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at: https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-21feb18-en.mp3 Adobe Connect recording: **https://participate.icann.org/p9if32erbpq/**

Attendance of the call is posted on agenda wiki page: https://community.icann.org/x/ngu8B

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page http://gnso.icann.org/en/group-activities/calendar

Coordinator: Recordings are started.

Julie Bisland: Okay great. Thank you very much. Well good morning, good afternoon and good evening everyone. Welcome to the Next Generation RDS PDP Working Group call on Wednesday, the 21st of February 2018.

In the interest of time, there will be no roll call. Attendance will be taken via the Adobe Connect room. If you're only on the audio bridge would you please let yourself be known now? Okay, hearing no names, I would like to remind all to please state your name before speaking for transcription purposes and please keep your phones and microphones on mute when not speaking to avoid any background noise.

With this I will turn it back over to our chair, Chuck Gomes. Thank you.

Chuck Gomes: Thank you. And welcome, everyone, to this week's working group call. I want to say special thanks to those who are calling in the middle of the night; I see quite a few of you that are in that category. And just to share the pain, I'm doing it as well because I'm on the East Coast today. So thanks again for

doing that, and happy to accommodate those of you who are almost always calling in at undesirable times, so thanks for doing that so often.

So, do we have any statement of interest updates? If so, please raise your hand. Okay, then let's jump right into the agenda. You can see it in the upper right of the screen. And if we can bring up the presentation too it'll be on the first slide there. Everybody now - it looks like everybody now has scroll control so if you go to Slide 2 you will see the proposed agenda.

And we'll jump right into Item Number 2. Just a brief discussion about the suggestions that were discussed on the list by I think one of them was by Mike Palage, regarding the possibility of getting some expert advice, and several of you commented in support of that. What the leadership team has decided is that it might be better to wait, if we do decide that's necessary, it'd probably be better to wait until we have some - a few more specific recommendations that we could ask about.

Also there's a practical matter, there are no funds available for doing that right now under the current year budget. And to request funds that aren't already budgeted really ensures us - we need to be able to ensure that it's really going to make a difference. We have quite a bit of expert advice we received over the last year plus and frankly we haven't used a lot of that because there's still - regardless people still haven't been ready to accept that. So at this time we're not suggesting that we pursue that route. That doesn't mean we can't do it later but that's the decision by the leadership team.

So let's go on then to the agenda Item Number 3, which is to try and complete deliberation on domain name certification. So if you will go down to Slide 3 you'll see a slide in that regard. Now I'm trying myself to get - well I'm on a smaller computer, that's why my screen isn't showing. So on Slide 3 the results of the poll from last week is on the - is at the link on the working group

wiki. So if you haven't looked at that feel free to do that. We're not going to pull those results up for this meeting but rather give a really brief summary.

So for Question 2, the 72% of those who participated in the poll supported domain name certification as a purpose for doing some sort of processing, okay, they didn't specify what type of processing, does not necessarily mean collection, okay? And then for Question 3, about 62% either agreed or could live with the statement that domain name certification would be okay as an opt in purpose for collection.

So the 72% is getting pretty close to 3/4 but we have - whereas we don't have a set number that we're looking for for rough consensus we usually try to get even a little bit higher than that. So at this point we're not recommending declaring rough consensus on that, hopefully in our work ahead we can get a little stronger support there and possibly declare that if that happens.

The opposition, and I'll give members of the leadership team a chance to comment on this as well if they'd like. We did review all the comments and the opposition to Question 2 where we had almost 75% support seemed to center around three concerns. The first one was, "Can consensus policy for gTLD registration data specify purposes that are in the legitimate interests of third parties?" In this certificate authorities. The second one was, "Does being a legitimate purpose for processing data also imply that data is collected for that purpose?" And the third one was, "There is a need for greater clarity around collection of data for this purpose."

So that's where the opposition was. We're not going to spend time on that unless somebody objects talking about those things right now. Instead we're going to move right ahead and go to Slide 4 where we have another slide there and look at the data needs, the data element needs associated with domain name certification as a possible purpose.

Remember the domain name certification definition that the drafting team from last year, late last year, gave us and it's in - on Slide 4 there towards the top. And so we're going to look at what registration data might be necessary for this purpose and is that data already collected by another compatible purpose and then if not, should it be optionally collected for this purpose? Okay?

The last bullet then on Slide 4, as you can see we're going to make at least one working group assumption or one assumption and moving forward. You recall that we had quite a bit of discussion a few weeks ago, a few meetings ago, about the idea of whether a purpose is compatible, a purpose for which data is not collected but if it's compatible with another purpose for which data is collected that it appears that that would be allowable under the GDPR.

Now what we found out, and a small team was formed to look at this issue and they I think are - may still be doing that and that's good, but it looks like it's going to take a while to get anything definitive on that. So for the sake of keeping our deliberation moving what we're going to do is we're going to assume compatibility of the domain name certification purpose with two of the purposes for which we've already identified data could be collected and that's the technical issue resolution purpose and the domain name management purpose.

Now keep in mind, and sorry for doing so much talking, keep in mind that the - we haven't gone through all the purposes so it's possible that we will decide at least at a rough consensus level that other data may be collected for other purposes but we haven't gotten there yet, if and when that happens we'll deal with it so that's what the very last sub bullet says there.

Okay, going on then to table - or excuse me, Slide 5 then, we have a table that gives us some information. Now it's important to understand what's on this table, okay, so let me quickly review that. And I said I was going to give leadership team members a chance to comment on anything I've said so far

and I forgot to do that earlier, so let me pause. Does anyone on the leadership team want to add anything to what's been covered so far? Okay.

