ICANN
Transcription ICANN63 Barcelona
GNSO – Understanding the RDAP and the Role it can play in RDDS Policy
Monday, 22 October 2018 at 1030 CEST

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.

Rick Wilhelm: All right, good morning, everyone. This is a session on RDAP and understanding RDAP and the role it can play in RDDS policy. Welcome to ICANN 63, 22nd October 2018. I'm Rick Wilhelm for the record and we're going to have a panel style interaction this morning. We're going to do some opening presentations that will take some chunk and certainly not the entirety of the time. So please be preparing in your notebooks, or your laptops, or whatever some form of questions because that way we can carry the discussion forward. Because the most interesting part of this discussion will be your questions.

I have here on the panel along with me, from your right to your left, I think, Roger Carney from GoDaddy. I think it's about the direction not about the person. That's definitely Roger Carney from GoDaddy, Francisco Arias from ICANN staff, Stephanie Duchesneau from Google, Mark Svancarek from Microsoft, and Jim Galvin, fresh off the plane, from Afilias, looking fabulous and desperately in search of coffee. If you want to be at the top of Jim's gift list for this holiday season, bring a double espresso and you're guaranteed to get there.

So without further ado, we're going to flip into a couple of slides. So the style of our meeting this morning is going to be a few slides from each of the panelists, and then as I mentioned open Q&A. If you're a member of the RDAP working group, RDAP pilot working group, you can certainly please come join us at the table. And then you can also be one to participate in the Q&A as we go forward. But like I was saying, as we go through these

presentations, please take your notes throughout the Q&A so that we can have a lively discussion subsequently.

So we'll go ahead and flip the slide and let's go ahead and go in. These are some slides that I have to thank Francisco for helping to assemble. We repurposed some slides that we had previously used at some ICANN meetings were used in its purest form. As software engineers, we all appreciate that. So you can go ahead and - so I've got a slide in the Adobe Connect that's different than what I see on the screen in front of me. Is that a bug or a feature? That's okay. It's no problem. I'll look at the Adobe Connect. But the Adobe Connect and the screen behind me are out of sync.

Person with black shirt WHOIS walking with purpose and knows what he's doing. Okay. While he's doing that, I'll just talk about the first slide, which people on the Adobe can see, and now, you can see it too thanks to the magic of whatever he did to the display properties. Okay. So there have been a number of well-discussed issues with Port 43 WHOIS, which you can read here on this slide.

Some of these have been identified in various documents in and around the ICANN community. Perhaps, most importantly there was SAC 051, which is published by the ICANN SAC in 20117. However, prior to that, dating back all the way to 2002, SAC 003 was published which dealt with issues in and around WHOIS. First version of that was December 2002. It was updated a few months later in 2003. There is also SAC 027 and SAC 003. Those are both published in 2008. Make for interesting reading mostly about the issues about how long ago we've been looking -- we the ICANN community -- have been looking at the WHOIS challenges.

027 mentions, when you go back and read that, you'll read about something called the, CRISP, C-R-I-S-P working group and it mentions a set of RFCs built around a set of protocols called IRIS, I-R-I-S. You'll notice that those are

not the same set of protocols we're talking about now. RDAP, because the community elected to solve the problem in an entirely different way.

But these problems that you can see here have been around with us for a long time. WHOIS is a very old protocol. Its RFCs date way back to the earliest days of the internet, three digit RFCs and such. These here aren't a full compendium. They're not a ranking. Not all of them are explicitly identified by ICANN SSAC but they are all issues that have been identified from time to time by various members of the community.

You can go ahead and flip the slide please. Connection lost. Computer. So the next slide is going to be about some of the timing related of ICANN, the implementation of RDAP. Here comes the guy with his very purposeful walk again. Now, with the black squiggle above his head, frustrated at the Wi-Fi people because his displays are working brilliantly.

So in the RDAP implementation, in and around, this slide is going to talk about the implementation of RDAP in and around the gTLDs. One of the things that's worth noting is that while we're here focused on RDAP in and around gTLDs, RDAP has been implemented also in the RIRs, the regional internet registries in and around numbering. And it has been a collaborative effort between the domain name community and the ICANN - and the numbering community also.

So that's an important thing to remember. One of the reasons that RDAP is structured the way it is, is that it's designed to accommodate both of these use cases, domain name registries and number registries. That's an important thing to realize. And the other thing that it's targeted for is actually only those use cases, unlike other directory access protocol mechanisms, such as something like LDAP. RDAP is only tailored towards registries.

When the slide comes up, one of things you'll see is that it has a timeline that speaks to come back in September of 2011, SAC 051 was published. I

mentioned that prior. And then there was a board resolution to adopt the recommendations put forth by SAC 051 only a little bit over a month later, in 28 October of 2011. So that would actually be about seven years ago at the fall meeting.

And then in 2012, there was a roadmap that ICANN staff published to implement that. And then there was some work put forth in the IETF that was starting the RDAP protocol development. A lot of work went on subsequently and it wasn't until 2015 that the actual RFCs were published. It's a gap of about three years until March of 2015 for those RFCs to be completed. So you can see that it takes a while to get things through the IETF process

And so then subsequently, there was a document called the RDAP profile that was published in 2016, about a year later. And what we have updated recently was the - that version of that document. Now, when we go to the boundary between 2015 and after the profile, there was something called a request for reconsideration. And Sue, you can flip the slide in the other window. For those of you who are following along in the Adobe Room, you can keep up with this. It did? Okay, we'll let that propagate.

So there's a timeline there about the request for reconsideration and that was accepted. And so then the - which called for the delay of the implementation requiring removing CLND from - removing RDAP from the CLND policy. Now, as we go-forward with this, one of the things that was interesting was that during the RDAP profile development that ICANN staff that was working with the RDAP pilot working group, one of the things that's interesting is that the group had to respond to the development of the temporary spec.

And so that happened during the spring of this year. Okay, let's keep going. You can go ahead and flip to Slide 8 please. Let's go ahead and talk about some features. Are going to have any luck showing this on the screen? We're trying. We're trying. I'm sure there's a bit of comedy in here somewhere. We're looking for it.

So from the perspective of RDAP features, RDAP, we've got a set of five different RFCs, 7480 through 7484, and it provides a number of things. The key things it does is a standardized way to query the registration data. It provides JSON formatted queries and responses. And unlike WHOIS, it provides a query and response that occurs over HTTPS. So that's really one of the standard protocols that the web runs over. And it's extensible, which is important, and it also allows differentiated access via some other features that it enables.

You can go ahead and flip to -- all right -- you can go ahead and flip to Slide 9 when you get a chance. One more please. Should look like this only without the ink on it because your version doesn't have my underwriting. One more maybe. It shouldn't have the block. Two of two. Okay, very load. We'll let it update in a second. We're rolling now. All right. Wi-Fi gremlins dispatched.

