ICANN
Transcription ICANN Panama City
GNSO: RySG – RDAP Pilot Working Group
Tuesday, 26 June 2018 at 08:30 EST

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page
http://gnso.icann.org/en/group-activities/calendar

Marc Anderson: Good morning everybody. This is Marc Anderson. I see we're at the - at our starting point so why don't we go ahead and kick this off? Can I ask you to start the recording? Okay.

Good morning everyone and welcome to ICANN62 and the meeting of the RDAP Pilot Discussion Group. Again, my name is Marc Anderson. I'm the chair of the RDAP Pilot Discussion Group.

As a reminder for everybody in attendance, please make sure you state your name for transcription purposes, and for everybody in the back of the room or around the room, we have plenty of seats up at the table with microphones, so I encourage everybody to come to the table and join our discussion

Man: Come on.

Marc Anderson: All right. For people behind me, it is hard to see if you have comments so I'll try and keep an eye on the back of the room, but.

So we have an agenda up on the board and we have a full timeslot ahead of us so we'll try and cover everything on there. I think we'll have an opportunity to get through everything. I encourage everyone to participate. If it's just me talking the whole time it'll get pretty boring for everybody, and I don't even like the sound of my voice, so please feel free to speak up, join the conversation.

If you have questions, comments, anything that you'd like add any point, please do so.

For everyone remote, I'll try and keep an eye on the chat, make sure your comments are being included in this. And are people remote able to - do we have audio for people remote as well? Yes. Okay. So we should have audio for people remote as well so if you want to - if you're remote and you want to speak up and join the conversation, please raise your hand in chat and I'll try and get you added.

With that does anybody have any comments or questions before we get things started? All right. Seeing no comments. Again, people are still trickling in but that's fine. We'll get things started with an overview and background. Seeing this is a open session and a public forum, I want to spend a little bit of time providing a little bit of overview and background on what the RDAP Pilot Discussion Group is, what isn't, and what we're trying to accomplish. And so we'll kick off with that.

And, (Sue), can we move to the next slide? I think we have a slide for this.

Sue Schuler: Marc? You didn’t send me another slide.

Marc Anderson: That's it? We don't have another slide? Okay. Apologies. Then let's stick on this slide for the overview and background then. As I said, I wanted to spend a little bit of time teeing up the conversation and giving some background on, you know, what this group is and this group started in - I guess the idea of this goes back I think to the ICANN meeting in Copenhagen where we were - we had a meeting with ICANN Org talking about how to proceed with RDAP, which was developed as a specification by the IATF.

And the idea was thrown out that, you know, what we really need is operational experience doing this new protocol, and a great way to do that would be having a pilot where end users would be able to sort of kick the tires, try out this RDAP protocol and provide feedback on what works and doesn’t work.

And that led some discussions between the Registry and Registrar Stakeholder Group and ICANN staff that I think culminated at the ICANN meetings in Johannesburg where the Registry and Registrar Stakeholder Group proposed having a time-bound pilot period that would run until July 2018. And the goal of that was to have a new profile that registries and registrars would agree to implement.

And so the goal of this pilot group was to give registries and registrars operational experience and give end users the chance to try out RDAP, see what works and doesn't work, provide feedback, and use that experience and feedback to develop a profile that would guide the implementation.

And what this group isn't, and I think this is very important to note because it's important as we go through all our discussions, is this group is not a policy body. So it does not have the ability or the, you know, there's nothing within its remit to change policy. This group is focused on the technical implementation of the RDAP protocol. And so nothing about changing the policies related to RDS, registration data services, is within scope of this group.

And so the work we're doing is, you know, is bound by existing policy, which of course has changed over the course of the pilot. And so at the start of the pilot we had consistent labeling of display was probably the most relevant policy beyond the RDS requirements in registry and registrar contracts, and sort of that policy and contractual obligations guided the requirements for an implementation of RDAP.

But as the pilot went on, GDPR of course became a bigger and bigger conversation. We had the cookbook proposed and we looked at what an RDAP implementation using the cookbook would mean. And then when the temporary specification was published, we adjusted from the cookbook to that, you know, again, using that as guidance for what an RDAP implementation would look like under that policy.

And so, you know, that's - you know, that guiding principle is, you know, is important. You know, we can focus and look at, you know, the technical implementation and sort of the question that often that often gets discussed within ICANN forums is what is policy and what is implementation.

I think it's important here because policy is clearly outside of our remit and scope but, you know, we have a, you know, I think we have a clear charter and guide to focus on the technical implementation, you know, what are an implementation - what does an implementation of RDAP for registries and registrars look like that makes sense and is going to be something that's usable and implementable for contracted parties and end users looking to access those services.

So hopefully that was sort of a helpful overview and background on the RDAP Pilot, you know, Discussion Group, you know, where it came from and what we're trying to accomplish, what it is and what isn't. Does anybody want to add anything to that?

Rich Merdinger: Hi. Rich Merdinger with GoDaddy. I have a question, not so much to add, but you mentioned that the policies and the approach of what the RDAP is intended to encapsulate has changed over the course of the pilot so far. During that process, have you found that there are material changes to the data or the authentication mechanism that have been discussed that have caused major shifts in the pilot or do you think that the structure of the pilot is handling it well in stride?

The reason I ask is that if we are finding the changes in the policy are causing directional changes to the pilot or the systems, then maybe the systems are a little too tied to the policies and not as agnostic as they need to be to simply provide a mechanism for the delivering of whatever the policy requires.

Marc Anderson: Excellent question. I think that's probably a real good lead in to the second agenda item I think where we'll talk about that a little bit more. But does anybody else want to answer that for their experiences with the pilot and thoughts on that?

Rick Wilhelm: Rick Wilhelm Verisign. The RDAP pilot that Verisign has been running absorbed the temporary specification changes relatively quickly, right? So that amounted to changing the output on, you know, the different types of contact and then the way that Verisign chose to implement the temporary specification regarding redaction of contacts in the European economic area. So it absorbed that relatively simply. That may have been a quirk of the way that we implemented but for our implementation it went relatively quickly.

Marc Anderson: Thank you. Any other questions or comments? Okay. Let's go on to the agenda item number two, the status of the profile and I want to talk a little bit about the approach we took. And I say this because there are sort of decisions that this group made early on in its deliberations, which has lasting effects I guess throughout the pilot.

And the first one is the discussion group very early on made the decision to use the ICANN staff-developed profile as its starting point. And so for background for everybody, after the RDAP RFCs were made available, ICANN staff, you know, created a profile which outlined how registries and registrars should implement RDAP. And that was agreed upon to be the starting point for the profile that we would publish as this working group.

And so using that as a starting point, I think the other thing this group decided early on and again has said sort of, you know, ramifications on our approach and how we proceeded was that we wanted to separate out the technical and policy aspects of that profile. And so the original staff-developed profile intertwined policy and technical in a single document.

And, you know, what it did was it captured, you know, technically how registries and registrars should implement RDAP but also the aspects of that were driven by policy. And I mentioned, you know, I guess I should say policy and contractual obligations, so the obligations on how to implement an RDS service were driven, you know, largely by the consistent labeling and display policy but also the contractual obligations and the registry agreement and the registrar agreement contracts between ICANN and registries and registrars.

And this sort of leads back to the question Rich asked earlier as far, you know, policy is going to shift and change over time, and, you know, one of the drawbacks of having the policy and technical aspects intertwined in a single document is that as the policy changes, you know, it would necessitate a change to the entire profile, which could have more, you know, more impactful ramifications on implementers of RDAP.

And of course, you know, we know as we go through this that, you know, as we went through the pilot we knew that the Next Gen RDS PDP was underway and so we were expecting changes to RDS input. As discussions around GDPR became, you know, more and more to the forefront, we knew that we were going to have impacts from whatever solution came - was developed for GDPR. We now know that there's a, you know, a temporary specification and that there's going to be, you know, likely be an EPDP to address that.

And so we know that there will be impacts to RDAP implementers that we're going to have to make changes as policy evolves. And so it was, you know, it was decided early on that we needed to separate out the profile into, you know, sort of two documents, one that focused simply on the technical aspects for implementers of RDAP and another that, as we put it, created a glue or a mapping between the policy, RDS policy, and how to implement that in an RDAP implementation.