And as you can tell Lisa cannot be with us today but we've got Caitlin and Marika on here so from staff and then of course our vice chairs. So and it looks like at least two out of three of the vice chairs are present.

Okay, not seeing any hands I'll talk about this table. The - you can see on the left there, and this is not a new table so sorry for repeating for those who have seen this several times, you can see the column, Registration Data Needed for a Domain Name, and then the different elements, in some cases just categories of elements and not broken down to specific data elements and we may talk about that a little bit later.

So for the purpose of technical issue resolution we at least reached rough consensus that the data elements marked with an X in the second column there should be collected for that purpose. Now in the case of registrant contacts, we didn't drill down into which contacts so at some point we'll have to do that and drill down a little bit further. Does it mean phone contact? Does it mean email contact? Does it mean postal address? Etcetera. So we didn't drill down that far yet.

For domain name management, again, you see the data elements or data categories X there for the ones that we reached rough consensus should be collected for that purpose. Now, what's shown in domain name certification is different, okay. We haven't reached any rough consensus on domain name certification in terms of access as you've seen from our poll from last week, or collection.

But the drafting team that worked on this purpose the end of last year, identified the elements that are marked with an X as those that are used by certificate authorities from existing Whois. So our purpose today is to see if we can reach any sort of agreement in terms of what if any data elements

would be appropriate for possible access for the domain name certification purpose. Now let me pause, I see Steve's got a hand up so, Steve, you're on.

Steve Crocker: Sorry, took a second to come off of mute. With respect to the domain name certification, the fields that are listed there are provided by the account holder. What assurance does the domain name certifier have or require that that information has any relationship to the domain name?

Chuck Gomes: Good question, Steve. This is Chuck. And anyone else who'd like to respond feel free to raise your hand. That may come down at least in part to what we decide in any future RDS with regard to accuracy. That's one of the - one of our first five questions from our charter, one that we haven't spent any time on yet. But does anybody have anything to add to that? Maybe somebody that was on the design team if you have a thought? Alex, I think you were on that drafting team, right? Go ahead, Alex.

Alex Deacon: Thanks, Chuck. Yes, it's Alex. To answer Steve's question, I mean, really - I guess it depends, which is a terrible answer but it depends on the type of certificate that is being authenticated and verified. In the case of EV certificate, kind of a high end, high assurance, highly authenticated certificate, it is the job of the certificate authority to ensure that the information in the Whois matches information from third party databases and that that same organization or individual in fact has control of the domain.

So that's essentially how it works but clearly there's details there and in some cases depending on the style of certificate, that may or may not happen especially for those certificates that just require proof of control of the domain name, which may or may not actually require any access or validation of RDS or Whois information. I don't know if that answers your question but that's basically how I see it.

Chuck Gomes: Go ahead…

Steve Crocker: Let me chime in. So in collecting this information and saying it's for the purpose of domain name certification, there is no automatic or no intrinsic representation about the quality of that information with respect to its accuracy or the meaning of those - of that field or whatever the people listed take any particular responsibility or oblige to respond, all of those properties are left to the certificate authority to separately identify and authenticate.

Are we prepared to make such a statement covering this disclaimer basically that I've just said that publishing this information in the Whois provides no authentication as to whether that information is relevant or accurate and hence serves in the lingo that we might use, merely as what you would call a hint and leave it to the certificate authority to take it from there?

Chuck Gomes: And, David, you want to respond first or Alex, either one. But David, you've got your hand up, let me go to you.

David Cake: Yes, the - in the case of the registrant email, the - that is one of the ways that is used to confirm control by the domain name - by the registrant - by the - sorry, one of the ways it is used to confirm that that registrant who is applying for the certificate controls the domain. So it's - it is certified as correct in that process, but it's only one process, it's not guaranteed it's ever done.

And all of these - however they're used in the process the certificate authority does not monitor them, so they could always be changed after the certificate is granted. I mean, sometimes I think the certificate authority might, you know, if the - if some details are obviously very different they might query them but in general all the information on the certificate is verified separately by the certificate authority by means outside the RDS and they - the certificate authority makes no guarantee about information that is in the RDS.

Chuck Gomes: Thanks, David. And I'll get back to you in a second, Steve. Let's see what Andrew wants to add.

Andrew Sullivan: Let's see if this works. Can you hear me?

Chuck Gomes: Yes.

Andrew Sullivan: Good. Thanks. So the - I'm slightly confused about this because the certificate authority business is a competitive market and so different certificate authorities, as I understand it, and I think this has been represented on the list as well, have different policies around how they do this. One thing that is true is that the current arrangements don't really allow a certificate authority to use the RDS as a reliable pass through mechanism but of course we could - we could actually make that a feature that is available through the RDS if we wanted to.

So one of the things that seems to be missing here is the potential to enable the RDS to be valuable for these ancillary purposes that the domain name market seems to be providing. And I should just point out that you know, Google has already announced that Chrome is going to treat HTPS sites - or HTP sites that don't have a TLS certificate as failures in the future. That is they're going to mark them as insecure rather than putting the, you know, rather than putting the padlock on they're going to try to change their user base and convince them that everything that doesn't have HTPS is insecure.

So it does seem to me that there is some pressure on the Internet to try to continue to build more security apparatus atop the DNS. And I think that, you know, basing the entire discussion on what CAs do today according to the CAB Forum is maybe a little bit - is sort of optimizing for a use case that is yesterday's rather than tomorrow's thanks.

Chuck Gomes: Thanks, Andrew. And I suspect at least part of what you're saying is why Alex said "It depends." But just a little side note I just received a message that the chair of the CAB Forum is going to join our working group, unfortunately he's traveling today so whatever decisions we might come to today and any polls we have we'll certainly call it to his attention. Of course he's got some

catching up to do since he'll be a new member in the working group, but that'll be a nice asset to have going forward. I don't think that needs to delay us making possible decisions today but it will be nice to have him in the working group.

