ICANN
Transcription ICANN61 San Juan
RySG- RDAP Pilot Discussion Meeting
Sunday, 11 March 2018 at 10:30 AST

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.

Marc Anderson: Hey good morning everyone. I think we're going to go ahead and get started. It looks like we have critical mass and people are settling in so can we go ahead start the recording?

All right great. Good morning everybody and welcome to the ICANN 61 meeting of the RDAP Pilot Discussion Group. My name is Marc Anderson from Verisign. And by virtue of not saying not it quick enough I ended up as your co-chair to this - or your chair to this group. So I've been facilitating this discussion and trying to keep it moving with some degrees of success.

We have an agenda for everybody here. It's up on the screen and in Adobe. If you're not in Adobe you can connect and follow along but we'll have screens projected here in the room. We're going to start things off with a little bit of an overview.

At the ICANN 60 meeting Francisco from ICANN staff provided an overview of RDAP, the RDAP pilot. And I thought that was a good way to sort of introduce the session and the topic with a number of people in the room who are new to it. And I think it's good to set a ground, you know, same understanding for everybody in the room.

We have a number of pilot participants. And I see many of them in the room and so we'll also give them an opportunity to give an update on the status of

their pilots, how things are going and anything they'd like to highlight. I also have a guest speaker here today. Greg, I hope I'm saying it Mounier?

Greg Mounier: Yes.

Marc Anderson: Greg if you're at ICANN 60 Greg is the individual whose name I could not for the life of me remember for the entire meeting. And so I now know that this is indeed Greg and I promise not to forget your name again. But Greg offered to come speak to us about some of the law enforcement requirements, some of the needs of their group in helping us develop a next-generation RDS solution. And so I thought that was a great opportunity to hear from one of the key user groups of the RDS tool so I took him up on that opportunity. I think this is a great chance for us to hear from Greg for talking about law enforcement needs.

As everybody that's been a part of this group knows the output or the outcome of this pilot is a new profile. And so one of the things we've been struggling with as a group is how to work on defining a new profile. So we'll talk about that for the remainder of the time. We'd have feedback, welcome feedback from anybody in the room. This is an open session so everybody is encouraged to participate, ask questions, provide feedback and input. We have plenty of mics at the table if anybody wants to come up and comment. You're welcome to do so.

Can you go to the next slide? So, we also have a plug here for the Registration Operations Workshop the ROW. ROW Number 7 will be 17 May 2018 in Vancouver. This is – if you're following along this immediately follows the GDD Summit. So if you're attending the GDD Summit already and would like to participate in the ROW it's actually the second half of the last day of the GDD Summit. So they've been, you know, they been co-located to sort of ease the travel burdens on people. So if you're interested and especially if you're attending the GDD Summit already encourage you to attend.

Did you want to add anything to that? Okay, right. And with that if you go to the next slide I'll turn things over to Francisco from ICANN staff who's going to give us a little bit of an overview on both RDAP in general and specifically the RDAP pilot, how we ended up with the RDAP pilot sort of its goals and next steps.

Before I do that though I see some people standing. Don't be shy. We have seats up at the table. Feel free to sit down. I'm not going to call on anybody just because you're sitting at the table. But thank you. Francisco please go ahead.

Francisco Arias: Thank you Marc and hello everyone. So let's see how we - who do we (have) here. And so this is the quick agenda. And let's keep that and go directly to the issue.

This is the background. So this started in - back in 2011 when the Security and Stability Advisory Committee to ICANN in their SSAC 51 set of recommendations. They recommended the ICANN community to evaluate on a (law), a replacement for Whois. That was adopted by the board shortly after and they start with the staff to work with the community to develop a roadmap to implement this set of recommendations.

And in parallel in the IGF work started also in 2012 to develop these protocols that would be the replacement for Whois. And that work finalized in 2015. Now we have the RDAP protocol, the (rescission) data access protocol that was published to us and standard by the IGF in March 2015.

Then going back to the ICANN sphere we started work on a profile for the gTLDs registries and registrars in 2015. The reason for this work is that RDAP there, the standard is you can think of it as a menu of a functionality that can be implemented and it doesn't tell you which ones you turn on or off. It depends on the local policy. That's what I believe the term used in the

standard and it's not referring to consensus policy so it is calling in ICANN it's a completely different meaning there.

And the point is there need to be some definition of what features have to be turned on or off in the gTLDs. And that was the intent of developing this profile. So the work on that profile culminated in July 2016 the first version of that profile was published. Fortunately shortly after ICANN received a request for reconciliation regarding the inclusion of this RDAP profile and (unintelligible) in general the committee permit RDAP in the constituency level and display policy.

And in February 2017 that was - that policy was revised and the requirement to move in RDAP was removed. In the meantime discussions with the Rights Holders Group and the (Right for) Stakeholder Group continue. And we receive a proposal from the contracted parties registries and registrars to - how to implement RDAP. And this was a accepted by the ICANN organization in September. And the main requirement - the main request in that proposal was to start (of this) and to start a pilot which we started in 5 of September and to work towards having a profile or profiles agreed for gTLDs registries and registrars with the aim to have this done by July 2018.

