DUBLIN – Registration Data Access Protocol (RDAP) Implementation
Wednesday, October 21, 2015 – 12:30 to 13:45 IST
ICANN54 | Dublin, Ireland

UNIDENTIFIED MALE: October 21, 2015. This is the Registration Data Access Protocol Implementation. We are in Liffey Meeting Room 2. This session will run from 12:30 to 13:45 local time.

FRANCISCO ARIAS: Hello, everyone. Apologies for the delay in starting the session. Some of us were in another meeting room. Apparently there was a room change. Let's start. Could I ask if the lights could be lower in the front, so we can see the slides? Has the recording started? Yes, thank you.

This is Francisco Arias and Gustavo Lozano to my right. We both work within the technical services within the GDD (the Global Domains Division) at ICANN. We are here to talk about the registration data access protocol implementation.

This is the agenda for today. Let's start with a bit of history, why we are here. This is about a place in the WHOIS protocol, also known as Port 43 protocol. This is two [inaudible] – or no, not two. Three. So it's not a protocol that has not been there since

the 80s and has many issues. Among others is the lack of [inaudible] format. You can see there just three examples of how it [inaudible] that you have. Not just the way the fields are represented, but what fields are present.

There is no support or internalization, so there is no encoded defined in the protocol. So it depends on what client you're using. You may get what the server tried to send you or not, like in this case.

Of course, it doesn't offer an opportunity for authenticating users. Therefore, you're unable to provide [inaudible] service. For example, you wanted to have one level of service that you would provide to anonymous users, those who do not have any authentication, which is the only option you have with Port 43. And if you wanted to offer another set of information – potentially more information for users that register with you – there is no way to do this in Port 43.

The transport is insecure. There is no support for encrypting the transport. There is no bootstrapping mechanism. There is no way to know what server to query. There are many hacks that are implemented here and there, but there is [inaudible] and there is ways to know where to query so you can get the information they're looking for.

Another thing that may be interesting, for example, for implementation of thick WHOIS is there is a [inaudible] reference so you can point to where the [inaudible] information. For example, the information on the registrar side is present. There is no standard mechanism to say that in Port 43.

We know that Port 43 WHOIS has many issues, but how can we go about changing this? So a few years ago in 2010, actually, there were a series of discussions among the community. Well, I should say that's the latest iteration of this. There has been, of course, many [inaudible] previous that tried to fix this issue, but the latest incarnation of this started in 2010 with a series of discussions in ICANN meetings.

In September 2011, the SSAC (the Security Stability Advisory Committee) issued advice to ICANN recommending to replace the Port 43 WHOIS. That advice was adopted by the board in the same year, and that led to the implementation of a roadmap developed by staff that was put for public comment and was also adopted. That roadmap, it contained a series of steps to get to the adoption of the replacement protocol, which is called registration data access protocol.

The development of this protocol started in 2012 in the IETF. At the same time, they were forced to negotiate with legacy TLDs and some of them adopted the language in the agreement that

requires them to implement [RDAP] [inaudible] is standardized and once they are required to do it by ICANN.

This similar provision is in the new gTLDs. So all the new TLDs have this language. And also in the [2013] Registrar Accreditation Agreement, they have similar language. With this we have coverage in the majority of the gTLD space.

The protocol was finalized by the IETF last March. We now have a protocol that we can request contracted parties in ICANN to implement. However, the way it was defined, the protocol, is you can think of a menu of functionality that you can implement. It doesn't tell you which of the different sets of functionalities you implement.

So for this, we started the task of drafting what we call the gTLD RDAP profile. That profile provides the description of what set of functionality has to be implemented by the gTLD registries and registrars. The first [draft of] this profile was shared with the community just last September in the gTLD tech mailing list, which is an open mailing list and everyone can join, gtld-tech@icann.

So this is what the RDAP profile [inaudible]. By the way, the main topic of discussion in this session. We have the RFCs that define, as I mentioned before, how you go about implementing certain functionality. We have on the ICANN side the consensus policies

that contracted parties are required to implement. For example, the latest one, the [inaudible] additional WHOIS information policy.

We have of course the contracts that the registries or the registrars have with ICANN that define what are their obligations. In this case, with regards to WHOIS, what information they should show when they [record it].

So we put all of this together and we drafted the profile. So the profile is – you can think of mapping the contractual obligations from the contracted parties to RDAP.

Because before, moving into this I should say the profile is mapping only the [inaudible] requirements that are in the agreements. There are certainly more functionality available in RDAP in the RDAP standard. However, the profile is not required in the registry to implement any of these new functionalities. For example, differentiated access or limiting what [inaudible] should be shown in the WHOIS output. It still has the same set of contractual requirements.

If changing that, changing the requirements of what registries or registrars have to do in regards to the output is something that is either would be the subject of either a contract negotiation or policy development process, which is outside of the scope of this

for to just get RDAP implemented so that we can start building on top of the base functionality of the protocol.

So this is how the transition looks like at a high level. I should introduce here the term that is used in the registry and registrar agreements. RDDS, this is the registration data directory services. That's how it's called. And this is referring to the collective of two services that are [inaudible] required in the contracts.

First is the web-based RDDS. This is having a page that you can access – a webpage that you can access in a web browser – so that a common user can query for a domain name and get the information that they are looking for. And of course there is the WHOIS the Port 43 that you access in a common line and get the information.

So those are the current two services that are collectively referred to as RDDS in the contract. So when we do the transition, we will be introducing a new service, the RDAP service, which is what is shown in the middle of the slide.

