ICANN
Transcription ICANN Kobe
GNSO EPDP Team Meeting
Sunday, 10 March 2019 at 17:00 JST

Rafik Dammak: Okay so I think it's a good time to start. I think we have everyone here. So today it's our meeting with the colleagues from the Technical Study Group and I think it's an opportunity to learn more about their work, what they did and I think what also they delivered just two days or three days ago.

And so maybe help us to get better understanding of what they tried to work on and maybe if they have a question for us or something they want to know I think this is good opportunity and I think we received the presentation a few hours ago. I hope that everyone had the chance to review it, but still I think it's a good opportunity to make the presentation and have the discussion and dialogue. So we have Ram, I think you are the chair of that Technical Study Group so if you want to start and…

Ram Mohan: Thank you, Rafik. I'm Ram Mohan; I'm the coordinator for the Technical Study Group. My apologies for being a couple of minutes behind, I was working on my step count from the (KIC) to here. We have a presentation to provide here for you and we're going to use that, but the idea is to have the presentation really be a guide, if you will, for a conversation.

The primary goal of the TSG, the Technical Study Group here in Kobe is to look at - is to listen and to invite feedback on the work that we have done. What we have done so far has - is the best way to characterize it is we have

a draft technical model that we think might be a feasible model for implementation. But we don't know. It's a bunch of us who have real experience and expertise and specific technical areas. It's a group that I've put together. Scott, there's a seat right here right next to me if you want to come and sit? And I thought that that would be a good opportunity.

So with that, if I may just ask for the Technical Study Group members who are here if you could please take just a moment and introduce yourselves and then we'll go through the slide deck. Let me start with you, Gavin. Great, come on, John.

John Crain: I'm just staff. John Crain, staff support on this technical support.

Gavin Brown: Gavin Brown, CTO of CentralNic.

Jody Kolker: Jody Kolker, Go Daddy.

Jorge Cano: Jorge Cano, NIC Mexico.

Benedict Addis: Benedict Addis, SSAC.

Steve Crocker: Steve Crocker, newcomer.

Ram Mohan: Yes, I don't know if we have - I think that's it, right, that's the set of folks that are here. Okay, let's get the slide deck…

((Crosstalk))

Ram Mohan: Tomofumi, why are you sitting there? Please, there's a sit right here, right next to me.

((Crosstalk))

Tomofumi Okubo: Tomofumi Okubo, DigiCert.

Ram Mohan: Okay, thank you. Let's get the slide deck up. Okay, fantastic. What we thought was - we'd walk through the work that we have done and just, you know, this is what we have in the agenda. If we could go to the next slide? Thank you.

So just to give you a sense of the motivation behind the creation of the Technical Study Group was to balance both data protection requirements with the legitimate interests of third parties through access nonpublic gTLD registration data. That was one of the motivators. And the other was an intent to reduce the potential liability faced by gTLD registries and registrars when providing such access.

But that's really not the TSG itself. And this just tells you, you know, what prompted Göran to ask me at the end of the - or somewhere towards the end of the Barcelona meeting to put a team together. And so I did. I put a team together and what we sat down and we talked about was the purpose of the Technical Study Group, which is to explore technical solutions for authenticating, authorizing and providing access to nonpublic registration data. And it's built on the RDAP protocol underneath of all of this.

Now, one of the things that we've been very clear from the get-go and we continue to be that way and if you've had a chance to look at the technical model draft that we have put out, is that the - in our remit we do not make any decisions or recommendations on policy questions. So we do not have any opinions on who gets access, what is access, which data fields should or should not be accessed, under what conditions should any access be provided, what is the meaning of a legitimate interest.

Those are the kinds of questions that we are specifically not either looking to answer or looking to provide recommendations on or any decisions about. So that's a sense of what we've got. The charter of the TSG we made it public as

soon as we, you know, we had some consensus around it. The TSG has met several times on the phone, several times in person. The notes and minutes from each of those meetings is public. The mailing list that the TSG uses is accessible and is public. So we've tried to keep as much of what we've - or what we're doing in the public eye and open for input as possible.

Next slide please. This gives you a sense of who are the people in the Technical Study Group. As you know I'm the coordinator, Benedict is from the registrar of last resort, Gavin is from CentralNIC, Jorge from NIC Mexico, Steve Crocker from Shinkuro, Scott Hollenbeck from VeriSign, Jody Kolker from Go Daddy, Murray from Facebook, Andy Newton from ARIN and Tomofumi from DigiCert.

We've had an excellent team from ICANN Org who's been providing support for the work that we've been doing. But that's - these are the members. And if you have quibbles with who the members are, etcetera, you know, I'm the person you should blame. And if you like the members who are there, please tell them that you really like that they're there.

On the next slide, this is our model, how we've run our process. We've worked on being consensus-driven. The process is iterative in the way we work. And the focus has been quite relentlessly technical in its nature; that's been - but those are - that's been the fundamental engagement model.

Here is what we did, we began by defining key questions and considerations. Then, we sat down and we said to make any further progress what are the key assumptions that we make? So we identified a bunch of assumptions. Then we identified some use cases and we also looked at what the user journey is. The user journey, some folks will listen - will also think about that as what are the user experience, if you will, okay.

Then we said what are the system requirements? And the system requirements that we sat down and thought about are functional

requirements, operational requirements as well as management requirements. Once we did that, we were able to get together and come up with a functional requirement as well as mapping what the functional requirements with what potential model might be.

We then built actor models which are who are the actors and what do they need, and then how do you do then go about responding to the needs of these various actors, right, so we built several actor models. And then we thought about if you want to implement a solution, what are some of the considerations that you have to keep in mind? So we went and determined those considerations.

And when all of those prerequisite steps were done, we were able to sit down and arrive at a proposed solution. And we did that in really some fabulous face to face session that we had I guess three weeks ago now was it, Gavin, I don't remember, three weeks ago maybe, four weeks ago. But it was iterative, you know, we had some proposals, we thought of a solution and then we were able to break it down and say, that doesn't work, this part may be good, here is an idea but it may fail. So it was that process, okay.

And when we were done with that, you know, thinking about it several times over, we were able to come to a - what we thought was a pretty good draft technical model.

Now as we were doing that, what also became apparent was that there was a whole set of other considerations that we thought were - we were uncovering these considerations but it was clear but that those considerations weren't in our remit, okay, it wasn't for us to actually do anything with these considerations, but since we had uncovered them, we wanted to make sure that we actually documented them and that we made them available for the community, we made them available for the policy makers, for everybody else who has to go work on this area, that they look at them, right.