All right, fingers crossed. Okay, and then the Connect will catch-up in a second. Okay, so we've got some other features here that now you can blissfully read on the screen as everyone's neck pulls up from their laptops. It's got a bootstrapping mechanism. It's got a way to be able to find the authoritative server for given types of queries. We talked about that it's built on top of well-known web protocols. It also has internationalization support, which is something that WHOIS doesn't, and it has a basic capability of searching capability.

You can flip to the next slide. I want to keep going so I can get to our other presenters. Are we good there? Okay. We're good. We talked about internationalization in both queries and responses, JSON formatted. We discussed that and we're going to keep going. Doing a good job of talking ahead of my slides. Last, I believe, two more slides here to go. In terms of bootstrapping, one of the things - what this means is that without any information, where do you know to go find the query? Where do you know to go find where to query something?

So with new gTLDs there's a standard way that you can read here on the slide, WHOIS.nick.tld. Now, in RDAP, there is a mechanism that there's a bootstrap thing that's built-in with registering with IANA to be able to provide the way to find these things. So what happens is, is that you put your data into the IANA registry that you can see there at the bottom of the slide, data.iana.org/rdapdnsjson. You pull that out of there and that's a way to be able to bootstrap it. This is important for scalability because it doesn't require relying on the convention of the WHOIS.nick.tld. While that's important and useful, it's only a contractual mechanism and doesn't provide important technical flexibility.

You can flip to the next slide. Then also, one of the things that RDAP does is provide a referral mechanism for situations where there's thin data where it allows a referral using standard HTTP mechanisms, where the registry RDDS and data service only heralds a referral to the registrar. And what it will do is along with providing the data for which the registry is authoritative for, it can send a referral for the registration data down to the registrar and have the registrar provide that authoritative.

RDAP also allows for the response to be provided in the thick registry using that, where the registry can provide the thick response. So it allows for both models to work seamlessly in a transparent fashion.

And I think that we have one more slide. If we go past the divider. Good and flip. We're fine. So this one is about implementation status. The temporary spec calls for RDAP to be implemented as part of it, with implementing the requirements of the temporary spec. Yes, the one right after this. Yes, this one here.

And then we had a public comment - the RDAP profile was out for public comment. That public comment period closed last Saturday, 13th October and there's work that's ongoing on RDAP SLA and registry reporting

requirements. The RDAP public comments are available for everybody to view out there posted in the usual spots. Work on the RDAP profile is ongoing. The RDAP pilot working group is meeting weekly to both address prior comments submitted by ICANN staff, as well as to review the comments that were submitted by the public.

So that's a quick overview of some things and then now, I think we're going to go to Stephanie and Mark. And we've got some slides from them so we'll go ahead with them.

Stephanie Duchesneau: I made the slides this morning so if they don't show up, they don't show up. So one thing worth emphasizing from Rick's presentation is that the launch of this pilot effort occurred prior to and was distinct from the effort to GDPR proof WHOIS operations. And the real origin of this was that ICANN was anticipating the development of the successor protocol and included very general language in the registry contract and specification for it that said registries would have to provide a reasonable implementation period, implement the RDAP once it was finalized by the IETF.

Of course, this language is really high level and doesn't deal with any of the technical or implementation requirements. So it was sort of put back to us to work in collaboration with Francisco over the past year or so to get a standard profile for what these consistent technical requirements around the RDAP was going to look like.

At a high level, what the profile working group has been doing is answering the question of what elements of the protocol were going to be implemented in the context of a domain registry. And the advantage of the pilot approach is that it was also going to allow registries to conduct some experimentation with the different features that were provided by RDAP in advance of having to sort of drive a consistent set of requirements for it.

But importantly, the goal here was never to set of change policy around WHOIS or registration data. It was just to mirror both what I call the big P policies and consensus policies, as well as the little P policies, so the requirements that already existed in the contract, applying these to the new protocol.

Mark Svancarek: So are the slides - current status, temp spec plus EPDP. Thanks. Okay. So here's a small list of some policies that could be changed during the EPDP process or subsequently. And it's not meant to be completely definitive. I see Alan and Steve in the audience so if there's anything I miss, jump up to the microphone, and just add it on.

So here's a few things that might change. For instance, should the tech and admin fields be treated differently from the registered name holder fields? And by differently, there's a couple of versions of differently. They could be entirely removed. They could be revised. They could be (smallified). They could be combined. They could require consent. They could be optional. Those things would impact the response profiles.

Should we apply different rules for legal versus natural persons? So you would have to capture that somewhere during the registration process and that might need to be reflected in a response profile. Would adding country codes to the RDAP responses help with jurisdictional balancing test evaluations? If so, we would have to figure out how to add country codes. If we do need to collect user consents for the processing of data field and that could be any data field, not just the admin and tech contacts that I mentioned before, although those are really the only ones we're thinking about. How do we need to change the profiles?

What about maybe not providing contact information or just saying redacted. What if we provided a contact ability field? So a link to a web form or an anonymized form of the email. If we did that, we would have to figure out

how to do that in the response profile. There's a field called remarks that's being discussed for instance.

Should the response profile include information about requesting redacted data? So right now, if you want data and it comes back - and your query comes back as redacted, a lot of people don't know what to do. And to some people in the room you say, well, it's obvious. Just go to the abuse contact information. That's always public. That's always in there. But actually, most people don't think to do that. I've encountered quite a few people who say, oh, I just thought I was out of luck. I didn't know I had any recourse at all. And then of course, not everybody is using the contact field to support these requests.

So it would be nice if we had a standard way to do this, which would probably need policy and then that would have to be expressed in a response somehow. And then something that's not related to EPDP but is a pending policy is IDN variance. If you've been following the IDN world, you know that IDN TLD variance has been investigated a lot. A proposal was put out earlier this year for feedback. It's not policy yet. There's still things to work out but that's a pretty interesting thing if you're in the IDN world and we would have to figure out how we would support that in a response profile.

Two sort of general things that are related to the temp spec and the EPDP. There's a term in the temp spec called reasonable access. Reasonable access is sort of like commercially reasonable efforts. It's a term everybody kind of understands the intent of it, but the specificity of it will need to be determined. And so authorization and authentication models will be related to this reasonable access discussion.

So how do you determine who a person is and what permissions they have to which data under which circumstances, if a balancing test must be performed under the law or whether the data can be delivered without a balancing test. Those sort of things are related to reasonable access and I'll talk about this a

little bit more in subsequent slides. So just keep that concept of reasonable access in your mind.

Stephanie Duchesneau: So I'm mindful that so much of the policy underpinning WHOIS, their domain registration data is in flux, and all of the ways that Mark covered. It might seem surprising to look at the version that went out for public comment. And the goal here is - which largely just describes the current state of play, the current state of operations and that was the intent. The goal hasn't changed much with the version that just went out from when the pilot was originally launched. It was to provide the set of technical requirements that were going to underpin the provision of registration data. We're not dealing with any of the policy questions that Mark had covered.