In the future, at some point, which is one of the open items that needs to be discussed with the community, we foresee that Port 43 WHOIS should be retired. Of course the question is when. I personally think there has to be some sort of overlap in which [inaudible] timing which you have both RDAP and Port 43

working so that you give the users an opportunity to migrate. We're talking about a migration on an [inaudible] scale, so it would take some time. We're talking about, I would think, potentially months – maybe years. Who knows? That's something that needs to be discussed and agreed.

Now, getting back to the implementation of RDAP, this is the timeline – the current timeline. So at this point, we are discussing the first draft with contracted parties and other interested members of the community in the gTLD tech mailing list. If you are not part of it, I'll encourage you to join.

The intention is to close that discussion early in November. So in a couple weeks. And update the draft profile with the feedback received. With that, generate a new version that we will put for formal public comment. So this is the second half of November. That public comment we envision it will run until early January, giving enough time for people to provide input. This will be, like I said, a formal public comment.

The idea will be to have an update, get another updated version of the profile by the end of January 2016. That would be the final gTLD RDAP profile. And once we have that, we can go to the formal list of sending the legal notices to the contracted parties, requiring implementation of the RDAP Service.

The plan is to give the contracted parties six months, so that on August 1st – we envision August 1, 2016 being the effective date when RDAP service has to be turned on by the contracted parties.

And then you can see below that a couple of extra things that need to happen. When developing the draft RDAP profile, we identified a few issues, a few things that need to be developed as extensions in the RDAP protocol. Did I mention that the RDAP protocol is [inaudible]?

You can add functionality to RDAP as need be, so there are a couple fields that are missing in the RDAP base standard that are in the consensus policy. So RDAP contracts, [inaudible] contracts. So we need to add those – I believe three fields. I can't remember exactly. There are a couple fields that are missing and there is already a proposal in the IETF to add those fields. The results [inaudible] issue with the status of the domain names. The RDAP [inaudible] standard defines only so many statuses and there is the latest policy [inaudible] which is very recent. It requires registries to use exactly the same status as EPP. So there is need to add some more status back.

Like I said, RDAP is extensible, so it's not that complicated to add this, and there is already a proposal to add this missing status.

There is also functionality that need to be added in regards to search. RDAP does support searches. However, it's missing some [operants] as required by the registry agreement for only certain registries, I should say. This is not base functionality that everyone has to implement. This is only applicable to certain gTLD registries that opted in during the application phase to implement this searchable WHOIS. So only those that implemented this functionality. We think that that functionality will be slightly more complicated to add to the RDAP, as in it would take more time. Not that it's not possible, but it will take more time to get general agreement within the technical community on how to go about this. So that's why we're putting it later in the future, but we don't think that's a showstopper to start with implementation of RDAP.

There is another thing that I should mention here. There is previous [inaudible] in the context of the implementation of the thick WHOIS policy to bundle the implementation of RDAP with thick WHOIS policy.

In the context of thick WHOIS policy, for those of you who were not this morning in that session, there is a proposal to have three phases of implementation of the thick WHOIS policy. The first two deal with what is called a consistent label [inaudible] display. That is harmonizing the output in WHOIS – sorry, I

should say RDDS as a general term for all these services. Harmonizing the output with what is required by the 2013 RAA.

It has two phases because there is the need to add functionality in EPP, with EPP being the protocol by which registrars pass information to the registries. There is a need to add also an EPP extension to allow [inaudible] for a couple of fields that are not currently passed by most registrars to registries. So the results of functionality need to be added. That's why there are two phases that.

And there is a third phase in the thick WHOIS policy that deals with the most complex case on the thick WHOIS policy which is to actually go – the three TLDs. There are only three gTLDs that are thin. That's .com, .net, and .jobs. Those three we foresee it will take more time to do the migration from thin to thick. There are challenges that go beyond the technical dimension. There is still not even a finite timeline on when that will happen.

So when I say here in this slide that we foresee implementation by gTLDs in August 2016, that's for everyone but jobs, net, and com. Those will take more time before they are required to implement RDAP, once all the other issues are sorted out.

As I mentioned before, there is here open questions, one of which I think we have the answer. We hear from the community

in the previous meetings. Well, I guess I should start with the first one.

The first question is when to turn off Port 43. We need to discuss that, and once we get to the questions and answers section, I will encourage those who have an opinion voice it here.

The second question is where there should be still a requirement to offer web base. This is a webpage for, let's say, the common user to the queries once we transition to RDAP. I think we already hear the community and also within ICANN. When we were doing the analysis, we thought that that is still something that has to be [inaudible] because RDAP was not designed to be focused on the end user. It's not something that is necessarily easily understandable by the end user. It's focused on being very structured, standardize, [inaudible], etc., but not focused on the end user. So for that, there is the need to still offer this web-based [RDs] service.

But I should add that doing the transformation for [inaudible] output like RDAP is to [inaudible] HTML page is something that is not – that is very simple to [inaudible].

So that's why we think the second question is not really open now. I think that's still… The requirement to offer web-based HTML is to remain and that's what is reflected in the current draft of the thick WHOIS policy. Like I said, thick WHOIS policy

implementation on RDAP are considered bundled and that's where this definition is. We are only saying that the only changes that need to be done now are on the web-based HTML output.

I think that's all I have on my side. With this, I will pass the microphone to Gustavo to discuss the draft RDAP profile.