Steve, let's come back to you.

Steve Crocker: Sorry, I was on mute. Thank you very much, Chuck. I want to align myself with what Andrew's just said and take it a step further. It seems to me there are two possible stable states in this; one either we within the design and operation of the RDS provide a level of certainty that the information provided is meaningful; or we give it up entirely and say why bother? In which case the certificate authority in this case can have its own interaction with the certificate - the person requesting the certificate and they can supply whatever information they want and the certificate authority can do whatever validation they want.

Let me draw a comparison. It's standard practice in contracts, and Chuck, now I'm entering into your territory more than mine, that toward the end of the contract there will be something about legal notices should be sent to the following address.

And that information to my non lawyer understanding, has real meaning that is it is a commitment that certain notices that are sent to that address will be treated with - as having been received and that if incorrect information is supplied in that or if - to take the analogy at David Cake raised - if they stop paying attention to that address, change their address or whatever without giving proper notice to change the contract, then they're liable for whatever harm comes from getting formal notices that they don't pay attention to. Are we going to reach that level of practice and commitment?

Chuck Gomes: Thanks, Steve. That's a really good question. And I think we can, I mean, that is an option that the - if the working group can reach consensus - fairly strong

consensus on taking that approach there's nothing to prevent us from doing that. That's part of I think why we have to first of all decide whether domain name certificate is a legitimate purpose looking at ICANN's mission, looking at the RDS and so forth, is it legitimate for providing some access, not necessarily collection. We could also decide that something should be collected for this purpose.

That's really what this whole exercise right now is all about because not only from the point of view of the GDPR, but also if you look at the EWG report, and most of you are familiar with that, they used a purpose-based approach - suggested a purpose-based approach as well. So it really comes down to whether we decide I think whether this is a legitimate purpose for some sort of access and if so, which data elements? Let me jump over to David…

((Crosstalk))

Steve Crocker: Well let me just push it that…

Chuck Gomes: Oh go ahead. Go ahead.

Steve Crocker: The question that I'm asking it's actually going to apply across the board. If we collect information and make it available what obligations on behalf of the person supplying that information are attached to that?

Chuck Gomes: Clarify for me what you mean by "what obligations" what guarantees?

Steve Crocker: Yes.

Chuck Gomes: Okay, that's what I thought you were saying, I wanted to make sure. That may be more of a Board decision than…

((Crosstalk))

Steve Crocker: No.

Chuck Gomes: …what we might make.

Steve Crocker: That's not the Board's role. That's not the Board's role at all. It's the role of this group or some other group to lay out a coherent and usable and workable model. The Board simply - I can speak with some authority having been on the Board for a long time, the Board's role is to oversee a process and see that something sensible comes out of it but not to impose its own value system on it.

Chuck Gomes: No, agreed, agreed with that, no argument there. But if we make a recommendation that a certain commitment should be made, so that domain name certification authorities can rely on that, of course the Board would have to approve any recommendations we make. And I think that's what I was trying to say.

Steve Crocker: Sure. But the same question will come up with respect to any other role. When you publish something as a tech contact, does that mean something?

Chuck Gomes: Well as we all know, it hasn't meant a lot historically in Whois because of inaccurate records. I think probably, and somebody correct me if you think I'm wrong on this, and I could very well be, we're going to probably have to deal with that more when we get to the question of accuracy. You know, if we take more steps than have been taken to date to ensure accuracy that may impact what you're saying and I'm' probably not doing a very good job of answering your concern. But let's again let some other people jump in. David. You're on mute, David.

David Cake: I think that - I think the question - I think the answer to this question about what are our - I mean, essentially if we took the one road and said we are granting no - we have no concerns about the certificate authorities and we are not going to make any guarantees or supply them with any of this data,

then anything from the RDS or make no guarantees to let anything in the RDS, most of these fields we're talking about, it's in the nature of a hint. It might make the process go a little faster, but if it's removed the process is essentially unchanged if slightly less efficient.

The one exception is registrant contacts in the sense that - or registrant email in the that email can be used to demonstrate (unintelligible) and the one I guess issue where even tracks on what ICANN does, if we found that that - the mechanism of using the email to demonstrate control of a domain name was being abused or in some way used to mess with the CA process, or to - try and undermine the CA validation process such as people who were not authorized to get a certificate somehow obtaining one, then it might become an issue where we wanted to look at that and verify - or look at what that means in terms of - I would say a security commitment because a, you know, making sure certificates exist is arguably a significant part of ICANN's mission.

It's just before we could get the CA browser people to simply not allow that mechanism and to always use alternate mechanisms for demonstrating control, which includes well - normally would be directly via the DNS these days but not always. And I don't think - I mean, I do think that Steve has - from a very important issue about what ICANN's commitment in terms of the validity of the data in the DNS, I do think DNS certification isn't a very good issue to demonstrate that because it's not a big - the change really does not - will not interfere with the CA browser's business very much.

In many ways it's really the opposite way around, what do the CA browsers - well CA and Browser Forum people - what do they say - what does the DNS say to them and what do they say about the DNS? So I think it's an important distinction but it makes so little difference in the case of the domain name certification purpose that it's a poor example.

And really I think I mean, I think if we said officially the CA Browser Forum we offer absolutely no guarantee about any of the data contained in here, please don't use it, the practical effect would really be that they just stopped using email as a method to demonstrate control of a certificate, which really is one of alternate methods and would be relatively small change to the way the browser certification industry works.