So by that time the idea is to finalize the pilot and to have an agreed timeline to take out of the production and have the profile or profiles agreed. And after that I mean whatever timeline is defined that's when we will have an RDAP service in production. So that's the timeline that was set by that proposal.

For those of you that are not familiar with RDAP or why we went to all of this trouble let me provide some background on why we think - why it was thought that Port 43 Whois need to be replaced. So some of the issues that this protocol has is that it's barely a protocol. It's a very simple thing that just says you said something you get something back. And so there is no standardized format on the output. And here are just a couple of examples of what you can see out there with some registries.

And there is no support for internalization and so there is no way to say I'm going to provide for the server, the registry for example or the register to say I'm going to provide you output in decent coding and - or so there is no way for the client to know what he's getting and there is no way to know how to interpret so you get things like this.

Other issues with Port 43 Whois is there is no support for differentiate access. That is there is no way to give certain output to certain users and other output to other users. For example us defining in the draft model for GDPR compliance there is that idea of having some minimum output and some - a full output to authenticated user that's not something that is really available in Port 43 Whois.

Another thing in - another limitation in Port 43 Whois, is its lookup only protocol. There is no functionality for search. So you can only search for a given object, a given domain name or contact or a name server, et cetera. With RDAP you have the option to support search in a standardized way.

Another thing there is no similar ways to (unintelligible). For example in thin registries and thin registries only have a portion of the data. The rest of the data is hold by the registrar. And with Whois there is no standardized way to – for the registry to say here's a portion of it I have and here is where you can find the rest of the information. And there is no bootstrapping mechanized studies. There is no way to know who to query.

So if I want to - if I'm there - the user and know that I want to know who is the registrant of ICANN.org and I need to know in Whois who to query to get that information. It's also an insecure protocol. There is no way to authenticate a server or to encrypt the channel between the server and the client.

And where the other pictures were and not surprisingly they are basically the opposite of the issues that we find in Whois Port 43. And so it's a - it has a

standardized query response and other messages. It has secure access to data. It's run over STTP and a (session) can be run over STTPS. It can be extended easily. It was designed with that in mind so you can add different output elements depending on the needs of each registry or registrar.

It also enables differentiated access to have different levels. You can define who gets to see what. The protocol of course does not say who gets to see what. And that's a decision that has to be taken by someone else.

And it has a bootstrapping mechanics so in RDAP it's possible for you to just tell the client I need to know information about this domain name and the protocol will take care of finding what server to query and get the information. It has also a way to do private action reference. This is the mechanism could be used for thin registries so that the server says here is the data that I have and here's where you can find more information for example to the registrar, (unintelligible) into the registrar RDAP service. And I already mentioned it's built on top of STTP. So that makes - it should make life easier for implementor since pretty much everyone is running our Web service these days.

It has it comes with (international) session support from scratch. So you can have internationalized (rate) session data RSS names, et cetera. They can be in whatever script is supported by Unicode which is the factor standard for internalization. It also enables searches of objects. Again it does not mandate that they are done but it tells you how to do them if you want to do those.

And so some resources that may be of interest ICANN we have set off a page. You can find it there icann.org/rdap with some links to the resources that we have there. One of those is then the pilot that is running. And in there we have currently six registries that cover 50 plus gTLDs that are participating so far in this pilot. And we're encouraging people to use the gTLD tech mailing list. You can see the link there where you can provide a general feedback program in the pilot.

And all right now I'm going to do a quick demo of the RDAP output for those of you that have not seen it. So one thing you should know about RDAP when I set up this thing is RDAP is intended to offer a standardized output and is not directed to the end-user. So the idea there is that RDAP provides a standardized output that can be easily converted to something that a normal user will want to see in an HTML page. So that's they really don't using the RDAP information but you should know that the output in RDAP is of – it's something that perhaps only techies can immediately understand.

So I'm using here an example from one of the registries participated in the pilot (.dean). I hope I'm pronouncing this correctly. So here you can see I did a query for the domain name (nic.pm). And another interesting thing you can see the registration when the domain name was created. You can see it here, when the domain name expires.

And let's see little bit more here. Entities that's the names and RDAP for contacts. So here is where you find the registrant, the admin, the technical billing contact, et cetera -- whatever context the domain name has linked.

So in this case for example this contact and FN means full name. This is the name of the contact. It's an organization. And the name of the organization is TLD box. And I'm going to try to pronounce that (Hedazavis). So here's the name of the element so you can see so that's the address.

And the telephone number you can see a number here. What else we have here? There is a fax number, there is an email. And the last piece of information this contact has the role of technical contact for this domain name. So that's - another interesting example of this is another contact but here interestingly oh - is this the one I'm looking? No I don't think so.

There was one of the contacts I think it was on the top that is redacted. And so in RDAP you also have a way to redact information. So where is it? Sorry the feedback is not helping me here to do this.

Here it is okay. So in this case the registries redacting the information and saying this is protected under privacy law, et cetera, et cetera. So you cannot really see any of the information. And so this is one way you - in which you could do this. Of course another way is just simply you don't provide the data which is how other participant in the pilot choose to do that.

So this is Google. And here you can see you have information about the domain name so way it was registered, transferred, when does expire, last update, et cetera. But when you go to find the entity, the only entity you find here is the registrar. And the rest of the contact you don't find in there and there is a message below that will tell you that oh here are the name servers.