GUSTAVO LOZANO: As Francisco was mentioning, if you go to the agreements right now, you will see that there is term called RDDS. So when you see RDDS and ICANN requires RDAP, you will need to… I mean, RDDS at that point will cover WHOIS Port 43, web WHOIS, and RDAP.

For example, if you go to a new gTLD agreement and you go to Specification 10, you will notice that ICANN monitoring RDDS. That means that at that point in time we are going to start monitoring not only Port 43 and web-based WHOIS, but also RDAP.

So this is just a note, so when you are reading the agreements and you see RDDS, that means Port 43, web WHOIS, and [inaudible]. Next slide, please.

The sections right now that we are in these slides are the main work items for registries and registrars. So what we are trying to identify on this part of the slides is what you need to do or what

is going to be the main work items that you need to do if you are a registry or a registrar.

For example, the profile requires you to provide [inaudible] service under HTTPS. So right now you have all this load in Port 43 and that load is pretty simple to manage. It's basically a TCP connection that is an encryption, but once we start requiring RDAP, all the traffic is going to be migrated to where HTTP is. And if you notice RDAP is basically an API, so you will need to follow all the best practices to manage an API under HTTPS that is going to be open to the public.

So there are some challenges there, so you should be aware of those and you should be considering this, because in the future, it's going to e required to support RDAP.

Another thing that is interesting is we are requiring in the profile that the host name that you use for RDAP shall be [inaudible] related using DNSSEC. Right now a lot of registries in the new TLD world, they have WHOIS that [inaudible] TLD and that's not DNSSEC signed.

So when you start working with RDAP, you are going to be required that that host name is signed with DNSSEC. So that's something else that you need to consider. Next slide, please. This is also important for registries and also registrars. So right now the profile requires you to provide the RDAP base URL for

that registrar. So that means that if you're a registry, you need to get that information from that registrar because you are going to be required to put that information in the RDAP response.

Also, I shall add that in the thick WHOIS policy, the registry will need to show the abuse contact for the registrar. That means that, in addition to this, you also need to collect the abuse contact information from the registrar.

So basically if you're a registry, you need to modify your systems that handles that relationship with your registrar to also get these additional data points. Next slide, please.

Monitoring. Right now, ICANN in the new gTLD space and for some legacy TLDs, we are monitoring the critical functions services like EPP and RDDS and DNS. Those are provided within the service level requirements. So in the future ones, [inaudible] is required by ICANN, we are going to monitor that your RDAP service is provided within the same service level requirements as RDDS.

So this means that usually what [inaudible] internal processes and you should modify those internal processes to handle those kinds of alerts, because in the future, you are going to receive alerts. Hopefully, not. But it's possible that you'll receive an alert for an RDAP issue. So you [inaudible] should be able to understand this and handle these kinds of alerts.

The monthly report. So right now, registries are required to provide monthly reports that basically specify the number queries that you receive in DNS or WHOIS. So we are going to require you to modify those monthly reports in order to add the fields you are seeing in this slide.

The idea is to be able to identify the load that you're receiving on RDAP. You can see the fields. Those are listed in the profile. And if you go and read the profile, you will see what is the definition for each field.

So those were the main work items for the [inaudible] registrar once we require you to implement RDAP. So now we are going to start looking at the basic details, or some extended details, on the profile. So next slide, please.

So as Francisco mentioned, in RDAP you can have extensions in order to extend the functionality. So the profile requires you that if you are going to provide extensions in your RDAP response, you should raise those extensions within the IANA registry. And for registries – and this is very important – if you're going to provide an extension, you need to submit an [inaudible] ticket and the extension basically needs to be approved by ICANN.

If in your register agreement, you are proving searchable WHOIS or you are required to provide searchable WHOIS, then in the

case of RDAP, you are going to be required to support RDAP search queries.

And in the future, once [inaudible] Boolean search in RDAP, then you're also going to be required to support Boolean search in RDAP. This is basically to normalize the functionality of searchable WHOIS within RDAP. Next slide, please.

Consistency. And this is very important. It's possible that you have different databases for RDAP and WHOIS Port 43 and WHOIS web – whatever way you want to differentiate those databases. But the important thing is the information that you present on RDAP, WHOIS Port 43 and Web WHOIS should be consistent.

So if I go to Port 43 and the technical contact for a domain name is Gustavo, then that – if I go to RDAP, that technical contact should be Gustavo for that domain name.

As with other registry services, RDAP must be supported over IPv4 and IPv6. This is already the requirement for RDDS Port 43. It's already the requirement for DNS. So RDAP is also going to be required to be provided under [inaudible] protocols.

Regarding IDNs. IDNs support is a must in the profile. That means if you receive a query that contains a [inaudible] support IDN lookup queries in RDAP.

And also if you have variants or if you support variants, then you need to support variants in the RDAP response. Or in other words, you need to provide a variance in the [inaudible] response.

Thick WHOIS policy phase one and phase two. The RDAP profile already contains provisions to allow you to comply with that thick WHOIS policy.

For example, the RDAP profile allows registries to provide [inaudible] information. Right now, for example, in WHOIS, if you want to provide [inaudible] information, you need to submit an [inaudible] ticket and ICANN will approve you to provide that output in WHOIS.

In the case of RDAP, it's not the case anymore. The [inaudible] is there, so once the thick WHOIS policy is in place, you can just put the [inaudible] information in the RDAP response and that's going to be okay.

