ICANN Transcription
Next-Gen RDS PDP Meeting
Wednesday 18 January 2017 at 0600 UTC

Note: The following is the output of transcribing from an audio recording of the Next-Gen RDS PDP Meeting on the Wednesday, 18 January 2017 at 06:00 UTC. 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. Attendance may be found at:
https://community.icann.org/x/EbTDAw
The audio is also available at:
https://audio.icann.org/gnso/gnso-nextgen-rds-pdp-18jan17-en.mp3

Nathalie Peregrine: Good morning, good afternoon and good evening to everyone and welcome to the Next Generation RDS PDP meeting on Wednesday, January 18 at 0600 UTC. In the interest of time today there will be no roll call and we'll be taking attendance via the Adobe Connect room only so if you're connected via your telephone could you please let us know right now? Hearing none...

Daniel Nanghaka: Daniel for the report. I'm connected through telephone.

Nathalie Peregrine: Thank you very much, Daniel. This is noted. Anyone else? Okay hearing none I'd like to remind all participants to please state your name before speaking for transcription purposes. Please keep your phones and microphones on mute when not speaking to avoid any background noise. And with this I'll turn the call over to Chuck. Thank you very much, Chuck.

Chuck Gomes: Thanks, Nathalie. And hello, everyone. Welcome to our next meeting for the RDS PDP Working Group. Let me ask if there's anyone who has a statement of interest update. Not seeing any hands or hearing from Daniel, I'll go ahead and move on.

The agenda is in the upper right. One of the things - just a logistical thing I'd like to do right now for those of you who are in Adobe Connect, I don't - some of you I remember what geographic region you're in, some of you I don't.

I know David's from the part of the world where this is a fairly decent time. Are there any others on the call besides David Cake that are in Australia or Asia or the Pacific somewhere? Raise your hand if you are. I'm just curious what kind of response we're getting.

We can obviously go through and check that by looking at the membership list but anybody else besides David Cake who's at a decent hour? Are most of us from not so decent hours? Okay, not seeing any hands it looks like I compliment all of you, except you, David, on taking part at a undesirable time. I'm glad you're on the call though, David.

All right well, enough jesting. Let's go ahead and get going with our call tonight, tonight for me, excuse me, today, morning for a lot of you, middle of the night for many of you.

So if we can bring up the results of the poll that we took last week. It ended on Saturday night. Thanks for the smile, David, appreciated. You can see the first question is up there. And you should have scrolling rights. It's okay to give them scrolling right now, thank you. And you may want to just look at this, scroll down a little bit, you'll see the numbers there. So we had a total of 29 people responded to Question 1 and it was 28 to 1.

So the conclusion that the leadership team came to that we would record in the key concepts working draft is that the technical issue resolution is a legitimate purpose for thin data collection. Now, and keep in mind we're only talking about collection right now. And we will get to access and display, etcetera, later on. So we had 96% plus of the people. Just one person didn't agree with that statement.

Now there were four comments on this, and we're not going to go through those comments unless somebody desperately wants to do that mainly because the comments that were made pertain to other data elements. And we will address those in subsequent deliberation. So certainly if you still want to talk about any of the comments you can see them if you scroll down. And we'd be happy to do that, otherwise we will just move on to Question 2. Okay?

And let me say, like I end up saying every week is, is that all of these things we will have opportunity to come back to and look in even more detail and refine or change our positions. The reason we're putting them in the key concepts working draft is to keep a record of our progress. It doesn't mean we can't change it later, but we need to have a record so that we can review that periodically and revisit it as needed.

Question Number 2 then if you'll scroll down a little bit you can get to that. And I'll do the same here. I'll let you read it, I won't read it for you. Hopefully all of you read it when you took the survey. The - again, we had very strong results for Question 2 which was the second purpose that we went through last week. And we had 28 responses and it was 27 to 1 with a yes answer.

So on that tone, barring any discussion indicating differently right now, we will record the conclusion that technical issue resolution is a legitimate purpose for thin data collection. Any discussion on that please raise your hand, or Daniel, speak up if you want to say something. Okay.

Now Question 3, for those of you were on the call last week, you will remember that we didn't get too far on Question 3. There was definitely some different opinions. And we agreed to continue that. You know, forgive me, I'm going to back up to Question 2 a second because there were a couple comments we wanted to discuss and I skipped right over that.

So if you go back up to Question 2 you'll see there are five comments. And I want to call attention especially to Comment 1 and Comment 2. Comment 1 you can see what it says there, this comment is actually to Question 3. But so we're going to get to that when we get to discussing Question 3. So we'll just kind of call that to your attention right now.

Comment 2 on the scope of technical issue resolution there you can take a look at that one. And the - on that particular one we'll address that further when we reach the point of deliberating on specific definitions of each purpose. We can talk about it right now if somebody wants to, that's okay, but you may need to deliberate further on the purposes for collection of thin data when we fully define each purpose. So and we will have to do that. We decided that probably it's not good timing to do it now, although we're not totally opposed to that if somebody else wants to do it. And certainly the person who submitted that comment is welcome to chime in as well.

Now Susan had some input that she was going to try to send via email. But recognizing that she's on a cruise in the Bahamas I don't think that happened. Did it, Lisa or Marika? Did you see anything from Susan? I don't think I did.

Lisa Phifer: No, Chuck.

Chuck Gomes: Okay. All right well hopefully she can get that in a later. If somebody else wants to comment just raise your hand on that. So now not seeing any hands, let's go back to Question 3, sorry for missing those comments. Question 3, now keep in mind that on - Question 3 had to do with the third purpose that we looked at.