So here Google choose to hide the contacts and is telling us that. They also provides the times of service for the RDAP service you can find. And I think that's it for a quick overview of how you will see things in RDAP. All of this is in JSON which is a standardized format that can easily convert it to HTML page that a normal user would probably prefer to see. So with this I turn this back to you Marc.

Marc Anderson: Great, thank you Francisco. I appreciate you once again volunteering to give us the overview and provide a demo of some of the typical output. I think it's useful to be able to sort of see and touch start of the JSON output that you would expect from a RDAP query. Did I – do we have questions or comments before we move on?

No, okay. I do want to add sort of one thing to what Francisco said. The RDAP protocol itself was not designed specifically for registries. It's register - or sorry I should say domain name registries. So it's a registration data access protocol but it can be used for things other than domain name

registries. The ITF specifically created it to be a little broader than just domain name registries. And that's one of the reasons why you see us working on a profile the profiles in part to define how a domain name registry would implement the RDAP protocol. So just a little more color on why that's important to us.

At this point I'd like to turn things over to our guest speaker Greg. Greg is from Europol Cybercrime Division and is a member of the GAC Public Safety Working Group and a active participant on the next GEN RDS PDP. And so he comes to us with some expertise and again thank you very much Greg for agreeing to come and talk to us. So with that I'll turn it over to you.

Greg Mounier: Thank you very much Marc. Good morning everyone. I'm laughing because guest speaker that's probably a bit too much. I just have a few comments to make really and give you a bit of an update.

So after the meeting the RDAP had a project meeting in South Africa last time where (Aranya) from the FBI the Bureau and I attended and we volunteered basically to facilitate the communications and the engagements for the law enforcement community which might be one of the main clients of the RDAP protocol.

So what we've tried to do is first of all really just raise awareness about the reform of the Whois in light of the GDPR taking effect in May with the law enforcement community and then telling them of course that there was also a new protocol being worked on which might be replacing the Whois protocol and which we'll have the feature of differentiated access. So that was already a (set thing).

So what we've done is that we've organized in parallel to our public safety working group intersectional meeting that we had in Brussels in February so we have every year a meeting outside of ICANN meetings. We've organized a meeting with some of the registries that are part of the pilot program. And

we were very grateful for Marc and (Rick) from Verisign to be there and also and Francisco gave their presentations to about 30 cops from various countries in Europe but also Canada, the US and so on. So we went through what RDAP might be all about. We explained the various features and we've asked for feedback.

To be honest with you we've also sent the link to the portal as well for them to try to play around with your - with what was available at that time. To be honest the feedback we got was very high level in the sense that, you know, they haven't got into, you know, what Francisco showed. So they really provided us with like a few big high level principles that they would like to see implemented at least for them to be able to use that protocol.

So first of all really the main feedback is great features, standardized format for (unintelligible). That's great, search support, differentiated access. That's all good. But then one of the main issues they would have is that when we sent - and that's maybe something that you could clarify. When we sent the various link to the various portals so the FES portal, the Verisign portal Google portals, then the first question from grassroot investigator was are we going to have to create different portals or is it planned within the RDAP project that at some point there will be a central access portal where you could query the information? So that's really one of the main feedback.

And again I'm just throwing that to you. If you have straight on an answer I'm happy to take on if you – but otherwise just we can also continue the discussion. So that's really practical very down to earth support. The other issue they came up with was the fact that they are worried that the Whois queries might be tracked and logged. And that would be problematic because it would of course compromise the confidentiality of investigations. So if the central server that will be operating RDAP, I don't know exactly how it would work, but would log every query that for instance the French accredited law enforcement entity whoever that might be the (NIA) or the French police or whatever and then if somebody could see in log okay they're doing these

types of queries they might be, you know, investigating these type of domains.

Maybe they're trying to take down this type of (unintelligible) net. Then of course for us it would be an issue. So I've heard that (Scott Halemback) and some others were making may be on some features like do not track double features. Again we haven't talked about the technical details about how would that be implemented but that for us really a redline.

We understand also that from a privacy and data protection perspective we need to be able to audit what accredited entities would be querying in a database to be sure that they're not overstepping, they're not abusing the system. But at least at (unintelligible) level would want to have the log. So this Catch-22 type of situation could be and according to us solved if the login was done at local level.

Let's say that a national accredited law enforcement entity has a legitimate purpose to us so access nonpublic information in Whois, they do their request but then the queries would be logged by that national entity. And so a DPA, national DPA would have access to the logs in order to do the auditing. But then that central global level so the access to the Whois then they wouldn't be in any log. I don't know if that makes sense for everyone. I'm not sure if I explain myself correctly but if you see the – yes please?

(Vladir): (Vladir) (unintelligible) with the (unintelligible). So quick question on that. What is really (unintelligible) with regards to login? So you do a query, come through a server, we track IP address and everything else for our logs and for auditing purposes. So does (NIA) believe that then we're going to turn around and notify, you know, that the registrant or the accused party for some - I mean at the end of the day if that is a concern can we not put that somewhere within a policy as part of credentialing underline or something of that nature and that we track that somewhere else instead of on a (technical) level?

