ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 03 August 2021 at 16:00 UTC

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. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/YgTpCQ

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page
http://gnso.icann.org/en/group-activities/calendar

JULIE BISLAND: Good morning, good afternoon, and good evening. Welcome to the Transfer Policy Review PDP Working Group Call taking place on Tuesday, the 3rd of August 2021 at 16:00 UTC.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room. For today's call we have apologies from Jim Galvin (RySG) and Steinar Grøtterød (At-Large). They have formally assigned Beth Bacon (RySG) as their alternate for this call and for the remaining days of absence.

All members and alternates will be promoted to panelists. Members and any alternates who are replacing members, when using the chat feature, please select either Panelists and Attendees or Everyone in order for all participants to see your chat. Observers will remain as an attendee and will have access to view chat only.

Alternates not replacing a member are not permitted to engage in the chat or use any of the other Zoom room functionalities such as raising hands or agreeing and disagreeing. If you're an alternate not replacing a member, please rename your line by adding three Z's before your name and add, in parenthesis, "Alternate" after your name, which will drop you're your name to the bottom of the participant list. To rename yourself in Zoom, hover over your name and click Rename.

As a reminder, an alternate assignment must be formalized by way of a Google assignment form. The link is available in all meeting invite e-mails.

Statements of Interest must be kept up to date. If anyone has any updates to share, please raise your hand or speak up now. If you need assistance updating your Statements of Interest, please e-mail the GNSO secretariat.

Please remember to state your name before speaking for the transcription. Recordings will be posted on the public Wiki space shortly after the end of the call. And as a reminder, those who take part in the ICANN multistakeholder process are to comply with the Expected Standards of Behavior.

Thank you. And over to our chair, Roger Carney. Please begin.

ROGER CARNEY: Thanks, Julie. Welcome, everyone. I just have a few comments before we jump into our continuing—and I think maybe our last—focused discussion on the Auth-Infos before we move on to some other topics. And obviously we'll be circling back on these as we make further decisions, but I think we're going to try to wrap this up today so we can move on.

I just wanted to let everybody know that the additional comments that we requested from the other SOs, ACs, and everyone else—the rest of the community—I think is due back this week. Their comments are. There hasn't been many. The last time I heard last week, there wasn't any yet, additional comments. I think that's kind of what we expected, as everybody was pretty involved in getting this going and everybody here is involved with the majority of the groups anyway.

The other thing I wanted to mention was just to, between now and next week when we're going to be switching up, make sure everybody takes a look at the Auth-Info working document and gets their comments put in, especially paying attention to the small groups—straw man and principles ideas lower in the document. But anywhere in the document, really, if you see anything please provide some comments. And hopefully we can get some clarity around anything that sounds confusing or needs more clarity.

I think that's all I had to get us going. I think that the majority of our time today is going to be spent walking through those straw man ideas again, the small group ideas that they produced. And staff put together a good interactive Zoom polling to lead us down the path, and hopefully we can make some good decisions and get some good discussion out of it.

If anybody has any questions, let me know. But I think we'll go ahead and jump into our polling questions and hopefully get some things ironed out moving forward. So Julie, if you would like to … Yeah, thank you for pulling that up.

Question 1 for our polling. “The registrar creates the TAC and has it hashed at the registry.”

Again, we're going to make some statements here and I want people to say, “Okay, that sounds good” or “That maybe we need some modification.” So I want to see what people think about …

I support the requirement. I support as an industry practice, or more as a best practice versus an actual requirement that we're going to make. Or I do not support all, or I do not support partially and think that some of it needs to be changed.

So I think I’ll give everybody a minute or so to answer. And then we'll go over it. Oh, okay. Chat. Oh, “Host and panelists cannot vote.” So our poll looks like it's not quite usable. Thanks, Emily, for putting that up there.

JULIE BISLAND: We're looking into that. I’m so sorry. One moment.

ROGER CARNEY: No, no problem. Thanks, Julie.

JULIE BISLAND: Roger, I’m going to end the poll real quick so I can make some adjustments. Okay?

ROGER CARNEY: Okay, no problem.

JULIE BISLAND: Thank you.

ROGER CARNEY: Thanks, Julie. And as we get this poll going, I just want to remind people, let's have the members do the responding and everyone else doesn't need to. We’ll try to get just the active members themselves. The alternates and everyone else, you don't need to answer. We'll just have the members do it once we get it up and running.

JULIE BISLAND: I know everyone wasn't able to participate in that poll. Would you like me to restart it?

ROGER CARNEY: Yeah, if we could. That would be good.

JULIE BISLAND: Okay, great.

ROGER CARNEY: Perfect. Thanks, Julie. Yes. Thanks, Jothan. Just members. No alternates need to do it. You can just close it. Just the members we'll have answer these.

Emily, please go ahead.

EMILY BARABAS: Hi, Roger. This Emily from staff. Since it's quiet and while people are doing this initial polling, I just wanted to maybe remind folks what this is about and where it came from in case anyone has been away for summer holidays and you're just catching up again.