Chuck Gomes: Thanks, David.

((Crosstalk))

Chuck Gomes: Steve, you want to jump back in before I go to Jim Galvin?

Steve Crocker: No, I think I've said what I wanted to say and I'm typing some comments in in the chat rather than just taking up air time.

Chuck Gomes: Thanks, Steve. Okay, Jim, you're next.

Jim Galvin: So Jim Galvin for the record. Steve has touched on something which resonates with me and so I wanted to call it out. I have generally been arguing against domain name certification as a reason for (unintelligible) data and I have said that I don't object to domain name certification being used for processing although I still don't support it. And the reason that I've been saying that is because ICANN is not in the certificate business and therefore we don't have a role to play in that space.

Now folks have argued that the DNS you know, in its requirement - in ICANN's requirement to support a secure and stable DNS, you know, certificates are sort of natural and complementary to that if not obligatory and therefore domain name certification should be an obvious reason to collect data.

And I think Steve's comments about the fact that - and he's even writing this in the chat room here too, you know, the thing which is interesting to me is the data really just doesn't mean anything and there's no obligation that it mean anything. It's always struck me as odd that certificates, you know, we're building this quote, secure web, if you will, based on data of dubious origins and in fact even ICANN is collecting data of dubious origins. You know, there's accuracy of the data from a syntactic point of view and there's accuracy of the data from the point of view of does it really represent something?

And I think this has always, always bothered me in this space. You know, now we could change that. I guess the real point here is if we all believe that or, you know, if you believe that then I think as we've also been telling ourselves we get to change that and I think that that's an important point to bring up here. If we really do want to support domain name certification, then I think that that also obligates us to create a new kind of system where the data actually means something. And if we're not going to go down that path then I'm going to stand strong on domain name certification not being a valid reason for data collection and always be doubtful of whether or not it's a suitable processing point.

What most - what at least the Let's Encrypt certificate vendors do is really more after whether or not you control the domain name and that's how they decide whether or not you can have a certificate for that domain name. That makes perfect sense to me but this business of whether the name for the registrant and address all make sense, I just don't get it. Thanks.

Chuck Gomes: So, Jim, Chuck with a follow up question. So if I understood what you just said, wouldn't email - the email contact be useful for confirming that you have control of a domain name? Not necessarily definitely but as one check?

Jim Galvin: I think it's a part but it's not as definitive as whether or not you can put a text record in the DNS for the domain name. That actually demonstrates that you

really do control that domain name. The email address, it's just a point of contact like your postal address and you still need some other step, some other point of verification, you have to confirm that that is in and of itself valid data, not just whether or not you control it.

The email address you can just prove whether or not you control the email address or at least that there's a person back there, you still need to confirm it's the right person, right?

Chuck Gomes: Correct. Yes, thanks. Appreciate that, Jim. Let's go to Maxim.

Maxim Alzoba: Maxim Alzoba for the record. I'd like to, yes, to add to the James idea that on our registrar part of business we often see situations where the access to the email box was compromised and some bad actors are using that to (change) domains do any kind of things. So I'm not sure that in current world yes, most mailbox systems are the sure way to say that it's the person who started this mailbox. It's not always - works, it doesn't work this way in all occasions.

And it seems to me that some of registrants, not all of them, really might need some optional fields, for example, they need - want to have some super strong certificate which includes delivery of the letter with a special code they need to enter into the web portal which proves that the mailbox they provided, I mean, postal box, is the one they use.

But also the influence on control of the domain is higher if the person can arrange some text record into DNS system, it means that way more things have to be in place before this change and it's a stronger way to ensure that the person who controls the record was the same person who asked for the certificate.

Also, there is an issue if for example, we collect some particular field for all registrants and they really required only to those of them who want some kind of special certificate, it means that for big number of registrants we say that

the reason of collection was this particular certificate, but we never use data for this reason and if we use the same data fields for some any reason it kind of violation of consent with the registrant that this data we're gathering will be used only for this reason.

So I think the exit could be - now the way to resolve it could be optional fields and if the registrant wants to use it they have separate consent and separate web portals of handling so we don't create station where large number of registrant their data - they were told that that data were going to be used for some special reason and in reality is used for something else. It creates issues with the privacy laws. Thanks.

Chuck Gomes: Thank you, Maxim. Let's go to Andrew.

Andrew Sullivan: Hi. It's Andrew Sullivan again. So I feel like we may not be attending to all of the distinctions that some of our privacy and security activists have been - or rather defense activists have been talking about on the list. I'm sort of wishing that Allison or maybe even Rod were here to try to bring some of this up. So I'm going to try to do a job of it but I'll probably miss and maybe others can beat me up for it afterward.

When you try to identify who is doing something with you on the Internet, and you need actually strong evidence about who that person is, it isn't a binary - it isn't a binary operation, right? People - the discussion so far seems to be suggesting, well, that the Whois have this or does the RDS have this information or not? But that's not quite it.

The way this works in my experience anyway is that people have a bunchy of heuristic pieces of evidence and if they fit together in a package according to, you know, some data gathering and some algorithms, then you - you believe at that point that the person you're - or the supposed person you're talking to is in fact the person you think you're talking to. And you have some sort of Bayesian probability distribution about, you know, how likely that is.

And I think that the way the RDS works today is that more evidence across multiple domains and across multiple users and so on, is what those kinds of people are doing and that's one of the things that, as I understand it, certificate authorities are doing. So I'm a little uncomfortable with this idea that this is the kind of binary switch where oh, well you look up the account and if they, you know, if the email address matches then you're fine. I don't believe that any CA works that way.