Greg Mounier: I don't know. I suppose it would be possible but I don't know if the community – I think that the community, the law enforcement community would need to have, you know, proper guarantees that, that would be implemented. So I suppose I'm also turning to you (Anga) but I suppose if it was not technically possible then they would probably feel safer, you know. But rather the yes there is a log but then there is a policy that said that you can't (unintelligible) the log but yet what if the server gets hacked or something? I don't know.

But I mean, you know, again this is really high level. So I think from the CROP's perspective it would be great if it's from a technical perspective that would then be possible but I don't know if it's realistic.

Marc Anderson: Yes I think it could be done either way. I think we're not ignorant to the fact that, you know, when we query it's logged anywhere now. That's the reality. But I think the difference for us and maybe we don't get this fully but then when you're connecting that to an authenticated account that's where we get concerned is that when if you're authenticating us as law enforcement and logging it and you can make that connection then it gets really interesting for people who maybe want to get tipped off or maybe want to lead or something like that. That would be a confidential issue for law enforcement.

Jim Galvin: So thank you, Jim Galvin from Afilias for the record. I guess I want to understand the requirement or the ask if you will from a policy point of view and separate this out. You obviously I mean in today's world of course, you know, logging happens, you know, all queries get logged. So I think to translate this requirement to something more actionable what you're looking for if I understand correctly is anonymous full access. Would that be fair, a fair characterization?

Greg Mounier: Yes. I think it would be fair. I mean if you think that law enforcement accredited entities have a specific profile and that profile would have anonymous access and full access then yes I guess it would be okay.

Jim Galvin: So to take that a step further you're actually asking that in particular maybe not full anonymity but the requirement is more that it not be known that law enforcement is making the query. That's really the critical thing. So and I'll take it a step further, characterize this in a certain way. I'm trying to get to a place here. So what you want for law enforcement to not have any accountability for having made the query?

Greg Mounier: The accountability would be taking place at local level. So a DP - a national DPA would still be – I mean I'm talking about an ideal solution would still be able to see what type of grades have been done but it wouldn't be of available at a global level.

Jim Galvin: So which is interesting. So it's – there's a distinction here right? And that's why I said that I tried to get there from a first statement is that that law enforcement wants anonymity or just that the individual in law enforcement wants anonymity and do you understand the difference I'm trying to distinguish?

Marc Anderson: Yes. So I think I don't think I'd wade into the accountability argument as much as we'd be concerned about the request itself being anonymized because I think we - sorry I think creating RDAP to kind of replicate the existing ecosystem as much as possible would be I guess a better context.

Jim Galvin: Okay because what I'm – the problem that I have from a technology point of view okay is providing sort of pure anonymity if you want from a technology point of view is actually not – I mean that's not a trivial thing, not at all in any way shape or form for anybody. Even the do not track options, you know, are sort of well you're assuming then that everyone is a good player and on their good behavior. And that's probably true for most of us okay. It's certainly true for me. I don't know about anybody else. But no but seriously, you know, I mean it is probably true for the most part. And so I think that you're already by definition going to be making a compromise because you're always at risk

of, you know, malefactors and the malefactors servers if you will, you know, still recording and keeping that data and not anonymizing it out.

So if you start from that premise that you're already in a compromised position and what I want to offer to you is conceptually something to think about. You know, what if it really was known that law enforcement was making the query but you could only know that law enforcement at a regional level was making the query?

So take it more specifically all right, there has to be some kind of central authority that's issuing the credentials okay whatever that's going to be and that's its own discussion. What I'm imagining is that central authority would actually assert that in individual countries or whatever region you want to define but I'm assuming we're talking about countries there would be an authority in the country that would issue credentials okay? Only that country would know who the individual is that's associated with the credential. They could certainly issue what are essentially pseudonyms, you know, and that's what they would offer up to – that would be the credential that someone who got accredited would get. And they could use that at any registry.

What that means is for anybody who's offering you a response they would know it's law enforcement and they would know what country it is but that's all the data that they would have. And arguably if you want an audit to work okay if we're expecting that -- and this gets into issues that we're not going to answer here all right -- but if a DPA needs to come in and audit all of the queries and know where they are you'd need that information anyway.

I mean any server would have to log that much information because they need to be able to say go talk to this authority if you really want to know what's going on I mean otherwise even the servers are not protected at all. Would that level of pseudonymity work for you or are you really trying to lean towards more of a pure anonymous kind of scenario?

Greg Mounier: I think if, you know, if it's one country law enforcement is making that (great) authority. For some CROPs that's already too much. So if we could go a bit further even if it was - okay if it's just law enforcement profile regardless of, you know, the countries or anything maybe that would be acceptable. But ideally for the CROPs it would be, you know, there's no queries being made. And then but it could still be audited at the local level. Again maybe I'm asking something completely impossible but that's, you know, ideally that's what they will be looking for.

Jim Galvin: So I mean I can imagine implementation. As long as we're allowing for a pseudonym but…

Man: Morning.

Jim Galvin: Well good morning. As long as we're allowing for a pseudonym then the only question is that, you know, how much information is being given away? I mean obviously there are implementations where even if you had a hierarchy where you have a central authority and then a regional level authority of some sort you could find a way to issue identifiers in such a way that you would know it is' law enforcement but you would have no other data about where it is. Only the central authority would be able to decode the pseudonym if you will into something interesting. I mean would that be a model that would work for you?