There was a pivot in the work of the RDAP working group that Rick covered also, where we did shift to incorporating the temporary specification for relevance because this defines the new minimum set of registration data that registries are required to put forward. But when you look at the version now, we're not trying to seeking to address the questions that are still in play.

Importantly, lost track. Yes.

Steve DelBianco: Rick and Stephanie, would you take a question from the floor just while you're finding your track?

Stephanie Duchesneau: Sure.

Steve DelBianco: This is Steve DelBianco at the BC. The response profiles that were proposed by contract parties and that we commented on, they did include an element of policy. Every time we saw the word must or may in a response profile, well, that is policy. Maybe it's small P, right.

Stephanie Duchesneau Yes, little P policy.

Steve DelBianco: And that's fine. And Stephanie, you know, and Mark who is with me in the BC, that we did not attempt to indicate policy in our comments to all of you. But where you said must or may, we reacted to that. So there is some policy involved. Let's just own it and have that debate today. And then with respect to reasonable access that is individually determined by each and every registrar and registry, a couple of thousand of them, as to how they would grant that subject to their own risk profile and applicable law. And that is a different kind of policy.

And it's unclear to me how RDAP could assist at the provision of reasonable access unless a registrar received a request by whatever means it asked for. It analyzed its legal risks and then decided -- a balancing test -- and then decided to provide an answer. Well, they might just send an email back to the requester or they could give the requester an authenticated credential so they could grab it through RDAP. That would be great too but I don't think people will wait for RDAP to provide that sort of tiered access. They'll just, in a reasonable way, return the answer to the requester. Okay, thank you.

Stephanie Duchesneau: Yes, and I think in response to the first part, the goal with where we've put must or may is to reflect things as they currently are in the temporary specification. There was no effort to change the existing requirements around that. I think there's a couple of places that in response to the public comment were going back and revisiting if the correct language was used.

Rick Wilhelm: Yes, there's a couple of - Rick Wilhelm for the record. There's a couple of spots and we will scrub it, Steve. That's a fair point that we will be reviewing for. But typically, in the RDAP profile document when we're using those, we're using them in the IETF sense for complying with where we need them in compliance with the RFC. So complying with the RFC where the RFC uses must or may.

So it's moving in that direction where there's spots in the RFC where the RFC uses those words. Now, we will go through and make sure that the uses of those are - and we might have to do some referencing in order to make clear where the must and the mays are pointing. And I'm not sure if it's downstream or upstream, what the correct term would be, towards IETF direction or towards policy, ICANN policy.

Steve DelBianco: Thanks, Rick. Steve DelBianco again. That's very helpful. I started to stand up when Stephanie said we were reflecting the must and may per the temp spec. You've corrected it to say we do must and may to reflect the RFCs. But it's important to highlight what the RFC would say about a must or may, and Stephanie, we should indicate what the temp spec said about it. But the temp spec is not policy. We're in the middle of the EPDP to determine what policy is and the temp spec isn't policy. It's temporary for compliance purposes. But it's great to be as transparent as we can. Here's a must and may with respect to fields that are blank.

And a must or may, what does the RFC say, what does the temp spec say, and then it's an invitation for the community to determine what we'll do in the policy we develop, not only for the replacement of the temp spec with consensus policy, but also for a unified access model that would truly leverage RDAP in the way in which to do that in a single standardized way. Thank you.

Jim Galvin: So Jim Galvin for the record and speaking as an RDAP pilot working group participant, I think Steve that you're asking some really good questions and I think it's important that you continue to ask those questions and others should ask it too and look carefully at the output from this workgroup.

One of the discussion points that we've had in the group is this distinction between technical issues and policy issues, and it's been a bit of a struggle in the in the last few weeks as we were trying to quickly and urgently get the work products out the door. And it's one of the things, which caused a little

bit of tension between the comments that the ICANN team was giving to us, which were very valid and right on comments. But it actually highlighted the fact that we were sort of moving into talking about a little bit on the side of talking about policy and we really shouldn't have been.

We're really trying hard in this working group to stick to talking about technical issues. So where we cross that line it's helpful to get questions, and advice, and comments from the community so that we can better focus our efforts and do the right thing. So I hope that that's helpful too. Thanks.

Roger Carney: This is Roger Carney. I think Steve you said it the right way. I'm not sure how small a font we can get on the P because that's what we really tried to do was tried to avoid that as much as possible. We didn't actually get into this until the temp spec came out. We were focused on the technical implementation guide for nine months before that. And then that came out and we thought we needed to respond to that so that that technical guide had some meat to it.

Mark Svancarek: Okay, if we could go to the two policy development phases slide. So if you're wondering how this policy is being developed and how it will intersect with future versions of RDAP profiles, right now, we're in Phase 1. Phase 1 is dealing with the gating questions. We're going through the temp spec and looking at the viability and sufficiency under the new law, of the various aspects of it in order to create final policy. So that means that we're finding legal bases and purposes for collecting each of the data fields and for processing it in the various ways that it needs to be processed.

And during this Phase 1, we are deliberately not talking about reasonable access. This is just a practical consideration - oh sorry. The EPDP working group or whatever we're called. The people that have been dragooned into working on the EPDP. So we're not talking about the access models. From time to time, it comes up and it's unavoidable but actually it's been

reasonably practical to keep to maintain this partition. I admit I was skeptical at first but I think it's working so that's what we're doing.

So right now, we're just going through and saying if we collect this for the following purpose, is that purpose valid? It is lawful? Can it be defended? That's the phase we're in now. When that is complete we will start defining reasonable access and that means we will have to talk about access models. How do you facilitate the balancing test - well, in the cases where access or disclosure requires a balancing test and there are many cases that do not under the law.

In the cases that do, we'll have to figure out how does one evaluate that a request is lawful and proportionate. And if we set up a system where everyone has to make their own decisions, as Steve mentioned, we have to make this as easy as possible. And so at that point, we would be talking about things like accreditation, authentication, rights descriptions, and then authorization to exercise those rights.

So then assuming that the request is lawful, what did these responses look like? So once the balancing test or once the legitimacy of the request has been determined, what do you return? So which data is returned? What are the fields? What are the sources? So incoming sources like who am I, what is my purpose, here is my justification if it's a token or something, and then what you return.

And what you return might be different from the original PII that was in the system. So I use the technical contact field all time and I want to keep it being collected. But I don't ever have to actually know that contact information. If you gave me a web form that said send an email to the technical contact that would serve my purpose fine. And so maybe that's what we return. Maybe return a link to a web form. We could define a policy to do that.

And then that would have to be reflected in a profile. And then there's something that's not really related to RDAP that would be part of reasonable access model would probably be are there liability issues that need to be addressed.

Stephanie Duchesneau: And there's going to be work for this group that parallelizes what's going on in the EPDP. So when you look at Phase 1, you might see something like an updated consent requirement, or different fields, or as Mark described, maybe it's the same field but there's a different data piece that's returned when you go for that field. So those are the kinds of changes that we'll be looking at as part of the Phase 1. Francisco has approved the working group, the RDAP pilot working group to continue in parallel to the EPDP. So we're going to continue to look at the technical questions that parallel the policy decisions that are going on within the work of the EPDP.