So each of these items on the straw man list were proposed as potential security measures for the Auth-Code that the small group brainstormed. I think it was Jothan that used the analogy that these were sort of Lego pieces that they wanted to put in a pile in front of the working group to potentially assemble a solution. So the purpose of this poll I think, to remind folks, is really to look at some of these Lego pieces and see if there are some that can be kept in the set and potentially assembled into something that the working group likes.

So hopefully that provides a little bit of additional context if anyone has missed some calls or just wanted to get up to speed. And of course, we can answer any questions. Thanks.

ROGER CARNEY: Great. Thanks, Emily. All right. Thank you, Julie. It looks like the majority of people think this a good idea as a requirement, and a few people thought that it may be better as an industry practice.

So I think that this is good. I think we're leaning toward a good idea here, making it a recommendation or a best practice. At least the group is agreeing that it’s a good concept. How we get there? Obviously, it leans toward making it a recommendation, but we can work through that, I think.

All right. Question 2. Oh, yes. “It’s not stored at the registrar and it is stored at the registry, but it only exists at the registry when the transfer is in progress.”

So this was the discussion we had, and there was quite a bit of feedback on this. I think that the registrars … There are examples of when registrars thought that they may need to store them, at least temporarily for certain reasons. Some of the reasons I heard were customer service, different registrar models being resellers, and things like. They may need to store it, again, temporarily. I think a big point of this one coming out of the small group was the registry really only having it during an active transfer idea, anyway. You know, the registrant requested it.

So please go ahead and answer. As a requirement. As a best practice or an industry practice. Or you don't support it or you think some changes need to happen to it.

Thanks, Jothan, for the thought there. And I think the need to discuss … Please check “do not support at the time.” And again, I mean, this is informal. We're not actually making any recommendations out of this, so I would say if you want to discuss, please select “do not support” and we'll discuss the reasons. Maybe it's just a small language change or maybe it's a half-of-it-doesn't-make-sense or all-of-it-doesn't-make-sense idea.

So, yeah. Thanks, Jothan for bringing that up. If you want to discuss it, please mark “do not support” and we'll talk about it.

Okay. I think that's long enough. Let's go ahead and show the results. I think this kind of fell along the lines of our previous discussion, I think that … Those that marked “do not support,” I invite you to come up and talk about thoughts of what doesn't work here, what would need to change, and any thoughts on that. So anybody that marked “do not support,” please raise your hand and let's discuss. Okay. 40% said they don't support. No one wants to talk about it.

There we go. Theo, please go ahead.

THEO GEURTS: Yeah. So I wasn't actually prepared for this and I didn't read any of the documentation. So it sort of jumped on me and [I] was going like, “Okay, let's settle down. Let's discuss it and see what it’s all about.” So that's why I voted no support for now. [inaudible].

ROGER CARNEY: Okay, great.

THEO GEURTS: You know, there are some long-term implications that will be down the road, so it's kind of hard to figure that out on the spot here. Thanks.

ROGER CARNEY: Yeah. Thanks, Theo. And again, as I mentioned before, I know that a couple concepts of not storing it, the piece of this that says "not stored at the registrar." There are some pretty logical reasons that we talked through last time that would change that. But I think that the second part of this the interesting thing. We had a little bit of a discussion it and there were some questions about why and how. And again, I think this gets back to …

One of the questions the small group came up with was, are there other reasons people are using the Auth-Info today that if this was a requirement would break that. If we're only setting the Auth-Code when the registrant requests the transfer and then once the transfer is done, it's gone, does that hurt other practices currently going on? I think that's a big question out of this, and a big question that small group had as well.

Okay. Anyone else? Otherwise, Tom, please go ahead.

THOMAS KELLER: I think, at least from what I gathered in the chat, maybe the language is a bit misleading or maybe I'm not getting it. So for me it's only stored at the registry and there it is hashed. It does not mean that the registrar cannot have the code in clear name, actually. I mean we all need that for customer support issues. Right? If someone's calling up and saying, "What does that mean again? It's still valid for seven days or something?"

So I think a lot of people complain about that. Not that it's stored in the registry, but it should be in the registry. And if it is in the registry, it should be hashed.

ROGER CARNEY: Okay. And Tom, what are your thoughts on it existing at the registry only during an active transfer? You know, basically once a registrant has requested it to be transferred.

THOMAS KELLER: Yeah. This I would completely agree with. I mean, that's one of the issues we're having with the current transfer process. That the Auth-Code is basically valid for any given time and any given links. And even if it is in the system, even if no one really wants to initiate a transfer. So I'm definitely for that, but I think we need to split that into two questions, maybe. And maybe be a bit more explicit in what we mean about "only stored at a registry" because apparently some people have issues with that.

ROGER CARNEY: Okay. Thanks, Tom. I think that makes sense, that we could split this up into multiple concepts to get to a better result out of it.

Okay, any other comments on this one? Okay, I think that's good input. All right, great. Thanks. All right. Let's move on to the next one.