And we're now in step 10, right, community feedback. That's the primary thing that we're doing here in Kobe. And when we do that, when - on Wednesday the Technical Study Group I believe with the exception of Murray, all the rest of us are here, and on Wednesday we're going to spend the entire afternoon together face to face again to synthesize what we are hearing from the community here in Kobe, what's coming on the email list, etcetera to sit down and say, what were the things we got wrong? What were the things that we seem to have some validation for?

And hopefully that process we can then turn around in the next couple of weeks' time to put out the next and hopefully the final version of our technical model. We're expecting to meet face to face in mid-April and in that meeting we expect to wrap our work and deliver something to the community that then, you know, will take a life of its own or not but that's really the plan.

If you go to the next slide, in the key questions, this is at the very start of our work, right, we sat down and we said, there is a whole bunch of questions and a bunch of considerations, what categories should those questions and considerations be? And I'm not going to read through all of the words that are there on the slide, but that gives you a sense of the breadth of the considerations and the breadth of the questions that we started with. If memory serves me right, we started with something like 17 or 18 questions that we thought needed to be thought about and answered.

So that was - that was where we started. The key questions and considerations are actually listed as part of our charter document that we published I believe in November or December. So if you want to go look at these and look at the questions under any of these categories, if you go to the page, it's just ICANN.org/tsg, if you go to that site you will find that there's a charter, in the charter you will find these key questions as well as the - the categories as well as the questions underneath them. Next slide please. Thanks.

So we - when we walked through all of that, as I've shared with you before, what became clear was we had to actually identify what assumptions we're making because having clarity on the assumptions meant for us that we didn't have to go reinvent that wheel, right? We could say, these things we take for granted and all the rest of the work that we do are based on that foundation of the assumptions. So that was where we started. And I have some, you know, several folks here who are going to help me help walk through those.

Steve, do you want to take the assumptions slide?

Steve Crocker: Thank you. So Ram was asking me to speak about the assumptions which comprises this slide and the following slide. In the report I listed 12 assumptions, numbered 1-12 of course, and the numbers in parentheses on this slide and the next slide refer to those. The basic picture is the one that you have here, you have queries aimed at or directed toward the nonpublic information of gTLD data. And the whole structure of this is that ICANN is reducing the liability - the GDPR liability for - on the registrars and the registries by interposing a functional gateway that involves checking credentials and interacting with the credential process and the holders of the various data.

So the main elements - the main assumptions are the ones listed here that RDAP is the mechanism that will be used, the Port 43 will be deprecated and that it's only the access to nonpublic gTLD data; that queries from unauthenticated sources will be handled in accordance with policy but they will be handled; and that ICANN oversees the credential protection and validity.

Next slide please. Oops.

Ram Mohan: Yes, Steve, this is…

((Crosstalk))

Ram Mohan: This is a short deck.

Steve Crocker: Back up. So there are 12 assumptions. Read the report. Over to you. The slide that's missing basically partitions the 12 into the ones that are here and then others which are kind of supporting and mainly talk about what the evolution and flexibility has to be - what dimension the flexibility and evolution have to be built into the process and those have a consequence in the later portions of the design process but the details are in the report. Thanks.

Ram Mohan: Thank you, Steve. If you move onto the next slide, that gives you again the report details all of this, this is a quick summary. I didn't think that we wanted to go through every single piece of it. We will go through every single piece of it tomorrow in the community session that is scheduled at 1:30 in the afternoon so all of these pieces will be presented there. I just didn't want to, you know, go through all of those here. But happy to field any questions that you have on any of these.

But in summary, 12 assumptions, five use cases that we defined and deriving from that were nine system requirements, okay. Next slide please. These are the five use cases that we came up with. And what we did after defining the use cases was we put them on a matrix and we said, you know, which of these are critical use cases that we must address and which of these are useful but not necessary?

And as it turns out the first four use cases we thought were all critical and necessary. The first use cases that authorize users, require access to domain records and that access might include both single queries or multiple queries. The second use case is that a user receives authorization online and gets data immediately. And the authorization that the user receives may - could be broad and ongoing so they don't have to keep coming for authorization or it could be specific and constrained.

And when we say “constrained” what we're saying is that it may be constrained to you may be allowed access to a record or data pertaining to a record, right, so that was the second use case that we considered.

The third use case is unauthorized, unauthenticated users request access to data elements that are associated with domain records, right. The fourth use case is authenticated user requests data for which that user is not authorized, okay. So that was the fourth use case. And of course the fifth use case is that the subject of - the data subject requests their own data and the way they request that data is by coming through this system, right? So those are the five use cases that we came to.

The next slide. So again in the document, the draft technical model that we have put through - put out and, again, we’ll go through this tomorrow in the community workshop, but this gives you at a high level the proposed solution and the proposed technical model. I’m wondering whether Jody or Jorge, whether you want to walk the group through that and I’m picking on both of you because I’m thinking perhaps, you know, you might cover individual pieces of it. Shall I ask you, Jody, first?

Jody Kolker: I will do my best here but I’ll ask Jorge to keep me honest. Basically the way that our design would work is that the client would be able to be authenticated by an authenticated provider only after getting an accreditation basically. They would send a request to that ICANN RDAP access service. So the only way that you would be able to get the nonpublic or the private information would be through the proxy that ICANN's going to provide, which Steve has just covered.

From there, there would be an authentication that would be done by the access service basically any kind of a - what I want to say Gmail, Facebook, anything like that to provide authentication so that ICANN would not have to have user names and credentials.

There would also be an authorization service which would be basically providing whether who has access to receive that data. That would be provided by a credentialing service such as LEA, maybe DNS providers, etcetera, or the DNS community.

Once that is done then that request would then go to the registry or the registrar, whichever contracted party is closest to the Whois for that data or the contact data or the nonpublic data I should say.

Ram Mohan: Thanks. Jorge, did you want to add anything?

Jorge Cano: Just (unintelligible) need to access to the public data you will use it - the simple RDAP standard way.

Ram Mohan: Great. Thank you. There are more details in here and those details are in the document. And again, those details we will go through the specifics of those details in our presentation tomorrow. The next slide please.

I had mentioned earlier that, you know, as we were going and putting together a proposed solution we had discovered considerations that may be of relevance to other parts of the community. And we thought that our job was to document these things, make these observations, document it, and make it available for, you know, others including the EPDP group, others to actually go think about it and decide if they wanted to do anything with it.

Gavin, did you want to take this?