And in Phase 2, there's' going to be obviously the possibility that new functionalities are opened up. So I think the plan is to continue work within this working group for as long as we need to, to ensure that the technical implementation requirements are supported. Importantly, nothing about what has been published so far is intended to foreclose further development of the RDAP profiles in order to be responsive to the needs of the EPDP.

Steve DelBianco: Take another question. It's on the Phase 2 not being part of the pilot. I'm eager to understand if the level of a challenge for the group to define a couple of extra fields, not only for the response profile but for the query profile so support Phase 2. So suppose that we were successful at defining RDAP as the tiered access method for the non-public WHOIS for authenticated users. And if we did that, we'd turn to you and say, quickly, can we add a field for the authentication credentials of the requester and a reason code, a purpose code, which could be a reference to a table of lookups or it could be just text.

And that probably wouldn't affect the response profile. It might affect the rules that go on back on the server to come up with what to stick into the

response, but the response profile is probably the same. So I'm anxious to understand without you ever making policy can you now put placeholders in for these fields, like purpose and authentication codes, that those fields could be part of the query profile.

If it turns out that it's trivial to add them later, then great. Tell us that. But for them to be missing gives me concern that were we to come up with a policy and get the data protection board to endorse the legality of a centralized RDAP service, we would then turn to you and you guys come back and say, well, it's going to be a year, sorry, while we come up with the new fields. I'm pretty sure that's not the case.

But how easy is it to put placeholders for those fields in the query profile now? Thank you.

Roger Carney: This is Roger and actually, it was kind of funny, because when Mark put up his slide about Phase 1 and Phase 2, I thought he was talking about the working group because that's exactly what we did was we broke it out the same way and talked about let's not worry about authentication, authorization until we actually get this first part done. And now, we're actually rolling into that next piece. And our goal is to actually be ahead of the EPDP to maybe at least guide some things and say, well, don't get too crazy because we're not sure that that's possible.

But that's our goal is to take that next step. And the few things that we are looking at do allow that to be easily added.

Mark Svancarek: And Steve, to your point, we've published - VeriSign has published an internet draft by Scott Hollenbeck, who a lot of people in this room probably know. Hollenbeck (reg exed) RDAP open ID and so it captures a mechanism for query purpose in there. So that there's standards-based work underway and we've done coding, right. We've prototyped that and it's working right

now. So we proof of concept that. So there's capability there that's been technically proven to capture that.

Mark Svancarek: Do we still have time?

Rick Wilhelm: We should keep going. We've got until the top of the house.

Mark Svancarek: Well, I mean do we have time for me because - so I have these two pictures. I know with that attitude. Yes, I just have these two pictures, which we could - I mean they're in the deck and see them later, and talk to me if we don't have time to do them or we can show them now. It's entirely up to the moderator.

Rick Wilhelm: Flip them up real quick and let's go.

Mark Svancarek: Okay. So before you flip up the first one, I just want to say, okay, well, there it is. Where did these pictures come from? When I'm sitting around talking to attorneys about, well, why can't the disclosure be justified under 6.1B, performance of a contract, as we all do, I was forced to draw these pictures and then they would say, oh my God, the ICANN structure is so screwed up.

And so that's the purpose of this. You can see there's this anonymous users going to the contracted parties and getting a whole bunch of data, whatever data they want. And those are the big grey arrows going up to the top right. And in the original concept, we would - those arrows were Port 43 and then we would just simply put RDAP in there instead. It was the same contract and data flow structure. It's just that the transport got changed.

So don't show the next slide yet. Then other conversations come in and say, well, what about this and what about that, and if we did it this way, would that be supported, could that be supported technically, would that make the contracts easier, would that make the legal - would that support - would that be sustainable under a legal review and stuff like that.

And so there's another concept that I will show you here. It's just a concept. I know that ICANN Org is thinking about it. Some of us call it the hub and spoke model. I hear that ICANN Org sometimes calls it the star fish and spider model, which is apparently some sort of an inside joke. Goran says, well, we have our own codename and it's based on food, of course, but he wouldn't tell me what it is.

So I'm going to just show you the hub and spoke model because I don't have a better name for it right now. Okay, so next slide. So here you can see - and let's be clear, this is just a concept. It's just for discussion only. There is no policy around this right now. This is not a done deal and don't assume that this is achievable right now today.

So there's lots and lots of caveats here, but for discussion purposes you can look at this hub and spoke query model. You can see the anonymous user has been replaced with an accredited user and there's the concept of accreditors and accreditors is something that will have to be defined in a reasonable access model. They could be legal entities in various jurisdictions and they would deliver some sort of an accreditation list, again, not defined. Is that a list of names? Is that a list of names and purposes? Whatever.

Conceptually, it's a list of names and purposes. Law enforcement has access to this many fields. Cybersecurity people have access to this many fields and there's certainly no guarantee that any one party would actually be able to achieve accreditation at all. So people who have access to the data right now might not be able to be accredited to get the access to the data in the future or maybe only some fields, or maybe only in some jurisdictions. So your mileage will vary.

And then the thing here though is you show the accredited user in this model no longer going to the contracted parties but going to a central source, in this case, ICANN. And then ICANN performing RDAP queries to the contracted

parties to pull the data that's needed in real time. And the reason that you would do such a thing -- it looks different and complicated -- is that now the balancing test, where required, no longer needs to be performed on a case-by-case basis by you, but is done in a centralized place and one body has accountability for it.

Rick Wilhelm: One thing I do need to say without commenting on what's on the slide here. Just for clarity, this is not a lower case or capital case proposal by the RDAP pilot working group. Right, because the RDAP pilot working group is expressly about RDAP mechanism, not policy. We are - that group stays away from elements of policy. This group, the RDAP pilot working group hasn't discussed any of this in our working group sessions at all.

Mark Svancarek: That is correct. This is a policy discussion. I felt confident showing it here because I showed it to Goran and he said it has a codename. But pure speculation at this point.

Rick Wilhelm: Steve?

Jim Galvin: Jim Galvin again for the record. Just to jump in ahead of the questions just a little bit. We are going to have a little bit of discussion here about authentication and access control in RDAP. So the technical side of this discussion. I just wanted to say that in advance of questions if maybe we want to wait until we get all of the pieces out here before we get too far in the discussion. Thanks.

Mark Svancarek: So I'm done with this part.

Steve DelBianco: I'll respect Jim's point and not talk about the accreditation piece. I'm just going to suggest that Mark, you've conflated reasonable access with this conversation. Reasonable access, as in the temp spec, and the GDPR is individualized. It's not central hub and spoke. Reasonable access is a registrar or registry giving a response that is presented to a request and the

request could arrive by phone, email, or RDAP, who knows. But that is individualized reasonable access. The minute we talk about central or unified, that's what the word unified is. It's a distinct method and it is not in any way related to the reasonable access that each registrar and registry would have to give. So I would say that don't conflate those two and I appreciate that this is potential here. This is just potential. It's not policy. It's not protocol. It's about potentials. And it would be great to - I'll get out of the way and let you continue the discussion, but don't conflate this with the reasonable access required under the temp spec.