And for EV certificate providers, I think they're doing quite a lot more work than that. One of the things they do is exactly one of the things that Steve mentioned in the chat, they get you to put something in a zone file and then they look it up. Everybody who uses Google apps or Google Docs or anything like that today with their own corporate system look it up at the top level of your domain there's a TXT record that has to do with Google. That's what that is. So every provider is already asking you to show that you have control over that DNS record.

But this is a different problem, it's not control over the DNS that we're talking about, the question is do you also have control over the registrar account and do you have control over what goes into the registry for that domain? And what goes into the registry for that domain you can't put arbitrary text records on the parent side of the DNS, and so there's a legitimate question about whether you have, you know, just because you have control over the DNS for a given domain name right now does that mean you have legitimate control over that domain name and its registration?

And I think that the RDS has always been about the legitimate control over the records that should be - that should be in the official record rather than the things that are actually in the DNS. And gaps between what's actually in the DNS and what's in the RDS are a good clue that there's something wrong. And so to the extent that we're unable to, you know, provide some mechanism by which those two things can be linked up we're failing the

people who are building security models on top of this and that most definitely includes you know, the certificate authorities and the browsers and everybody else is dependent on X509 certificates on the Internet.

So it seems to me that we need to provide some mechanism for this, that doesn't mean that it's, you know, everybody's name and address and telephone number but it means that we do need to have some mechanism that we're providing here that allows for X509 certificates to be linked up between the actual behavior in the DNS and the legitimate control over the registration of that domain name and that is exactly where the RDS lives. Thank you.

Chuck Gomes: Thanks, Andrew. This is Chuck. So if I understood you correctly, Andrew, you're suggesting that some sort of access to some RDS data elements would - you believe it would be useful. Did I conclude too much there?

Andrew Sullivan: It's more than just useful. The current environment on the Internet has built a large trust framework around domain names. And one of the gaps in that framework has to do with the link between the control over the domain name itself, that is in the DNS, the control over the zone file if you will, and the control over the domain. And at the time of certificate issuance, and further at the time of validation of whether this certificate remains valid, there is some validation that needs to be done there.

The second of those, that is when you're doing this validation all the time of checking whether the people who were in control of this domain name when the certificate was issued, are they still in control of it, that remains quite problematic. There are a few tricks to it right now that we have some support for it, but it's not (unintelligible) is in fact that link particularly if we use - if we use RDAP because it can be cryptographically assured from end to end, we could actually provide greater strength to the certificate authority system and the certificate system that we're using even today, a strength that we don't currently have.

There's a gap right now in the system when if somebody manages to subvert your registrar account they can take over your DNS operation and issue all kinds of new things and you have a serious problem there. But if there were, you know, additional links there, cryptographic links that were outside of that system, but that were published within the system, then it would be, you know, even harder to subvert it. So it's not merely useful, it's actually a link that we're missing today and it could provide something.

So again, I'm not doing justice to this argument, I think it's one of the arguments that some of our colleagues on the list have been trying to argue, maybe having putting it across as well as - I think that this is actually one of the areas where the current heuristic models that people are doing are trying to produce that information and maybe what we need to do is provide a positive bit within the system so that it's easier to do rather than it being some sort of heuristic that people have to work out for themselves.

Chuck Gomes: So, Andrew, a follow up question again, and then I'll get to David. So are you possibly thinking of a new data element that should be in the RDS? And by the way, let me clarify, Stephanie, we're not talking about collecting - we'll get there eventually (unintelligible) probably but we're not necessarily talking about collecting things, although if it's a new data element it would have to be collected for some reason, but we're not there yet so don't worry about the processing including collection. We will have to deal with that but nobody's - at this point at least my understanding is suggesting that we would collect it for this purpose. So just responding to some of the comments in the chat.

Now, Andrew, are you talking about a possible new data element or data elements that would facilitate the domain name certification purpose?

Andrew Sullivan: It might be new element, new element or new elements, and it might be optional ones that are useful in the cases where somebody is trying to get higher value certification under a CA and otherwise is not necessary. So this

doesn't - I mean, it does of course, at that point, have privacy implications because you're revealing something but it's also something that you're revealing on purpose, you know, in the interest of gaining some other thing and presumably you're doing that willingly and thoughtfully rather than just, you know, collecting everything all the time.

I think that this has been the other area where we've struggled a little bit because you know, sometimes we talk about elements as though everybody has to provide them. And these are, I imagine, and I'm, you know, this is only sort of proto-imagining so I don't know that I'm all the way there, but I sort of imagine that these are elements that are not required of anybody but that are required be possibly collected, that is it's possible to - every registrar is required to be able to pass them through or to be able to collect them or something.

And under those circumstances, a registrant can provide them such that they can be useful for the rest of the Internet ecosystem without necessarily requiring that anybody participate in this. Of course, it could be that if you don't participate in it, then you are scored badly on, you know, reputation analyses or something like that but that's your choice and I don't want to prescribe what people must do, I just want to ensure that we build a system that actually provides the necessary infrastructure so that the shared operation can respond appropriately. And I think that's what I have in mind.

So I mean, the short answer is yes this might be a new data element or new collection of data elements but I don't think they're new mandatory elements for anyone to provide even though they might be mandatory elements for people to provide the capacity to collect.

Chuck Gomes: Thanks, Andrew. So the third question in last week's poll tried to deal with the whole optional thing. Now we didn't get - we got about 2/3 of the people that kind of went with at least one version of the wording and some of the wordings were not really very different as many of you noted in the poll.

When I responded to the poll one of the things, and I'll throw this out, it was one of my comments, I think it was to Question 3, that in the case of optional there's a couple different ways to approach it. You could require registrars to always collect it but you would never give any access unless the registrant opted for giving - for example certificate authorities access, assuming those could be credentialed or whatever term we want to use.