Gavin Brown: Yes, happy to. So yes, as we deliberated we - a few things came up and we realized that, as Ram said, we couldn't answer them ourselves. So I'll just go through - do we have two slides for this? Yes, okay. So the first one is the question of data retention. So one of the - the models that we - well the operating model that we've taken doesn't assume that any personal data

would be held by ICANN or the service provider that operated the access system because it's all coming from the contracted parties instead.

Nevertheless, we felt it would be appropriate for some form of data retention policy to be in place. It may also be the case that the authentication and authorization service providers may in fact store that information and therefore the data retention would be something they should consider.

Second item is service legal agreements, we felt that, again, it was in - it would be important I think for users of the system to be able to rely on it and service level agreements are a key part of that. The - they would have to apply to all the different actors in the system because of the way that it's architected, you know, each component in the system relies on one of the other components.

So the RDAP gateway relies on the contracted parties. It also applies - or sorry, relies on the identify providers and authorizers to be available so it can make a determination about whether to allow a request. And obviously the users of the system rely on all of those systems, all of those providers to do their jobs as well. So we again suggested that service level agreements for each of the different actors in the system should be produced and a way for them to be reported on and enforced would obviously be part of that.

It became quite clear that the model we proposed could potentially apply quite a lot of operational burden on ICANN Organization if they end up being the entity that runs the request system. So we are recommending that the organization do a feasibility study on that on any system that they're required to operate and that they should gather expert feedback through a public comment system to determine whether that, you know, their feasibility study was up to scratch.

And also as a coordinating party there are legal and operational risks because they're relying on third parties to do things that if they do them

wrong ICANN could shoulder some serious liabilities and so it would be appropriate again for ICANN Organization to assess those risks and take steps to mitigate them again through data sharing agreements and other mechanisms.

Next slide please. So again the risk to the contracted parties, we can't comment on whether the system does eliminate or reduce that risk. And we feel that the contracted parties themselves have to make that determination.

Finally on so last one, transparency, we think that transparency on how the system runs is vital, it's quite common for large organizations who are hosting or providing access to data to provide transparency reports on what data is being asked for, not necessarily in specifics but in terms of, you know, general statistics about what sorts of requests are being made, who they're coming from, what sorts of organizations they're coming from. And we again would recommend a transparency report that ICANN should publish about how the system is being used.

And finally a mechanism for handling complaints, we obviously accept that there will be cases where a requester submits a request that they are not satisfied with the outcome because they get rejected or they don't get that data they think they were expecting, and so there may be a possibility that ICANN Organization will receive deletion requests which may or may be able to satisfy and so we suggested that again ICANN Organization or the elements - the actors within the system need to be able to handle complaints and escalate them accordingly. Thanks, Ram.

Ram Mohan: Thanks, Gavin. If we can go to the next slide. Our plan is to get input from the community here in Kobe and incorporate that into the daft technical model. We have I think three or four more targeted meetings that the Technical Study Group intends to do. We've been doing it on the phone for the most part but we've also been meeting face to face and I anticipate that the - we will likely have to meet face to face again in April to integrate all of the inputs.

And one of the things that became apparent to me and to others in the Technical Study Group was that as we were putting together the document to be ready for publication, you know, in time for Kobe, it became clear that there were entire pieces of it where we had in the TSG because of the work that we had done, we had developed a shorthand. We had, you know, certain concept that we just automatically knew because we'd discussed it or we'd spent 30 minutes, you know, putting it up on a white board.

We had words you know, there was a glossary, there were several pieces that needed - that need to get done and need to get put together and it's - if you want to have a document that is going to be - reference quality then we'll need to spend that time for it. So I expect that, you know, by the 23rd of April we have a, you know, we've said that as a specific deadline on the 23rd of April our intention is to publish the final technical model.

And really the way this has been set up, publish from our point of view is we're going to hand it off to Göran who, you know, is kind of the sponsor of this whole thing. We're going to hand it to him and he's got other things that he's got to do. But our - we will wrap our work and I'll be very happy to get to that because if you go and look at our charter, the - one of the most important pieces of our charter on our work plan is Item Number 13, and we can only achieve Item Number 13 after we finish the 23rd April deadline. So that's it and open up for discussion and questions.

Rafik Dammak: Okay. Wow. Wow. Wow.

Ram Mohan: This is great.

((Crosstalk))

Rafik Dammak: Okay.

Ram Mohan: Give me a second.

Rafik Dammak: Yes.

Ram Mohan: (Elisa), you're here, right? So (Elisa), can I, from the TSG side, can I please task you with taking note of the questions and, you know, actions that may arise from that? Thank you.

Rafik Dammak: Okay thanks, Ram. So with many cards, I'm not sure what order but so bear with me, guys. So I think we have Tatiana, sorry, I cannot read the name, Sara, James and then I think Margie, Georgios, Ashley and Alan. Okay, let's start with Tatiana.

Tatiana Tropina: Thank you very much. Tatiana Tropina for the record. My first question is about the timeline. I see that you're going to finalize the model in April. On the EPDP yesterday we were talking about restarting the work on the Phase 2 probably in April. So basically you're going to finalize this model without any policy implications that might occur in the Phase 2. It's just why I'm talking about this like for example, on the EPDP we are now discussing whether we should call it access or disclosure, for example, and some other issues.

Then some of the cases looked very policy-related to me or they must rely on policy sometimes heavily. So this final technical model, the word "final" is just a kind of fiction? Are you going to adjust it to the result of the policy discussions? Thank you.

Ram Mohan: Thanks, Tatiana. Great questions. It's final just because the TSG will cease to exist after that. But our hope actually is that the model will live on and that, you know, EPDP, other folks in the community will take that foundation that we've built and will go modify it. You know, if in our document we use the word "access" and the word that you know, you come up with and the decision is is "disclosure" then you should take it and make it disclosure, right?

So the pride of our work is in actually helping provide a foundational start to the rest of the implementation and the decision making. All of the policy things that have to be done - we fully recognize it has to be done and our intention is not to go presume what those decisions are, it's to say if there is a question on is such a thing feasible, can there be a Uniform Access Model and if such a thing feasible?

Hopefully you can look at what we've - the work that we've done and say, maybe there are elements that you can use, co-opt, as you go forward. So we actually don't know from the TSG what the future of this final technical model is going to be. What we know is that this is the final thing that we will do. Steve.

Steve Crocker: Just to build on what Ram has said, that's a great question and we've actually done a little bit of thought exactly along that line, how do you build a, you know, a (unintelligible) design that is intended to take any policy if you have no idea what the set of possible policies are going to be.