Mark Svancarek: Thank you for confirming that. Reasonable access is lawful. It's transparent. It's reliable. It's consistent. But it is not this is a delivery mechanism. This is just an idea. It is not reasonable access in and of itself.

Keith Drazek: Thank you, hi. Keith Drazek with VeriSign. One of the concerns that I've heard and that we've heard about the concept of a uniform access model or particularly a centralized system is the concern that one entity would be required to hold all of the data. In other words, if it were ICANN acting as the central access point for the data that there might be some requirements that the data from registries and registrars, all of the registrant data be collected in a centralized database.

But - and I think I understand this but I just want to make sure everybody understands, what this is proposing is the referral model, right. The referral system where the data would continue to reside at the registrar, registry, and that there would be basically a query process that would pull the data and then present it to the accredited users.

So I just want to make sure that everybody understands and correct me if I'm wrong that this actually provides for a system…

Mark Svancarek: That is correct.

Keith Drazek: Where the data would not have to be held in a centralized location.

Mark Svancarek: That is correct.

Keith Drazek: Thank you.

Man 1: (Unintelligible) just a comment that this model seems to suppose that WHOIS registration data is going to flow from registrar to registry and this is not a given. Why would this be referenced in temp spec. This is possibly something that won't be found by the EPDP as lawful. So it's more likely that the registrar would be the data source and not the registry.

In that case, the registry query would only be used to know which registrar to query. So we might want to look into a small registrar query profile for domains. Because today, if query RDAP for a domain and the registry doesn't have the data, it will say which one is the registrar and say owner redacted or redacted. We will simply provide a lot of useless answers to that query. So if we could establish some pattern of I just want to know the registrar on record for this domain.

This could be possibly available to anyone, not just ICANN, because it's a very simple query. And this would ease up the process of following the referral chain. Thanks.

Mark Svancarek: So as a matter of policy, the EPDP group is looking at when should data be delivered from the registrar to the registry, which fields should be transmitted, and under which purposes. Is that for continuity of business in the case of failure? What are the cases when that would be required and lawful?

Rick Wilhelm: And technically, this - as Keith mentioned with the referral model, technically your concerns could be addressed with the referral as you (unintelligible).

Jim Galvin: Jim Galvin for the record. Just to emphasize an important distinction. Rick had said this early on in his introduction to this whole session. One of the features of RDAP versus WHOIS is the fact that it supports this referral model. And because you have built into the protocol the ability to provide referrals, it offers the option to support a variety of different policies and where the data may or may not exist and how you do or don't get at it. And that's what's important here.

So this is one example of something that could be supported as well as you're raising some important questions that as Mark said are certainly under discussion. But those are policy questions that have to be answered, and the technology is there to support whatever the community decides it wants to do. That's what's important. Thanks.

Alan Woods: Alan Woods from Donuts. I'm a member of the EPDP team for the registries. I just want to make a very small clarification there. It is not the job of the EPDP team to determine lawfulness. It is job of the EPDP team to make a risk assessment and do a data protection impact assessment to see whether or not it is likely to be deemed lawful were it to be looked at.

So it is not our job to say A is lawful or not. So I just wanted to be very clear on that.

Mark Svancarek: That decision is done on a case-by-case basis. We are defining policy, which would inform the creation of technology, but the decision has to be made elsewhere. It's not being done by the RDAP team. It's not being done within the EPDP team. So thank you for clarifying that.

Jim Galvin: Okay. Thank you. Jim Galvin for the record from Afilias and I'm going to talk just a little bit about authentication and access control in RDAP. Again, as we've been discussing here along the way with other things, most important thing to take away from this is to understand that RDAP, one of its benefits is

the fact that it inherits a rich set of mechanisms and methods for providing, in particular in this case authentication and access control.

So there are two actual mechanisms, which have kind of shown up, that seem sort of obvious choices to make use of in RDAP, which seem most likely to be useful to this community and our needs in the domain name industry. As Rick had pointed out earlier, one of the technologies of course is open ID and he pointed out that his team at VeriSign have actually done some work in prototyping that and demonstrating that it could work in this model.

And in fact that's what this diagram here shows. I'm not going to go deep into this diagram. I should take one moment - a step back and point out that these diagrams that I'm going to show you and the charts that will come up in a moment are actually taken wholesale from work done by Tomofumi Okubo at Digitcert. He presented this in detail at the GDD Summit back in May. So I just took these slides to put here and put them in this record here.

The takeaway here is just that this is what it looks like if you're using open ID. This is just the RDAP presentation. This is just the technical details of the sequence of message exchanges and transactions that are happening underneath the hood when RDAP is active because you happen to be using open ID. And if you go to the next slide, it gives you a look at what happens if you're using certificates. Is the other technology a certificate based mechanism for doing your authentication of your client and your server and using that.

And you can see here that this is the sequence of transactions that take place when you're doing a query and you're trying to do a validation of the user who's making that query. And this is what it looks like.

If you go to the next slide please. The important takeaway here is what Tomofumi had done was to go through a number of features, which would be

important and useful in the domain name industry as we're talking about access to registration data, what kind of features would we expect from our authentication and access control system?

And he looked at both the federated authentication using open ID and certificates underneath TLS client authentication. And he ticked off some boxes here on what is good and bad about each of these two particular methods, and which things could be could be done. The important thing that I want to point out at the bottom of this slide is there's a reference in there to bind identity to the credential and you'll see there's a no in the federated authentication column and there's a yes under the certificate client authentication column.

And I think that's an important distinction to highlight here because it's an important part of the discussion and getting access to registration data. There is a bias towards individual accountability when talking about GDPR for most kinds of accesses. And so it's useful to point out that this is set of technology that has an important distinction in how they can be used and what you can do with them.

So next slide please. Steve, go ahead.

Steve DelBianco: Steve DelBianco. Would you take a question on this slide before you go ahead? Thank you. The very last line about binds identity. While there's a no under the federated, we understand that if the data protection board said that, I don't know, Interpol was the accreditation authority for law enforcement officers and law enforcement officers obtained credentials, used federated authentication to do queries, under the impression that these queries would be logged, there would be a way to bind their request and their credential to their identity. But it would have to be done by an authority that has access to look at those logs and to bind them for the purpose of determining and auditing about whether they were making appropriate requests. Were they

doing too many or too few with respect to what they were allowed to do within their authority.

So does the word no mean no never, or just no because it requires an extra step?

Jim Galvin: No because it requires an extra step. And I'll come back to a little bit of that when I get to my observation at the end, if you don't mind. Next slide please. The next slide, when it does come up here in the Adobe Connect Room is just a few other line entries in the chart comparing these two things. And I don't really want to go through the details in this forum. You can certainly go back and look at the GDD presentation, and you can take these back and you can look at these elements yourself.