And I think, you know, I think we saw some benefits of that when we had a - we had sort of a - we had separated out the document after the cookbook was available and so we created a policy-mapping document for the cookbook and a technical document at that time. And when the temporary specification was finalized, there were changes between the cookbook and the temporary specification.

And so for the pilot that meant that we just had to change the cookbook document to make it reflect what was in the temporary specification, and the technical version of - or the technical document for the profile didn't need to be changed at all. And so I think, you know, we got a little bit of proof of concept there that the approach of separating out the technical and policy aspects of the profile makes sense moving forward.

Like I said, I think we have to anticipate and assume that we're going to have further changes as we get more clarity out of an EPDP and maybe some of the long-term GNSO efforts around RDS. You know, it's not going to be, you know, this isn't going to be a one-time deal. We're going to have further impacts to our implementations. And so having these things separated into two different documents I think it's going to pay dividends in the long run.

I'll pause there again. Does anybody want to jump in, talk about that at all? Comments, question? Okay go ahead.

(Christian Evans): Hi, Marc. (Christian Evans) from the NC in the UK. Just a quick question on I don't whether it sits here better or temporary spec or uniform access but there's quite a bit of mention of tiered access and different - I'm sorry, quite a lot of mention for tiered access and different amounts of data maybe for different users and different user groups. So from an implementation point, are you looking at multiple profiles to do that or a single profile which will then apply some security procedure to block bits out our add bits? What's the sort of implementation process you're thinking about?

Marc Anderson: I have an answer to this but again I'll put out it out the group, see if anybody else wants to go. I saw Jim's hand go up first but I'll work my way around.

Jim Galvin: So Jim Galvin from Afilias. This is my favorite topic so I guess I get to speak first. You know, I like to separate terminology. There's this notion of a full profile which is a specification for what all of potential objects might look like in a response and what RDAP would return, given that that element was to be returned. And then the other piece of terminology is to call it a response profile. And what you're asking about is what are the response profiles in different circumstances?

And, you know, the position that I always try to represent is that this group itself won't define response profiles. Response profiles should come out of accreditation and the uniform access model work. As part of that work, as part of getting approved for getting access and getting a credential, you will also have defined the set of things that you're allowed to have, because as part of getting your credential you will have to find a reason for getting it.

So this group doesn't care about those kinds of issues. I mean we will test different kinds of profiled responses just to make sure that, you know, implementations can do the right thing in different circumstances but, you know, our only - I believe that our only obligation is in making sure that the full profile, full response actually interoperates everywhere because that way we at least know that we all understand what all the elements look like and how they might be used, and response profiles come from elsewhere. Thanks.

Marc Anderson: Thanks, Jim.

Alex Deacon: Hi. Alex Deacon. So, Jim, I agree but I think the open ID connect is flexible enough to allow not allow for the determination of a profile on the credential, the identity, but also on what they're asking for in the purpose, the authorization part of it, the (O-off) token, which says I'm Alex and I'm asking for this data based on this legitimate purpose. And so I think we could even fine-tune it at that level if we wanted to. And. But again, that's policy that I think can be supported by the technology already.

Rick Wilhelm: Rick Wilhelm, Verisign. Yes so I'll agree with Jim in that a key thing here is defining the terms but even the thing that we have defined now in the current thing that applies to temporary spec is not really a full profile because it considers a redaction in certain regions, for example the European Economic Area.

So all of the responses are going to be in a particular context, and so part of the job of the profile is to capture the policy-driven context and then provide some tactically correct ways of capturing those responses. So generally in agreement but I think that it would - those would all be captured in the same profile and it just has to respond to capture the appropriate policy.

Marc Anderson: Roger, did you want to add on to that?

Roger Carney: This is Roger. No, I agree with Jim. And the one thing that Rick has done is taken that next step and to your question really is I think that the document that Rick generated and is working on is that document that has to go to the policy group to refine and create new ones and change - and create the other profiles for it. So.

Marc Anderson: So may I ask, did we answer your question there? Okay. Thank you. Any other questions on this, you know, particularly around, you know, our approach to separation of the policy and technical and, you know, again I think this will have implications on us as we move forward and as, you know, as additional policy is developed on - by the GNSO on - around RDS. So an important topic that we want to make sure we get right.

Alex Deacon: Alex Deacon again. So not being part of the working group, this may be a dumb question but so you're - you have a date of July, the end of July to deliver a profile from what I understand and I guess the question is toward what end? What will be required of whoever once this profile is - has been I guess published, if anything?

Marc Anderson: Sure. Good question. Again, I'm happy to answer that but I'll throw that out. Does anybody else want to do some talking here? All right. So I guess the, you know, so I'll quote sort of maybe two things here, you know, maybe not quote but I'll recap from the top of my head.

The additional proposal for an RDAP pilot was that, you know, registries and registrars would participate in this pilot program to find a new profile and, you know, following that they would develop a timeline to implement it. With the temporary specification, the temporary specification included some, you know, some things that were a duplicate from the pilot profile. Particularly they specified, you know, the July ending of the pilot with the goal of developing a new profile, but then they also put it the timeline.

And so the temporary specification called for ICANN to trigger the 135 days to implement. And so following, you know, following the July 31 date where registries and registrars and ICANN, you know, staff was - been participating and involved in this as well, we'll, you know, publish this profile document and then, you know, ICANN has indicated they'll trigger this 135-day, you know, clause, which is - comes from our contracts.

In the registry and registrar contracts, there's language around implementing successor protocol. So I think the language in that temporary specification was designed to be in line with that.

Alex Deacon: Okay that's helpful. So the profile you're working on is that profile that's referenced in the temp spec?

Marc Anderson: That's correct.

Alex Deacon: Okay.

Marc Anderson: Francisco, did you want to add anything to that or is that fair?

Francisco Arias: Nothing to add at the moment.

Marc Anderson: Thank you. Any other questions or comments? Okay. So. Sorry, go ahead, Rick.

Rick Wilhelm: Rick Wilhelm, Verisign. On the topic of the pilot, one of the things that's interesting is that as we get towards an authentication model and stuff we may need - I mean we haven't talked about this. One of the things for the group to consider is that we might need to spin up another pilot for authentication, right, because this has been a pilot around unauthenticated access but we may need to spin up another pilot around authenticated access, something for us to consider. We haven't talked about it on a call yet but it's something that we might want to think about.

Marc Anderson: Thanks, Rick. I think that's a really good point. One of the things -- and no we didn't coordinate that ahead of time.

Rick Wilhelm: It just popped into my head.

Marc Anderson: Fair enough. No, that's a good point. I think one of the bullet points in the proposal from registries and registrars to ICANN staff was, you know, included the possibility or the option of kicking off additional pilots if necessary. And I think it's, you know, sort of worth noting one of the key agreements for us to do a pilot in the discussion between registries, registrars and ICANN staff was that this pilot be time bound.

And so I think, you know, a key sort of agreement in, you know, constituting kicking off this pilot was that, you know, it wouldn't be open ended and last forever. And so we agreed to have it time bound and end July 2018, and I think it's important that we stick with that but I think there's also recognition at the time that there may be outstanding items, particularly around authentication that we may need to spend additional time on.

And, you know, I'd like to say that we were wise and saw ahead and knew that this would all happen but I think that would be giving ourselves too much credit. But that said, I think that's really the way it's played out in that, you know, there are still additional questions around authentication and I was actually talking to Alex about this a little bit before the meeting kicked off in that it took us awhile as a group to really get up to - you know, get our legs underneath us. We were slow to form and slow to make initial progress.

And, you know, it took a while to get people on, get us into a cadence of meeting weekly and setting agendas and getting people participating in this. And so I would hate to see us stop and have to restart again from scratch once more is known on how authentication and unified access will work. Yes I would hate to see us lose that momentum.

So as we get, you know, closer to the end of July I think we maybe want to talk about, you know, what do we do post July, how can we, you know, sort of keep some of the momentum we established and, you know, help keep us from having to start over from scratch on authentication later.

Alex, go ahead.

Alex Deacon: Thanks, Marc. This is Alex. So - yes, so that's good to know. So if you - if this current profile doesn't profile the open ID connect authentication and authorization part of it, then I'd just like to kind of point everyone to the open ID connect profile that I wrote, and it ended up in one of the millions of annexes in the BC - so-called BC IPC authentication and authorization -

sorry, I forget the - the BC and IPC accreditation and access model document as, you know, information to use to start to debate or not. So I just wanted to flag as work that's been done that could be leveraged if it makes sense.