"Two-factor authentication by whatever means the registrar sees fit." We've talked about two-factor authentication several times now—I think—early on and just in the past week or two—about that's a great additional security mechanism.

Please go ahead and answer the poll. As a requirement or a practice. Or needs discussion. Again, the do-not-support or needs-discussion-again kind of thing.

Jothan, to your question in chat, being UX or EPP system, the SRS. Yeah. Think that that’s, again, the question being registrar is going to be more of a UX question. If it goes beyond that ,it's beyond the registrar itself.

Okay, Owen good point. Very true. And again, we're not using this poll as a final result. We're just trying to spur some discussion and make sure we've got things covered and the ideas that everybody is leaning one way or not on. But, yes, that’s a good point that I think the industry standard … To me, I think you would still call that a requirement. It's an optional requirement. But good point. And I think that maybe that could have been an additional question. [Just] didn't think about it. Thanks, Owen.

Owen, please go ahead.

OWEN SMIGELSKI: Yeah. I’ll just go ahead. There are some jurisdictions where, if you don't follow an industry standard, it could subject you to liability. So while I think that doing two-factor authentication is good, some registrars may not be able to implement that for various reasons. So I think having that as an option but not calling it an industry standard would be better so that those registrars who can't conform to that aren't then subject to potential liability down the road for not following the “industry norms.” Thanks.

ROGER CARNEY: Great. Thanks, Owen. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I don't think we should use the wording "two-factor authentication." I think it can be very misunderstood for many years going forward since this policy is going probably to be used for many years. So I think we need to change it into something like "the Auth-ID needs to be transferred to the registrant in a secure way" or something like that.

Putting it down to two-factor authentication would block different kinds of systems, maybe, where a reseller is taking out the Auth-ID via an EPP system or something like that. It could be way too limited on both the current business models today, but also what will be in the future. Thank you.

ROGER CARNEY: [inaudible] Kristian. Okay, just a question back to you. Would you support something like a multiple instead of two-factor? A multiple factor?

KRISTIAN ØRMEN: I still think that wording could be too limited.

ROGER CARNEY: Okay, thanks. All right, let's go ahead and show the poll results.

Before we get into this, I just wanted … There are a couple questions on two-factor, and I think Jothan kind of pointed to this early. Two-factor being a UX thing which … Many registrars support a two-factor authentication, so for those that wonder if it's possible or not. Yeah, I mean it's definitely possible. And I think that the idea of two-factor on the system level or the EPP level gets very tricky, and I don't think anybody here is suggesting that. It's more of a suggestion that the registrars could use two-factor within their own systems for whatever reasons they deem necessary.

Okay, let's get back to the poll results. Oops, I'm sorry. I didn't even see that. Julie, can you show that once more? Thank you. Theo, please go ahead.

THEO GEURTS: So I voted "do not support." I think when it comes to the security or whatever that is required to make things safe, that it is completely up to the registrar and will be dictated by laws—data protection laws, security laws—anyways. In my point of view, you shouldn't name anything very specific, especially into contract requirements.

You should avoid the use of two-factor authentication, multi-factor authentication, encryption levels—all that kind of stuff—because technology will change very, very quickly. So as soon as you make a very specific recommendation on how security should go down, that will be obsolete in a couple of years or maybe even quicker. So I do support very strong security, but that is up to the register and that will be dictated eventually by industry practices.

If everybody is using a certain form of encryption or multi-factor authentication, whatever that is, that will be the standard anyways and you will be benchmarked against those practices which are common by many, many registrars. So that will eventually make sure that you as a registrar will always follow the highest security practices that are around there. So I would not … Yeah, don't mention very specific solutions because they will be obsolete. Thanks.

ROGER CARNEY: Thanks. And I think that kind of goes along with what Kristian was saying as well. The one question I would have on that, Theo, for you is if ICANN Complaints got a complaint because a registrar added additional security features to the registrant making it seem harder to transfer though, how do you handle that if it's not written in policy that they're allowed to do it?

THEO GEURTS: That is always going to be an interesting discussion [inaudible] practices already in place by several registrars. I mean, I've seen registers that require that you [inaudible] a phone number that supports SMS in some cases. There are extreme examples in the past that you're required a fax as a registrant to obtain your Auth-Code. So that is an ongoing discussion.

So if you would put into the requirements very specific security operation requirements, then you will allow a registrar to put those in. If you do not put them in the contract and you leave it up to the law but a best industry security practices, then you don't have it baked into your ICANN requirements, you still will have to comply with the ICANN RA which sort of lays out that you should provide the Auth-Code, the TAC, within five days. But I don't think that our contracts stipulate anything on how that must …

That is just a very complex question there, Roger. [inaudible].

ROGER CARNEY: Yep. All right. Thanks, Theo. I appreciate that. And something to note for everyone. Caitlin just posted that the term “secure mechanism” has been used in the past and it's been defined fairly well, as well. So take a look at the chat for that as well—if that's something we can push forward using. Tom, please go ahead.