And none of the - and so what we did, now keep in mind we didn't reach any conclusions on Question 3. But as a means of just kind of getting a preview of where people are preliminarily for Question 3, which has to do with the domain name certification purpose, we thought we would - we did a little poll of where people were giving a range from no support for a purpose to 5 is neutral, you're not sure, you haven't made a decision, all the way up to full support.

And the preliminary results, and we're not going to use these results for any conclusions because we said it was just your first thoughts on it, so don't worry about that. But we do want to - we do want to note that there really wasn't any strong opposition. In fact, there was fairly good support for that as a purpose. Not strong like Questions 1 and 2, but there's fairly good support.

As far as the data there, and you can see what you see in blue - in the blue bars is the average score that people assigned to that and in red the standard deviation. And for those statistical experts for the statisticians among us, you know, probably we don't have a good enough distribution, a normal enough distribution and sample for standard deviations to be too reliable, but it's a measure, again, that we can look at and none of them are too far apart from one another as you can see on that.

All of the purposes range between 6.68 and 7.58 in terms of an average score. And the - nearly half expressed full support or 10 - nearly half of the people - 10 people out of 27 or excuse me, how many were there - I think I got the wrong number on that. Flip over a page here just to see that so that I get that number correctly. There were total - well, let's see, I don't know how many people responded to these. Each of these had - didn't all have the same number of responses.

But 10 people, which is over - nearly half of those who responded to Question 3 - put 10 as full support, okay, which was kind of an interesting thing. So there are quite a few people that look at this as a legitimate purpose for collecting the information about thin data. So that's just a point of reference for starting our discussion.

Now a minority of the members express no initial support for all of these purposes, okay. So what we're going to do now is restart our discussion on collection of the thin data for the purpose of validating domain names for digital IDs or certificates.

And what I'd like to do is to start with is to call on Geoff Noakes from Symantec and Geoff is one that's been involved in this particular usage of domain name data for quite a few years. And I also welcome anybody else who'd like to talk about this area from a point of view, first, not pros or cons right now but for the sake of those on the call and those who will listen to the call later, who may not understand this particular purpose how it's used, whether you agree with it as a purpose or not, but we'd like you to first of all understand what this purpose is, how thin data is used for this particular purpose.

And, Geoff, I'd like to call on you since you agreed to help us in this, to talk about it a little bit from a point of view of helping the working group members understand how thin data is used in this regard and why it's helpful. And then I'll open it up for questions just about understanding it. After that we will get into the pros and cons and try and see if we can reach any rough consensus position in terms of this particular purpose.

So I've talked too much already. Let's turn it over to Geoff.

Geoff Noakes: Thank you, Chuck. For the record this is Geoff Noakes with Symantec. So Symantec was the first certificate authority and there are many more since the - since we were created in I think it was like 1995 or 1996, about that time. And one of the things that certificate authorities do when we receive a request for a digital certificate is that we authenticate who the organization is and in some cases the individual is, that is applying for the certificate.

There are a number of standards that are set by the CA Browser Forum, which is the, oh probably controlling authority for these things. And all of the CAs use pretty much the same practices or processes. They may differ a little bit, but at the end of the day when we receive a request to create a certificate for Google.com, for example, we want to make sure that it's - that the person and the organization that we're dealing with is with Google and is authorized to enter into getting an SSL certificate. If they're not then they could be a phisher, they could be a state-sponsored terrorist, they could just be a thief.

So what we're trying to do is bind - I'll loosely call it bind - the identity of the person who is requesting the certificate or the organization that is requesting the certificate with the domain name. And I attended the session - the conference call on January 10 but I had to drop off about a half hour early for another commitment that I had. And when I listened and reread the transcript of that meeting I got the impression that there was a move afoot to not make available the same data fields in Whois as almost every certificate authority has expected in the past.

And so, I mean, almost every certificate authority, when we receive a request for the certificate we're going to want to authenticate, you know, do I know the company? Do I know where they're located, what their phone number is? Who the person is? What their domain name is, the email associated with their request, all these types of things. And the first place that every CA that I now of starts with is the data that's in Whois and presumably that would be in RDP.

So let me pause for a moment. Chuck, is that a - enough of a high level...

Chuck Gomes: That's good, Geoff, thanks. This is Chuck. And feel free to jump back in. Before I open it up to questions let me see if there's anybody else - several of the rest of you have some experience with this, maybe even from a little bit different perspective than Geoff, who deals with it directly in his business.

Anybody else like to add any thoughts, just in terms of understanding how this is used? Michele.

Michele Neylon: Thanks. Michele for the record. As a registrar and hosting provider, you know, we're familiar with how CAs try to do this. The problem we run into is that outside of gTLDs, how a lot of the CAs try to do this with ccTLDs is incredibly frustrating because they don't understand in many cases how the Whois works from the ccTLDs. So we constantly get validation emails sent to the wrong email addresses for ccTLDs which is rather frustrating because many ccTLDs do not publish the registrant email address in the public Whois.

An example being, say, dotBE or dotEU where during a Port 43 Whois lookup would return the registrar's contact details as being the only email address that's publicly available. In terms of whether this is a valid use or not, yes, it's a valid use whether or not it, you know, it's a whole other conversation about whether there's other ways that they can get the data or not, I think we've had briefly in the past. Thanks.

Chuck Gomes: Thanks, Michele. Now let's not - I'm going to caution us, let's not get into whether it's valid or not yet, okay, we're going to get there. But for right now make sure people understand what it's being used for. Please ask any questions that you have, no question is dumb, okay. If there's something - if there's a question that you need answered to understand what this purpose is.