But it seemed to me reflecting on the data minimization principle that's at least part of the GDPR, that it would be better - and I guess I'm just throwing this out for reaction - to only collect elements - optional elements if the registrant opted in to have them collected and possible access given. But I'm curious, is that a meaningful distinction to make? That would certainly - would collect less data that way, you would only collect it if the registrant opted in. Does that make any sense?

And I've been - David's had his hand up for a while, you can think about that if anybody wants to respond, feel free. David, go ahead.

David Cake: I think I just want to clarify a bit about what Andrew is talking about in that, I mean, I'm not really - I see where the - some of the things - the process verifying domain name control using registrant email and so on is - could be described as a bit of a heuristic and there may be some issues as we come more aware of the, you know, need for validation of data. But the system that seems to be replacing that is to cut the RDS out entirely, that is to - the connect certificate validation, which obviously can then be used for other things with - to demonstrate control using a text record in the DNS.

There's a specific you know, there's a protocol now that's sort of standardized or, you know, we're working on the standardization process to do that but it's a defined protocol. Is this gap that Andrew is talking about a gap if - is it a gap that is best removed by adding things to the RDS or is it best removed by removing the RDS from that process of connecting a certificate to a domain entirely? I'm not - I don't know, I'm asking for clarification really.

Chuck Gomes: And, David, is that a clarification from Andrew that you're looking for?

David Cake: Yes, yes.

Chuck Gomes: Okay.

Andrew Sullivan: Well, okay I can - it's Andrew again. I can speak to that. The Acme protocol you're talking about does this automatically and the traditional domain name validation thing, it does just check whether you have control over the domain name. And certificate authorities who do either organizational validation or extended validation, you know, and the EV is the thing that makes the address bar green and all the rest of it, to the extent that that continues to be true, that - those are all additional efforts that are an attempt to show that the certificate holder that you're talking to really is the person or the entity that you think you're talking to.

So and this is why I was talking about heuristics, right, the goal is not - the goal of all the OV and EV approaches is not to provide kind of, you know, transcendental under the eye of eternity certainty that you're talking to the right entity but to provide a very high level of probability that either you're talking to that organization or you're really, really we're sure talking to that organization, that's basically the difference between OV and EV.

And I think that the reason that many of these distinctions came into effect because back in the day of course, DV was all you got. The reason that these kinds of validations came into effect was precisely because you couldn't rely on the evidence from domain name validation to give you evidence that you were talking to the real entity.

Now when you're talking to your bank that counts for a great deal. And the problem is that humans, normal users, can't really tell the difference between DV and OV and EV and all the rest of it and yet we want something along

those lines. And of course for the domain name industry of whom I guess many people here are, you know, are participants in that industry, it's very important that that trust model continue to grow and be useful.

So either (unintelligible) for additional…

Chuck Gomes: You broke up. You broke up a little bit so the last sentence or so that you said, Andrew, didn't come through.

Andrew Sullivan: I'm sorry. Is this better?

Chuck Gomes: Yes.

Andrew Sullivan: Either we're going to provide the necessary mechanisms in the RDS to build those kinds of assurances, or else the industry is going to move on. But if they're going to move on they're going to build those assurances without respect for domain names. They're just not going to use domain names as the basis for this because it becomes obvious that domain names are a lousy way to do it.

And I guess the problem is that domain names are the foundation for both the resolution part and for the X509 certificate part right now and so we have the opportunity to build the relevant - the relevant infrastructure underneath all of this to increase that kind of trust. But if we don't do it I think the industry will move on.

Chuck Gomes: Thanks Andrew. Now I want to bring you back to the table on Slide 5 there. If we, as a working group, decide that there should be some access, controlled access to some elements of the RDS for this purpose, which ones would it be? And let's focus on the ones with access right now. Which elements, and I'll let you raise your hand or respond to this, but which if any of the elements that have Xs next to them, and we don't have to restrict ourselves to those, but let's start there. But do you think would be legitimate for giving access,

assuming you could control that access, to domain name certificate authorities, which ones of those data elements do you think we would include in that list?

And the leadership team members, if you can word that better than I did, please feel free to do so. Steve, go ahead.

Steve Crocker: Yes, so Chuck, what - which of these elements are we prepared to offer to the certificate authority some level of assurance about? And if we're not prepared to offer assurance about them, then what value is it to either the account holder or the certificate authority? Let them have their own interaction on this.

Chuck Gomes: Okay, thanks, Steve. So this is Chuck again. And so in other words, if we recommend some access it would only be meaningful if we offer some assurances as to what they're getting, I think that's clear. And if - assuming we offered assurances, would you pick some of those data elements?

Steve Crocker: I don't know, you know, you'd have to start from scratch and, I mean, from my point of view, the current use of the terms "admin" and "technical point of contact" and "billing point of contact" and even "registrant" start out as having no particular meaning whatsoever except that those are names of fields that the account holder has filled in. So I think it would be best to start with a clean slate, what information does the registrant or sorry does the account holder want to supply? What is the - what representations is the account holder making about the meaning of those and what level of assurance is being provided?

As it is now these are simply fields that are being filled in, no assurance is being given except the very weak one that somebody's done a syntax check to see if it really is an address or really is a phone number, etcetera, and the whole thing is extraordinarily squishy.

Viewed from that perspective, something I've said several times and probably say several times again, it's amazing that the system works as well as it does rather than decrying the inaccuracy I would applaud the fact that as much of it is accurate as it is, certainly the bad guys have no interest in improving the accuracy, and there's nothing we're doing that makes it particularly hard for them to keep a low profile and supply the minimum amount of likely looking information that has no validity whatsoever.