Marc Anderson: Thank you, Alex. And just to note, Alex sent me a copy of that and I had promised to forward it to the list but have not done that yet, and so apologies for that but I will send that out to the list for everybody. I think - Jim, go ahead.

Jim Galvin: Thanks, Marc. Jim Galvin for the record. Since Alex has mentioned open ID twice, I guess I have to say certificates once and then seven more times, right? I've got to say it eight times so people remember it. Only because I want to go a step further than what Rick said in all seriousness.

I think that we actually have an obligation even now to start planning to do more with authentication. We have no chosen between open ID or certificates - versus certificates. You know, we happen to be focused on a certificate-based implementation ourselves and I know that others are. I won't speak for them. They can speak up if they want to.

And I think that's an important consideration. We haven't chosen which technology we really want to deploy widely and broadly and we don't know enough I think about either one of them to really know the answer to that. That and I think when this pilot started, we had a very different appreciation for the needs of authentication than we do today.

I mean the buzz word that none of us know anything about is GDPR, okay, and of course it's coming to bear on us all, and it has changed what authorization and access means to us and changed what it means in this RDAP pilot than what it did a year ago when we started and we created ourselves. So I think even, Marc, you suggested we have four weeks to think about what we want to do. I would say no, I think we need to make a decision today and decide that we want to start moving forward on the next part of the pilot, which is to really focus on authentication.

We've done our part to create the profile for kick starting RDAP so that we're in a position that we're probably - and certainly I would think by the end of July we'll be in place where the need to mandate through an appropriate community is an option for ICANN to go forward with. It's pretty clear that that's a path that they would like to drive come August 1.

But I think focusing that authentication, there's work to be done on our side because we haven't chosen a technology. We have all of this work going on around us in the uniform access model, okay, and accreditation and access and EPDP work, which of course is not directly relevant to us. It's policy work. We're focused on technical details. But it matters and all of that work we need to be doing authentication testing while all of that policy work is going on.

You know, I just firmly believe that myself even here today we don't really know what any of those things are going to turn into and what they're going to look like. The councilors are sitting all day in a meeting, for those who haven't noticed, drafting the charter of this EPDP, and whether or not authentication is in there is an unknown thing. So, you know, I just - yes I'm sorry. I've rambled a little bit getting to the point.

To summarize, no, we need to decide if authentication is our next pilot activity and decide that we're going to focus on that begin to arrange to have this part of the pilot shut down and be done on the 31st so that ICANN can move forward with the deployment of RDAP. There are a lot of reasons why that's important, not just this. But let's do that and then the next pilot is to focus on authentication and we get to do that in parallel with all the rest of the stuff that's going on, which I think is essential. Thanks.

Marc Anderson: Thank you, Jim. Well put. And, you know, just to try (unintelligible), yes the GNSO Council is actually meeting next door talking about that right now. So, you know, so definitely something to be on our radar. So sorry. Go ahead?

(Alex): (Alex) from Tucows. I think I would pretty much echo what Jim was just saying. We don't know if access will end up in the EPDP or not but regardless whatever is happening in the next 12 months will be heavily focused on policy creation and no one will really talking about implementation. So I think the terms we have with continuing our work is developing implementation options and technology options as we go so that we are not starting this discussion once we actually know what the policy is but we're already there.

And yes we will operate in uncertainty and we will not know what the outcome is but we will at least have been testing different options and know what works and what does not work, and just need to be careful to be open enough to accommodate whatever the policy outcome will be. But I think there's tremendous value in just keeping up and continuing this work and making progress as fast as possible there.

Rich Merdinger: And I'm going to - as I was listening to Jim explain his need to mention a certain word eight times and things along those lines, fun aside I've heard two major registries now mention that the technology that they've selected for their pilot with an implication that potentially that could be the technology that they are endorsing and in the face of the lack of concrete information on what needs to be supported, how it needs to be supported, I think that we need to make sure that, as Alex suggested, we keep a very open mind and evaluate the technologies up against the requirements that the policy is going to bring forward.

Rick Wilhelm: Yes, just Rick Wilhelm, Verisign, echoing what Rich said. And while Verisign hasn't made a decision, we think that the requirements are more likely to be and rather than or based on our examination of the facts thus far.

Sean Baseri: Sean Baseri from Neustar for the record. I think that I have to agree with what Jim had said that I think that the next evolution of the process does make sense to look at authentication. For us I think that we've looked at the past and we've focused all of our efforts on the certificate-based approach as we see inherent strings with that approach. So I just wanted to mention that I seen inherent advantages.

Roger Carney: This is Roger. I think everybody's kind of in agreement and everybody's walking down the same path, so I think that's good. One of the things I have mentioned before I want to mention now is when we get into this authentication pilot or whatever we're going to call this, I think we have to look at helping policy by making sure if there's any true implementation roadblocks that policy knows that ahead of time.

I don't want policy coming to us in a year saying I want this and we're finishing our authentication pilot saying that's not possible. So I do want to - what Rich mentioned is, you know, we want policy to make decisions but we all - we want to help them as well. So I think our pilot needs to be fairly quick and maybe done this year yet so that it does help policy moving forward.

Marc Anderson: Thank you. All good comments. I want to sort of echo what Roger said because that's a concern of mine. I want to - you know, there's a little bit of a chicken and the egg I guess between some of this but from perspective I think it's important that we make sure that what comes out of the policy discussions is implementable. And so we need to I think make sure that we're communicating with our colleagues in policy working on that and making sure that the policy they come up with is something that, you know, is reasonable for us to implement.

Go ahead, Jim.

Jim Galvin: So thanks, Marc. Jim Galvin again. I want to just come back around to something that Rick had said because he did say that - I mean I raised the question of choosing technologies and we really have two on the table and he, you know, was kind of making the assessment that it actually might turn out to be both. And I actually I have some sympathy for that position.

I don't like that position, I really don't want it to be both, but I - this is one of my concerns about even deciding now whether it's one or the other or both. And the - I think what makes the fact that we should focus some attention on this project in the future, I think the uniform access model and all those discussions are going to help guide us. You know, we really do have to wait and see the requirements and what that system is going to look like before we can decide.

I mean I hope we don't end up with two technologies but I can see where that's actually an option that we have to be thinking about and consider. But anyway, thanks.

Marc Anderson: Thank you. Before I get to you I've been neglecting the chat here and so I want to read something Scott Hollenbeck put in the chat. He rephrases a question. He says, "Certificates and open ID do not need to be mutually exclusive. Open ID does allow for cert use and an authentication mechanism, currently optional in the OIDC spec." So he wrote that as a question but I think that's maybe a comment.

Roger Carney: And I think that's important because, you know, open ID connects - Open ID and the open ID connect spec provides a framework that allows for different authentication technologies, whether it's using a password or kind of client cert based.

So I think, and we may be getting out too far ahead here, but if it seems to be a pretty logical choice with regard to technology as it allows for one or the other or in fact both, and that would be, you know, how we define that will be a matter of profiling what technologies must be supported on the client side, what technologies must be supported on the server side, so everything kind of works interoperability together.

Rick Wilhelm: Rick Wilhelm, Verisign. One of the things that we will need to remember as we think about authentication technologies is they are almost inevitably and inextricably tied to authorization mechanisms. In other words, you know, who you are - who the querier is defined to be and then also what they are allowed to see.

Those things are going to be likely tied pretty strongly together, especially as we move from the notion of old style Whois approaches where you are given sort of run of the house access to where you're IP white-listed on port 43 to something where you get access to a particular query string like star names, star, or something like that. So those are going to be linked together and we need to remember that when we think - when we pick or think about authentication approaches that authorization is going to be linked together.

Jim Galvin: So Jim Galvin from Afilias, and far be it from me to speak on behalf of Scott Hollenbeck from Verisign but he said something interesting in the chat which I wanted to read out for folks in the room. And it gets really to part of the question of why we need to continue to look at authentication. You know, certificates and open ID really do have their differences and the difference really you have to think about the use cases and what is it you're looking for.

As Rick is over there talking about authorization, one big distinction between open ID and certificates is how well they work in different use cases. You know, certificates will lend themselves better to connection-oriented authorization services, so are you providing a response profile based on the accrediting agency as opposed to the individual who's making the query.