Now notice that there's been some discussion about more than thin data. And we're focusing on thin data right now. Don't let that disturb you, we'll get beyond thin data later. And for right now the fact that the certificate authorities, CAs, you know, look at more than thin data, doesn't mean that we're getting off track here, it's just a fact of life in terms of that particular purpose. And we'll look at purposes for data other than thin data later. Stuart, it's your turn.

Stuart Clark: Stuart Clark for the record. In terms of the data that are used and how it's being used, I'm aware to a certain degree having (unintelligible) certificates myself, but you mentioned quite a lot of different pieces. So how much of that is actually used for different type certificates and how useful is it? So for example, I know trying to look for email addresses for validation emails but equally some CAs just send it to sort of postmaster@domain name and things of that nature. And for things like addresses, how often is - and those details.

How often are they used and how reliable are they if, say, the organizational name is slightly different to what the request said.

Chuck Gomes: Any - Geoff, do you want to respond to that?

Geoff Noakes: Happily. So the last question - there were two questions there. One was sort of which data elements do we look at and does it vary by type of certificate I think was it. So the lowest level of certificate is what's called domain validation. And I will say that in about one month there's going to be some very public information recommending that people start to move away from using domain validated certificates especially if they're doing ecommerce.

But a domain validated certificate we will get a request for Chuckgomes.com and the only thing we will know about it is that we get an email from somebody, call it ssladministrator@chuckgomes.com, we'll send an email to that address. And if somebody can respond to it they've demonstrated that they have control over that domain. And those certificates are done in near real time. And that's true for all certificate authorities.

And so for all purposes, no real authentication has been done, right? You don't really know who is behind the domain, you don't know the person, you don't know the company. You've got nowhere to start. This is the area of the Internet where almost all phishers and terrorists and bad guys kind of lurk. They buy these domain validated certificates so that they can do business.

The layers - the types of certificates that really do authentication are what's call organizational validation or extended validation. The organization validation is we will look at the name of the company that's in the certificate request and we will try to authenticate that this person is really with that company and they exist at the address and country and other information that they provide.

And our people, we have a lot of automated processes that do this but we also have people and they act like detectives. So for example, in the United States there's a very well-known chain of grocery stores called 7-11. And the number of permutations that the organization name, 7-11, is actually typed into a - the box it's at least dozens and if somebody said it was hundreds I'd believe them because some people will use the numeral seven, hyphen, the numeral 11, as one example; some people will spell it out with seven hyphen eleven, sometimes they won't use the hyphen. Sometimes they'll add in words like incorporated or inc or corporation or anything.

And it's not necessarily a bad thing, oftentimes the person enrolling for the certificate doesn't know the company's legal name. So it's our job to kind of hunt that down and tell them hey, you typed this in, the rest of the information looks good, but you need to come back with this organization name.

The other type of validation is called extra validation. That's the highest level that is available. And in addition to doing all the things that we do for organization validation, we also get the information about the person who's actually submitting the request, you know, name, title, phone, email, that type of thing. And we essentially contact the HR department at the company and we say, is this person an employee of Chuckgomes.com? And is he authorized to submit an order for this type of SSL certificate?

And because that's an out of band thing and we've got to actually talk to people, it slows things down a bit, but it sure traps a lot of the people that want to masquerade as bad guys. Or, I should say and, it also traps the people that, I don't know, might not have the company's best interest at mind. So they want to register a domain and an SSL certificate for some company but the rest of the company doesn't know about it type of thing.

So there are - I hope I've answered that - the questions from that last person. Does that help?

Chuck Gomes: Stuart, let me let - turn it back - this is Chuck - let me turn it back to you.

Stuart Clark: Yes, it does. Just on a - from a purely thin data perspective, obviously most of what you've been mentioning for the extended and organizational is address contact detail data. From a purely thin data perspective, is there any usage of that or is it really just the contact and organizational data?

Geoff Noakes: So the truth is, is we use all of the data that we can get whether it's thin data or thick data. We also - and the minute we have any of that we have all sorts of automated processes that try to look up information about the people and the organizations that we're now dealing with, with external data sources. So we will use data sources from Experian, for example; we'll use it from the Secretary of State's, in the US, each Secretary of State maintains a database of all the companies that are registered to do business in a given state.

We will look - and we've probably got 200 databases that we tap on this. And what we're trying to develop is a sense of do we know who we're about to issue a certificate to? And how do we know that?

Chuck Gomes: Does that answer your question, Stuart?

Stuart Clark: Yes, thanks.

Chuck Gomes: Thank you, Stuart. Rod, go ahead.

Rod Rasmussen: Yes, Rod Rasmussen for the record. Just wanted to expound upon the domain validation cert and I'm curious to know what the (cab) forms coming out - as soon as (cab) forms come out with some information around domain validation as a benchmark so that will be interesting. But one of the things - well several things around domain validation certs is really to provide a bit of control over domain name. And that provides you a certificate, you can do commerce with that, which is kind of the way people typically think about things, they want the padlock and the icon and all that good stuff.

But it really - the number 1 thing it does is provide encrypted http or https for secure http communication. So this is used for providing secure ways for people to interact with each other across the Internet with that particular domain name. And that's used not just for commerce but for communications of all types. And with the projects that are going on there's a three SSL project going on out there and they rely on domain validation as well.

You end up with a lot of people who are trying to, you know, provide a quick and easy and, you know, as close to free as possible service for encryption and you could think of that as they're good and bad, right, uses out there. But it's certainly a way that people are taking advantage of the system for being able to, you know, provide encrypted services tied to their domain names at a very low and reasonable cost. And those often get tied to lots of the interest people have for privacy and protection of their data and information.