So there's no guarantee but we actually did ask that question and got a positive answer in that for the set of things that we think are on the table and likely to be involved, this passes the test. But of course the proof will come after you - what comes out of the policy development process and then that may force some evolution and so forth. But a good faith effort at anticipating that question and trying to do it without guaranteeing because you can't and so your question is right on point.

Rafik Dammak: Okay thanks, Steve. So we have Sarah and then James.

Sarah Wyld: Thank you very much. This is Sarah Wyld. I want to thank the team for joining us today. I appreciate your time and I look forward to the session tomorrow as well. I note that your assumptions and consideration slides say that this system reduces potential contracted party liability. I would like to hear more

about exactly how that is accomplished. The two slides do seem to contradict each other. The assumptions says it does limit liability but the consideration 5 says you cannot comment on if it increases or reduces or risk, so how does that work?

Also I'd like to hear more about what happens if a contracted party does not agree with the decision to disclose data, is there room in this model for that to be disputed or disagreed with? Thank you.

Ram Mohan: Thanks, Sarah. Great questions. We went in not questioning the assertion that a Uniform Access Model may reduce the liability for contracted parties, right? So we're just stating that; we're not saying that we agree with it or we don't agree with it, we're saying that's kind of a base condition that has been provided. And with that base condition we went about our work to go and look at what a model might be.

As we went through that process, what became clear was that that assumption may or may not be valid which is why in the considerations we're saying hey, you know, we flagged at the very start that was an assumption but each party who is actually present in this thing has to arrive at their own decision on whether the liability is reduced or not.

So that's why - we actually don't have a dog in the hunt as far as whether it reduces or doesn't reduce the liability. What we are focused on is how do you get the access to nonpublic data done if ICANN is the primary gateway to - or the sole gateway to get that data?

Could you remind me of the second question?

Sarah Wyld: Thank you, yes. What happens if the contracted party does not agree with the decision to disclose data in a specific situation? Can we say no?

Ram Mohan: Sounds like a policy question.

((Crosstalk))

Steve Crocker: We have the Queen of Hearts solution.

Rafik Dammak: Okay thanks, Steve. So let's move to James and then we'll go to Margie and Georgios.

James Bladel: Thanks, Rafik. James speaking. And my question was very similar to Sarah's so I put my card down but then when I heard Ram's response I put it back up because I have a follow up question. It sounds like the - one of the initial assumptions is that by having ICANN be essentially the clearinghouse for these types of requests and having them manage the credentials, that that assumption alone reduces the contracted parties' risks.

But I think what we've heard consistently from ICANN is that that's not necessarily the case and we shouldn't assume that contracted parties are off the hook at all. And so my question is, what requires a contracted party then if we are then obligated to seek our own legal guidance on this, which is I think part of the statement in this model and I think consistent with what ICANN Org is saying, why should a contracted party participate in this at all?

Ram Mohan: I think that's a great question and you should talk to Göran about it because I don't think that's something that the Technical Study Group…

James Bladel: Is he here?

Ram Mohan: I don't know. But I don't think it's something that the Technical Study Group is actually capable or even qualified to answer. Gavin?

Gavin Brown: Yes, so I just wanted to say, the reason why we put that in - the assumption in our assumption section is because if we didn't take it as an assumption, then the group would have just stopped on the stopped on the first meeting

because if it's not true then what's the point in doing it - designing a system? So we took it as - we said assuming that this is the case, then what would the system look like? Because if we said assuming this is not the case, then there is no system to design, so.

James Bladel: Okay so the assumption is, and if I'm mischaracterizing it please let me know, the assumption is that by having ICANN as the centralized authority for these requests, that model reduces the contracted party liability. We should take it that way if that's what you're saying.

((Crosstalk))

Gavin Brown: The TSG has no comment on that and we can't feed into that. I mean, I guess one thing I would say is I suppose theoretically there are other models where ICANN isn't that would also have the effect of reducing liability, but I don't - we didn't - we weren't asked to produce a model where that was the case.

Ram Mohan: Yes, just briefly, what you see on the assumptions is us reflecting assertions that have been made. Right? It's not us endorsing those assertions, right? It's - but as Gavin was saying, if we didn't actually take that on board then the rest of the work would have just stalled.

James Bladel: And that's fair. No, that's fair.

Rafik Dammak: Okay thanks, James. So let's - we still have many people in the queue. Okay so Margie and Georgios.

Margie Milam: Hi, this is Margie from the BC. So what was the intention for what would happen to the model once it's published? Does it go to staff? Does it go to the Board? Does it come to the EPDP? I'm just trying to understand like what the expectation was once you finished the work that was you know, done here.

Ram Mohan: Thanks, Margie. Fairly straightforward, I'm going to send this back to Göran and then from there I don't have visibility into what else happens to it. My hope and expectation is that, you know, I mean, certainly sent to Göran but it'll be published in - it'll be public just like all the rest of our work product so far is public so that'll happen.

But beyond that, what's going to happen to the model, what's going to - how will it evolve, those are questions that the TSG is not focused on because I've been fairly clear from, you know, when Göran asked me last year to - last October to do this, I told him that I'd only do this if it was a defined project with a specific deliverable and after which this group would dissolve because it really - the rest of the work has to be done in other venues, right?

This is an expert - technical experts group that is coming up and saying here's a model and we think it's a pretty good model, right. And then beyond that we're not looking into that piece.

Margie Milam: Okay, and then I have a follow up question. In our report we have the idea that there would be different layers of elements - data elements that (unintelligible) depending upon the purpose so, you know, if you have a particular purpose and you're accredited you have access to certain amount of data. Does this model accommodate that kind of difference in delivery of data?

Ram Mohan: We believe it does. We had quite a bit of discussion about that. And we stratified it multiple ways not only dependent upon purpose but it could also be that the - it might be that there's an organization with specific individuals, there might be differing levels of authorization based on the identity. And so the model actually accommodates those various permutations and combinations.

It's possible that we've missed some of those and that's what we're looking to get some feedback on. But the model in its core design is - it accommodates

not only your specific case but also accommodates things like the authorization is for only one query, for one element, once; or all the way to it's persistent across a period of time for a larger swath so - and inside the spectrum. So the model accommodates all of those.

Rafik Dammak: Okay thanks, Ram. So we have Georgios and then Ashley and then Alan. Please go ahead.

Georgios Tselentis: Yes, thank you very much for the work. I think it's very helpful to see already a model that puts in motion what we discuss at policy level because we visualize and I don't know if we can - if we can put back a slide - slide you had, 11, where you have the design - the schematic design in which I think is very helpful to see how things are going to be implemented.