THOMAS KELLER: Thank you. I think, personally, we should probably stick to the process and define the process and not try to define what additional business practices registrars might have. I mean, depending on a model that can look very, very different … And we currently, as far as I know, have a regulation that retrieving the Auth-Code cannot be more complicated than changing anything else in the given [inaudible] control panel or setup. I think this where we should leave at currently.

I mean, we still need to discuss the whole lock issue and whether this is a second factor, but I’m totally with Theo that we shouldn't be too overly descriptive with the whole thing.

ROGER CARNEY: So Tom, what are your thoughts—not that you’ve had any time to read the chat here—on the “secure mechanism” wording?

THOMAS KELLER: I think we should probably leave that for later. So once we know how the whole process looks like, we may dive into how can it be abused by someone who wants to abuse it. And then maybe come up with wording around that's probably. That's probably easier than trying to fix the problem right now.

ROGER CARNEY: Yep, that makes sense. Thanks, Tom. Okay, any other comments? Questions? That was good on that one.

THEO GEURTS: Yeah, just a quick jump in again there.

ROGER CARNEY: You bet.

THEO GEURTS: You mentioned how registrars may abuse strict security requirements for blocking transfers and creating barriers. You know, when we created a change of registrant policy, you already saw certain registrars trying to make a process as easy as possible, but you also had, yeah, actors within the industry that would come up with very specific requirements to accommodate the change of registrant policy and would hide behind it to make it more difficult to transfer out. And that is just a key example. If you go to specific wording, setting specific requirements in how a process should be followed, there will be always actors that go like, “Oh, that's a handy framework. ICANN created the exact opposite of what its policy or requirements of framework wants to achieve.” So you always need to be agnostic there and not be solution driven.

ROGER CARNEY: Great. Thanks, Theo. And just to follow up on what Tom was saying. I think that, again, looking at this as we circle back around, the comments that we got back on the issues report indicated that if the FLA was eliminated, then a lot of people thought their security was an issue on the Auth-Code and how to make it better.

And again, as Tom mentioned, I think that we will circle back in on a lot of these things once we get further along and decisions made, and that we're looking at a real solution that we can see where and if there are any gaps in it.

Okay? Oh, great. All right, let’s move on to the next one. Thanks, Julie.

“Minimum character count for the TAC.” I don't know if we have any other questions, but think about not just a minimum character, but maybe talk about the syntax. Should we eliminate zeros and O’s and things like that. But here we're talking about a minimum length or a maximum length, even, to make sure of that.

Let's go ahead and vote on if you support a minimum character length for TAC. Or if you think it's better as a practice. Or if you don't support or just wanting to discuss and talk about what that means. So please go ahead.

Okay, let's go ahead and show the poll. That was a short one. All right. So a majority of the people support it as a requirement. At least one person did not, or are a couple people did not—or want to discuss, I should say.

Theo, please go ahead.

THEO GEURTS: Yeah, I was reading the question. I was wondering. How do you come up with a minimum character count for the TAC? And when does that number become obsolete? And how do you adjust it then?

In my view a registrar should use common sense there, and if it needs to be higher … They start off with whatever. Say it's 20. And at some point you go, “Okay, that's not really handy anymore. We need to up that.” Then as a registrar, you go up to 25 or 30 or 40 or whatever is required. It still needs to be workable also. So that is just, how do you set the minimum character count there?

ROGER CARNEY: Yeah. And again, I mean you’re kind of talking about future proofing this a little bit. But I think that the idea here is that sending someone four characters—is that enough to think about getting rid of the FOA? And they're setting four-character Auth-Infos or TACs.

I think that, to your point, yes. I don't think you can say that needs to be 64 characters or anything like that. But I think there could be a minimum that we don't want less than eight or something. And as you've said, obviously that could change later on, so a maximum's a little hard to set, I think. Thanks, Theo.

Any other comments or questions on this one? Okay, a question in chat. Farzaneh, yeah. "What's the industry standard?" That's a tough one. I'm not sure that there's an industry standard. I don't know if our security people can let us know if there's a general one, but I think that you go to Amazon and it's something. And you go to your bank and it's something different. So I'm not sure that there's an industry standard. Yeah, exactly, Tom. I think there are several.

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. Yeah, I work with a lot of ccTLDs as well, and they have basically, each of them their own standard almost on this.

You said that it would be difficult to set a maximum and I was just thinking why would that be difficult? Personally—system wise, support wise, customer wise—it would be nice to know that a gTLDs Auth-ID is always, for example, 32 characters. It would just be nice to be able to do that quick validation that we know the link. Thank you.

ROGER CARNEY: Yeah, Kristian. I think that would be a nice thing to have. But to Theo's point on looking at this in the future, if we said the minimum was 16 or the maximum was 32, what happens five years from now when that 32 is fairly easy to break and they can break it within the first 15 minutes of the day? How do we change that? And maybe it doesn't even come down to character count at that point. Maybe there are other mechanisms to do it. But just my thoughts on that.