You know, open ID would probably lend itself more directly to a use case which is individually based and doing that level of accountability. You know, I don't know which way the uniform access model is going to go, you know. I mean is it going to be individually based, is it going to be accrediting agency based. These are just sort of requirements we don't know the answer to and they really are fundamental to the choice that has to be made yet.

So I just want to keep emphasizing the need for wanting to really do more with authentication in the future that we can't deploy that right now. We really do need to understand what we're trying to achieve before we know what to deploy and what to pick. Thanks, and thanks to Scott.

Marc Anderson: Thanks, Jim. And I want to take a moment to mention the, you know, the discussions that happened at the registry operator workshop in May. A lot of that was focused on just what Jim was talking about right now, the different use cases, and I thought that was covered really well. (Tomafoomy) and Scott actually had a great panel discussion on that where they, you know, specifically to what Jim was talking about, they went into what those different use cases are and cases where one technology might make more sense than the other technology or cases where they might complement each other.

I know from looking around the room many of you were actually there so you're familiar with that discussion, but if you're not I believe those sessions are recorded and available. Francisco is nodding, so yes. You know, I encourage you to check out the material and maybe listen to the recordings. You know, I thought they covered that topic really well during that (row) session, so some really good background for anybody wants to dive into that a little bit more.

Any more conversations on this topic? I may - sorry I was just looking at chat there. So I think we - that was a good discussion and I take that as, you know, as agreement that there is a need to, you know, sort of draw a line in the sand for where we are with the existing profile, sort of finish up those documents and get them out the door.

But that there, you know, there is a need and I guess willingness from the group to continue and look at, you know, the authentication, access authentication and how that can be implemented in RDAP, make sure we're feeding and communicating the policy work that goes on, make sure that we're informing those discussions and make sure what comes out of there is implementable at the end of the day. I think that's, certainly from my perspective, I think that's important and the conversation here seems to support that. So thank you everyone.

I'm looking at the next agenda item is actually a discussion on the temporary specification on RDAP and I'm not sure that agenda item hasn't been overcome by events at this point. I think we covered most of what I wanted to talk about just in the course of covering the other agenda items. So first I'll just sort of throw it out there. Does anybody want to say anything about the temporary specification and RDAP in general?

All right, you know, just sort of to wrap this one up I guess before we move on is that, you know, I think what we're going to end up with in July is a profile that defines how to implement RDAP in accordance with the temporary specification. I think that's what the document looks like today and, you know, and what we're going to end up agreeing to and publishing in July. I think that's the, you know, that's the state we're in and where we'll leave this.

I think I'm comfortable with that. Hopefully - I'm seeing some nods around the room and nobody's raising their hands to object, so I take that as agreement. Jim wants to object, or?

Jim Galvin: No, I didn't want to object. So - Jim Galvin, sorry, for the record. I actually wanted to add to it. I think you said this but I admit I distracted my attention so I'm not quite sure what you said. You skipped over agenda item four there, the SLA and reporting requirements.

Marc Anderson: Haven't gotten there yet.

Jim Galvin: Okay. All right. As long as you're going to get there then I'll be quiet and wait. Thanks.

Marc Anderson: Thank you. Anything else on temporary specification and RDAP? All right. So our next agenda item is SLA and reporting requirements discussions for Jim and - thank you. So on that, you know, assuming, you know, I don't want to assume anything here, so for anybody that’s not aware, in the temporary specification there is language around, you know, registries and registrars and ICANN negotiating in good faith to agree on SLA and reporting requirements for RDAP.

And so we have the requirement in the temporary specification to implement RDAP for the profile that we're developing here within this group. But then we also have an obligation to discuss with ICANN SLA requirements for those RDAP implementations. And correct me if I'm wrong, I believe the reporting requirements are only for registries. I don't believe - and Francisco's nodding. Registrars don't have reporting obligations on there. So that's a registry obligation. But there's still SLA reporting requirements.

I want to say that's not specifically a discussion that's in scope of this group. There's a separate group that was formed. Jeff Neuman is facilitating those discussions and so it's a separate track from this one but I think it's important that I raise it here, make sure everybody's aware of this conversation and highlight the fact that, you know, we will have to, you know, come to agreement on what the SLAs around this RDAP implementation will be and at least, as far as registries go, what our reporting obligations to ICANN are.

Jim, did you want to add on to that?

Jim Galvin: You just said a phrase that caused me to think. You just said registries have reporting requirements. Again, maybe it's not for us to say but I mean ultimately if registrars are going to have to run an RDAP server, why wouldn't they have reporting requirements? I mean that becomes a policy consideration but, you know, certainly these - I think that what we're doing here should be framed as RDAP reporting requirements.

Leave it to policy to decide which way it goes because, again, it's all going to depend on what ultimately is the - what the actions that ICANN takes after this pilot closes and what the rest of RDAP does based on policies that are coming. Maybe that's a little vague. Did that make sense?

Rich Merdinger: Thanks. Rich Merdinger here. You made a comment or used a phrase in there I'd like to get clarification on. You said reporting requirements as part of what we're dealing with here as opposed to reporting capabilities that we would be trying to define and build out. Wouldn’t the definition of the requirements be part of the policy and then the solution that we're trying to implement be meeting those requirements? And I think it's an important distinction.

Jim Galvin: So thanks, Rich, for word-smithing for me. No, I agree with you 100%, all kidding side. You're absolutely right. I mean we're trying to be careful here about what we're saying our work project is going to be and draw the appropriate lines, but you're right.

I mean we're sort of agreeing on what are the metrics that are available, the capabilities that are available and I think that's appropriate for this working group to sort of say these are the options, and then ultimately who's required to do them will come from somewhere else. But I - so yes. I think the notes have got all of the right story here. It's the RDAP reporting capabilities and, you know, it's up to someone else to decide the requirements.

Rich Merdinger: Marc, if I could just to be clear as representing -- this is Rich again -- representing a registrar, if there's going to be reporting we need to be involved with all of the capability definition, et cetera, et cetera, just like registries are now. I'm not suggesting that it isn't the responsibility of a registrar running an RDAP server to do this similar reporting.

Jim Galvin: So, sorry, Jim Galvin. And one last comment then. I think also this is going to be one of our work products, right? We're going to be done with this in four weeks, right? So in addition to the profile we'll have the reporting capabilities all together. And I see shaking heads so let's have some discussion about that.

Rick Wilhelm: So I'll just - the reporting requirements are not part of the profile. Right now in the temporary specification, Section 6 requirements applicable to registry operators, only 6.2 is the thing that refers to the reporting requirements. And in the draft temporary proposed gTLD temporaries - temporary spec, there was an Appendix H that had an addition of adding fields to the monthly registry functions activity report, which Rich reads every month because he occasionally suffers from insomnia.

And that added fields 38 through 56, a substantial widening there and added a number of fields. So this is part of the temporary spec, not part of the profile, the reporting requirements, sorry.

Marc Anderson: Just quickly, administrative, (Sue) notes in chat if you would like to be added to that discussion group please let her know. If you want to let me know, I'm happy to facilitate that as well. But that is a separate conversation but it's important that, you know, there's a lot of overlap between that conversation and what we're talking about. So I think it's important that you're, you know, everybody in this group is aware of that and plugged into what's going on there. Did you want to - your hand's hovering near the button?

Jim Galvin: So Jim Galvin again. Sorry, I'm just taking a moment to collect my thoughts a bit. I think the way that I want to respond to Rick, I want to say that I agree with him but let me frame my position about all this a little bit differently.

The details of how the reporting capabilities come into existence, you know, I agree with what you're saying there, Rick. I sort of misspoke about, you know, how to represent that. It's not really part of the profile per se. Nonetheless I think - I mean I'll just state that, you know, we, Afilias, we're supportive of the reporting capabilities, don’t really have any issues with that, and I would fully expect that those reporting capabilities will be somehow become a requirement in the deployment of an RDAP server.

And I just think that – I'm putting that out here in front of this group, I mean, if we're going to object to that then if the group wants to object to that then we probably need get on a path of coming to some conclusion about that. I think I'm saying that as part of our work products, let's also produce these reporting capabilities as part of the profile and expect that this is going to happen. That's all. I mean, and so I'm looking for us to either decide we're supportive of that or if we're not we need to have a discussion about how to defend that not being true. So thank you.