The first question here is regarding the access service, do you see this access service to be at the central and only one place? I'm asking here regarding the question about were full registration data are going to be transferred or not and there are questions about jurisdiction, there are questions about where data transfers are taking places or not. So it's - it's important to know whether you have in your assumptions you made the assumption that we are talking about one place or we are talking about multiple places there?

The other question you partly answered that, that you may have several authorization services depending on the requestors. But do I understand that this is - this could be also completely outside from the whole system, so as an external service to that? Or it has to be embedded there? I think I'll stop here.

Ram Mohan: Thanks. Good questions. A couple of things, we didn't spend a great deal of time thinking about how the access service would be implemented operationally. And, you know, we could imagine multiple ways of doing it. But that was - so we didn't spend a great deal of time on that.

In terms of the data itself, our fundamental assumption, and I think Gavin spoke to that as well, is that the data stays where the, you know, where the data has been stored. So we're expecting that data is not being passed to another place to be stored in another place, right. So that's one of the foundational things that we started with.

Similarly, on the credentials, we're also making - in our proposal we're saying credentials are not, you know, stored in some single centralized place. The credentialing - that's why we have introduced this idea of an identity provider and, you know, this authentication provider and an authorization service. And even though the schematic here shows them to be separate, we did that intentionally. You could imagine that it's all consolidated, but we intentionally have marked them out as separate because it could well be delegated elsewhere rather than all held in a central place.

Do others from the TSG want to opine on the questions there? Benedict?

Benedict Addis: I think it's good to think of these as separate modules, the authentication and authorization as very separate modules. I think we considered various models for the - specifically for the access service, this kind of pass-through function. And it seems as if there are certain benefits to having that as a middle man. And for example, you've got - it facilitates transparency reporting, so and just to be very, very clear, no data will be stored there, it's purely a pass-through.

But for example, one can envisage that that could log requests and that those logs could be reconciled with the logs held by the registry or the registrar. So you could make sure that everybody is playing straight and you could also provide transparency reporting as a sort of extra benefit of having that uniquely in the middle. So the access service does seem as if it is - if that brings some value.

Where it's located, that's one for the lawyers. We simply didn't consider the jurisdictional implications of that and - but again our hope is that the model is flexible enough to accommodate whatever the legal advice is and whatever the policy decisions are.

Rafik Dammak: Okay. Okay thanks, Benedict. Okay so next will be Ashley, Alan and then we'll go to Alan Woods, Stephanie. Ashley, please go ahead.

Ashley Heineman: Thank you. Ashley with the GAC. First of all congratulations for being able to stay out of policy. I would have expected it to be a lot worse so I don't know how you did it, kudos. And I think what's really interesting about this that we haven't really recognized to date, which is liability is spread out here. It's not just liability of the contracted parties and I think that's a conversation that we'll start having to have in Phase 2; it's not all on the contracted parties.

And I think that should make you feel a little bit better and perhaps, you know, trying to have more detailed - because something that's not even up here, and it shouldn't be, but there's a whole accrediting process as well, which is going to be difficult.

But what I wanted to say, and I apologize in advance, so I represent the GAC and we have some very eager beavers who've put together a long list of questions. I'm going to do my best not to ask them all and I admit in advance that they might go too far into policy and you can just quickly dismiss them as such if appropriate.

I'll limit them now just to the report and some of the questions we have, have to do with confidentiality of requests, how that would be addressed. Where and how would the logs of queries be stored? Who would have access to the queries? And how would auditing work? And I think from a very technical perspective, how does this all relate to the August deadline for RDAP implementation…

Ram Mohan: Ashley, I'm sorry.

Ashley Heineman: Too much?

Ram Mohan: You have now exceeded my capacity to remember…

Ashley Heineman: Okay. I know, I'm trying…

((Crosstalk))

Ashley Heineman: …ask all your questions.

Ram Mohan: So why don't we go hit them one at a time and see if we can't address them?

Ashley Heineman: Okay sure. Do I have to say it again though?

Ram Mohan: Please, just…

((Crosstalk))

Ashley Heineman: Okay, all right. Confidentiality of requests, have - did you think about in the development of this schematic in terms of how that would be addressed?

Ram Mohan: Any of you want to respond to the confidentiality? No. Benedict.

Steve Crocker: I do. I do. We talked a bit about the logging of requests and audit-ability of the system and so forth on the one hand. And the potential issues of confidentiality of certain classes of requests. I think I speak for us, we didn't try to make a decision about it and we didn't try to, you know, say we're in charge.

But the discussions we had came out on the side of this, that for the transparency and credibility of the system there has to be basic functions of

logging and audit-ability. For protection of sensitive queries the balance is handle those in some way that protects that information but does not discard it and dispose of it so that it is then accessible to that class of people who might have the authority to look into it.

So if - just shifting to, you know, how classified information is handled, even if information is classified you still have to have processes inside of that where you have appropriately cleared people who can look at things, otherwise experience tells us that things go sideways one way or another either by slack, you just lose control of the system or you get abuse or something like that.

So in sorting those two things, gathering the information and having it be in auditable form is fundamental and then protecting stuff at the level that it needs to be protected is added onto that and those things can fit together.

Ram Mohan: Next question, Ashley.

Ashley Heineman: And I will spare all of you, not exceed anymore real time here. And I'll skip to this one question. So do you envision that there's - first of all, is this going to impact the adoption of RDAP by the August deadline? And do you think there'll be a practice of having to have several upgrades to the RDAP protocols to be implemented over time? And then I'll stop.

Ram Mohan: Great questions. We didn't specifically speak about impact on RDAP and I'll speak personally and, Gavin, you might want to speak as well. But inside the group we've actually had some demos on RDAP services that, you know, several folks have stood up. Seems to be in a pretty robust shape and seems like there is continuing momentum there. So just speaking personally, I'd be surprised if this impacts RDAP implementation.

There was a second part to your question, Ashley.

Ashley Heineman: Do you foresee changes in RDAP as a result?

Ram Mohan: Oh, yes, we spoke about that and, you know, this is our draft model. We don't know that this is what is going to survive contact with reality. Eventually, you know, whatever that evolves to might well end up resulting in, you know, some new RFCs. Gavin.

Gavin Brown: Yes, I'm not sure I have much more to add to what Ram had already said. The August deadline for implementation of RDAP is an implementation of RDAP that complies with the temporary specification and therefore only talks about nonpublic data. So this is kind of orthogonal to that.