So it's a - it's used by a lot of different folks out there and it's also, you know, it's kind of the low bar for doing things and, you know, as Geoff was saying is there's lots of different ways for validation to occur, the thin data is typically not sufficient, you have to get into thicker data as it were, for an email or something like that to prove control. But there are indicators, mainly name servers, if you're using databases to try and associate folks where thin data is actually useful in that case.

But most of these systems are set up to at least use an email address, which would be from a more robust data set than the current thin data. Thanks.

Chuck Gomes: Thank you, Rod. Michele, go ahead.

Michele Neylon: Thanks. Michele for the record. And I just, you know, following up a bit on what Rod and a couple others have said. And also if you look in the chat Alex and others have said the same thing. I mean, the thing with SSL certs these days, I mean, it's - the encryption aspect has become more and more important. I posted a link there to an article from Motherboard and Google is now - sorry - Google has been using SSL as one of their ranking factors for SEO for quite some time.

And they're rolling out some changes now in the Chrome browser, which will basically flag websites that aren't using some form of SSL as being slightly less trustworthy or, I'm not sure exactly how that's going to appear. So we're seeing a lot of people looking for SSL certs, which has got absolutely nothing to do with, you know, ecommerce or anything like that, it's more just to do with keeping Google and some of the browsers happy.

In other words saying that, you know, the communication between the user and the Website or online service is encrypted in some way. So from our perspective as a hosting provider we're seeing a lot of our clients moving to completely free SSL services such as (unintelligible).

Chuck Gomes: Thank you, Michele. Now I have a question - well before I ask my question let me again ask does anyone else have a question in terms of understanding what this particular purpose is? Again, whether you agree with it or not or whether you've even made a decision on that, is there anyone who still doesn't have a clear understanding of what we're talking about here? Okay.

So then - and I'll come back to Geoff but others are welcome to respond to this question as well. And this is Chuck speaking again. Geoff, what - how would it impact Symantec, or for that matter any CA, if you didn't have access to RDS data, even thin data.

Geoff Noakes: So I spoke with our authentication team that does this, and they all shook their head and they said, is this like a bad joke or something? And I think the truth is it would require a lot of thought about how - what a Plan B would be. So for example, if you don't have access to the data that we normally think of as available in Whois, where would you go to begin to tie or to bind, if you will, the identity of the requesting person or company with the actual company?

So if somebody said they're with Bankofamerica.com or, you know, Bank of America, there are all sorts of ways that we could get information about Bank of America, but without kind of knowing anything more than that, you quickly run up against a wall because you don't know who the person is who is requesting this thing. And so no authentication can be done that way or you start with Bank of America and, you know, the people - my authentication team say well, and then who do we talk to, right? We call their headquarters number and then what do we do?

So the data in Whois has shown itself to be a very useful starting place for us to do our detective work to make sure that we know the person and company that we're about to issue and SSL certificate for. You know, it is just the beginning of the place. We're going to end up vetting all that information against multiple databases and perhaps with out of band phone calls to humans.

Chuck Gomes: Thank you. Does anybody have any questions of Geoff regarding this particular purpose? So that brings - this is Chuck speaking still. So that brings us back to the question in the poll is authentication a legitimate purpose for thin data? Now we understand from our discussion in this meeting that they use a lot more than thin data, but for now we're going to - and this discussion will help us when we get to thick data as well. So we won't have to duplicate it all.

But a lot of people were undecided when they did the poll, and understandably. Is there - are there any folks on the call that think that this is not a legitimate purpose? Now keep in mind, we're not talking about whether we're - whether any of the thin data elements would be public or gated or whatever, we'll get there. Okay, and hopefully all this ground work we're laying will make that even easier later on.

But is there anyone on the call that questions the legitimacy of this as a purpose for thin data? Michele.

Michele Neylon: Thanks, Chuck. This is Michele. No, I'm not going to question anything, though I'd love to disagree with you because I haven't disagreed with you recently.

Chuck Gomes: True.

Michele Neylon: Jokes aside, I think there's a bit of confusion here because with a lot of what was being discussed about the domain validation moves beyond thin and into the thick data. So, you know, using email addresses, telephone numbers and all that, that's thick data, not thin. So if we're talking about thin data and thin data only, that's a slightly different paradigm. I'm not quite sure how much domain validation you could do with just the thin data by itself. Because all you're really going to get is (unintelligible) list which name servers does it use and very little else. Thanks.

Chuck Gomes: Yes, thanks, Michele. And I think everybody probably understands that, that - and especially when we're talking about something like this particular purpose that - and I'm sure Geoff and his colleagues would be very upset if all they could get was thin data. So we get that. Thank you. Rod, you're up.

Rod Rasmussen: Yes, I was just going to add to what Michele just said. This is Rod Rasmussen. The name servers are slightly useful in this case because you can compare that against known entities that you may have other certificates for. And as more of a scoring factor, at least that's my understanding how the process works. So it is useful.

But if we consider thin data a subset of thick data which, you know, we could debate that, but I think you could - one could argue that thin data is a subset of thick data - it really requires thick data to do the kind of validation we're talking about whether it's in simple domain control type of validation or all the way - even all the way up to the most rigorous forms of validation, the process involves looking at thick data which would include the name server data. And thin data on its own is not enough to supply the necessary kind of information for the current domain validation processes that CAs use. Thanks.

Chuck Gomes: Thank you, Rod. And notice that Lisa - Lisa must have been reading my mind because this is the exact document that I was going to ask be put up next. You can see now we've already made decisions on domain name control and technical issue resolution. We've been talking today continuing from last week the proposed purpose of domain certification, okay. And we'll come back to each of these for thick data as well in subsequent weeks. So we're on domain certification now.