Kristian, do you want to follow up?

KRISTIAN ØRMEN: Sorry. Just forgot to take my hand down.

ROGER CARNEY: Okay, no problem. That's a good one, Volker. Theo, please go ahead.

THEO GEURTS: Yeah. On the question “what is an industry standard,” there must be one. Again, industry standards which we need to comply with are already being set out in data protection laws and in future cybersecurity acts. I mean, if you look now at what the state of New York has done on how you must protect data, that’s some pretty heavy requirements you have if you are a registrar there or you have a lot of [citizens] of New York State there.

If you look at the European Security Act which is currently an ongoing project, sector by sector where certifications need to be met, those are the industry standards which you as a registrar—as a company operating within whatever jurisdiction you have to comply with—those requirements set there are usually very broad to make sure that technology will not be outdated. You will always need to have the latest of the latest.

For example, a 256-bit encryption is pretty much used by everybody, but in a couple of years from now that could totally change. So if you look at a Temporary Spec where someone made a suggestion that a registrar should have 256 AES encryption, that is not very wise to put in a contract or a Temporary Specification because by the time you put such a requirement in, even though this was an example in Temporary Spec, it could be outdated very fast.

So that is why GDPR is extremely broad in what an adequate level of protection is. It just forces you to have very, very good protection. And you always need to benchmark yourself against others and other companies because you are forced to. Because if you don't do it—if you don't have multi-factor authentication, if you don't have very strong levels of encryption—if you do get breached or get hacked or get ransomware or whatever and you are being investigated by a DPA or whatever institution that can prosecute you and it comes to the conclusion that you didn't do squat or you had very light levels of encryption or whatever, yeah, you're going to be very, very liable and a fine will be very, very high if you didn't do anything or not enough.

So it forces you to make sure that you have very high security levels. And if you get breached or hacked and you did everything humanly possible, what is out there as the industry, then the fine will not be as high because you did your best. And you cannot expect you will not get hacked. I mean, that is just simply impossible.

So that is somewhat the industry's standard around here. Thanks.

ROGER CARNEY: Thanks, Theo. All right. And again, I think the general agreement here is that a [minimum amount] could be set. And I think that we could address those ongoing, as everybody says, and not get detailed, but get smart with our wording to allow this to grow and adapt over time. Okay, I think we can move on to the next one.

Alright, so this continues on with the same discussion about the syntax and thing. “Require uppercase and lowercase letters, numbers, and special characters. Prohibit use of dictionary words.” Again, several of the standard configurations for secure—more secure passwords, I should say. Let us know if you support this as a practice or would like to discuss. Thanks.

All right. Let's go ahead and show the results. Okay, actually a fairly good split on practice or a requirement. And I was thinking that as we were going down each one of these, and as Mike mentioned in chat, what dictionary? And that always gets to be kind of a tricky one, obviously. People pick one or companies pick one that they use and don't allow it.

Yeah, and I wonder if this statement/question actually comes down to, some of these may be useful and some of them may not. Maybe the dictionary is just not going to work out. As Mike points out, what dictionary are you going to use? But maybe having a few of these items, like a lot of passwords require now two of these three—or two of these four items, something like that.

But I think that something here makes sense, at least as further discussion of making this a required part of the overall syntax or making it a good practice for the community at large. So does anyone have any comments on this one?

Jothan, go ahead.

JOTHAN FRAKES: Thank you, Roger. And I’m sensitive to the fact that I’m an alt, but I was part of the small team that helped to put this together. What we basically wanted to do here is just to ensure further uniqueness and complexity of strength. And that's really the objective here. The use of dictionary words was something to just ensure that you wouldn't end up with something like a “password123” situation, that the term was too simple. Thank you.

ROGER CARNEY: Thanks, Jothan. Okay. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yeah, just in regard to … I agree completely in terms of the uppercase, lowercase, numbers, and special characters. The use of prohibitive dictionary words? I get why Jothan's doing that, but maybe restricted words would probably be easier. So just maybe, like you said, “123” and just certain words that may be a bit too simple like “password,” for example, could be restricted. “Test,” for example. Just the ones that people generically use as opposed to all dictionary words.

ROGER CARNEY: Thanks, Keiron. A lot of good chat going on. I don't know if people are keeping up on chat or not, but if anyone in chat has too much to type or wants to come to the mic and talk, that may actually spur some good discussion as well. So I encourage anyone to come to the mic.

Theo, please go ahead.

THEO GEURTS: Thanks, Roger. You know, just saying, “Don't use dictionary words” makes complete sense to me. I mean, if you want to brute force anything, the first thing you're going to load up is the entire dictionary and clash that against the database to see if you can get a hit there. If that doesn't yield anything, then just use a couple of breaches from all the leaked passwords. It usually gets you a good chance, also, to get in, to brute force something. So, yeah, it makes complete sense to me but I yield to the group. Thanks.