Chuck Gomes: Thanks, Steve. And by the way, and this is before you were on the working group and others as well, but one of the agreements we came to a long time ago was all of these terms however we use them, have to be very explicitly defined so I think there's agreement in the working group that if we're going to use "registrant," if we're going to use the term "admin contact" or "technical contact" that we have to - and any terms we use we're going to have to make sure in the end that there's no ambiguity in terms of what we're talking about, so we'd have to do that.

Steve Crocker: Well that's very helpful, but let me ask why you say "in the end"? Why not in the beginning because if I don't know what they mean then I don't know how to have this discussion about whether the information should be collected and who should have access to it.

Chuck Gomes: Yes, it's a chicken and egg problem that we continually deal with. Stopping at the time, I think that - and leadership team please jump in and help me if you think I'm not saying this right, but spending time on the definitions at the time I guess we decided that it was - it's a quite a ways back but - and I think we decided that defining them may be hard until we get further down the line. Now that may be wrong, okay, that was a decision that was made there.

Steve Crocker: Well, the benefit of being new to this discussion but having been around for a long time, without any embarrassment, let me say I think it was wrong now to try to define these things. And I think in the process of trying to define them you're going to find that there's some fundamental questions that you have to

face. And if you are able to define what they mean and including what operational roles they have and what responsibilities and authority they have, then I think the rest of this discussion about what uses and what level of access and so forth will become much, much simpler, much more straightforward.

Chuck Gomes: Okay, so you definitely believe we should define each of the things in the first column in this table now or soon?

Steve Crocker: Well, yes, and decide whether they belong in the first column. And I think further, let me raise the ante, I think once you go down that path the GDPR problem goes away.

Chuck Gomes: Okay. Now, I don't think, except maybe for Andrew's comments, that I've heard, you know, we had nearly 70 - nearly 3/4 of the people who responded to the poll, and that was only 25 people, I know, that's more than we have on this call, supported some sort of access for this purpose to RDS data elements that need to be defined. I haven't really heard from people that are in that - in that 75% category, or 72%, whatever it was. Are there none of those people on this call that support access?

Steve Crocker: Let me raise the ante even further. I don't want to be particularly unpleasant but I'm reminded of some state legislature that decided that the value of pi should be 3.00 because that would be more convenient. That doesn't change the facts of the matter, it's just an expression of interest by some set of people. I think we're in territory here where first you got to have a logically meaningful discussion and not just a poll of people saying yes, I think it should be this or no, I think it should be that.

Chuck Gomes: Okay. That's fair. Well Andrew, your hand went down. Go ahead.

Andrew Sullivan: So I - it's Andrew again. I'm having - apparently connectivity (unintelligible) who has just completely failed today. But so I'm sorry if I drop in and out

again. The - I don't think that these polls have been polls in the sense of popularity contests; I think they have been, you know, attempts to take a sounding of people's arguments. And I suspect that the reason we're having trouble with this case is along the lines of what I've already tried to argue, that is people feel that there is something in the domain name space where we would like certificates to work and yet nobody believes that, you know, finding out your home address in order to solve that problem is the right answer.

And so maybe the difficulty is that we have been going at this with the structures that we already have in the existing Whois rather than trying to tackle this from the point of view of figuring out what kinds of things we need. And so, Chuck, when you asked me earlier, "Well, are you suggesting new data elements or something?" I think it may be something along those lines.

And maybe the problem is - the difficulty that I've been having in expressing is that I'm not quite sure what it is that I'm thinking about but it does feel to me like we have been working through this, you know, with the basis - on the basis of the stuff we already have and is it in or is it out. I mean, the problem is, you know, if we try from the other direction how do we solve this use case? What fields or one kinds of fields would be useful rather than what fields in the Whois today would be useful, what kinds of stuff would be useful, maybe that would be a way to make some progress on this area.

Chuck Gomes: Okay. Daniel, go ahead.

Daniel Nanghaka: Daniel for the record. I hope I can be heard clearly.

Chuck Gomes: Yes.

Daniel Nanghaka: I would like to say that the polls have been great for discussions and helping to drive consensus during this deliberation process. When it comes to most of the cases that Steve is speaking about, we discussed all these things - the different use cases of the different data elements, we went ahead and also

discussed the verification of the data elements, the addresses, the email address (unintelligible). So in these cases, how are we going to be able to drive consensus, because already the issues that are coming from the Whois are affecting the different uses and different levels and also (unintelligible) the GDPR that is coming into protect the data elements of the European citizens, we have to make sure that we come into compliance with all these (unintelligible) laws.

So if we look at the technical contacts, the administrative contact, just - and the other fields that are coming of the data elements, then the user doesn't even mind about filling in these fields because they're only using one point of contact, yes? And others even don't know what is happening in the background. So I think we have to come up with a way of these data elements can be able to - how can I put it so simply like (unintelligible) - I will get back to you, thank you. Back to you.

Chuck Gomes: Okay. Thanks, Daniel. And that's what I was trying to get us to heard towards, some data elements. I'm going to do something a little bit different, let's go to Slide 6, I don't know if this helps or not, but we thought it might, whether it helps in where we're at right now I'm not convinced myself. But on Slide 6 is a set of tentative working group agreements that we've reached so far, some of them quite a while ago, that kind of impact that table you were looking at especially not only for the three purposes we're looking at now but future ones as well.

Notice that - and I'll go through these quickly because you can read them, but 47 we decided previously that the following information will be collected for the purpose of technical issue resolution, associated with domain name resolution. And that's where those - that's basically what was checked off in that first column under Technical Issue Resolution. And then we did the same thing for domain name management in Agreement 49 and that is what is in the column for domain name management.