And you can see the actual proposed purpose. And so no one has raised their hand or said anything in opposition to this as a purpose for thin data. So I'm going to assume, unless somebody speaks up here quickly or puts something in the chat, that those on the call today are in agreement, certainly no opposition, that domain name certification is an acceptable purpose for thin data. And we'll test that in a poll so that those not on the call can weigh in. And I hope those, especially those who do not understand this particular purpose will listen to the recording to get the discussion that has taken place.

Any more comments? Stephanie, I know - we're not talking about disclosure yet. Okay, we're going to get there. So but for right now just collection and we're going to have to get to disclosure as well, and then we're going to - and then disclosure means a couple - several different things, at least a couple that I can think of off the top of my head, one of them is public disclosure and one of them is gated disclosure. And we're going to get to those two as part of our charter.

Okay so that being said, let's go on to the next proposed purpose which you can see on the screen. If you haven't scrolled down at all it's still showing, it's the business domain name purchase or sale. And you can see what that includes. So if you wanted to buy a domain name you might want information about it, you could go to thin data certainly to see if the domain name is available. Of course a lot of registrars provide that service directly, probably all of them do. And so forth.

And some of the thin data elements that could be useful for that particular purpose are listed there. And then you see the links for the use cases on the right like we've done with the other proposed purposes. That being said, does anybody have any questions about understanding this particular proposed purpose? Okay.

My big monitor went blank on me so I'm having to read small print so if I'm a little slower you'll understand why. Okay, so no questions on that. Well, is there anyone who thinks that this is not a legitimate purpose for collecting thin data? Okay. Not seeing anyone. Hear we got a comment. Good. Stephanie, please go ahead.

Stephanie Perrin: Stephanie Perrin for the record. And I know you're going to tell me we're going to get to disclosure, but I really think we've got a problem here. If we're not collecting any new data elements specifically for domain certification or, you know, cert validation, then, we're collecting for this purpose alone, it is a valid use of disclosure. So I think, you know, this is a valid purpose for using data that is already collected. And I think it gets down to what Geoff's guys who are doing the certification are concerned about is a failure to disclose. If they lose that ready, easy disclosure in Whois, there will be a problem.

We don't want them to stop authenticating domain certs or however you phrase that, you know what I'm trying to say, it's too late here. But we need to set the parameters for the use and disclosure. So I kind of think we're having a - this is a bit of tautology. We're gathering the data anyway, we're discussing another use of it. Thanks.

Chuck Gomes: Thanks, Stephanie. I think you expressed that well. This is Chuck again. And keep in mind it is a little bit confusing for people, I understand, in terms of just focusing on collection because if you collect it and don't use it in any way at all then why are you collecting it? So understand that we could - once we really get down and dig into display and gated access and so forth, we may come back and say we don't need to collect that. That's an option.

But all we're saying right now is these appear to be legitimate purposes for collecting the data. We may decide later on that well, yes, it seemed like a legitimate purpose but we don't think it can be shared with anybody so why collect it? You know, I'm talking somewhat hypothetically, but I think that's a realistic possibility in terms of where we could end up. Rod, go ahead.

Rod Rasmussen: Yes. Rod Rasmussen here. To put a finer point on that. So a certificate is a - something you add to a domain, right? It is something you desire to add as a service for your domain in order to authentication and encryption. There's various purposes that you want to have that certificate for.

The system is set up so that to use public information, you know, and let's face it, you know, people who set up CAs took advantage of the fact that this data was publicly published and said, hey, there's a very convenient way for us to validate the thing - the very thing that people are trying to do which is to say that they have control of a domain name. And so we have an industry that's been born on that. But that industry is providing a very low cost and efficient - extremely efficient way of providing that kind of validation service.

So the people who want certificates, want that to be, I'm assuming, but I think we can probably all assume that people want that to be as easy and as low cost as possible, most people don't want things to be hard and high cost, and they want to actually get those certificates and have that done. And so being able to provide that information for that purposes seems to be - is something that we would be, you know, a reason for them to provide that information willingly through a - through a methodology that they can then, you know, is a well-understood public process, right, to be able to do that.

So I think for people wanting to see certificates, this system works quite well and it works very well obviously for the CAs as well because they can automate it and provide low cost services etcetera, etcetera. So you have at least a subset of people who are domain registrants who would like, in theory, the collection of this data for this purpose. So that may not apply to all domain holders, because not all domains have certificates attached to them.

So it may be something that would be a - not necessarily a ubiquitous, everybody would need it, but it certainly is one - is a current existing practice that you would probably want to support in the future regime based on the fact that both the people who are providing information for collection and then subsequently disclosing it so that the certificate authorities can validate that - everybody is in agreement that that is actually what something - a good process that needs to go through and happen.

So I think from that perspective, and regardless of thin versus thick, you have a legitimate purpose that there is agreement on all sides if this a good reason for collecting and displaying this data. Thanks.

Chuck Gomes: Thank you, Rod. This is Chuck. And several people throughout our meeting today have pointed out that it's not just the CAs that benefit from access to this information if and when they get access in the future like they have today. Don't share that with your colleagues, Geoff, they will be looking for me. But just to keep our working group neutral at this stage.

I can tell you that my own company uses encryption and certificates internally, not for commerce but for all of us so that if I get an email from what looks like one of my colleagues and it's - I don't see the padlock, I get suspicious. And so it helps me know whether I'm getting legitimate communications from even one of my colleagues.

And there's no commerce involved there. But I benefit from that because it makes sure, and all of us I think know how easy to is to spoof emails. And so it's - the point is well taken that it's not just CAs that - or people doing commerce that could benefit from this, but for other purposes as well.