Let's go one more slide and this is my last slide talking about observations. What I really want to do to bring to this forum is to talk in particular about what the RDAP pilot can do with respect to authentication and access control. One of the things that was interesting over this first year as we were doing, which we're now calling Phase 1. We had not intended immediately to have a second phase but realizing that as privacy issues, GDPR in particular came to bear, we got to thinking about what it meant to do authenticated and access control inside of RDAP. There really are a lot of unanswered questions, and a lot of them are policy driven.

So we couldn't really make a decision and really make a choice about them because we need for the policies to come together and to sort out answers to certain questions. But I think it's important here to notice about these two technologies in particular, these ones that we've kind of picked out at the moment that seem most applicable that they really don't collide. That you can actually use them both and there probably are circumstances under which you might want to use them both.

But these again are questions that need to be driven by whatever the policy wants you to have. Open ID has the interesting feature that it has a greater convenience factor for implementation and that makes it especially useful if you're looking for a quick identification or if your level quality of the credential, in the sense of how tightly bound you are to an identity is not as high a risk to you. So then the federated authentication model is entirely appropriate.

So law enforcement presents a unique opportunity where that might be the appropriate technology of choice. Another potential use case for that technology is cybersecurity researchers who frequently don't need detailed access to data. They'll take pseudonymous data. And in that context maybe you don't need a very tightly coupled accountability to an identity. But this is a question that has to be answered by policy. The important thing here is that technology allows that to be true. So you can make an appropriate technological choice.

The key difference between these two technologies really is about the quality of the accountability, right, the identity of the user to the credential. In the case of certificates, we're used to certificate technologies, certificate authorities who issue those things and they can do varying degrees of testing of that identity. And you simply give them criteria that you want to be met and they'll make sure that that happens. Then you can use that certificate, and validate it, and decide what data you're going to give them or not give them. Or you can have a softer set of criteria for deciding who gets credentialed. And then again you can have a limited or different kind of response that you might give them based on the technology.

So it's entirely possible here in all of this that a hybrid model was what we want. The primary message to take away from all of this is just that part of the goal of the RDAP pilot is to explore what it takes to deploy the RDAP technology. And I think the message here is that the technology is available and is ready to be used. There's just our choices to be made that we're not quite ready to make yet.

So we will do some continued experimentation. We'll do some prototyping as we continue into Phase 2 here and into a second year of the pilot. We're ready to deploy a version of RDAP for public publication of data, whatever that turns out to be, whatever we decide. The temp spec has one idea. EPDP may come up with something different or whatever the community decides. But we're now in a place where we can begin to examine which kinds of technologies are best suited for particular use cases and we're waiting for the community to decide those use cases.

But we can start to do some prototyping and experimenting, get in front of that. We can influence some policy discussions about what is best as well as listening to the policy tell us what the requirements that we need to meet are so the technology is ready. We just need the rest of the policy and community discussion to come around. So thanks.

Rick Wilhelm: Thanks, Jim. I think we've got a slide from Roger in there. I think so. Is that correct, Sue? Okay, very good. We'll now see Roger's PowerPoint wizardry.

Roger Carney: This is Roger and I'll give credit where credit is due. This is Jody's PowerPoint wizardry and I'm just reviewing it quickly here. One of the things I'll start with though is at one point, and I don't know, a couple years ago now, we had almost had registrars out of the WHOIS business with our contracts stating we didn't have to do Port 43 lookups anymore for thick registries. And we have a couple more to go but we'll see how that turns out as well.

But now, I think we're definitely back into registrars providing WHOIS and through RDAP. So it's one thing that two years ago we were looking about getting out of this and now, we're deep into it again. So just a few things Jody noted here. Definitely, from a registrar's perspective, RDAP will help us out a lot. It will cut down all the white listing that has to happen for 43 access now, and all the blacklisting that goes on as well, as well as the next step in universal acceptance. Moving onto something that actually thins support

natively and consistently, multi-scripts. So another big win for us and all of our customers.

And consistent data structure, which I think has actually happened fairly well in the ICANN community the last four years I would say with CLND and everything else coming out. It got fairly consistent, which I think helps RDAP move along faster as well. But it will be nice to have something now electronically that we can get to, a nice JSON small package that is consistent every time. So from a registrar perspective, I think that's the big items for us.

Rick Wilhelm: Very good. Thank you Roger. And I think we're going to now flip over to Francisco who's going to do a live demo without a net. So hold your breath, everyone. And then we will be flipping over to open Q&A. So please prepare for that. We're going to switch the screen here. That's going to go brilliantly.

Francisco Arias: Thank you, Rick and hello everyone. Let's see if this works. So one of the questions that has come up in some of the discussions around RDAP is what does RDAP output looks like. Can you - oh, something is going wrong there. Great.

((Crosstalk))

Keith Drazek: Rick, you might want to go to Q&A while we're getting the technical difficulties?

Rick Wilhelm: Sure, go ahead, Keith.

Keith Drazek: No, I don't have any.

Rick Wilhelm: If there's Q&A from the audience, or appropriate jokes.

Roger Carney: This is Roger. One thing that I didn't mention that I always try to mention is RDAP is just a protocol. There is no such thing about RDAP display. RDAP moves data from one spot to another and it's done. So there's no RDAP database. Just want to make things clear for everybody.

Jim Galvin: Yes, I want to - let me emphasize that and maybe say that in a somewhat different way also. This is either a feature or a misfeature depending on your point of view. Okay, but from the point of view of just the RDAP protocol, it's really quite a feature. So I know that, for example, our prototype at Afilias that we have standing up that runs an RDAP server for .info, it literally just dumps a JSON blob at you as a response. And people who look at that, look at that and say, this is broken. This doesn't look like anything I've seen before.

And the reality is no, that's exactly the right thing you're supposed to get. The feature here is that you can build RDAP clients and you can build special-purpose clients that do all kinds of interesting things given that you've gotten this JSON blob. This is the advantage of RDAP versus WHOIS. So your client itself should do all of the formatting. It's supposed to take that, and present it, and format it any way that you want, including interesting things like it could take the labels of the data.

Now, you get - in WHOIS, you get that ASCII blob just dumped at you, right, with a tag value pairs. You could have an RDAP client, which translates those labels into whatever your preferred local language is and then displays the data for you so that you now know exactly what you're looking at, okay, and that's an option for you because your client can do that. Your client can also do all kids of magic things with the data if it wants, format it in any way that works for you. And this is why the referrals work because the client should take referrals and it can then go do the second query while you're waiting and you don't even know that it's making two, three, or four queries to collect all the data and pull it all together.

So it's important to appreciate the advantages that you get here and it is also true that browsers today do not automatically format your JSON for you. So it often does look like garbage. It just looks like a blob of stuff that you get. But I suspect that browsers will come along shortly enough and they'll probably do some basic formatting of the RDAP blobs, at a minimum anyway going forward.