Now, as part of the thick WHOIS policy, the registry in the RDAP output and the registrar, they need to provide a link to the WHOIS inaccuracy complaint form. So once the thick WHOIS policy is in place, the registry will also need to provide this information and the RDAP already considers this in the output.

As I was mentioning, as part of the thick WHOIS policy, the registry needs to provide the registrar abuse contract, and the profile already contains sections to allow you to provide this information in the response.

As part of the thick WHOIS policy, the registry and the registrar both, they need to provide that registrar registration expiration date. And this is different from that – registry expiration date of the domain name. So the profile already contains text there to allow the registries to provide this information. Next slide, please.

There are some registries that are not using host objects right now. They are using name servers as attributes of the domain name object. So the RDAP profile contains text and sections to allow these registries or to guide these registries on how their response in that case should look like.

So if you have a registry and you are using name servers as attributes of domain names, then you're already covering the profile. Next slide, please.

There are three TLDs right now that have some provisions for privacy in the WHOIS. Those are – well, I don't remember the exact TLDs, but there are three. Yeah, [inaudible]. So the RDAP profile contains sections that allow them to continue providing

this privacy data, but under RDAP. So for those three TLDs, they're already covering the profile and [inaudible].

As Francisco was mentioning, in WHOIS, there is no bootstrapping mechanism. In the new gTLD world, the bootstrapping basically is based on the name that is standardizing the contract.

So if you want to find information – I mean, the WHOIS server for a new TLD – you just need to go to whois.nad.tld. But in the case of RDAP, there is a bootstrapping mechanism and registries are going to be required to use this bootstrapping mechanism.

You need to populate new information in the bootstrap registry once the service is available under IPv4 and IPv6. That I think is important section from the profile.

Regarding the registrars and the response – and this is a question that we received also when we were developing the WHOIS clarification document. The registrar is only required to provide information for domain names in which the registrar is sponsoring the registrar.

And if you are not sponsoring the registrar, you need to respond with a 404. We received some feedback of why we don't allow that registrars to provide accreditation to another registrar or other RDAP server in case they know that they may have more

information. But the thing is, as part of the profile, we are defining the mechanism. For example, for thin registries that could allow them to say, "Hey, I have this information and this registrar may have other information."

So if we don't have this provision, we are opening the protocol to loops, because for example, that registrar may look to another registrar and then they may look to the registry.

So in order to not get into that potential issues, we're saying that basically if you don't have the information and you are the registrar, then you should respond with a 404.

So these are the open issues that we identified with the RDAP protocol. These open issues are identified in the profile and we're working on solving some of them. So let's see the first one. Next slide.

So as part of the [inaudible] policy, registries are required to provide the EPP status of the domain name in the WHOIS response. So in the RDAP, we have a status in the base protocol, but not all the EPP status are on the base RDAP [inaudible] protocol.

So there is a draft by James [Gould], and this draft, the idea is to create in the [inaudible] registry on the RDAP registry, is to

create this missing status, so that registries can still [inaudible] with the [inaudible] policy once RDAP is required.

So if you go to WHOIS right now, you will see that, at the end, there is a line that says, "Last update of the WHOIS database." So there is no way in the RDAP based protocol to signal when was the last time that the RDAP database was updated.

So this was identified and there is a [inaudible] draft that is trying to address this issue. So basically, we are trying to create a new [inaudible] action that could be used by registries and registrars to say, hey, this is the last time that the RDAP database was updated. Next slide.

Boolean search capabilities. So in searchable WHOIS right now, we have… If you go to the registry agreement and you see that some registries are using searchable WHOIS, searchable WHOIS defines some Boolean search capabilities. Those are the [inaudible] in RDAP right now, so there is… I mean, the community needs to develop a mechanism to support those kinds of search criteria in RDAP.

There is at least one registry that right now defines the external host objects in a way that multiple external hosts [inaudible] for the same name server. So if you have [inaudible] .example.com, that name may match several objects within the database.

RDAP supports name server lookups and the registry agreement requires registries to provide support for name server lookups. But there is nowhere in RDAP to say, hey, this name server lookup matches several items in the database.

So here the idea or the proposal is for the registry to act link member, and in the link member, specify that there is a relation of collection to other objects. I have not sent this idea to the mailing list, but that is one way that we could solve this issue.

And as I mentioned before, the thick WHOIS policy requires the registry to provide the registrar expiration date. There is no support for this in the [inaudible] protocol and there is already a [inaudible] that is trying to address this issue. Next slide, please.

So the profile is required. Registries and registrars, they need clear requirements on what they need to do regarding to RDAP. So that is the idea of the profile. The idea of the profile is to provide with clear requirements that you can follow and you can develop or implement your RDAP service.

We have identified five issues around the base protocol that we need to solve in order to have complete functionality equivalence with WHOIS. And there is still the open question on when we should retire WHOIS Port 43.

So with this, I open the mic for questions.

FRANCISCO ARIAS: Thank you, Gustavo.

JIM GALVIN: Thank you. Jim Galvin from Afilias. I have a comment. I'll respond to the question when to retire Port 43 and I would say immediately. I think there should just be a flag day and cut-over. As soon as RDAP is turned on, turn off Port 43.

Really, the point that I'm getting at is I'm wondering what the rationale is for continuing the Port 43. I mean, strictly speaking, you leave it on until you're told to turn it off I suppose. There's no real issue there as far as that's concerned. But it would be nice to get rid of it as soon as possible.

I really have one question that I wanted to ask. Could you expand a bit on why you would want an [RSEP] in order to include an EPP extension in the RDAP output?