Greg Mounier: And it - that could be a good compromise yes. I mean that – the again we haven't made up our mind and it's just the fact that we're having this discussion and you're stirring these type of comments is great for us. It's really cool so…

Jim Galvin: So I'm sorry Marc. I know I've been kind of monopolizing the discussion here (unintelligible) thanks. I just want to point out…

Maxim Alzoba: Maxim Alzoba for the record. Currently (unintelligible)...

Man: (Unintelligible) or has incorporated means of doing credentialing. But I can't - and it's a legal thing whether you get access to the data or not. It's not a technical thing. If you can agree on it you have to have a certificate IP-based or whatever access that's RDAP. But whether the government of let's say the principality of Liechtenstein has access to any of the Whois records that we have stored there because they have an issue with one single .green domain name this is kind of GDPR definition that we cannot solve in here.

I can then for Francisco one remark on the (Casoni) model which says a central repository for credentialing or giving access to law enforcement parties I really can't imagine that is going to work because if – just because a government somewhere in the world has a GAC representative that says it's okay if this law enforcement body is listed in this repository and then having access to all the data of all private persons that for example is stored with the .green registry this for sure - and I'm not a legal. This for sure is against GDPR principles.

So it's a technical solution yes and it will be - take very much burden away from the registries to have a list – okay access, not access but from the legal point of view this won't work, my personal opinion.

Maxim Alzoba: Maxim Alzoba for the record. Actually there are two things about that I will be short. First the language is extremely EU-centric. Basically if you're not in one of European Union police - polices I (think) or credited by police, for example some company is accredited with for example here in Poland or in Romania then formally they will be able to use the special allowances for police but is - that's it. For example police officer from Beijing or Moscow or (Minsk) or (Kiev) they have nothing to do with the definition. They are not even police on the GDPR formally outsiders no provisions for them.

And the second thing is trans-border issues because you need to know where you send information to. You have to know – you have to have an

agreement actually for that. And impossible to have an agreement with or in (unintelligible).

Marc Anderson: I'll jump in (unintelligible) putting in a centralized or federated authentication provider would definitely be helpful in moving the pilot forward. I think ideally it would be a registry operator that's providing that service though. You know, I think it's been pointed out, you know, many times in many places it's not ideal that, you know, we don't want to have each individual registry doing their own, you know, authentication. And so, you know, where we could have a registry volunteer to provide that service, you know, ideally it would be better to have somebody else do it. You know, I don't know if ICANN would be willing or to even entertain that idea. Do you – are you willing to jump in or…

Francisco Arias: This is Francisco from ICANN org. I – this is a question that's supposed to be on my pay grade but I take back and put and I can take this internally and come back to you with an answer.

Marc Anderson: Fair enough. Thank you I appreciate that. And I agree I think, you know, that would be a good step for the pilot if we had a, you know, and (O-off) provider that could issue credentials and, you know, the different registry operators could all use the same one especially in light of GDPR in the cookbook and it would be a useful next step. Any other registry operators want to - or pilot participants want to jump in? I can call on people you could pass?

Jim Galvin: All right so Jim Galvin for the record from Afilias. You know, I don't have an update anything to change from the last time that we met although I guess this is, you know, the first time we're meeting sort of in this very public group here at a ICANN meeting in the Adobe Connect. I think that where we are – I mean we have a server that's running. You know, you can ask for queries and we're running it off of our dot info so you can make queries and you can do a RDAP and see and all of that works. I think the issue for me with this group as this is a bit of a self-directed group. So I guess I have to take at

least part of the blame. But, you know, we all kind of have this as an action here is we need to create steps. We need to figure out what we're doing and sort of propose to do it. I think the suggestion for an open ID server so that we can actually issue some credentials and try some things in fact actually I'd say it would be nice if we got, you know, two servers so that we could try federated stuff and see how that works because I really think long term that's the kind of system that we're going to have.

So we probably need Francisco I mean if you're going to go down this path it would be interesting to see if you could find a way to set up two of them so we could issue credentials in two different ones and we could all see how that works too. But that to me is the issue. We're not giving ourselves actions here so there's like nothing to say for meeting to meeting. And I think that's kind of important.

We have to figure what we want to do here and move that forward and make that happen. So that's really what I'd like. And when we met last time and, you know, we just have our own mailing list so the folks in the room who are just here because it's ICANN don't know this but we decided last time to move to having weekly meetings. And I had suggested that. And part of the motivation for that was to just this issue.

You know, we need to start setting actions and activities for our self in steps so that we can move towards being done with this pilot in July and have actually accomplished something. So we've got to figure out what that is and what we're trying to achieve. In credentials to me is the big thing so I'm on board with the server and then we can start talking about how to make use of it and what to do with it. So that's a little more than an update. Sorry, thanks.

Marc Anderson: No good points. Thank you Jim. Cyrus would you like to jump in?

Cyrus Namazi: Yes thank you. I'm Cyrus Namazi with ICANN organization. So to follow-up and continue on what Jim was saying we got together a smaller subset of this

group back in June of last year in Johannesburg and came up with the timeline and a plan which I understood the would conclude by the end of July with an agreed-upon profile. I don't see us having moved the needle much. I mean some of the conversations here are so at least to my sort of not technical understanding of it is preliminary to actually having had shortly after the June meeting to sort of get us on the right path.