Okay, I want to jump back to the fourth purpose, which was business domain name purchase or sale. So if somebody wants to register a domain name can they use RDS data to do that, thin data to do that? And I won't repeat what I said before that's shown in the table. But let me ask the question point blank again, is there anyone on the call who disagrees with this as a purpose for thin data?

And again, I know it's - Stephanie, I know it's very hard for you to be patient and I'm sorry if we're going way too slow. I'd love to go faster too but we're trying to be very deliberative about this. So you're going to hear me say it probably dozens of times that we will get there. Sorry.

All right, nobody is objecting so I'm going to make the conclusion that we will verify in a poll item in the coming days that the people on this - there's nobody on this call that objects to business domain name purchase or sale as a purpose for thin data. Okay.

Let's go now to the next one, which is academic, public interest DNS research. And let's see, I should look and see the academic - there was about - the average score for that one was 6.97 so pretty good support for that, not as strong as we're ending up with the ones we've spent time talking about. But we were just asking people to give their preliminary thoughts.

So you can read the tasks associated with that, the data - thin data elements that might be used for that and the use cases are listed there as well. So let's start with Sam as the first person on this one.

Sam Lanfranco: Okay. Thank you. Good morning. Can you hear me?

Chuck Gomes: Yes.

Sam Lanfranco: Sam for the record. Okay, I just wanted to flag an issue that would come up here and there's no clear place to plug it in, and that's that any academic research that involves a set of data where there is now an academic publication, usually there is a requirement either by the journal or the funding agency that the data set be archived and available to viewers - to readers - so that they can replicate and build on the research.

So there's a question in the back of my mind here, and I don't know what the answer is, and that is, is there a risk here that the data set that is pulled together by the researcher, then goes into the public domain in a way in which it shouldn't?

Chuck Gomes: So even if it was gated access, this is Chuck speaking, so even if it was gated access where the researchers were authenticated in terms of giving them access to it, if they were then to make it public, they - it just kind of violated our gated access and it's just like being public data. And then I'm sure you're saying even more than that. But that's a very good point.

And that's why we're going to be looking at the privacy and data protection aspects of these things as well as the other issues that we're dealing with like right now we're focusing on purpose and even users as well, academicians and so forth, researchers, but we're going to have to put all this in the context of privacy and data protection as well. So I'll say to you what I've been saying to Stephanie over and over again, we have to get there to that part 2.

And that may cause us to go back and say okay, yes, we may decide this is a legitimate purpose but can it be granted and still be in compliance with data protection laws in various jurisdictions? Did you want to say any more on that, Sam?

Sam Lanfranco: No, I just wanted to flag that now so that we don't lose that issue.

Chuck Gomes: Very good. Thank you. Is there anybody that disagrees with this as a possible purpose for thin data? Can I then conclude that this also - that there's no one on this call that disagrees with this as a legitimate purpose for thin data - for collection of thin data? Again, apologies for those that don't like the word "collection." Okay. So that'll be tested in a poll as well.

Let's - I don't know where you're at on your screen but let's see, let's go to the next one then, which is regulatory and contractual enforcement as a possible purpose. Again, I don't need to go through the routine, I don't think, or if I do let me know. You can see the information in the table there, the four columns including the middle column.

The - and you can see the use - a key use case here is registry and actually it would be registry and registrar agreements, both probably for compliance and so forth. Any disagreement with this one? Okay. Without belaboring it, let me - again, we will test that conclusion with the full working group. And again, all of you have the opportunity, like you've heard me say in previous meetings, that if for some reason you all of a sudden think you disagree with this, you can do that in the poll even if you don't disagree today. So and you can add comments.

All right, there seems to be support on this call for that one. So that'll be another poll question. So there'll be more poll questions this time but hopefully they'll be relatively quick to respond to and you'll have opportunity for comments.

Skipping ahead, the next one is criminal investigation and DNS abuse mitigation. I don't know how many of you looked at the block schedule for the ICANN 58 meeting in Copenhagen, but there are, as I understand it, four high interest topics and one of them, again, continuing from last time, has to do with DNS abuse mitigation. So this particular purpose, as proposed in the Expert Working Group, is one that is a live topic in the ICANN world right now and has been for quite some time, probably will be in the near future.

So again, I'll let you read the items that are in the table there. Does anybody have any questions on this one? Okay. Does anybody disagree with this one? Object to this one for collection of thin data? Okay, I will conclude then that we have another point of agreement for the people on this call, or again, at least a point that nobody objected to. So we're making great progress today. Hopefully this is a sign of things to come, although we all know we've got some more difficult things to get to in the not-too-distant future.

All right, the - then the next couple proposed purposes - actually were addressed in the EWG report but not as specifically as the other ones that we just went through with regard to thin data. And so the next one is legal actions and that came - that came out of, I think, the poll before last, not too critical I guess to identify which poll. But it actually came out of a poll.

And before I say anymore let me let Lisa talk.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. Just wanted to maybe clarify what's in the two table rows here. In the poll we had I think it was the week before last, two people suggested as additional purposes for thin data intellectual property rights enforcement and other legitimate investigative purposes. And in looking at those two additional purposes it seemed to me that they fell in what the EWG described as legal actions.

The reason that legal actions wasn't on the list in that poll in the first place was that when the EWG described the data needed for legal actions, it didn't necessarily flag thin data as being needed for legal actions. I should say thin data, other than domain name. And so it wasn't one of the listed purposes. But of course, it was an identified purpose and the description of the tasks here come from the EWG's report and its description of legal actions.

I hope that helps explain how the two different perspectives were merged into this one row.

((Crosstalk))

Chuck Gomes: Thank you, Lisa.

Lisa Phifer: Same will be true for individual Internet use.

Chuck Gomes: And, Rod, you're next. Are you on mute?