ROGER CARNEY: Thanks, Theo. And that's actually one of the ones that came up. It’s tough because the dictionary is, again, who's dictionary? And maybe it doesn't even matter whose dictionary as long as you're using a well-known dictionary. It's interesting because it'll change requirements from registrar … Just thinking out loud. But if you're using that mechanism, even if it's your local dictionary, it still makes it better than nothing.

Tom, please go ahead.

THOMAS KELLER: Thank you. I think one thing we should keep in mind that if this process is limited in lengths, brute force attacks on single Auth-Codes are very unlikely. So it's not that you can guess a transfer to the registry and then bombard it or whatever. There's are different mechanisms there as well. So I support having a basic coverage of good sense of security, but if we want to enlarge it in the direction of [inaudible] words or other things, I would be very skeptical that this is suiting the purpose and is still something people deal with at the end of the day. Even though the registrar is coming up with all of that, setting the bar too high in that case doesn't really make any sense.

ROGER CARNEY: Thanks, Tom. Theo, please go ahead.

THEO GEURTS: Yeah. Maybe a different approach is just to mirror NIST requirements. You know, these guys gave out some pretty good advice on how a password policy should be. You could mirror that and then you should be in pretty good shape. Thanks.

ROGER CARNEY: Thanks, Theo. Okay, any other comments on this one? Tom, I assume that's an old hand. Thank you.

Okay, let's move on to the next one. “Registry checks to ensure TAC meets minimum requirements,” whatever those are. Should the registry do a check when the Auth-Code is set from the registrar? So indicate your support as a requirement or a practice, or do not support, or want to discuss some more.

All right, let's go ahead and show the results. Okay, heavily leaning toward support as a recommendation. One or two people thought that they do not support or want to talk about it, so let's go ahead and jump into that and see what we have here.

Comments from those that don't support this or wanted to see it change slightly or for clarity. Anyone that clicked the "do not support." Barbara, please go ahead.

BARBARA KNIGHT: Thank you. I wanted just to discuss it a little bit further because from my perspective, it seems like if the registrar is creating this and passing it to the registry, it seems more appropriate that the check should be done at the registrar to make certain that it's compliant before sending it over to the registry. So I just thought it would be good to have a little additional conversation surrounding that.

ROGER CARNEY: Great. Thanks, Barbara. Yeah, and I think the thought here was to hopefully encourage, let's say, fringe registrar actors from not doing what we're saying in policy. So if we said that was a 16-character code and some registrar just set some to five characters, where's the check to make sure that that is actually going to work or not? And is that, again, a fairly simple syntax check? Not trying to get into policy or anything on the registry side, but is it worthwhile, I think?

Theo, please go ahead.

THEO GEURTS: Yeah, it sort of makes sense to me. I mean, most of us I suspect … Let me rephrase this a little bit. When we are implementing a TLD—ccTLD or gTLD—we follow the requirements from the registry. And we often encounter that there are several checks within the registry where if we generate a TAC which does not meet the requirements of the registry, it just bounces back an error that it is an invalid TAC.

That also makes sure that everybody is following the same guidelines for that registry. It just makes implementation easier as it creates an even—it forces everybody to follow the same requirements. I think that is just handy for everybody and it's something already in place by most folks. Thanks.

ROGER CARNEY: Thanks, Theo. Yeah, and that's something to notice. Today, most of these things that we're talking about are server-side policy, so the registries are setting the complexity level today. And the issue being that, as Theo mentioned, they're variable right now. You go from one registry back into another and it's a different set of requirements.

Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I would be surprised if registrars would not do the check themselves, but I don't think that should change anything on the registry level. I think the registry levels should always check if Auth-ID is good enough. It could be when you set the Auth-ID or it could be at the transfer since they can't do the transfer if the policy is not followed.

ROGER CARNEY: Great. Thanks, Kristian. Thanks, Barbara, for bringing this up. Good discussion. Others have comments? Okay, great. All right, let's go ahead and move on to the next one. Thanks, Julie.

Okay, so we did discuss this a little bit. And I think that maybe I even changed the wording here maybe to try to make it a little more straightforward.

"Failed attempt identification/notification after a certain number of requests to initiate a transfer." And I think this gets to what Theo mentioned just a little bit ago about people trying to brute force a transfer and try to guess that Auth-Code. And should there be a limit on 10 per minute—10, even—that after 10 tries, there's some kind of notification or at least an identification that there were quite a few attempts to make this happen.

Again, please vote your support for a requirement or a practice, or do not support or would like to discuss further.

All right, let's go ahead and show the results. Great. And this was a little nuanced. It gets a little deep into it. Sarah likes the idea of notification, in chat there. Again, it looks like a good support for a requirement or a best practice. Someone obviously doesn't like it.

Theo wants to talk about it more. So, Theo, please go ahead.

THEO GEURTS: Yeah, so I voted no because at this given point I have no idea what would happen if we put it as a requirement. An industry practice could be maybe an idea there. I'm not totally against that. I'm more sort of afraid of what would be the consequences if you said, “Okay, five is the magic number here. If we see five attempts, then this and this and this is going to happen.”