Thirty one then was data enabling at least one way to contact the registrant must be collected and included in the RDS, okay that's kind of a broad agreement but we did reach agreement on that. Thirty was at least one element identifying the domain name registrant - we're calling the registered name holder - must be collected and included in the RDS.

Now back to Steve's suggestion on definitions, correct me if I'm wrong but isn't domain name registrant pretty well defined in contracts and so forth in the ICANN world? It seems to me it is but maybe I'm Wong. Does anybody disagree with that? I agree that technical contact and admin contact, even billing contact, based on some of the discussion we had on the list this past week, may not be as well defined, but isn't domain name registrant pretty well defined in agreements and other documents in our world? Steve, go ahead. We're not hearing you, Steve, so looks like you're off mute. But…

Steve Crocker: Yes, I was - well, I'm calling in via Skype separate control for the mute. When the registrar has an issue with the person controlling the domain name, does he use the registrant information or does he use the information in his records as to who the account holder is?

Chuck Gomes: Well account holder is a new term we're using, okay, so and I don't have anything against that term, but the registrant like for example with regard to domain name transfer, just to use one example, I think is pretty well defined. Now here are registrars and registrants on this call, if you disagree with that, and Stephanie used the term "registered name holder" I think that's synonymous with registrant but what do others think? Go ahead, Steve.

Steve Crocker: Well in the case of transfers, and I'm not 100% up to speed but I think there is a defined role and email sent to an address that's listed there needs to be responded to and if it's not responded to it's taken as implicit consent, or something like that. Now as I say I apologize for not being 100% up to speed.

But my - but before we get into the details of those particular functions, the point that I'm making is that - and the term "account holder" is the person who actually has the keys to interacting with the registrar. So I use Go Daddy, for example, for some of my domains, and I have some credentials for interacting with Go Daddy, I have an account and a password and so forth. And Go Daddy, presumably, knows how to reach me and if the information I've given Go Daddy about how to reach me isn't good, when they try to reach me and they fail, bad things are going to happen to me probably.

The information that I publish and label as "registrant" is really my choice. And I don't know that there's anything that forces - I don't know anybody who checks to see whether the information that I supply as the registrant information is in any way related to the information that Go Daddy has about me as the account holder.

Chuck Gomes: Okay so you're using - okay so I see the difference between account holder and your relationship with the registrar and what we call in Whois and things in the past as the registrant, and those two may be different. So, I mean, I don't think we can go down the path of getting the account holder information that the registrar has for you as their individual customer in the RDS, but so are you thinking that maybe registrant isn't defined enough?

Steve Crocker: Yes, I'm thinking registrant is not defined enough, and…

Chuck Gomes: Okay.

Steve Crocker: …I'm not sure why you say we can't get the account holder information into the RDS. Looking at it from a slightly more holistic point of view, the account holder hands over quite a bit of information to the registrar and some of that goes to the registry. Some of that is the technical information for the domain operation, the name servers and so forth and some of it is sensitive information about billing, credit card numbers, and so forth. And some of it is this very squishy otherwise unnecessary information, unnecessary in the

sense that neither the registry nor the registrar needs it or uses it, it's just put there for historical reason and has some accumulated imputed meaning and, you know, and practices associated with it, but it's not intimately related to the relationship with the registrar or the registry.

If you start from a clean slate one would say well, why bother doing any of that? If you really want to contact the person who has the control of the domain name, why not have exactly the same information that the registrar has?

Chuck Gomes: Okay. No I get it. Thanks. I appreciate you taking the time to explain that. Now we're just about out of time, really quickly I'd like you to look at the rest of the agreements, 32-36 there, and not in any particular order as you can tell, not numerical order anyway, keep those in mind. Now, I don't think we have any basis for a poll this week, if somebody thinks of one that would be great. We're going to have to figure out some way forward. Now hopefully next week we'll have the CAB chair on the call as well.

What I'm going to suggest is that the leadership team regroup on this one and see if we can figure out - and also figure out a suggestion for better defining the terms, I won't say better, defining the different types of contacts. So and we - that's going to be hard to do on phone calls like this. So I'll ask the leadership team to meet on that.

Now for the sake of the leadership team, and staff, if you can help me on this, let's do a Doodle poll to see if we can't find a slot, not too late on Friday, for David's sake since he's in Australia, to do a meeting before our regular Monday meeting because I think this is going to take more time than our usual meeting time. So action item out of this is for us to absorb - the leaders to absorb what's gone on and see if we can put our heads together and come back with some recommendations in terms of how to proceed on this and how to proceed on definitions and hopefully that'll help us on other purposes we have to deal with as well.

So excellent participation and discussion. I know we haven't made any progress in terms of further agreements but we got to get it right and we'll keep trying. So any - is there anything else we need to cover on this call before I adjourn this meeting? The action items are mainly for the leadership team to try and come back. And by the way, as always if any of you have suggestions in how we might be able to zero in on some progress here with regard to this purpose, absolutely welcome. And several of you made suggestions like the definitions and some of the things that Andrew said, and we'll take those into consideration.

Okay, Steve, is that an old hand or did you want to add something?

Steve Crocker: No, I'm sorry, that's an old hand.

Chuck Gomes: That's all right, we all do it. So okay, thanks, everybody. And a pretty good participation for our off cycle call. And the leadership team has a big action item and we'll try and come up with some ways that will help us move forward. That said, the recording can stop and the meeting is adjourned.

Steve Crocker: Thank you, everybody.

Julie Bisland: Thanks, everyone. Today's meeting has been adjourned. Operator, (Kim), would you please stop the recordings? And everyone, have a good rest of your day or night. Thank you.

END