GUSTAVO LOZANO: Well, basically we're trying to match what is in the agreement right now. So in WHOIS, if you want to provide more output or more information in WHOIS, you need to get approval from ICANN through [inaudible]. So we're just trying to do the same

on RDAP. There is no logic there. Just following the agreement, basically.

JIM GALVIN: Okay. Then the comment that I would offer is to go back and maybe possibly revisit that. I mean, let's have a little more discussion about that in perhaps a different forum or in a different way. I mean, I make the observation that presumably if the data there, you've already gone through an RSEP for whatever reason you need to, the input side. So whether or not I add it on the output side, not clear to me why that would matter, especially since with RDAP, everything is nicely labeled. You've got a nice tag value kind of stuff going on there. And the default is if you don't recognize something, you don't do anything with it. So when the client gets it, it's not like you're going to confuse anybody.

I think there's an opportunity there to simplify requirements and we'd like to see that thought about.

FRANCISCO ARIAS: Just to clarify, Jim. I think what Gustavo meant is that you need have an RSEP, registry service – you have to go through the registry services [inaudible] process. And as part of that, you will

cover both. How do you get the information and how do you output it? There is no need to have multiple RSEPs. It's just one.

All that Gustavo was saying is if you are modifying your registry services as your contract already says you have to go to RSEP. It's all that is saying.

JIM GALVIN: Okay. The thing to understand is what quality of changes to the RDAP or the extensions… Are there limits? One of the problems you have in WHOIS now and the way that that output is done is it's all very precise. It's all very exact, because it's laid out precisely in the contracts and all of that. And I'm hoping that we're moving away from that a little bit with this new RDAP protocol. And in that context, there ought to be an opportunity here – some flexibility – to make certain kinds of changes, I would hope, to the data that's in the RDAP that does not have to be reflected back as an RSAP, and in fact require any kind of contractual change. So that particular thing just jumps out at me as something. It just seems overly rigorous.

I'm fine with the idea that, yes, if I'm doing an RSEP anyway and I'm doing a registry extension, and as part of that whole specification, I'll probably include an indication of what's going to be displayed and what's not and the rules that go with that.

But there should be some opportunity for flexibility on the other side for things that are unrelated to anything else that's new.

FRANCISCO ARIAS: I appreciate the comment. I just want to say that this is just what the contract says, section 1.4 of specification 4. It says, "This is a minimum set of…" I'm paraphrasing here. It says specification 4, this is a minimum set of fields that you have to offer. If you want to offer more, you need to get approval from ICANN. That's all it says.

And to your point on retiring a WHOIS, I went and checked, as Gustavo mentioned, registries [inaudible] currently required to provide a report that includes the number of queries they receive. Two of the field that are required are the number of queries they receive for web WHOIS for Port 43.

You might find it interesting that all the new TLDs, since they started reporting this in October 2013 when the first was delegated – the first four were delegated – and until September this year, which is the last report we have received so far. It's 2% of the queries are web-based WHOIS. So 98% are Port 43.

Andrew?

ANDREW SULLI VAN: I don't know if Scott was in line first.

UNIDENTIFIED MALE: I don't know that we have a line. [inaudible].

FRANCISCO ARIAS: Go ahead, Scott.

SCOTT HOLLENBECK: Scott Hollenbeck, VeriSign, and one of the coauthors of RDAP. I'm not going to comment so much on the bits that you have in the profile. I think there's a lot of technical detail there that reasonable engineers and policy makers will be able to find answers to.

But I am concerned significantly about a couple of things that aren't in the profile. We undertook the work to develop RDAP specifically with the goal of addressing many of the issues with WHOIS, one of which you identified – the issue of data privacy and internationalization. I'll leave internationalization off the table for now, but let's talk a little bit about data privacy.

I was also a member of the gTLD Directory Service Expert Working Group that produced a final report recommending that some steps be taken to provide ways of implementing [gated] access. We've got features in RDAP will allow us to do that.

As currently specified in agreements and in the profile – and remember, the agreements were written prior to the existence of these capabilities existing – we will perpetuate the issue that WHOIS has with all data including PII being available to anyone who wishes to ask.

I would caution this community to give serious pause to perpetuating that model and instead consider an approach that allows us to address that particular deficiency using the client authentication capabilities that are available in RDAP.

We have the ability to know who is asking, why they are asking, and any number of other features associated with the query and return an appropriate response based on the authorization of the client to receive that information. So I'd like to throw that out there for discussion.

Point number two. We use the IETF process to develop these protocol specifications and we have a longstanding practice within the IETF of using Internet draft documents and RFCs to document implementation profiles. I'd like to also encourage you to consider documenting this profile in an Internet draft and using the IETF's consensus-building process to gain a measure of consensus on the approach. Thank you.

FRANCISCO ARIAS: Thank you, Scott. As a quick answer to your questions, the first one in regards to adding more [inaudible] to the RDAP profile, particular support for [inaudible] access. That's something that is available for individual registries to go through the process that already exists in ICANN. If they would like to change that part of their service, they can go through them. I'm not entirely sure. I'm not the expert here. But RSEP or the WHOIS – I'm looking at [Krista] and she may remember the WHOIS policy for [inaudible] with local law or something like that.

So there is a way that registries have – individual registries have – to amend their agreements so they can offer this differentiated access as [inaudible] – I'm not sure of sure her name – went through the process or it was like that from the beginning. But [inaudible] I believe they went through the process to modify their agreement to have this differentiated access.