We do monitor our resellers pretty well, and users and whatever, and you see a lot of stuff going on there. And you can't always go, “Okay, those five attempts were actually malicious of nature.” There could be some script going loose. And if the script of a reseller is going wild, so to speak, and generates all those attempts and maybe it involves like 1,000 registrants and they all get a notification. I mean, the support lines of that reseller will explode. So I don't want to commit to anything of that.

I think the idea is pretty good. Like I said, we monitor some stuff ourselves and we always do manual reviews like, “Okay, this spiking. Why is this reseller spiking? What is happening here?” And there could be very good reasons why it's spiking and then you allow it. And sometimes you have to intervene. But put it as a requirement within a policy? No. Thanks.

ROGER CARNEY: Thanks, Theo. Just throwing out an idea. What if the registry tracked this and just sent a poll message to the losing registrar that said, “Hey, this threshold has been met”? And again, the registry’s not going to do anything but just notify the registrar about it.

THEO GEURTS: That's actually a pretty good idea. I think that should be optional. There will be registrars that will embrace that idea and will turn on that option at the registry because it's a good service for them. Speaking for the registrar I work for, I think we want to have that total flexibility ourselves and set our own thresholds and come up with our own notification systems to our support staff. Like I said, the idea is actually pretty good, but I want to have total control of the number of attempts.

ROGER CARNEY: Great. Thanks, Theo. Okay. Jody, please go ahead.

JODY KOLKER: Thanks, Roger. Yeah, I like this concept. One of the things that Theo has mentioned is that they're tracking that themselves. And I can understand that. We also do portions of that. But this would be another registrar that's trying to transfer domains away that that are registered at our registrar. We wouldn't be able to see the fact that those domains are attempted to be transferred away and being basically brute force attacked or anything like that.

And personally I'd rather the registrant doesn't receive that information, but it would be nice as a registrar to be able to see if there are attacks that are being done on some of the domains that are registered to us so that we can notify the customer at the registrants if we choose. Or we can put better security on those domains names. Thanks.

ROGER CARNEY: Great. Thanks, Jody. Okay, any other comments/suggestions on this one? Again, it seems like we're thinking that it's a good idea and we just have to maybe work through if that's a practice or an optional item, or if it's a full requirement or not. Okay, let's go ahead and move on to the next one then. Thanks, Julie.

Okay, so this an interesting one that I guess it gets to a timing thing here. "Lock needs to be off for TAC to be requested or updated." And "lock" here is interesting because we'll get into the client server, what needs to happen on this. So I think that we'll just jump into this and say does the lock need to be off to even make the request for the TAC or for it to be updated?

Let us know if you support it as a requirement, best practice/industry practice, or do you not support or maybe want to talk more in detail about it. So please go ahead and respond.

Tom, please go ahead.

THOMAS KELLER: Thank you. I don't really get this proposed requirement, actually. I mean the way transfer works for most of us is that you get the

Auth-Code and then you go to your registrar. At that point of time, you may have the Auth-Code for two or three days already, and then you put it into the registrar. And before you do that, you unlock the name and say, “Now I’m ready for the transfer.” But I’m not too sure whether there's a direct correlation on the timing between when you get the Auth-Code and when you release the lock.

There are various use cases where you can see that they don't need to be necessarily connected. Even if there's a TTL on the Auth-Code, why would you need to release a lock just to get the Auth-Code? I don't think this is how the process is [inaudible] currently, at least.

ROGER CARNEY: Thanks, Tom. Kristian, please go ahead.

KRISTIAN ØRMEN: I was just thinking out loud a bit. If we are not [with Auth-ID] as only active during the transfer and maybe with a TTL of some kind, that means basically that the domain is locked when you don't have the Auth-ID because you couldn't transfer it anyway. So in the future if that’s what [becomes to] the transfer lock status, it’s maybe not really needed anymore. But I don't see why it should be a requirement to have it off/on or whatever when you get the Auth-ID.

ROGER CARNEY: Okay, great. Thanks. Tom, your hand's up. Is that another comment? Okay, Theo, please go ahead.

THEO GEURTS: Yeah. I'm sort of thinking along the way Kristian is thinking. To me the question was, what is the added value actually here? Why do we care if a domain name is locked or not? And then you are only able to update the Auth-Code if it's not locked. Why shouldn't you be able to change the TAC when a domain name is locked? I mean, why don't we give the flexibility unless there is a very urgent reason to not? But I don't see it.

ROGER CARNEY: Great. Thanks, Theo. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I was just thinking a bit ahead. Showing the transfer lock status in WHOIS if you could only get the Auth-ID with the transfer lock off, that would basically also show publicly that an Auth-ID is currently existing. And maybe that's a kind of unwanted feature.

ROGER CARNEY: Yeah, that's interesting. It may not be the only reason that it would show that, but to your point it may indicate that possibly a transfer is in process. That's a good point. Okay.