Rod Rasmussen: Yes, I had to get - my phone was locked...

Chuck Gomes: Okay.

Rod Rasmussen: ...had to unmute it, you know, all that stuff. Rod Rasmussen here. So, you know, just one thing on legal action, there are some - there are two areas where I could see if we missed it in the EWG my apologies, but two different ways I can see that the elements would be useful there.

One would be name servers and, again, this gets into use of infrastructure and kind of guilt by association it's useful as circumstantial evidence when you're taking legal action to show that, you know, certain names are only used for domains that are used for, say, malicious intent and no other legitimate purposes. And that's the (unintelligible) when you're trying to prove a case.

The other is registrar, and just knowing the registrar of a domain is useful when you're trying to take legal action because that's where you go to serve papers on getting further information that only the registrar would have. So there I would argue that there is certainly with that particular use case area thin data is actually quite useful. It may not be nearly as useful as thick data, but it's certainly a couple of uses right there off the top of my head that I know people typically use that data for when pursuing legal cases. Thanks.

Chuck Gomes: Thank you, Rod. So I want to point out a little - make a little side note on this especially these last two rows here and the purposes in them. You've heard me say that the leadership team takes a look at all the comments and these are examples of things that came out of comments from - and I think I also think it was the survey before last so at least Lisa and I are on the same page there but regardless it did - these were added to our list of possible purposes based on a previous survey.

So now I'm hoping it's not just because it's the middle of the night that we're not getting too much disagreement. And I'm also hoping that really it's because for thin data there's not as much controversy about some of these elements even though some of them might be considered personally identifiable information.

But, Rod, I have a question for you. I'm guessing that you would suggest, and I'm supportive of that, of adding name servers, to the list of thin data elements in the third column, is that correct?

Rod Rasmussen: Yes.

Chuck Gomes: Okay. Does anybody have any others you think should be added? Thanks, Rod, for that. Okay. So here's my question again, do we - is there anyone who objects to these purposes here, the legal actions purpose? Okay. Intellectual property interests will be happy with that, although I know we've got a long ways to go beyond thin data elements and beyond collection so. All right, so that'll be another poll question to confirm this in the next few days.

Going then to the last one on our list, and by the way, if somebody wants to add another one that's possible, okay, certainly be thinking about that and share that. Individual Internet use, again, that came out of a poll, one of our polls, consumer protection and risk mitigation, consumer trust and verification. I think it was Michele earlier in our call - in this meeting that brought up the verification issue and other people have mentioned trust in the chat and elsewhere.

So you can read the tasks there. And the domain name is the only element that's listed. If you have a suggestion for other elements that would be useful here, please suggest those and we'll add those in future tables. And so let's let Lisa start off the discussion on this.

Lisa Phifer: Thanks, Chuck. Lisa Phifer for the record. I just wanted to point out there's been a couple of questions in chat and it's worth clarifying that every purpose will need domain name because that's essentially the key that gets you to the rest of data whether it's thin or thick. And I think the questions that we're asking here are really about the other thin data elements, not just domain name. Domain name is needed by everything.

Chuck Gomes: Thank you. Sam, your turn.

Sam Lanfranco: Thank you. Sam for the record. You have customer complaint there, I'd like to suggest partially tongue in cheek that we add good Samaritan. This weekend I was confirming staying at a hotel in East Africa next week and their Website went down. I went to their Whois and discovered that it had expired on Saturday, the domain name had expired on Saturday. So I was - I had another email address so I got through to them and they managed to get it back up on Monday. I had to call their registrar in the US who referred us to the registrar in France. But you might include, along with complaining, something positive like good Samaritan intervention.

Chuck Gomes: Thank you very much, Sam. That's a real live example of this particular category. Thanks for sharing that. And...

Rod Rasmussen: Well I think that falls under technical issues, by the way, but still great.

Chuck Gomes: Technical or business issues. But, yes, okay. Any questions on this one? All right, anybody object to this purpose category for collection of thin data? All right. Well let me tell you that you guys have proved the leadership team can be wrong, of course you all knew that already, but we thought there's no way we'll get through all these in one meeting. And it looks like we have.

Now all of these will be confirmed via poll. This should be a fairly easy poll to create so hopefully we can get it out tomorrow for those of you that it's already - or hopefully we can get it out on Wednesday - well I don't know, it's still Tuesday for me and a few of us on the call. But not very much longer.

And so anyway we'll shortly get a poll out with about the same turnaround time that we had. And we'll confirm each of these conclusions from the people on this call with the full working group. And we would appreciate all of you participating as well. It should be especially easy and quick for those of you who've been on the call to respond.

But keep in mind, you have freedom to respond however you like on those. And we'll share the results in our next meeting. And then continue our deliberation from there. Any questions or comments on these purposes before we move to the next agenda item?

Okay, so let me - so again, we will add the results that were confirmed in the latest poll, the one that we discussed the results on today in our key concepts document like I already said. So let's go to Agenda Item 3, if you don't have it in front of you in some other form you can scroll up in the discussion notes to the agenda there. But it's to continue deliberation with users, purposes, Charter Question 2.2. for thin data. So, I'm sorry, we - that's - we just did that so my apologies for that.

Agenda Item 4 is to confirm our action items and propose decision points. Well, I went through the decision points. If you scroll back up on this table that's on the screen you get a preview of what the poll will look like. And starting with domain name certification and going through the rest of them, we will confirm whether or not there is indeed full working group support for all of those as purposes for collecting thin data. So that's a key action item there. And that's what the poll will look like.

Now, will we throw in something kind of as a preview of the next agenda to get people thinking? I don't know, I haven't looked at that - in the last couple days myself. But the main part of the poll will be confirming what was concluded in this meeting today.