And the other thing I would say is yes, so Ram's mentioned, we have working implementations of RDAP servers that use the underlying authentication technology that we're working on and our model relies on which is namely (AWOF) and mutual TLS. So they are well - they're pretty well tested and well evaluated within the TSG and also the wider operator world as well.

Ram Mohan: And, Ashley, that list of questions please send an email in and we'll be sure to look and them and provide responses.

Gavin Brown: I just wanted to say we do actually have a meeting tomorrow with the PSWG so maybe those meetings - those questions could be brought there.

((Crosstalk))

Rafik Dammak: Okay. Okay so time check, we have 30 minutes left and still the queue is quite long so we'll try to cover, I mean, all the questions, so I don't want to say it, please be brief but let's try to do so. So we have Alan, then Alan Woods, Stephanie, Diane, Beth and Alex. Alan, please go ahead.

Alan Greenberg: Okay thank you. Thank you very much. I've got three questions and/or comments. Use case Number 3 implies that this new system will subsume

the current public Whois portal because if you're unauthenticated you get the redacted information and everything, so we're talking about a one stop shopping in terms of where to go to get information regardless of who you are. That's - I like that.

I'm curious about Use Case 5, I think it would be really useful how the something could you identify who the registrant is? Was that discussed at all? Yes, and let me ask the third question and I'll turn it over. You list obligations of ICANN Org, there's one clearly that is implied because of your assumed - your assumption that this will reduce liability, so ICANN Org has a huge task of trying to validate that hypothesis in some way that will give contracted parties a level of confidence.

Now it might not be yours to write that because you just assumed it, but it would be nice to know if there's a plan and how they think they can do that. Thank you.

Ram Mohan: Thanks, Alan. The third question is probably best addressed by the ICANN Org folks. And I think (Elisa), we should have that directed again to Göran. For Use Case 5, we thought that that's - there will be some instances where the request comes in, right, the law allows for it so it's likely to happen therefore you ought, from a - in a completeness of technical design, you ought to actually plan for that.

But as to how to actually implement it, we didn't get there because in our analysis we thought that was a case that was a nice to have case rather than a must fall case. And I think I answered your first question also. Thanks.

Rafik Dammak: Oh, Gavin.

Gavin Brown: You had a question about whether the system would become the single point of contact for access to registration data. One of the things that's nice about RDAP that Whois just doesn't have is the ability to natively redirect someone

to the right place. So we would not expect the ICANN access server to handle a proxy through a request for nonpublic registration data but is very simple for that server to provide a redirect to the right place. That's called (unintelligible) boot strap server.

((Crosstalk))

Alan Greenberg: You're talking about implementation, I'm talking about the - from the user's perspective. They go to a website, they ask the question, whether it's referred to someone else or you pass it through and massage it is rather moot from my - from a user's point of view, thank you.

Gavin Brown: I mean, so, I mean, ICANN already has a Whois.icann.org which does this.

Alan Greenberg: And that was the question, does this new model subsume that or do you need the unredacted version and the privileged one sitting side by side? I would hope not.

Rafik Dammak: I know there is some discussion about - we need to also to hear from others, sorry for this. So Alan, please go ahead.

Alan Woods: Thank you. Alan Woods for the record.

Ram Mohan: Alan just, sorry, this is Ram, just a moment. One of the things Alan, this other - one of our design criteria was simplicity and to try and keep the model as simple as possible. So I certainly think that what you're suggesting is feasible from a technical implementation point of view. But our - we did not preclude one or the other. Back to you Alan Woods.

Alan Woods: Thank you. So again, Alan Woods for the record. Well first things first, based on, you know, the task that was set for you and we understand the scope that was given to you, I mean, thank you very much and well done in getting into that particular - the globe that you were working within, so thank you for that.

I think from - we do have feelings about it and from that point of view, I mean, especially I think where it comes from me is when I look at the assumptions, and I think there's a - we need to appreciate that the assumptions that you as technical minded people and as I read the assumptions as a legal minded person, they're not necessarily on the same page.

And it's an interesting and I would love to understand what your assumptions mean from your point of view as opposed to from my point of view because they do tend to lead to different conclusions. So we have to be kind of careful on that. But again, what I look at this, as I don't blow up the mic, is, you know, you have created something that you know, is out there, absolutely, but I think there's an awful lot of ducks need to go into a row from a policy point of view that we are nowhere near yet achieving in order to attain this.

And so I'll leave at that saying thank you very much, it's definitely a good example of what potentially could happen but, I mean, we are on a long road of a policy route to get to anywhere near that at the moment. But again, thank you.

Ram Mohan: Alan, thank you. We had quite a bit of discussion about that, and our first, if you go back and listen to the recordings you'll find the first one or two calls we were struggling with exactly that, how do you actually build a system when you don't actually know all of the requirements and all of the policy pieces, right? How do you do that?

And that's what led us to say we better figure out what the base assumptions, you know, we have to say here is a set of assumptions, we don't say that these are true or false, we just say that they exist. Now with that set of assumptions, and let's make that open and explicit, with that set of assumptions what's a feasible technical model? Right? So that was the approach. And thank you for your feedback.

Rafik Dammak: Okay thanks. Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. Thank you for your work on this. As some may be aware, we had a workshop in Barcelona looking at standards for the access model and basically the research project for which I'm funded, is looking at this problem at actually in the reverse. I make the assumption that RDAP can do it for us and I look at what is required from a legal perspective. You have made the assumption that you're providing something that complies with law and you built it.

And thank you very much because my report's due at the end of the month and I now have all this good technical stuff that I can incorporate in my report. But I do think it would have been really helpful if you had brought legal and policy people onto your team so that they could point out a few pitfalls.

As to the liability question, I mean, I think that you have created a system that distributed liability in a way that is going to make your legal costs skyrocket because each one of these players in the chain has liability now. The breach notification is 72 hours under GDPR and anybody in that chain could be the culprit in a liability scenario. So I think you're going to have to change that to avoid the legal costs because it doesn't matter how smooth RDAP is, if you can't figure out how to get this contractually right.

There are some key policy questions in terms of who's going to authenticate. There are basic questions - the same kind of things that we've been grappling with from a legal perspective about the discreteness of an inquiry, and then there's the anonymous search capability that you need for certain security applications.

So I would just like to say, I haven't got any questions like I'm going to have a whole pile of questions which I'll send to you, but I'd just like to caution everybody that this ain't going to get built by April or August or whatever that deadline is that we were talking about at the EDPB the other day, the

February 29, 2020, you know, there's an awful lot of work to doing this in a way that isn't going to cripple people. Thanks.