Certainly, if there is appetite in the community to have this as a solution that everyone can offer, then the obvious [avenue] will be through the policy development process within the GNSO.

Regarding the other question, the other suggestion on having the profile documented as an IETF document, I just wanted to explain why we did it the way we did.

We did consider going through to write this as an internal draft within the IETF. The thing is this document [inaudible] place. It's

half technical and half legal. It's mapping the contractual requirements to a technical framework.

So we thought that perhaps the IETF will not be the ideal place. I certainly agree that the document has to have community consensus on that's the right thing to do, but I think IETF is not the only place. ICANN is also a good place where we are used to get consensus on the community before publish something and require people to implement.

I'm not saying no. I'm only explaining what's the rationale that we are using and I'm certainly happy to hear what others think about this topic. Thank you.

Andrew?

ANDREW SULLIVAN: My name is Andrew Sullivan and I work for DYN. I want to follow-up on that thread just a little bit more because it seems to me that the discussion here is starting from the premise that the existing WHOIS contractual requirements are the right ones, and then what you want to do is re-implement that in RDAP.

From my point of view, that is exactly backwards. We did all the work that we did on RDAP precisely so that you had these features so that you could get rid of the stupid hacks that are in

WHOIS today. It's a mess, and the reason it's a mess is because WHOIS didn't have these features.

So we built the features so that you could do this, and now what we're going to do is re-implement WHOIS and RDAP, and in five years, we're going to be going through this again. It's just a mistake, and what we should do instead is use the features in the protocol in order to provide these things.

With another professional hat on, I'm part of the IAB, but I'm not speaking for them right now, but the IAB has been pretty clear that privacy on the Internet is a really important thing. I'm really heartened that you're saying no, it's HTTPS all the time. Excellent. But keep down that line and say stop publishing this stuff to anybody who comes. Now we get additional features. Features that are already built in there, and they were built in precisely to solve this kind of problem. I really urge you strongly to look hard at the existing agreements and see what stuff could be done in RDAP according to the existing agreements and have a plan to get away from the hacks that we've got in WHOIS so that over the long-term, we can actually implement a protocol that solves the real problems that people have.

I'm not trying to say try to get things in or out of the WHOIS and I'm not trying to re-litigate the entire WHOIS discussion of the past 900 years here. But I am trying to say that we ought to have

a serious appreciation of the new features we have and let's have a plan to do a real registry data service. It will be a great thing. Thanks.

FRANCISCO ARIAS: So a quick response on that, Andrew. You said you were – I think I hear you saying that we may not have the right provisions in the contract. I'm not saying whether have them or not. It's not for me to say. We have what we have. This is the [inaudible] space that our [inaudible] and we have to follow that.

What we are saying is… What we are doing is just mapping what is there now. If we want to have this new functionality of differentiated access, then we need to go through the processes we have here in ICANN. So [inaudible] I see is we either implement RDAP now, what we… I think has to be something like what we have in the profile [more or less]. Or we wait. Who knows how much time before once all this set of policy issues are sorted out and then implement the right solution.

I really advocate more for the good enough than the best. That's all we're trying to do here.

ANDREW SULLIVAN: And I think what I'm trying to say is I appreciate all of that, and I am not trying to say let's not do anything while we wait for this.

But what I do think is that this document can c all out "here are a bunch of things that we're explicitly not doing and here is how you would do it if this capability were there."

Then you could take that to the policy side of the house and say, "Look, we've got this capability. It's already here. It's ready to go. And we've written the way to do it." Then you would just be able to turn it on if only the lawyers can agree to do it.

But what will happen if you go with this platform, yeah, but it may contain this stuff and so on. I want these features to be part of the profile turned off, because what you said before is individual registries can go through this process in order to reduce this. That's the default privacy off. I want default privacy on. I recognize that there is a legal-political problem here that is not part of what we should be discussing here. But I want this profile to have all of the facilities for the advanced use, so that… And my read of it is that it doesn't yet.

Well, this is just a may. I want to know how do I signal, for instance, I have this or I don't? What are the rules for that? And it doesn't seem to me that that's complete there. I'm willing to send text if you want.

FRANCISCO ARIAS: Sure, please and thanks. I think we have two more people in the line and then… Yes? [inaudible]? Okay, sorry.

STUART CLARK: A question and a comment. Question regarding the bootstrapping process. From an implementation perspective, when is that expected to be up and running from an implementation perspective? And from a comment side of things, the idea of freeing the reign for how [extensions] might be returned. The only caution I would have from more of a user's perspective is if it became a complete free-for-all, then some of the nice aspects of knowing how to use the system – for example, in a machine reader or [inaudible] may become more blurred because not necessarily knowing what different registries return and if there is any requirements for standardization and so on.

There's probably a middle ground between the two approaches, but I just [have] some caution on that.

FRANCISCO ARIAS: So regarding the question on the bootstrap mechanisms, I must confess I don't remember if it's already working. Maybe there's a lot of people here – Scott, no? Do you know?

SCOTT HOLLENBECK: Sure. There actually are some entries in the IANA registry right now, like for .br, .cn, and I think there's one other one. I should note that while it is possible to bootstrap queries for domain names, it is currently impossible to bootstrap queries for entities.

So if you are trying to, for example, start with an entity handle for a registrar or registrant identifier, we have no mechanism in the specifications or in the registry that allows a client to know where to send that search.

That's a limitation of the protocol, a battle I lost in working group discussion. But it is what it is.