I don't see us having come up with a timeline by which we will have a completed profile. My concern is that we're continuing down what I would characterize as a academic discussions but it's not really moving the needle in the right direction. I think we all need to come to the table, put a stake into the ground, have a timeline that says by which time we're going to have a profile. I think a big pole in the tent here is having the credentialing system identified.

We talked about actually having the people that have come forward and are experimenting and sharing their learnings and experiments to come up perhaps with a proposal that would inform the RDS PDP in that regard. I think the timing of the GDPR going into effect in May really I think exacerbates the need to have a Web-based sort of registration data services solution in place.

So I'd really like to encourage you to I think come up with a plan that actually has deliverables and timelines and get us to a certain meaningful milestone so that the solution is identified and we can move away hopefully at some point from this ultimate dependency on Port 43 and in light of all the privacy issues that are arising now in European Union and SUNY and other places have a flexible platform in place that will allow us without sort of having to rush to put Band-Aids on things be able to address some of these issues. Thanks.

Marc Anderson: Thank you Cyrus. And I agree. Thank you for your feedback and your comments. I, you know, I think that's well put and sort of in line with what Jim

said and, you know, I think the conversation we had on our last call as well so well put. So do we have a question to be read or a comment to be read?

Sue Schuler: There's a question from Ray Fassett. "Have the fees for data access been considered at all as part of this pilot discussion?"

Marc Anderson: Ray you can't really tell but we're shaking our heads in the room. I don't really think that's in the scope of what we can even consider as part of the - this discussion group unless Jim you want to…

Jim Galvin: I want to respond to Cyrus. Okay so Jim Galvin from Afilias. I, you know, I agree with everything that Cyrus said. And I know we have on our agenda up here a discussion you have - and a bullet item for profile status. I actually do have some questions and ask with respect to the profile to help move us forward. But I think the only thing that I would add to what Cyrus said is at least from my point of view I saw the pilot as having two principal purposes if you will.

I mean there's a lot of details I suppose in there but there were two things. I heard you focusing mostly on the profile and we'll get to that I guess in the agenda here and have some discussion about that. But it really is also about credentials and being able to talk about them. That was one of the key things in the pilot even from the beginning at least from my point of view.

So, you know, I think the fact that we are talking about moving the credential testing forward and asking for help in creating a credentialed server is movement in that direction. But nonetheless you're still right on the project management side. We really don't have, you know, a laid out set of agenda items and topics and timelines and recognition of our deadline of July. And, you know, I guess, you know, this is supposed to be a self-managed group and we're not doing a really good job of that. And we probably have to find a way to get past that. Thanks.

Marc Anderson: Yes all fair points. I do want to make sure we have time to get to the profile status but I also want to give other pilot participants a chance to provide an update. Don't feel like you have to Google or on line. Do you want to jump it at all?

Sue Schuler: They've been having difficulty with the audio on Adobe so that's why everybody has been typing. Have we gotten the – do we have it back?

Man: We've got good audio now.

Sue Schuler: We've got audio now (Brian).

Woman: And (Brian) just pinged that he had no updates. But like one very minor update is like we after seeing the data models the ICANN had put out like circled back and thought about whether we had to like change the output side because I think what has been included is slightly more extensive and - than what we've included in the redacted version because there's not finality around that. We haven't moved forward with updating.

But right now we're still relying on our own like very simple very narrow credentialing system so it'd will be interesting to engage with like the suggestion that Jim has put forward. But I think in terms of the field published that's a pretty simple change. So we've talked about it but are waiting for finality to actually make the tweak.

Ben McIlwain: And just to add on to – this is Ben McIlwain from Google as well. Just to add onto that I know RDAP as originally conceived was registry side only but I'm not sure how tenable that will be going forward given that under the GDPR model many registrars will not be sending full details to the registry. So obviously if we don't even have that data we can't expose it in RDAP. So for many queries the law enforcement guys are gone but for many queries like we can't provide data that we don't have so they'd have to turn around and

get it from the registrar anyway. So I think we probably need to be talking about registrar level RDAPs.

Woman: That's a good point. And I know from their presentation last week that Tucows was looking at RDAP as part of their solution to GDPR. So it would be interesting to see if we could fold them into this group in some way even though it was originally conceived as a registry conversation.

Marc Anderson: Thank you. Good points and, you know, I will point out that, you know, the pilot proposal did have support of registrars. I think there was a recognition from the beginning that this was a possibility as we got down that road. And we've been lucky enough to have GoDaddy participating from the beginning. So we at least have some registrar participation but, you know, point well made.

(Arnold): (Arnold) (unintelligible). Again what Stephanie said sending or not sending data over RDAP or even over EPP now there is a field included which has I think display don't display yes? This again is a GDPR issue. Will this end after May 25? Will they send data or not? We can store them using RDAP protocols or this is another area that has to be - and I know that Tucows is thinking that way of according to their GDPR probations of not giving away data because it minimizes their risks. So again and GDPR is a means to do it or to send or not to send to withhold, to forbid, displayment or whatever.

Marc Anderson: Thank you. Go ahead Maxim.