Ram Mohan: Thanks, Stephanie. And excellent remarks. No quibbles at all with anything you've said. I think we're on board with all of these things, clearly an understanding that this a complex undertaking in front of everybody. And we went into this with no intention or thought that this was going to be any kind of a silver bullet at all, right? If anything what we've tried to do is to say if you want to build a solution, here is a way of actually doing it.

And what may survive at the end of all of this might actually be the process of building a solution. What may also survive are some of the elements that may be relevant. All the rest of the pieces that are there we don't know what'll - whether they will survive reality or not, but we thought that the - regardless of all that, we thought that the work was still useful because it provides a way of - how do you get to something that may be feasible on implementation side rather than just have a theoretical discussion of it's so big, it's so complex, it can't happen, right? So that's really what we're trying to do.

To your comment on getting - adding more folks to the team and having it, you know, having a broader set of inputs would have been valuable, absolutely agree with you. But I have to say that as a person who put the team together I had a very clear focus which was how do you - which was really to demonstrate how can you build something, a technical model, and what is the process of building such a model.

And whether the model is precisely accurate or not time only will tell, right? But I'm hoping that the method of putting such a process together and working on it might actually be an example that might survive the rest of the work that has to be done.

Rafik Dammak: Okay. Thanks, Ram. Diane.

Diane Plaut: Thank you. Diane Plaut for the record. Thank you for this. This is much to what you're saying, this is the right framework that we need to go forward. And whether that's clearly going to be - need to be adapted for legal considerations, as Stephanie has said, and everyone has expressed. And just to start with some fundamental questions based upon the assumptions that you've made, I think it's important to focus on a few different things.

One is if there's going to be an SLA construct that exists here that if ICANN is going to also be responsible for an SLA, who is going to in fact oversee that SLA for ICANN? So that's an important fundamental legal question that's going to have to happen.

And the otherwise, the liability construct of for ICANN and for the Contracted Party House, so in the EPDP we have worked on that and we certainly all I think appreciate now that in having this framework that that question becomes more and more important. So whether it be through the EPDP group or through another legal component of your group that - those are the main questions that really need to be established to create that legal framework and that liability construct so we continue to push for that to happen.

Because then you go onto say that another assumption is that there has to be an escalation for a mechanism for complaints, and that also goes back to underlying questions on how the data subject or how the accreditation is going to end up handling that escalation of complaints and the liability behind that as well.

Ram Mohan: Thank you very much. Again agree with all of the statements you're making and that there is a legal piece that has to be done and policy work that has to be done. What we felt on the very first question on SLAs, what we believe is that they must exist. If ICANN is to stand up a service and if it's a service that a community of users is going to depend upon, then we believe that such a service ought to be subject to SLAs. It shouldn't be only other providers who

have SLAs applying to them that whoever is providing an important service like this ought to have SLAs apply to them, right?

So that's really the assertion we're making, that's a recommendation we're putting out. All the rest of it, how does it - what are the other implications, how does it get implemented, those are valid things but we think from a technical group we'd be derelict in our duty if we didn't actually say, if you're standing up a service, and it's a service that is supposed to be dependable, then there ought to be measures for such dependability. And those measures ought to exist, ought to be published, and ought to be reported upon in some transparent way.

Diane Plaut: So just as a follow up question, I mean, my thought is that there has to be an SLA that is in place - that ICANN has to live up to, right? So who's going to institute that because ICANN would be the person - the entity having to live up to that. But in taking all this into account, once the construct is laid out for the liability framework it seems to me a that part of your work has to include the recommendation that a terms and conditions is put at the end of this whole system so that it brings together all those liabilities and how they're going to be addressed.

Ram Mohan: That's great feedback. You know, it's not currently in our considerations list, but certainly I think that's something that we will discuss when we meet again on Wednesday. As to your question on who will stand up, you know, this - the SLA piece, I have one answer, it's not us.

Rafik Dammak: Okay, so we have Beth and then Alex.

Beth Bacon: Thanks. Beth Bacon for the record. I actually forgot I was in the queue, it's been a while. Thank you, guys, very much for, you know, coming and giving us all this time to walk us through the report and kind of taking the hits. I really appreciate the report, I appreciate that you've very much kind of fulfilled the specific and discrete task that Göran had asked of you and I think that it's

helpful in many ways. It kind of gets us thinking towards different sorts of solutions and different ways down these paths.

And I don't want to hit you with any more questions that are not really in your purview simply because you guys have clearly fulfilled your task of here are some assumptions, here are some models that could work technically. But I do - would like to put on the record just a question as we move forward what - after April where you are - you've officially closed your work, it will be interesting to hear from Göran as to what he sees as next steps for this because it is very much a top down approach, CEO-directed task for you.

And what could be done to either evaluate it, use it in some way. It's not necessarily part of the EPDP process right now which is the more multistakeholder process. So I think those are important things to remember and we'll look forward to hearing from Göran. I don't expect you guys to make a judgment there but really appreciate your time. Thanks.

Ram Mohan: Beth, thank you. And again (Elisa) will take note of that. Tomorrow in the public - in the community session Göran is actually going to be there at the very start to make some introductory comments. And what I'll make sure to convey to him ahead of, you know, between here and tomorrow is some of the questions that are being directed at him and perhaps he'll have an opportunity to speak to, you know, what his intentions are. Thanks, Beth.

Rafik Dammak: Okay, thanks, Ram. Alex, so just to give all these - what we have in the queue, Alex, then Mark, and Hadia and I think, Kurt, you want to speak? Okay, so this is what I have in the queue so please go ahead, Alex.

Alex Deacon: Thanks. Alex Deacon from the IPC. I raised my hand a long time ago but maybe I'll also thank you and the team for this great work. I really like where you guys ended up and I have some questions and some clarifications, I'll just put that in an email.

But I just wanted to respond to some comments from earlier, I think, you know, clearly us in the EPDP we have a lot of work to do in terms of policy and but I think it's important that, you know, we as the community work on some of these things in parallel, there's so much to do and we need to take advantage of that when we can. And I think this is an important one to do.

The one question I will ask is, given where your recommendation and where you ended up, you define four actor models and it's not explicit, at least I didn't see it, but it seems like you've landed on - you're suggesting actor model 2, can you confirm that? I think that's where you are, right?

Ram Mohan: Yes, I don't remember all of them off the top of my head but I believe that's - I don't have a computer in front of me, can one of the other TSG folks take a quick look and confirm? We'll come back to you, Alex, on that. Thanks.