FRANCISCO ARIAS: Thank you, Scott. Yeah?

[JEFF NOKES]: Jeff Nokes with Symantec. A clarifying question. One of the requirements is that access to RDAP will be through HTTPS. Is the intention there that anybody who hits that web server is flipped into an SSL session or is the intention that the registrar has to have an account management system that people log into and that is what turns on the SSL?

GUSTAVO LOZANO: The first one. The first option.

[JEFF NOKES]: Thank you.

ALISSA COOPER: Hi, I'm Alissa Cooper. I'm one of the applications and real-time area directors in the IETF, which is the area where the RDAP protocol was specified. The role of the area directors is to do kind of the final check at the end when we're standardizing something new in the IETF. And in the case of RDAP, as Scott can attest, as much as the working group wrestled with many of the tricky technical issues, in its process we also had a lengthy discussion around some of these differentiated access issues when the document finally came to the end of the process. So I wanted to speak a little bit to what Scott and Andrew were saying and really support what they had to say.

I think the intention of everyone in specifying RDAP was that this differentiated access capability would be used and that client authentication could finally be leveraged as it is for many other kinds of sensitive transactions on the Internet. So I think it would be an extreme shame to not leverage that.

I fully appreciate that just because you specify something in a protocol doesn't mean that changing all the contracts

associated with its use is as simple. So fully appreciate that. But I would say if it is the case that you go down the path of doing a kind of limited profile like this that doesn't require support for these features, that at the same time the best practice profile also needs to be specified, so that even it's not contractually required, then everyone knows precisely if they're really going to be a good actor in this space how it is that they're supposed to use client authentication and execute on the differentiated access capabilities. So I think that's the absolute minimum standard here.

I would also as to the question of an informational RFC, another option that's always open to people is even if you go about having this policy document in ICANN, we can also do an informational RFC, and I think again that – very often when we specify a protocol and we have implementers who come with implementation experience and want to kind of document that, the informational track in the IETF is a very good for that place.

So it's not the case that it's an either/or is all I'm saying. Even if you go along this path of having this process that having an informational RFC where the folks who were part of the protocol development can also have input and review and provide that into the document I think would be very beneficial for the whole community.

FRANCISCO ARIAS: So regarding the second question on the draft and having input from technical experts, that's [inaudible] possible here. This is an open discussion. Anyone can participate. The [inaudible] mailing list that I mentioned is open to anyone. You don't have to be a contracted party to express your views there. And many people that are not a contracted party do speak there, even people from the IETF that are not linked to contracted parties as far as I know.

So we do – we also have an open discussion here that is… When we move to the next phase which is public comment, it's also an open discussion. Anyone can join. Like I said, I'm not saying no. I'm just thinking on what is that we win by publishing as an informational RFC, whether there's no formal working group. What is it exactly that we're winning when we can have still consensus within the different parties that – not only the ones that have to implement it, but also anyone in the community also here.

ALISSA COOPER: Yeah. I'm not really speaking to the openness of the process, just that it's in keeping with IETF procedure that we specify a protocol and then a bunch of people go out and actually use the protocol. They have some implementation experience with it,

which is sort of like this – almost, not quite. And then it's nice to have the accompanying RFC that says, "Well, here's how we actually decided to use this thing." It's a very common way outside of RDAP, outside of the applications area. We do that all the time. So it just would be a good idea is all I'm saying. Not because of this process is different or better or worse than that one.

FRANCISCO ARIAS: Okay. Point taken. And regarding the first comment that you made, I just wanted to clarify to see if I got what you were suggesting. You were saying it would be good to have a set of best practices on how to go about differentiated access. Is that what you were suggesting?

ALISSA COOPER: I guess all I'm saying is if you go down this path of specifying a profile which is really being driven by how can we make this work within the existing constraints of the existing contracts as opposed to what I assume people would think is the ideal case, which is if we didn't have these contracts and we could just have a document that told the world what's the best way to implement this thing, those two would probably end up looking very different – not very different. I hope not too different. But it sounds like somewhat different.

So what I would encourage you to think about is at the same time that you're doing the minimal "this is how we can do it in the constraints of the existing system" also do "this is the best practice." And if those are not the same, then having them both documented I think would be of great value.

I would still prefer… I'm still with Andrew that I'd rather not do this at all. But if you feel that you have to do it… And I'm not one to speak about this. This is way outside of my technical area. I am not a DNS person and I know that the PDP process is hairy but I've never participated in it myself. So if you feel that you have to go down this path, then all I'm saying is do both of those at the same time.

What you don't want is people to think that this is the end of the line and nobody ever uses these new capabilities that we worked really hard to get.

FRANCISCO ARIAS: Good point. This is certainly not the end of the line. There is already an effort in the policy development side of ICANN or in the gTLD policy development side of ICANN in GNSO. I think it's called RDS… I'm sorry, I can't remember the name. But there is a policy development process which [inaudible] that is built in on a set of recommendations that came from the Expert Working

Group on directory services or something like that which Scott was a big part of that.

There is already a policy development going on on ICANN to rethink on a wider scale what to do about directory services, how to change that drastically, not just evolution which is what we're trying to do here, going slow with the tools that we have at hand. I forgot the other thing I was going to say.

ALISSA COOPER: So that's good to know. I would just, again, think… Just talking about support for client authentication could be viewed as an incremental step and not this long-term evolution thing. So what belongs in which bucket I think is a good question. Thanks.