Maxim Alzoba: Just a small moment, actually it could be a perfect technical solution which contains on the GDPR protected fields for most registrants. But yes after all it might be working from technical point of view, not necessarily from a legal point of view. So I think it separates issues. And the best we can do is to suggest implementation which is at least not contradictory to that. That's it.

Marc Anderson: Thank you. I'd like to go ahead and switch hats for a second here and give a quick update on Verisign's pilot. We do have a little bit of an update in that we recently added career to our pilot implementation. Ray Fassett's online is the registry operator for .career or represents registry operator for .career and Verisign provides backend services for them.

We asked Ray to participate for a couple of reasons, you know, one to get experience with providing an RDAP solution. We're not the registry operator. We're providing backend services so that creates a different dynamic so we thought that would be a good test case. And .career also sort of represents a typical distributed new gTLD for us to work with.

But also what we added on top of that was authentication. We have previously had .com and .net in our RDAP a pilot without authentication. What we added with .career is authentication. You query a basic set of data without authenticating but if you use authentication you get additional data back in your query response. And we used a basic OAuth compliant authentication which means you can use Google, Facebook, you know, any other authentication provider that's OAuth compliant.

So you can see that in our pilot. If you want to test out how sort of a tiered access solution might look that's what we tried to show in our implementation. And, you know, again if you go there without authenticating you get, you know, essentially what looks like a thin response. But if you log in using one of the OAuth providers that are available you can see additional data, you know, simulating how a tiered access solution might work. So that's the latest on where we are with our pilot and before I go to you I want to thank Ray who again dialed in so on the online for this for agreeing to participate in the pilot and let us use Career as one of our test cases.

Man: Just a quick question. So the instructions and essentially manual on how to do the OAuth and everything else through the Verisign RDAP that's all on

your Web page? We can just go there just review and just start reviewing that information?

Marc Anderson: Yes it's on the RDAP on the RDAP pilot page. There's a - I think there's an about or a help or something on the bottom and it has all the details on how to set that up and test that out. All right any other questions or comments before we go to the next agenda item? Go ahead.

(Roger): Hi. This is (Roger). I guess when I asked the participants, the people that have a RDAP service set up I've heard a lot of people say yes we have authentication in place and you'll get public information if you don't authenticate. And if you authenticate you get more information. But a lot of the discussions today kind of started wrapping around this idea and I just wanted to bring it up and see if anybody was testing the fact of filtering even at a lower level based on credentials like Maxim had mentioned, you know. If you're law enforcement from Poland you can only see Polish addresses or whatever it is or, you know, or the RDAP solutions they're actually filtering based on other criteria than just hey yes I'm credentialed or I'm not.

Marc Anderson: Speaking on behalf of Verisign that's farther along than we've gotten. Certainly that something that's been discussed but, you know, we haven't gotten to the point of testing something like that out. I think really there from my perspective a federated authentication solution would, you know, would really be helpful in giving us the opportunity to test something like that.

Jim Galvin: Yes so Jim Galvin for Afilias. And the way that we've been thinking about this is that given authenticated access associated with that credential will be a profile template of what the response can be like. And then the deal is if that information is in our database then that's what you get. And so the question, the next question becomes okay how does that credential index to a response template? And, you know, we're imagining a variety of things. You know, for us as a large service provider we're imagining that some TLDs

might have their own rules for whatever reason so, you know, that'll be an index into find in the profile.

It's debatable as to whether or not the actual registrant rather the contact information is itself might require a particular response template. And you can imagine it - there's a lot of discussions around European citizens, you know, having limited data being exposed. I mean I don't know.

It's also possible the credential may have particular requirements. And so now once you start talking about the fact that there'll be multiple possible response templates based on the credential or something about the data now you get into priority discussions about which one takes precedence. And we have not resolved any of those discussions. So I think as Marc said we're at least thinking about the problem and providing, you know, at least a slot in our development for being able to index off of something and we have not solved the resolving what the indexes yet because that's really an open question. There's so much up in the air at the moment. Thanks.

Marc Anderson: Thank you. Sort of a time check we're looking at about 12 minutes left for this meeting and I promised Jim I'd give them a chance to talk about the profile status. And you had some ideas I think on how to help us move forward and just set some context here.

You know, Cyrus pointed out, you know, the clock is ticking. We're in March. We do have some opportunities to meet between now and July. We have the GDD Summit in May. We have an agenda item there I think to talk about the RDAP profile so we have an opportunity to get together there.

And then of course the June ICANN meeting. You know, I would think by the June ICANN meeting though we want to be very far along. We want to be talking about wrapping this up when we get to June so not a lot of time. And I know, you know, from my own perspective I think I've talked to other people, you know, GDPR is a distraction to use a term. But that's sucking all of the air

out of the room in a lot of cases but that's not an excuse for us to neglect this. So we need to really focus between now and that June ICANN meeting to work on making progress in moving this forward. But with that great leading Jim do you have a...

Jim Galvin: Okay so thanks Marc, Jim Galvin again from Afilias. I really had a question about the profile because I wanted to ask about its actual role in the bigger picture. In this question I think I've had this question for a while but it's become much more crystallized in the recent past. So I mean it's really a question for this group but it's really something, you know, for Cyrus to think about too I think specifically in all of this space.