Rick Wilhelm: I think we're still wrestling with the display mechanism. So Steve, please.

Steve DelBianco: Steve DelBianco at the BC. I'm going to add pressure on Francisco to get that demo working because half of us on this planet are very visual and need to see something to have it lock into our brains and understand it. And today, we can drop down to the console prompt and do a WHOIS, do a Port 43. And while the blob that comes back is somewhat unstructured, it is textual. I can read it in English and Latin script, and I can understand it. I get that it's not structured in a way that can be parsed easily.

But it is so essential for us to have a visual and if we can't demo it reliably in situations like unreliable Wi-If, one of the things we should present in the next pilot publication and on our wiki for this pilot is to put a couple of screenshots of what looks like if I were able to put some JSON extensions into my browser and have it parsed into the display, right. If somebody can demo that visually, so helpful to understand where it would go.

And I finally wanted to say that the BC had been concerned that the pilot group didn't include any end-users of RDAP. It included mostly the contract parties that would be implementing it. And that concern is something I had expressed to ICANN management, can we get somebody from the commercial stakeholders group on there. The good news is that several of you where multiple hats and are in the commercial stakeholders group.

But the best news is that I have to say that the work you've done is very client centric. All the work that you've done, the way you've communicated it, your

eagerness to accommodate future policy development strikes me that this is exactly the way it should work. And I appreciate all the effort you're doing and it looks like you're on the right track.

Rick Wilhelm: Rich had his hand up over there.

Rich Merdinger: Just a brief comment back to Steve regarding the console, and I totally agree. The thing is the very next update of whatever OS that includes it, that WHOIS client becomes JSON aware and you've got exactly the type of thing you're looking for. The point is we need the ecosystem around us to evolve. Because the data that you're getting out of the Port 43 is today either includes carriage return line fees, line fees only. So there's interpretation of the information coming back already. We just need to mature up that client to be able to do it.

And I think that will happen organically and also with pressure from this group to make sure that the ecosystem supports it. I just wanted to be brief. Thanks.

Rick Wilhelm: Okay, do you want to - Keith is going to hold his question and while we're going to hold very still, all right. There you go.

Francisco Arias: Thank you. So I was saying one of the - this is Francisco Arias from ICANN staff. So one of the things that we (care) as is out of the output of RDAP looks like. And so this may disappoint some of you. Here it goes. This is live query to Google in the pilot. So and the screen just froze.

Rick Wilhelm: It looks…

Francisco Arias: Francisco Arias: Yes, absolutely. The network here is having…

Man 1: Call compliance.

Francisco Arias: Oh, there it is. It's very slow. So you can see that it's very human friendly, right. So but one of the things that it has, it's very machine friendly. So for computers, this is very structured and intentional to the browser to show you where I really want to demo. This is just to show you that the RDAP output is intended to be or was defined to be something that a machine can easily understand. Human beings that are technical can make sense using something like this or even this and then you can see the data somewhat like you would see it in Port 43 WHOIS.

Sorry? Oh, yes. So but still, this is not exactly the most human friendly for people that are not used to technical work. So one of the things that we at ICANN are interested on having is something that is web-based, that is human friendly.

Keith Drazek: Sorry, Francisco. Can you explain what - can you go back to the other screen that you had with the JSON on it and can you explain what came back from the client that was in the text gobbledyblop – sorry, transcripter -- and what is being structured here, right.

Francisco Arias: Sure. Very quickly, this is again very human, sorry, very machine structured. So you have, for example, here the handle that the raw ID of the domain names are masking, the domain names being (nick.soy) that you can see here. So the domain name in ASCII form. Then we have the status, which is active. We have a few of the links. It's not terribly important for the purpose of this demonstration. Then you have something that are called events in RDAP. So you have one event that is registration. So that's a creation date and here is the date.

Then you have when was last transfer. Here's the date when that happened. I don't know what pre-registration is. I think that's probably something special to Google. Then we have the expiration date. Last change I think self-explanatory and something that is in the - coming from the registrar agreement where it requires a footer for the WHOIS output, which says when

the database from when the data that is being shown in this case from RDAP was last updated. So this is it. And then you have other things like the registrar in RDAP. You've got entities that contacts the registrars. So the registrar is one of the entities in this case.

We can see the handle and a few other items here in the output. But this is still not very human friendly. So one of the things that we in ICANN are very interested in having is something that anyone can use and some of you may be familiar with the portal that ICANN is with their ICANN.org where you see the output in a more presentable way, something that is easy to understand so you can see these type of things.

So we're working on making this - an update to this page to support RDAP and I can show you of the queries we currently have processed that is a working prototype. You can do any query on any of the domain supports. This supports already, this page supports already all the registrars that are in the pilot and even the registrars that are in production already. For example, there are some ccTLDs that are already offering RDAP service in production and they are listed in the IANA registry.

So this already supports that input. So for example, we can see one - start with thin registry. So if we go to ICANN.com, you will see that there is no information about the contact but this is taking advantage of the JSON output and quickly, easily converting to something that is more human friendly so we can see the information about the domain name here and this is very slow. So I'm pointing to the domain name information at the top. So that section you can see the domain name itself, (unintelligible) ID, the status. It can have multiple status per the EPDP spec. This is nothing new here and where it has the intersect, when it was created, dated, expiration date.

All the familiar things that you see in WHOIS and this can be formatted in any way you want. It can easily be converted because it's machine readable. Then the second section you can see there is the registrar section. So this

information about who the registrar is for this particular domain name and you have the information about the registrar that is provided by the registry.

And the bottom section is the name server for the domain name. So again, this is (unintelligible) registration so there is nothing returned from the registry regarding the context. There is nothing here. There's still the raw output here but this is just (unintelligible).

Rick Wilhelm: However, can I say - so one of the things, though that if you look, one of the things that we have in our -- Rick Wilhelm, VeriSign -- in our RDAP pilot server, we have a future called object tagging. And so if you see here under the registrar thing it says godaddy.com-VeriSign. So if you want to - if you know where the - that it's a GoDaddy registrar so you could use that to be able to go definitively and know where to go find the object and such. So it gives you a unique identifier on that.

So that allows you to use the - to be able to follow the links and such, which is different than the referral model here in this case.

Francisco Arias: Right, and there will be a referral to the registrar RDAP service, but unfortunately, the registrar doesn't have a pilot service yet.

Rick Wilhelm: You can see the link.

Francisco Arias: No, that link is to the registrar object in the registry services. There is no referral to the registrar because there is no RDAP service on the registrar side. So this is the - sorry, that was a thin example. So here is a thick data example. I can do the query if you prefer that. So this is (unintelligible) - (.mx) set up the service and they even have authentication. So if I enable authentication, and it's asking me what certificate I want to use so I click on the one I want to use.

And here, this is an example in (Talugo), I believe, (.tess), and you can see the domain name is shown in ASCII, domain name being shown in Unicode, and all the data about the domain name. Then comes next the data about the registrar, all this section. And then we have the contact information. All this information is - it's dummy data. It's not real data. So you have the registrant picking up contact, administrative contact. So you have all the information. This is the full output.