Rick Wilhelm: Nice (unintelligible). Rick Wilhelm, Verisign. So thanks, Jim. So and the stuff I was reading was from the proposed temporary spec and so I would encourage registry operators to look at the temporary specification and look at the number of fields being asked and also compare it to your current reporting obligations regarding Whois and note that currently on Whois you're required to report Whois queries, right, which is you've got a reporting obligation that's about one or two fields and in the RDAP – in the RDAP thing you're adding fields 38-56, which is about 19 new fields including obscure fields such as RDAP truncated load, RDAP truncated unexplainable, RDAP truncated authorization, which is a level of granularity of, you know, for utility that just to me is unexplainable when previously for Whois service it's been in use for many, many years, we were reporting just queries.

So I agree, Jim, that we would be – we as a registry would be expecting to report parallel an equivalent to what we would be reporting on Whois, which is, you know, one or two fields, not, you know, 18 or 19 fields. So that's kind of the issue that we would have with so I'd encourage registry operators to look at the proposed – that which was previously proposed and engage accordingly.

Marc Anderson: Thank you, Rick. Anyone else want to jump in on this one? Stephanie, go ahead.

Stephanie Duchesneau: Yes, I agree with the last point. I think it's important to look at the language in the temp spec also because it says if we fail to come to agreement, the fallback is that what we're going to comply with is something that's comparable to what we're doing now for Whois and I think it's hard to argue that twentyfold reporting requirements are comparable to what we're doing now for Whois. So I don't think that the fallback is that ICANN can require what's currently on the table.

Marc Anderson: Thank you. Yes, I thought it was a good discussion, I didn't want to derail it but just a reminder that, you know, there is a separate discussion group going on, you know, I think I don't think there's a next meeting scheduled but, you know, that group again headed by Jeff Neuman is, you know, their next step is to work on edits to sort of a comments to ICANN about what the SLA and reporting requirements would be. We focused on the reporting requirements aspect but don't forget there's SLA – there's an SLA aspect to that as well.

So I, you know, again I wanted to raise that here because, you know, it certainly, you know, tied to the work we're doing in the Pilot Discussion Group and you know, for contracted parties it's an important you know, it's an important obligation so make sure you're aware of that. You know, it is, you know, it is something that will be impactful to you. So you know, make sure you're a part of that conversation.

But sort of, you know, complementary to there, you know, I think, you know, and Jim made some interesting points about RDAP reporting capabilities, and so, you know, in my mind there's maybe a difference between what our contractual obligations are and what is capable and that, you know, what we're capable of providing and so that may be a discussion item for an upcoming meeting to talk about that as well. So maybe we, you know, put that you know, put that on the white board for something to discuss in more detail at an upcoming meeting.

Anything else on this one before we move on? Go ahead.

Rick Wilhelm: Were we going to talk about SLAs or just the reporting?

Marc Anderson: Happy to spend – if we want to talk about SLAs, happy to do so but, you know, I think, you know, I'm not, you know, I think the proper forum is the – that other discussion group headed by Jeff Neuman. You know, if there's something you want to raise now, please go for it.

Rick Wilhelm: I'd encourage registries and registrars to engage because you're – if you don't you're going to be signed up for SLAs for a service that you have not heretofore operated at scale and these SLAs have contractual implications.

Marc Anderson: Thank you. Well put. And, you know, Sue's noting in chat that the next meeting of that group will likely be the week after July 4, I think that's also the week of IETF so there might be some conflicts there but, yes, just to echo what Rick said, that's, you know, this is a service that hasn't been operated at scale, and, you know, there may be technical challenges or unforeseen issues there so we want to make sure that we're engaged and come to agreement on something that's reasonable.

Let's move on and, you know, we're going to have, you know, the next agenda item is on uniform access, what RDAP needs from authorization and accreditation and here again I'm realizing that the conversation from earlier really carried into this one a little bit already. You know, we've certainly already talked about this to some degree.

But I'll just, you know, I'll just pause here and throw it out to the group, you know, what, you know, what are thoughts on this, you know, realizing, you know, fully realizing that you know, in the room next door the GNSO Council is debating this very question as well. But, you know, I'll throw it out to the group. Alex, do you want to go?

Alex Deacon: Well it's a question or maybe a statement I asked in the chat earlier, have you guys created any use cases around authentication and authorization and he said, no, it seems to me that maybe a good idea, so we understand kind of terminology and what is required and you know, use it to – so everyone has a common understanding of kind of what may need to be built and what, you know, we can profile in the future.

Roger Carney: This is Roger. The group has not created any use cases for this. I think individuals as they've done their testing have done some of that. I agree, I think that would be very useful when we move into this authentication pilot that we actually do that, set those up front.

Rick Wilhelm: So I would temper that a little - Rick Wilhelm for the record. I would temper that a little bit. I would say that the use cases flow from – more from the requirements that are coming the other way from the, you know, I would – I'm really hesitant to have this group, the technical people, saying, here's the use cases, you know, let us know because when I'm used to building software the use cases kind of come this way.

Now there may be some use cases that after the technical team gets the use cases from them that we send back which might be – I'm guessing, and this is probably what Roger is thinking, some rainy day, quote unquote, rainy day use cases like well what happens when this user gets revoked or when some amount of time is expired, but I think the initial serve will come from the policy – from the accreditation side. Sorry.

Marc Anderson: Yes, go ahead.

Alex Deacon: Yes, I agree, I mean, that's the right way but it sounds like, you know, Roger, sounds like you've started some implementations and maybe Jim has at

Afilias. It would be interesting to understand, you know, what you guys have started to implement or think about implementing and add that to the mix so again, people are educated by, you know, what you've learned and what you think needs to be implemented, I think that would be useful, with the understanding that it's the, you know, the real requirements and use cases will come from the guys in the next room.

Marc Anderson: Thanks, Alex. Rick.

Rick Wilhelm: Rick Wilhelm, Verisign. Yes, I'm hesitant to build the implication of a dependency that that group wouldn't start until we send them something. Having been caught in that catch 22 in a prior life, in my day job, smiling.

Marc Anderson: Thank you. I do want to – I do want to talk about, you know, the Verisign pilot implementation real quick, not to spend a whole lot of time on this, but when we developed our pilot implementation we did spend a little bit of time on use cases, you know, just you know, sort of theoretical how we would implement it, and so our pilot actually has three tiers of authentication. We looked at sort of public access to the data, we talked about authenticated access to the data and we created a third tier that we called law enforcement access to the data.

And that was sort of, you know, what we used as sort of our pilot and, you know, it's, you know, it's not meant to sort of, you know, predispose any outcomes or – predetermine any outcomes or anything like that, it was just the, you know, the use cases that we wanted to test out for purposes of our pilot. So, you know, that's the use case that, you know, we used as our starting point for our pilot and sort of a three-tiered model for, you know, access to the data, you know, public authenticated and law enforcement access.

Rick Wilhelm: Rick Wilhelm, Verisign. Clarifying, that was done – we synthesized that use case and that was not done in cooperation with any law enforcement agency, quote unquote, foreign or domestic. And it was just us making up the use case.

Roger Carney: Maybe I can lead us into the next topic too with this. One thing Marc brought up, I don't know, a couple weeks ago is creating a report for finalizing this group's work, not just the profile itself but a report of saying how we got there. And I'm thinking, you know, when we talk about this next pilot, this use case idea would be good to use as a reporting mechanism saying this is how we got to the conclusions of the end of this, so.

Marc Anderson: Thanks, Roger. Yes, and good plug there. You know, it's – Roger's referring to something I brought up last week's meeting actually that I raised the idea that id on think it's actually enough for us as a group to publish just the updated profile, I think we also need to have some kind of a report of, you know, the deliberations, what we discussed, explaining sort of the decisions w made, how we got, you know, how we got to where we are and maybe even talk about some of our recommendations for a follow up pilot.

You know, so I think, you know, I think we're going to need to have sort of a little bit more, you know, than just the profile at the end of this and I think it's, you know, certainly, you know, some of us have spent a lot of time on here and I think it's worth, you know, sort of memorializing and capturing the work we did.

I agree the action item we've put together an outline of what that report might look like so that's with me. Once I have something reasonable I'll circulate that to the group but, you know, I think it makes sense for us to have some kind of pilot report that accompanies the profiles that we're – the profile documents that we're producing.