FRANCISCO ARIAS: Thank you. I'm not sure if it was Jim or Richard who was first.

UNIDENTIFIED MALE: Yeah, I'll just go. So we have a long list of technical questions that are probably better off sent to the gTLD tech mailing list. But the one question I did have is in the slide deck – and I was a little bit jetlagged watching that slide deck, so I apologize about that. But there was the three different phases of development. One is current state and then short-term future and long-term

future. And I think web-based WHOIS was present in all three of those. And I'm wondering if that's going to be true even for the long-term. Then what's the value of having these enhanced features in RDAP of the same… If the privacy features is only available for RDAP, web-based WHOIS is still exposing all this PII. What's the value of that?

FRANCISCO ARIAS: That's a very good point. RDDS is a set of services, as described in the registry agreement. Port 43 is the one that we are clear that we're trying to shut down in favor of RDAP. But Web WHOIS, there is still the question on where that should be and we think we have heard the committee saying that should still be there because RDAP is not about the end users.

Perhaps the one thing that is missing is to say that the set of differentiated access if a registry has, has to be mapped into Web WHOIS.

The reality is the three gTLDs that have differentiated access, if memory serves, they are required to implement this only in the web-based WHOIS because that's the only place that they implement it to begin with.

But perhaps there is some [inaudible] that is missing so that we say you have differentiated access capabilities in there that has to be mapped into your web-based WHOIS service.

UNIDENTIFIED MALE: So I'm unclear what the distinction would be at that point.

FRANCISCO ARIAS: RDAP is not for the end users. It's JSON. If you look at that, most of the end users probably will never be able to understand it.

UNIDENTIFIED MALE: So the differentiation is just that last presentation layer and that's it? Okay.

FRANCISCO ARIAS: Jim?

JIM GALVIN: Jim Galvin from Afilias. So I want to just take a step back. I should first say thank you, Francisco and Gustavo. I really did appreciate the presentation. I think other did, too, in the room. I think you guys did a very good job. And I like the way you highlighted the changes, and in fact work items for registries and registrars. I just wanted to give you credit for that up front.

I wanted to tie a couple of things together here and make hopefully a constructive suggestion for you to think about. I appreciate that the obvious thing to do is roll out RDAP and do it the same way that WHOIS is done. I mean, that's just sort of what you do, right? It just seems very obvious.

The problem is it really does feel like a short-term. It's sort of a short-term thing to do. Obviously you've heard the message around here in a couple different ways. I mean, I asked about the RSEP. Scott asked about the differentiated access. Andrew talked about privacy and Alissa did, too, to some extent.

We're down this path because we wanted something different and we were looking for the future. We really had a long-term goal here.

I think what's important is even if you believe that you can only go down a short-term solution which is to present an RDAP service that looks exactly like WHOIS did, I would suggest to you that you should frame that presentation in the context of a much bigger picture and indicate that you really are going to honor the long-term solution that was in progress here and what we were looking for.

Indicate what the next steps are going to be – the next three or four things – and the next projects or initiatives are going to take place to solve those problems so we can all feel a little better

about that, that we've done all of this work and this is not the end. So in the future, when you do that, I would encourage you to do that.

And I'll end just by saying that frankly I'm really not convinced that your only opportunity here is to propose an RDAP service that looks just like WHOIS. I'm not a lawyer. I'm not even going to try to pretend to be one and I'm sure you've done a thorough analysis on that. But I think I'd probably like to see a little more references so that we can share it with our internal counsel and lawyers to really examine whether or not we agree with you that we are obligated to stick with this particular model. It would be nice to have that discussion somewhere, which brings up the observation that gTLD tech is not really the right place to have all of this discussion. There are parts of this discussion that need to happen elsewhere and we'd ask to do that, too.

So, two things. Always couch it in a bigger picture. Frame it in a bigger picture. And two, we'd love to see the references, the analysis that went with why this is your only path and only solution. Thank you.

FRANCISCO ARIAS: Thank you, Jim. So regarding the big picture – sorry, the future work. As I mentioned in a previous comment, there is already that place where you can have that discussion because it's

policy work. And I apologize because I cannot remember the name. I think it's RDSBP that just started.

That's the place where you can have the discussions about what's the level of access that should be there and other deep discussions on the topic. Anyway… And thanks for the other suggestion.

Anyone else that would like to speak? Yes, [Eduardo]?

UNIDENTIFIED MALE: We have two questions from remote participants. First one is [Brian] [inaudible] from Google Registry. He asks, "If we have name servers as separate objects rather than as attributes of the domains, are we still prohibited from including those fields? I don't have the profile in front of me, but I thought it had implied that we would include the information.

GUSTAVO LOZANO: No, that's only for registries that use name servers as attributes, not for [inaudible].

UNIDENTIFIED MALE: And a second question from Jason [inaudible], no affiliation. "Is there already a .js or other code fully available to register JSON as a nice user-friendly webpage?"

UNIDENTIFIED MALE: There are some Firefox plugins that will pretty print JSON responses but I think that's as good as it gets right now.

FRANCISCO ARIAS: Okay. So we are two minutes before the hour – oh, [Krista], gave me the pointer. It's called a PDP on Next Generation gTLD Registration Directory Services, RDS. So it's RDS. Thank you.

So if you're interested on the policy discussion on how this directory services look like, [inaudible] current set of contractual policy requirements, that's the place to go in GNSO.

So with this, I would like to close the session. And thank you, everyone, for participating.

[END OF TRANSCRIPTION]