Our next meeting will be on the 24th. And that'll be at our regular time. Thanks, again to all of you who are - who participated very well in this meeting at some very uncomfortable hours. That was much appreciated. Michele, go ahead.

Michele Neylon: Chuck, one item that we did want to address in relation to the polls.

Chuck Gomes: Yes. Thank you. Are you talking about the agenda for next week and the - and that's probably why Lisa had her hand up too. Thank you. Because I did miss that parenthetical in the agenda. So one of the requests that was made by Stephanie after or in - I don't remember if it was in - it may have been in last week's meeting and we've had some interaction since then - was to make raw data available from the polls.

And so next week we want to discuss that in more detail. We as a leadership team don't have, I mean, we're not opposed to you seeing the raw data, but we want to respect people's privacy, okay. So how much raw data do we give? Do we give people's names with how they answered in these polls? Do we give their IP address? Because that's some of the information that comes out from the polling mechanism.

Are you comfortable with that? One of my concerns, I wouldn't want to do anything that reduced people's freedom to respond, okay. So next week we're going to put on the agenda this topic and we would like your feedback on that. And we will, for those who can't make it, and I hope that's not too many of you, but for that can't you'll certainly have opportunity other than the meeting directly to voice your opinion.

We are fine with being as transparent as possible. Hopefully nobody's distrusting what the leadership team and staff is doing with these polls. And I don't think that's the motivation for asking for raw data so that you can look at it yourself. But we want to - if we share raw data we want to do it in a way that you're all comfortable with and that doesn't reduce the freedom for people to participate openly in the polling mechanism that we have.

So, Lisa, go ahead.

Lisa Phifer: Thanks, Chuck. I just wanted to add one further point which is there are a number of ways that we can export data from the polling mechanism that we're using, which is Survey Monkey. There's a number of ways that we can do it and the best way to export it really depends on how you want to use the information. For example, we can export each answer individually so that you would see what respondent Number 1 answered to every single question, but you'd see that in a PDF that you couldn't then further manipulate.

Another way that we could do it is export to Excel all of the raw data and then you could perform further analysis. And those are just two of several ways. So when we talk about this next week in detail it would be helpful to get a sense of what you want to use the raw data for and then we can choose the best format to meet the goal.

Chuck Gomes: Thanks, Lisa, for explaining that. And thanks, Michele, for catching my miss there. Much appreciated. Geoff, your turn.

Geoff Noakes: Chuck, did I just hear you say that our next call is January 24?

Chuck Gomes: That is correct.

Geoff Noakes: And will that be from 9:00 to 10:30 am Pacific?

Chuck Gomes: Yes.

Geoff Noakes: Okay, thank you.

Chuck Gomes: Yes it will.

Geoff Noakes: For some reason it's not in my calendar.

Chuck Gomes: That's our regular time so except for the third meeting of the month the meeting should be at that time.

Geoff Noakes: Thank you.

Chuck Gomes: You're welcome. Michele.

Michele Neylon: Thanks, Chuck. It's Michele. Just on this entire thing around the - about what data is made available after polls and everything else, I mean, just adding a bit of flavor to what you were saying, one of the things that a couple of us said on the - our leadership call we had discussing this, the key thing is that while there might be data that's collected, which is just collected automatically by the polling system, we thought it was best that people were - had a clear understanding of what data would be shared prior to them doing any survey rather than people submitting responses to a survey, assuming that they have a certain degree of anonymity and then - then a lot more data being published or vice versa.

There was some discussion as well around whether some people would give kind of less filtered responses if they thought that their identity was obfuscated in some way whereas others, like myself, for example, I mean, I always answer things regardless. I don't really care one way or the other. So just something for people to think about. Thanks.

Chuck Gomes: Thanks, Michele. Chuck again. And very briefly let me say that so if there's a - if there is support in the working group - strong support for sharing raw data, we would be hesitant to go back and show raw data from previous polls unless the working group supported it strongly because people wouldn't have known that that was going to be shared beforehand. So that just - just a kind of a follow up to what Michele is saying there. So Stephanie, go ahead.

Stephanie Perrin: Thanks, Chuck. I've put some comments in the chat about what I'd like to be checking, but I would just like to enter a plea to hear the arguments for privacy. I mean, I'm a little surprised actually. If you're participating on this group, you're not here to comment, to participate in the debate and the discussion, I don't find these questions particularly revealing. And why should people suddenly be able to submit polling data that they're not accountable for? You know? I'm a little confused about the concern over privacy here. So please give me some privacy arguments.

((Crosstalk))

Chuck Gomes: And that's coming from our privacy advocate.

Stephanie Perrin: Well, I hate to see people losing accountability and hiding behind privacy.

Chuck Gomes: And, Stephanie, we'll give people an opportunity to do that next week. That's going to be hopefully an objective in the discussion on this agenda item next week. Now I can share one possible reason, it's not me, this isn't for me because I'm pretty open about it for my own responses, I wouldn't have any problem with all of you seeing everything I respond to.

But some people, because they're representing groups may be more cautious if the identity is known. They also have accountability to their groups and if they're speaking in their own capacity they may feel less free. I'm just saying that might be a possible reason that some people would have concerns. But we're going to talk about that next week.

Geoff, your turn. Is that an old hand?

Geoff Noakes: That's an old hand.

Chuck Gomes: Okay thanks. All right now I think our time is up. Thanks again for the great participation. Is there anything I have left out? Have a good rest of the week. The meeting is adjourned. And we'll look forward to your poll responses and continue discussion on the list as well as your thoughts next week on not only the continued deliberation but also on this question about sharing raw data. Meeting adjourned and the recording can stop.

END