Before we move on, you know, I'm looking at that item on authorization and accreditation and, you know, something that I often fumble around access to the RDS data is sort of the difference between authorization and authentication, and I think that's probably something that will come up a lot this week, and, you know, and maybe in the many months ahead particularly as the discussion on uniform access continues.

Is there anybody you know, I always do a horrible job explaining that but, you know, just for the purposes of level setting, is there anybody in the room that would like to take a stab at maybe, you know, delineating what it means when we talk about authorization and authentication and what the differences are? Jim, thank you.

Jim Galvin: So Jim Galvin. I think you can boil it down to two sentences; authentication is about who you are; authorization is about what you can do. It really is that simple.

Marc Anderson: Thank you. Makes me feel a little silly. But I also can guarantee I won't be able to repeat that later today so maybe I'll put that on a slide.

Jim Galvin: No, I mean, well, I see Alex has got his hand up, maybe I'll let him speak. I mean, one can nuance that and expand on it a bit but in a broad discussion if you're just trying to simply explain it, it really does boil down to those two questions, you know, and you can derive a lot of little nuance out of that but I'll let Alex add to that.

Alex Deacon: You know, I agree, Jim, I think that's what it is. I think – I'm speaking on the panel about access and – this afternoon and the way I'm going to explain this very, very briefly is similarly but I'm going to use who as who is the, you know, who you are, right, who is asking for this information and the why in terms of RDAP and in this post GDPR world, the why is what is the purpose? What is your legitimate interest? Why are you asking for this information?

And those two – those two questions, who are you? And why are you asking? Are both required, the authentication and the authorization are both required to return the what's which is the data that we will at some point, or they will in the next room, some point to find based on who you are and what are your needs. And so that's kind of how I see it working. And both are important.

And one thing that’s – I've heard over and over in these discussions in the community is that it’s not enough just to say who you are, you need to be very explicit about why are you asking for this information and that’s authorization part. So both are required and both need to be separate in any technology that is used. We can't lump in – I don't believe we should be lumping in the who and the why into a single technology; they need to be separate because we need that flexibility.

Marc Anderson: Thank you, everyone. You know, I think that’s, you know, those are important points and something I actually, you know, try and remind myself every time we go into one of our weekly calls, make sure I have that straight in my head but it’s, you know, it’s sort of, you know, I think that’s going to become more and more important as we delve into the questions around uniform access to the data, make sure we’re having the right conversations about authentication and authorization and how that’ll impact us as implementers of it.

Rick Wilhelm: Rick Wilhelm for the record. And then the other word that we’ll need to throw in there and mercifully it’s an A word, just to – is accredited, right, so you can be – you can be Jim Galvin and you can be authorized, you can be authentically Jim Galvin, you can be authorized to go anywhere but if you’re not accredited as a law enforcement person, or as intellectual property person, you still might not get whatever, right, so you're accredited as a – something, right, so that's a third word that will creep into – more and more into our lexicon and you're accredited by an accrediting body so that third word will wander in more and more so something else to think about.

Marc Anderson: And just to note from chat and Jim, your definition got some plus ones, you got, you know, nice job, Jim, plus one, Jim, so thank you for – thank you for coining that so well. Anything else here before we go onto the next agenda item? All right, so the next item on our agenda is additional technical standards work needed. Is this – sorry was this Roger, or did you raise this one?

((Crosstalk))

Marc Anderson: So I think it was Roger, you raised the agenda item on additional technical standards work needed. And I think you – I think you teed it up a little bit on the last call but if you could maybe introduce this a little this morning?

Roger Carney: Yes, this is Roger. Yes, and I think that the way the group has started to I guess move maybe this isn't as big a topic now and some of this gets pushed into the next pilot, if that's what we're doing. My concern here was if we were expected to come up with a authentication model in our publications, we are a long ways away from that. So and that's why I kept bringing up the technical. I mean, even if we all agreed today, hey, let's do open ID, I don't know how many people in the room have read the open ID specs that out there. So it's far from being done and I think there's a lot of work that still has to happen to iron out – open ID is great and flexible but you still have to set the parameters that you want to collect.

So and we would all have to agree that that makes sense to collect them and all this, so I was – and again, if we're not going down that path I don't think there's a lot to do here. I think one of the big things left is what the process is once we are done, you know, we write a paper and we hand that to Francisco or Denis and say we're done, okay, then what happens? I mean, the last time we had a profile created 2016, is that right, we had a comment period – public comment period for it. And that's actually when it got stopped was during the public comment period.

And I'm wondering if that same process is what's we're going to go through or what that next process is for us as a group once we do finish the document.

Marc Anderson: Thanks, Roger. And there’s a couple threads there so I want to make sure we don't lose any of them. And also I want to note in chat that it’s also come up I think you know, Alex raised it first around accounting but I think that’s – that also touches on auditing of who’s accessing the data so that's you know, maybe another thread that’s picked up in chat that we don't want to lose track of as well because that’s, you know, as was noted in chat, this is also potentially important topic that we need to keep on our radar.

So looking at that, you know, I don't want to lose any of those threads so maybe try and cover them one a time. So I want to start – in no particular order let’s start with, you know, the accounting and auditing here. It’s not something that we've brought up as a group before but I know this is, you know, I know from the discussions around GDPR, you know, that there are some auditing requirements you know, around GDPR that may be important and as was raised in chat, you know, there’s also concern from certain people accessing the data in some cases it might be – it might not be appropriate to track that.

So that’s a balance that we’re going to have to find as a group as far as, you know, what are our requirements and obligations for auditing, you know, tracking who’s accessing the data versus, you know, when, you know, when and how that, you know, that data shouldn’t be tracked. So I’ll throw that out there, does anybody want to comment on that here? One brave soul.

Jim Galvin: All right, Jim Galvin. I comment on everything so what the heck. You know, I really think that although I fully agree that auditing and accountability are important and essential, I think that those are policy considerations. We all would normally as part of our operations do logging and it’s that logging which will respond to auditing and accountability requirements. And I think that we’ll all just do that as an ordinary part of our operation driven by whatever requirements come down to us on the policy side. So I don't believe that there’s any discussion for us to have here about it except maybe to acknowledge its existence but, you know, I think we all know. Thanks.

Marc Anderson: Fair enough. Alex, do you want to add to that?

Alex Deacon: Yes, I agree, Jim. So I think this team is – should be specifying logging or somehow I think that's within scope but auditing, I agree, is out of scope. When it comes to law enforcement, unless you wanted to follow up on that? When it comes to law enforcement, I think I'd like to understand kind of the requirements there of what their needs are, so we could make sure that any implementation impact it may have is taken into account and fully understand.

I kind of understand at a high level what has been asked, and I'm looking towards you, but kind of what the parameters are is not clear and whether it's appropriate to talk about that now, I don't know, but I think that's something we should discuss now or put on the list to discuss because it's – I think it's something that comes up over and over and over and understanding what it means is important.

Rick Wilhelm: So I'll sort of hit at the rough - Rick Wilhelm, Verisign. I'll hit at the rough intersection of law enforcement and logging. And I'll agree very strongly with what Jim said that the discussion about what we log is actually more of a matter of policy than we might think because it goes to query tracking and such, law enforcement for reasons that might not be obvious until you spend a half an hour going into the – into a discussion with somebody from law enforcement, you realize the sensitivity of some of the searches that they get involved in.

And has a distinct aversion to having their queries tracked on quote unquote our side, right, on this side of the table and so they will end up agreeing to sort of terms where they do the tracking on their side, right, and then they'll do things that sort of say well we'll track and such. So they'll – they don't want – they prefer not to have us track on this side. And when I say "us" I mean contracted parties, that sort of us, not Verisign us.

Marc Anderson: Thank you. Did you want to jump in at all or…

((Crosstalk))

Marc Anderson: Put you on the spot?

Man: So realistic I think is probably out of your scope for this one, and (unintelligible) if you've got another pilot with accreditation and authorization whether you want to put logging into that as well, and it's that definitely something. We could probably talk for I think half an hour easy on our requirements for logging. We're not adverse to logging, we probably have logged and do log far in excess of anything that is a requirement of anything that we've got at the moment. So it's not the aversion to logging itself, it's to how that's stored and who has access to it and when they have access to it and that's very important obviously in an investigation for us.

So I think it's a difficult one but it's only difficult to get it in the right place. And once, you know, the actual logging is not difficult, because the answer is yes, but where that's logged and who has access to that and when they have access to that needs to be properly defined but the actual logging itself I think you know, we'd be in agreement and say well we already have some form if you can automate that for us then all the better, really I think that probably is as much as want to go in without taking up lots of time.