Gavin Brown: Sorry, so - just scrolling through but if I remember correctly ICANN, yes, actor model 2 is ICANN proxy using multiple identity providers but with ICANN as sole authorizer. So I think that's the one that we - yes, that's the one we think is probably the most workable.

Yes, so one of the things that's worth saying is that most of the actors within the system, you can merge them into one or merging two, you know, two of them together to make into one. And that could go into ICANN for example. But we wanted to allow for the possibility that they may be separated out and given to different entities but they could all be - it could all just be one system potentially.

Rafik Dammak: Okay, thanks. So we have 10 minutes left and I'm closing the queue so I took those who already raised their card but I close the queue. So Mark.

((Crosstalk))

Rafik Dammak: You didn't, oh.

Mark Svancarek: I put mine down a while ago.

Rafik Dammak: Okay.

((Crosstalk))

Rafik Dammak: Okay. Hadia, please go ahead.

Hadia Elminiawi: Hadia Elminiawi for the record. So my understanding that from a technical point of view this proposed technical solution is quite flexible. So when it comes to policy, for example, single disclosure for one time is possible and otherwise it's possible as well. And when it comes to confidentiality and transparency both are possible. When it comes to authentication and authorization, this technically can be handled in many ways.

So actually my understanding that this technical - proposed technical model is not setting any kind of policy or crippling or putting any kind of restrictions on the policies that this group, the EPDP team is trying to formulate. So I heard a lot of concerns with regard to the policy that we are trying to develop in Phase 2 and how this system impacts what hasn't yet been developed.

And my understanding actually that this technical solution doesn't actually impact our policy decision or development. And we can almost freely or freely, you know, go ahead and develop whatever policy we think is right and appropriate and this technical solution will be actually able to handle it.

So it's more like let's say it's a proposed model, where you have ICANN, where you have an authorization service, but - an authentication service, it's a proposal for a model but from a technical point of view and from a policy perspective, yet our work is to start and that does not by any means put any kind of limitations on it. Thank you.

Ram Mohan: Thank you, Hadia, that is exactly what our intention was, to not handcuff the policy development work at all. We do have in our proposed solution some suggestions as Gavin was saying earlier, we do - we have thought that an open ID model with mutual TLS might actually lend itself better to something like this rather than, you know, using certificate, as an example, on the front end, right?

But we're not saying it must be that. What we're saying is that in - technical minds got together and they looked at all of these and the recommendation from that is the recommendation from that is this - that this model might actually be better from a user journey, from a user experience, from an actual implementation point of view.

We had, I think at our last face to face meeting we had some folks come in through Benedict's help from Interpol and provide some, sorry, Europol was it, and provide some thoughts on what kinds of things would just not work, like, you know, don't expect great technical expertise at, you know, every part of the system, right? So, again, solve for simplicity. Thanks.

Rafik Dammak: Okay thanks, Ram. Kurt and then Stephanie.

Kurt Pritz: Great. Ram and to everybody, thank you very much for this and thanks for coming to our meeting. I have two that are really comments more than questions, one goes to Stephanie's question and about legal aspects, but those are really technical aspects too. If we have a 72-hour response time as a team, you know, how do we get that done in 72 hours? I don't know if that's feedback loops in the schematic or what, but there's a technical - we need some technical help to make sure that that can be accommodated so it's not purely a legal question.

And second, I want us as a group to take some care in our question back to ICANN Org about the limitation on liability and the effects on liability and not - we know that ICANN's working with the EDPB on different models but we'd

like to know now, you know, what are the aspirational - what's the aspirational model for reducing liability?

Is it the idea that the EDPB is going to pre-approve a process or that by doing something the same every single time that reduces liability? Or is it an insurance model, a shared liability? So I'd like to put that point on the question to ICANN so we can get sort of an immediate response about what the limitation on liability goals are.

Ram Mohan: Thanks, Kurt. The second question noted and we'll make sure that, you know, that gets passed on. To the first question, we did have some discussion about that and I guess the way I would paraphrase it is, is that we agree that there's a technical component - technical aspect to it as well; how do you facilitate that process?

I don't know that we've actually put the details of what we talked about in the document as of yet, but I think that's another note for us, (Elisa), that, you know, what we've thought about in that area we ought to expose that and see, you know, whether our ideas maybe feasible or not. So thanks, Kurt, for the comments.

Rafik Dammak: Okay thanks, Ram. Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. I just wanted to address the question that Alan Greenberg raised about that model where the individual gets access to their records. That's something you have to accommodate or somebody has to accommodate.

So if you're coming up with a unified access system, my first question if I were a DPA would be, well, why don't you allow the individual to access not just their record and their information but also who has seen their data, who you've disclosed it to because the - there are strict limits in terms of the

record keeping that you have to have on that and different jurisdictions have different requirements in terms of full disclosure.

So you need to build that is all I'm saying. And I don't see why you can't. In terms of the question about whether there's enough data to authenticate the user, well you could start issuing tokens to registrants and you can figure out that better than I can.

Ram Mohan: Thanks, Stephanie. Yes, I'll agree with most of what you said. The place where we - where we took a different path was we didn't - in our - in the five use cases in our prioritization we thought we should note that that's an important case that should be handled. We just thought that given the time constraints that we had we weren't going to build that. It certainly needs to be built, it's feasible to be built, we just didn't take that on as something for us to build.

Stephanie Perrin: And because I think ICANN has controllership in this issue, you have to build it. That doesn't preclude separate access requests going to the registrars for full file and the resellers and all the rest of it, but you're going to have to build it.

Ram Mohan: Thanks, Stephanie. (Elisa), if you could just take note of that, that the entity that is doing this work has to build it. When I hear you say, "You have to build it," I view that as the TSG has to build it and I think we're not going to do that in the time that is there but certainly acknowledge that it has to be done.

Rafik Dammak: Okay, thanks. I think we reached the end of - yes, one minute left to this meeting. So first I want to thank you and congratulation, you made people excited about technical document that I don't think that's happened often. Okay, so thanks. I think we got many question, many comments and we also we need to digest this and to see how also to - how we can use, we need to use your work in our discussion that we will start in Phase 2.

Last thing I want to say, thanks to Georgios for the chocolates. I think that's maybe…

((Crosstalk))

Rafik Dammak: So it's kind of (unintelligible) at the end so thanks, everyone. I don't want to prevent you from enjoying your night and the Japanese cuisine tonight. Okay thank you.

Ram Mohan: Thank you, Rafik.

END