When I think about the larger picture of this pilot and its role in the community okay it seems clear to me that there's going to be more than one profile for what a response looks like. And we're using this word profile to represent two things. We have this document which is describing all of the elements that might be in a RDAP response. And if you were to present everything in the response this is what it would look like.

But I'm a little cautious these days and this is becoming more of a concern as we move towards May 25 in calling that the RDAP profile. I'm – because that to me seems to suggest it has a role different than I think it really should. And I guess this is a question for the group and, you know, open discussion really to anyone. We do need a profile if you will. We do need a specification of all potential data elements and what they look like.

So we need, you know, the XML specification for what that's supposed to be. But the term profile, you know, I'm wondering what the terminology is here that we want to use. That is not in and of itself going to define what RDAP is going to respond to. RDAP responses are going to be dependent on issues entirely independent of that. So I'm just - I want to ask that question. I think this is a profile of everything if you're giving or a profile of what elements look like if you're going to provide them in a response. And I'm asking. I'm – I think

I'm asking specifically if that is the role of this profile document as opposed to calling it the RDAP profile. So thank you.

Marc Anderson: Go ahead (Roger).

(Roger): This is (Roger). Yes I mean and as we sat here and talk, you know, the profile from last year, two years ago whatever it was when we created it I think is different than what we're talking about because the question that I just brought up I think this profile has to answer is how do you - because I think we have to provide the technical bounds for what the policy can actually try to do?

Man: Right.

(Roger): So I think we have to come up with the fact of okay if we want to be specific about getting to a certain data and one person has access to one record but they still have to be credentialed to get to it how is that going to, you know, be done? So I - to me it's yes let's say what data is available. And I think that's fairly easy for all of us to do. But I think the harder part is okay how do we - and I get through the credentialing or whatever, you know, supply the technical ability to the policymaking.

Marc Anderson: Yes good points. And, you know, I think one of the things that are important for us to, you know, I think everybody to remember this is not a policymaking body at all. We don't have the ability to make or change policy within this discussion group. You know, we're talking about implementation details of the protocol.

Of course we can make recommendations to other bodies and that has been suggested numerous times. We have an opportunity to provide input into the NexGen RDS PDP which is the policymaking organization. And I sincerely hope that's something we take advantage of as part of our output at the end

of this pilot. But from my perspective I think it's important that we separate out the policy from the profile itself.

And, you know, I would like to see us focus purely on the implementation aspects in the profile document, you know, the output that we produce and make sure we leave the, you know, anything policy related to the policymaking bodies. And actually I want to see if I can put (Stephanie) on the spot a little bit here because I know this is something she has thoughts on as well. Are you willing to let me call you out?

Stephanie Duchesneau: Yes I'm just trying to think a little bit because I think we're stuck. And I think we're like stuck because we're in a challenging place and we have this sort of parallel like legal compliance problem going on and there's a parallel policy development problem and process going on. And we tried to make this a technical track but at a point where like all of our technical solutions and models are so uncertain it's being - and these other processes are also uncertain. It's being sort of paralyzing and hard to move forward.

But I think Jim is absolutely right that there's ways to split it up. I think there's like a couple of different questions and I'm glad you isolated one of them. I think we can answer the question fairly easily around provided that you're giving access to everything what does it look like? And I think we can take the current draft from ICANN and answer that question with relative ease.

And then the second set of questions and several people in this room are probably better positioned to articulate them than I am are around like credentialing and how that should work and what works best. So like maybe the next step from a project management perspective is just too like articulate the different buckets of problems that we're trying to solve are and the different components that we're trying to develop.

Marc Anderson: Thank you Stephanie. And I'm being told we do have a meeting at noon or a follow-up meeting in this room at noon so we do need to wrap up promptly. You know, Maxim a quick word and, you know, Jim if time permits.

Maxim Alzoba: Maxim Alzoba for the record. Just short notice, we do not have data design in place. We do not have process design in place because it's question on the legal side of things. So it's not possible to create something unified without understanding of the data you are trying to just work with and the limitations to the processes what can do with which part of non-designed yet data. So I'm not sure it's possible to design something which will not be completely destroyed and remastered later. Thanks.

Marc Anderson: Jim final word.

Jim Galvin: So I leave our chair, esteemed chair with a couple of specific suggestions for what we should do going forward. I'd like to see this profile move to being called the registration data. Oh I had a word. Darn it, I already forgot the word.

Man: (Unintelligible) RDAP?

Jim Galvin: Yes I did want to call it profile. It's the registration data specification okay? I had a different word and I forgot it already. And then what we can focus on is let's move into – so that's one issue and that's the way that we want to couch our work in this thing. And then we can move this thing forward and agree that it's the - we want to test the complete technical specification of how data is presented and available to be presented. So that's a good thing.

Then we can move forward with testing credentials. And what we can with credentials is demonstrate for ourselves that we can create different profiles out of that specification of output and we can demonstrate that all of that works. And I think that's what we need for - and with that the rest of the policy

discussions can do whatever they're going to do and we'll all be ready if we can make that work. I think that's kind of my baseline. Thanks.

Marc Anderson: All right thank you Jim and thank you everybody for participating in this ICANN 61 meeting of the RDAP Pilot Discussion group. We can go ahead end the recording and enjoy the rest of your session.

END