Marc Anderson: Fair enough. And I do want to note, you know, we did have some, you know, I think many of us are aware of this, you know, we did have, you know, some outreach earlier in the pilot program to some law enforcement bodies and at the last ICANN meeting Greg Mounier, hopefully I'm saying that right, from Europol came and spoke to us. And, you know, one - I think probably the topic we ended that discussion on was around you know, auditing and tracking of what those queries were.

You know, so we have had this as a discussion point. And -- you know, specifically at the previous ICANN meeting -- (Greg) came and spoke to us. So that was - I thought that was really useful. And that, you know, that chat and transcript is available as well. But you know, appreciate you letting us put you on the spot there.

Man: So we also had the - if you do want any discussions, I know, you know, any of (PRWG) members would be happy to participate in helping expand the knowledge of the group to get that process or the implementation properly sorted.

Marc Anderson: Okay. Thank you very much. I was going to throw it back to Roger for a second. So let's - sorry about that. Roger, so we had two other threads around additional standards, track work needed. And you - and one of them was around the OpenID standards.

You know, and the, you know, I guess I'm not completely clear on, you know, what additional work needs to be done there. And maybe - and what we can do. So can I ask you to expand on that a little bit more?

Roger Carney: Yes, this is Roger. And again, from -- I think from our pilot group -- maybe we can drop this discussion since we don't have to provide authentication in our profile? But for the profile pilot there's several -- and I didn't even know Alex wrote that, that's great -- but Scott also wrote an OpenID spec. And he has started some discussion at IETF.

And I don't think it's gotten a lot of traction anywhere. So yes, it's a draft that's probably, I don't know, a year old. Scott? I don't know how old it is. But it hasn't gotten a lot of attention.

And I mean that's not saying Scott doesn't write good stuff. I'm just saying it has to go through many iterations before it's even close. Even to a workable draft. I mean I think we're a long ways away from an OpenID workable draft.

So you know, some of the big parts of OpenID is this claims section that you can use to expand OpenID up quite a bit. And I think that we'll have to. And Scott had already started in his draft. And I don't know if - Alex, again, maybe you can talk to that on yours.

He already added a couple new private claims items to start tracking. One was logging for law enforcement and things like that. And I think that -- as we know more, requirements come through -- we'll be expanding that section. And how we can get as clear of a picture from our third-party authenticators about not just who but what they want before they get to the RDAP service.

Again, I want to press as much of that ownership and ability as far from us as possible. And then we'll make the jurisdictional calls if it makes sense to us, once we get that information.

But from the technical standpoint, I think the OpenID has quite a bit to go. Even if -- again -- that we agree that that's the way we're going to go. It still has a lot of work. And from the cert side, I can't even say. Because I haven't even looked at that.

I'm guessing from our last discussion we had -- at IETF -- on the certs, it would - too would take several months to iron out what needs to happen there. And the certs being somewhat less flexible would need to be defined ahead of time, where the OpenID is a little more flexible and can be changed. So.

Marc Anderson: That - thank you for that. That actually clarified it a lot for me. So I appreciate that. Thanks for letting me put you on the spot. Anyone else want to jump in on that? Or - and then you had a third thread that you brought up that I want to jump to in a second.

Just sort of a quick time check. We - the session runs till 10:15 so we have a little over 15 minutes left on this session. And we're winding down on the agenda, so I think we're doing good time-wise. But just thought it'd time check that for everybody.

The other thing Roger raised though that I think's important is a thread I want to spend a little bit of time on. And that's around, you know, what, you know, what's sort of the approval process for our work product. And, you know, for lack of a better word there.

And it's something that came up on the call last week. And it was originally raised by (Donna), actually (Donna Austin) asked, you know, okay what is the approval process? And Roger brought up the fact that, you know, the original profile when developed went out for public comment. There was a public comment period.

And so you know, I guess it's something. Until you know, just last week we hadn't really contemplated or considered is, you know, what's, you know, what comes next? What is the process for you know, sort of approval or finalization or acceptance for the work product of this group?

And you know, I'll give Francisco an out. He's been on PTO and maybe just hearing about this. But you know, I don't know if you have anything you'd like to add or share on that?

Francisco Arias: This is Francisco Arias from ICANN. And so I raised this internally. I don't yet have an answer for you, but we're working on that. So I'll get back soon.

Marc Anderson: Great. Thank you for that. And I don't know, does anybody have any input for Francisco? Maybe what we would like to see?

You know, Roger mentioned a comment period. Is there anything that we think is appropriate or is not appropriate? You know, we have an opportunity to give Francisco some feedback or suggestions if anybody wants to jump in. Jim?

Jim Galvin: So Jim Galvin for the record. Maybe a little clarity here, just to be precise about what we're asking for and what we're talking about. So you're talking about a public - potential public comment period on our profile and work product out of this?

Is that what we're talking about? Because I guess, I don't know. I mean we got here because of a public comment period. And, you know, the whole point of this is for the people to exercise all of that. I guess I don't really know whether ICANN processes suggested there ought to be another public comment period or not.

That's kind of interesting. I mean one could make the argument that just creates more delay in all of this, which is kind of what we're all trying to avoid. And aren't we here to sort of get past all of that as far as that's concerned? I mean I don't know that I feel strongly about it either way. But I guess I raise the question. I think that let's have the full context here.

If we're going to talk about a public comment period, can we motivate why that would be useful or helpful? Anyone have any ideas about that?

Marc Anderson: Before I throw it to Roger I'll just say I think that's - I don't know that we're advocating for or against a public comment period. I, you know, to be honest it's until it was - Donna raised it last week.

It's not even something that I had even thought about. And Donna raised that, it was like oh, good question. And so if Roger I don't know if you want to add to that.

Roger Carney: Yes. And again, I think that we had a public comment period when we created a profile before. And I think that's the only reason a public comment period came up as a discussion.

I think Donna's real question was when we publish these drafts, what happens? You know? What's the process that, you know, that ICANN is going to take to move them from an informal working group to actually something that contracted parties are going to use?

Jim, I think that -- if we went to the stakeholders' groups -- I think they'd be a little surprised that there would be no public comment, just because this is a small group that's making the decisions. And I - it, to me, it would surprise me that the stakeholder groups would not ask for one. But I don't know.

Marc Anderson: Anybody else, thoughts on this one? Okay. I guess we'll look forward to, you know, what Francisco comes back with. But, you know -- again, you know -- I think it's just not something that's come up. You know, what, you know, we produce a profile, you know, what comes next? What's the next steps that follows? So you know, I think it's - it would be good to get clarity on that.

Jim Galvin: So yes, Jim Galvin again. I guess I have a question maybe for Francisco. As far as I know there's only one definition of a comment period, right? Public comment period. I mean you don't do things like short comment periods or anything like that, do you? Have we ever done such a thing? Yes?

Stephanie Duchesneau: I think there has been...

Jim Galvin: No I think that's - go ahead.

Francisco Arias: I'm not an expert here on that. I think that's more of a question for my policy colleagues. But I think the length of the public comment it is not set. So you can define how long the public comment can run. I believe so.

Stephanie Duchesneau: Yes. From my recollection there's like standard processes for the comment period. But where we've seen exceptional need -- I remember in like the IANA context for instance -- there were a couple of places where we had comment periods that were shorter. And similarly there's been a couple of times where we've had comment periods that were longer.

Jim Galvin: So maybe then the only comment that I would add to this -- sort of think back how many times did I say comment? -- no, but seriously. You know, in the interest of just trying to get support and make sure that people don't see -- or don't at least perceive any kind of end run or unnecessary mandate -- maybe some kind of short comment period would be a reasonable thing.

And I don't know what the definition of short could be. I think I'll just stay away from that discussion, but somebody will know what that number ought to be.

Marc Anderson: Fair enough. Thank you. Any other thoughts on this before we move on? Okay. Our last agenda item is on OpenID and certificate-based access to non-public data. You know, again here we've touched on this, you know, a number of times throughout the conversation today.

So I, you know, I think we've already had a pretty good discussion. And maybe I'll try by, you know, I'll try and kick this off by maybe summarizing where I think we are right now. And maybe you all can jump in and correct me where I got this wrong.