And finally, you have the name servers and just like any domain name. And finally, I wanted to show you an example of something that is (unintelligible) - that is - this is a thick registry but it's doing some redaction. So this is not exactly compliant with the temp spec. Remember, this is a pilot but this is kind of how we would look like. You can see you don't see any data about the registrant, or the technical, or the admin, or the billing contact. You just see some redaction.

I don't believe that this is how it is (unintelligible) in the profile but this gives you an idea. And except this also works with the ccTLDs. In the case of IT, this is - .it, the Italian ccTLD, that's a test service that indicates a (BR). This is production service they have there listed already in the IANA database and this is how their output is shown here.

So this is all using JavaScript, the standard technology in browsers, and important thing in the sign of this is that the query has been done from my laptop to the servers. It's nothing being seen by ICANN. ICANN just delivers the client to my laptop in this case and my laptop is the one doing the query to the (racetrack) and doesn't see what the query is, the credentials, or the response in this case.

The only thing to note about this is in order for this to work, certain format has to go into the profile. That's one of the comments we made to the (unintelligible) parties into the profile that a certain header has to be parked on the registry and registrar servers in order to enable this kind of behavior.

Otherwise, the ICANN or whoever is providing the web service will have to see this information.

And that's all I had.

Rick Wilhelm: Very good. Thank you, Francisco. We have about five minutes.

((Crosstalk))

Jim Galvin: Sorry, I want to add something before you go to questions if I may. I want to build on what we were saying before based on what Francisco just did. So he's done an excellent job of showing right in the beginning and he showed that just the JSON blob, this is the response that you get. And he's now gone through and shown some clients and some stuff that you can do. And I want to abstract that back and make an observation to the community, especially those who were involved in policy development and in making decisions.

There's an important distinction here in the new - in a new version of an RDDS versus WHOIS, right. So those who are contracted parties, you're used to your WHOIS output being carefully defined exactly and precisely what it's supposed to look like as part of your contract and you're obligated to meet that letter for letter.

We need to move to a different model now with RDAP. And when you're RDAP as your protocol, this is why we talk about response profiles. What you want in a response profile is to talk about the data that you expect to get back, right. But we should no longer be in a place where we're talking about how it's supposed to be formatted and presented. It should be about I give you this data as part of the query and with that information you provide me this data in a response.

And the protocol will simply give it to you in a structured way. Your client will present it to you in whatever works for you as user. And I think that's an

important point call out here and to see, as you're seeing these couple of examples of what it looks like and then what the responses look like. So it's just a place that we need to move to in our policy discussions and as we migrate the stuff into contracts for enforcement purposes. Thanks.

Keith Drazek: Thanks, Rick, and everybody on the panel. This has been very informative and a great presentation and engagement. So recognizing that the RDAP pilot working group has been focused primarily on sort of the technological aspects, and I think appropriately so, sort of the dividing between technology and sort of the policy questions that remain open. And recognizing that many of you are participating in the EPDP, where there are a list of gating questions, policy targeted questions in that group.

At a high-level, looking at this sort of overall ecosystem that we're moving towards and whether it becomes the hub and spoke model or some variation of that. What's the next step for us as a community to identify the universe of questions, of open policy questions that we will need to define or at least identify to be able to appropriately use this technology?

And so you all from a technological perspective will have input into that, to say, hey, here are things that - here's what we can do but here are the open questions. The community, from a policy development perspective, whether it's the EPDP group responding to the temporary specification or the longer-term view of trying to tackle the next version of what we're going to build, whether it's hub and spoke or something else. How do we come together and identify that list of questions? Because until we identify that list questions, it becomes really hard to figure out which direction the next policy development process is going to go.

I know that's a big question and an open question. And maybe we don't have an answer for that today, but something that I think we need to consider. Thanks.

Mark Svancarek: We'll tag team. So your first opportunity to ask these questions I think is in the profile feedback process. So if you look at some of the feedback that ICANN Org provided, it does contain some - either some policy suggestions or implies certain policy suggestions. So you have a window right now to provide feedback. Just call out I am concerned about a potential policy, please think about how to implement it in the future.

Outside of that, though, I think I'd defer to Jim to describe how he'd like to receive that sort of feedback.

Jim Galvin: Thanks, Jim Galvin for the record. I think what's interesting about your question is what are the next steps or what are the questions that need to be left to be answered and how do we know what those are. For me, my immediate reaction was there's two responses to that. There's you can be very structured about that sort of interaction or we can be kind of informal, ad hoc, and unstructured about it.

And I think right now, we are very much on the unstructured, ad hoc side. Part of that, from my point of view is we don't have a baseline yet from the EPDP. We have this temporary specification and I feel like there's - we don't have a consensus policy baseline that's derived from that. And so we need for that to exist and then we can talk about whether we want to move to something more structured in terms of what do we need.

We do know that we need answers about authentication and access control. We need some input with respect to what those policies are going to look like so that we can begin to make hard choices in terms of the implementation that we want. But I think that right now we have all of the significant players appear to be in both places, both in the EPDP process, and in the RDAP pilot process. I think the ad hoc system is working at the moment.

If there's a piece of it that's not working, it's the bit about timelines. Okay, there's always the timeline question. There's always the deadline question,

"when is it due?", and that's a little hard to define and be precise about without a little more structure and we don't have that structure right now. But I do think that we're making forward progress as best we can. The EPDP has kind of a deadline and the pilot is just trying to keep up. And it's a lot of the same players, at least company-wise, a lot of the same players. And so we're all interacting with our internal teams and keeping it going.

But yes, ask that question next time around. Let's see where we are in March at the next meeting. Thanks.

Rick Wilhelm: Quickly try to get the question, I think we still have, like, 30 seconds.

(Mariano Suria): (Mariano Suria) (unintelligible) from Carnegie Mellon University and my question is regarding have you thought about providing some of the data fields of registrants in an anonymized format? For example, providing a (sole detach).

Mark Svancarek: That's a policy question.

Jim Galvin: Actually, more directly from a registry point of view as a provider of an RDAP service that issue doesn't affect me at all. I'm just going to give you the data that's there. So if I've been given the data that's what I'm going to put there. We're not obligated today yet to provide any kind of anonymized data. So that's not even something we're addressing at the moment. That's one of those policy questions we're waiting for an answer to.

Mark Svancarek: Yes, exactly. That's a policy question. It's related to reasonable access discussions that will happen in Phase 2 and so if you have feedback or requirements, just use the ad hoc process I guess to make sure that those requirements or suggestions are heard.

Rick Wilhelm: And very smart people who deal in crypto have particular opinions about the ability to sufficiently anonymize data. But that's a much longer discussion.

Thank you, everybody, for a lot of great questions. Members of the RDAP working group are around, most of them, all week. Thank you all for your participation. Really appreciate it.

END