But I think where we are right now is that we've identified two likely mechanisms for providing access to non-public RDS data. And that's using OpenID and certificates. But also has been noted that there's also an option where the two can co-exist as well.

I mentioned, you know, earlier that there was excellent discussion on this topic at that - the (row). Many of us in this room were there. If you weren't, it might be good to take a look at the material and recordings from that to get a little more background on you know, where OpenID and certificates might make sense, where they could co-exist, what the pros and cons of the two possible solutions are.

But I think that's - sorry, I just got the 10-minute warning. I think that's, like that's where the conversation is. But we haven't, you know, we haven't made a determination on which to recommend or what the solution will be. And that's okay. Because the, you know, sort of the discussion on uniform access and the policy work on that is - still needs to occur.

But earlier today we talked about how, you know, I think we want to keep the momentum going. Draw a line in the sand on the profile discussions for implementing RDAP for the temporary specification and move our focus to uniform access and looking at these technologies for providing access to non-public data using RDAP as the tool.

So I guess I'll stop there. Is that sort of a fair summary of where we are and what we're looking at for next steps? I'm seeing some nods in the room. And Roger, go ahead.

Roger Carney: This is Roger. And I guess maybe we can ask (Francisco Arias)'s staff to actually take back and is it appropriate that we're creating an authentication pilot to take this to the next step? Or is this something that is going to be coming from the EPDP or something else?

I have no idea is it appropriate. I mean this group was created kind of ad hoc a couple years ago. So I don't know if we can decide that hey, our next step is this. Is that actually what we should be doing?

Marc Anderson: Go ahead Francisco.

Francisco Arias: This is Francisco from ICANN. I think when the pilot was created -- last September -- the plan was to allow for experimentation with the technologies so that group inform policy decisions for lack of a better word.

In that context I think it's - it seems okay to me to continue experimenting with the pilot -- and the for example the authentication technologies -- so that will help inform the discussions around the accreditation model or the uniform access model. I don't know what's the right term now.

The - I think -- in terms of the pilot -- the temp spec I think allows for contracted parties to continue providing pilot services until the - a point where the other profile is required. Which is what (unintelligible) identifies after it's finalized and ICANN requires and so on and so forth.

So until the point where the production services are a requirement, I don't see an impediment for the continued experimentation with the pilot who does -- for example -- authentication technologies to see which is best or any other technology that we would like to test. That would be my input on this.

((Crosstalk))

Marc Anderson: Thank you...

Stephanie Duchesneau: Bill's on the - oh, sorry. Stephanie Duchesneau from Google. I realize I haven't been introducing myself. To build on what both Roger and Francisco were saying, first in terms - I can envision a situation where the might be an additional - an initial deployment of RDAP.

But certain aspects of it that we still need to be building off of or experimenting with based on what we're seeing coming out of the PDP. So I would encourage a little bit of flexibility here in that. If that initial deployment has happened but there's stuff that we still need to be testing, maybe it makes sense to like continue a pilot working group even beyond the implementation date.

And to me it seems -- regardless of what we're permitted to do -- it seems like we want to be kind of taking as much as we possibly can out of the core scope of this EPDP and parallelizing as much of the work as we possibly can.

So I think this is something where everyone benefits and to the extent that ICANN needs some sort of after correspondence on the table so we can move that forward. That's something that we could push up.

Marc Anderson: Agreed. Go ahead Alex.

Alex Deacon: Yes, Alex Deacon. I agree 100%. I think we need to parallelize as much as we can. And any work we could do on the implementation in parallel to what's happening on the policy side I think is time well spent and required from my point of view.

Man 2: Yes, also agreed. We - the implementation work needs to be done in order to help inform the policy work so it doesn't later - so the policy work doesn't end up wrapping the implementation work around an axle.

Marc Anderson: I think -- of all the times, you know -- I think we have pretty strong agreement here on this one. So not to - don't want to beat the dead horse I think. Any - so let's draw a line on this one. Anything else anybody wants to raise, you know, on this topic?

Okay. And that brings us to the end of the agenda. You know, I'll raise any other business. Does anybody have any other topics they'd like the raise? Anything new that we haven't covered? Go ahead Alex.

Alex Deacon: So for those of you who don't know me, I'm here representing the users of an RDS system or RDAP. And so I think this is important work. And you know, if there's a way I can be involved and add value to what you guys are doing I'd love to be involved. Again, I don't know what the process is to be joined into this group, but if it's possible I'd just like to throw that out there.

Marc Anderson: Go ahead Stephanie.

Stephanie Duchesneau: Thank you for showing up. I think that's the first step and we need to have more people participating. So I think it was really great, and hopefully you can continue to work with us.

Alex Deacon: Yes, I think this group originally was just you know, the contracted parties that have to stand up an implementation. But I think -- especially as we move into this next phase -- it has to expand so that we get the outside views and direction. So I think that'd be great.

Marc Anderson: Thank you both. Francisco, go ahead.

Francisco Arias: Thank you. So Francisco Arias from ICANN here. So just to add to what has been said in terms of participating in the pilot. And participating in discussions. I leave that up to you of course.

But in terms of what would be valuable input here as user, Alex I think it would be great if you could perhaps try to use the services that already provided in the pilot to test out the RDAP service as it is -- especially the corporations that are offering already authentication -- so you can see both technologies at work. And give your input on what you see there that is working or not working for you.

One venue that ICANN has offered for these discussions to happen, we have an open mail list called gTLD dash Tech at ICANN dot org. So if you search for that I'm sure you will find it. If not, I can provide - I'm happy to provide a pointer to you where you can subscribe there. And feel free there to -- absent other mechanics available -- feel free to use that forum to provide input on what you see in terms of the pilot. Thank you.

Alex Deacon: Thank you. Yes, I spoke to Marc a few days ago and so I will give feedback. And I have used the system. I didn't use the credential that was issued to me, but to someone else. But maybe I'll get my own and I'll rejoin the list you mentioned. I was on it previously but then I need to rejoin that. And then I'll post my thoughts there.

Jim Galvin: I'm sorry. Alex, did you just say you used somebody else's credential to do something you weren't authorized...

((Crosstalk))

Woman: Shush, shush...

Jim Galvin: ...shocking.

Alex Deacon: Yes, I did say that, didn't I? Let's keep it between us. Let's make sure we don't record any of this.

Marc Anderson: I think we can get you your own credential so you don't have to share. All right. Couple of administrative items to end here. Just, you know, we'll continue that conversation you know, with our following ICANN - you know, following the ICANN meeting.

We'll follow the conversation with our weekly Thursday meetings. Throw it out there, next week is Fourth of July week for those of you in the United States. That's a big holiday. Our regular meeting would fall on July 5. Do we want to meet that day? Any thoughts on that? Jim's shaking his head no.

I'm not taking the day off, so if people want to meet and it'll be a productive meeting I'll have it. But I don't want to be there talking to myself. So...

(Roderick): You can talk to me.

Marc Anderson: ...I can talk to you? Very good, thank you. All right, go ahead.

(Roderick): This is (Roderick). Yes, I guess I would vote not to have one. I'm not sure that we have anything that has to be covered. We've got to get the documents cleaned up and everything. But I'm not sure that we have to have a meeting.

Marc Anderson: Any objections to cancelling the next week - next - the July 5 meeting? Okay. So I'll - I think Sue's probably listening in and got that. But I'll coordinate with Sue. We'll cancel the next Thursday meeting, but we'll pick up the following Thursday our regular weekly calls.

And you know, try and keep this momentum going, wrap up this profile, and move on to the work on uniform access and supporting that effort. They - and I want to say -- you know, in closing up here -- I want to say, you know, thank you to everybody for a good and productive meeting.

I want to, you know, particularly thank Jim and Roger. I didn't have to do any work putting together this agenda, so I appreciate your help and support in doing that. And I, you know, and definitely everybody that's participated and provided input.

It's, you know, I'm not exactly sure how I ended up chairing this group. But the support I get from everybody has helped make that a - an enjoyable experience for me. So thank you everybody for all the help and support and participation. I appreciate that.

Jim Galvin: So thank you Marc. But if you're finding this an enjoyable experience we're definitely doing something wrong.

Marc Anderson: Fair enough. And, you know, I appreciate that. We're now one minute over the agenda items, so let's go ahead and end the recording. And if we - we can wrap it. Thank you very much everyone.

END