Sorry, Julie. Can you show the results? Jothan's comment about "maybe this one doesn't get into the play pile" makes sense. And again, I think this is more of a question of how and when. It seems like most people are commenting here that to get an Auth-Code, the locks don't necessarily have to be off. But obviously, specific locks need to be turned off for the transfer to go through. So it sounds like the majority think that to get the TAC it wouldn't be necessary to have the locks off. But obviously they would need to come off for the transfer to be executed so.

Okay, any other comments/questions on this one? Okay, great. Let's move on to the next one.

"Maximum TTL for the TAC." So should there be a policy mandate for a maximum X number of days that a TAC should be valid for? Let's go ahead and open it up. Please respond: as a requirement, industry best practice, or do not support or wants to talk about it.

Okay, let's go ahead and show the results. So it looks like a majority thought that a maximum makes sense as a requirement. And even some support it as a best practice there, or an industry practice. There are a few people that did not support this idea of a maximum.

Let's go ahead and jump into that discussion of getting clarifying issues on this. Those that didn't support this or are wanting to discuss it, please jump in and let's talk about it. Anyone that didn't support this idea of maximum TTL?

And then just to add on to this, something that we'll need to think about. That maximum TTL being similar to the syntax ideas, would the registry be involved in enforcing the max TTL? Obviously, the registrar can do that as well, but should the registry also be part of that max TTL? Meaning that if the [inaudible] is set for 30 days once that's stored at the registry, the registry will deny a transfer on day 31 unless it's been updated.

Jody, please go ahead.

JODY KOLKER: Thanks, Roger. I'm wondering if there should be two separate questions here. The first one should be, should there be a TTL for the Auth-Code? And the second one should be, should there be a maximum for it? I'm just curious if the pushback is just to have a TTL at all. If that's what may be not sitting well with people. Thanks.

ROGER CARNEY: Great. Thanks for the question, Jody. And actually, when the poll question was created, I think it was kind of assumed that TTL was somewhat accepted by the group. The exact implementation may be not ironed out for sure, but the idea of a TTL makes sense to the majority of the group. And I think the finer points of that TTL need to be ironed out. So again, I think that this was just added on to that idea that, yeah, we think the group supports TTL, and then should there be a maximum of that?

Yeah, and I think that's the issue that Kristian wrote into chat. There being TTLs and the idea of the TAC being only valid for the transfer window which is when the registrant requested it to that TTL, a maximum kind of helps encourage those registrars to not keep it on file for a year and someone can hack into someone's e-mail and get those and transfer them a year later.

Theo, please go ahead.

THEO GEURTS: Yeah, and it’s not just e-mail, Roger. I mean imagine if a registrar gets hacked and all those Auth-codes somehow were stored at the registrar level and were obtainable by a hacker. These things end up in forums and circulate beyond the end of days, so to speak. So if there is a TTL maximum, you can avoid a lot of problems.

ROGER CARNEY: Great. Thanks, Theo. And that’s a good point. Everybody brings up e-mail but, yes, there are multiple vectors there that obviously could fail and these can get out there. And to your point, once they're out there they're always out there.

Again, I think that the majority here supported there being a maximum. What that time is, is probably a good discussion. And also, I think a good discussion is, does the registry play a part in that to enforce that it can't be used beyond that maximum? Again, the registrar should be able just to reset it to a blank so that doesn't exist. But if it's still there after that time—the registry didn't update it or for whatever reason—should the registry enforce that? Okay, great.

Okay, let's go ahead and move on. And I think this our last poll question. “Should there be a minimum TTL for the TAC?” And I think this came up as an issue of, again, discouraging those registrars that want to act poorly and set the TTL to five minutes or whatever so that the transfer really can never happen. Should there be a minimum set, a minimum time on that TTL as well?

Again, let us know if you support that as a requirement. Obviously, we can discuss that, but more of just should there be a requirement on it. So should it be a requirement, an industry practice, or do not support a minimum or just want to discuss it. So please go ahead and respond.

All right, let's go ahead and show the responses. So again, as discussing I think there’s general support for the minimum. Obviously, there are some issues of the registry setting it and then changing it right away, but I think that's fairly auditable and trackable. So I think setting a minimum is a good step to that, and it looks like majority agree.

But someone wanted to talk about it, I guess—do not support this or just let's iron out any details here. So anyone that thought that this was not a good idea, let us know. Or maybe if you just want to talk about it. Not one person? Two people maybe? No? Maybe my extra talking convinced them that maybe it makes sense. I don't know. Okay.

Again, as Jody brought up just a little while ago, I think that the general idea was that it seemed that the group was very responsive to the TTL being in this recommendation set. So these are just two finer points on that, and I’m sure there are many more that we will end up covering. But good, okay.

I think that was our last one. Thanks, Julie, for that.

Yeah, Kristian, in the chat. I agree. I think that being a mechanism, obviously, if there's an issue, that it can be corrected. And it seems like a simple update to that by the registrar should allow any issues resolved.

Keiron, please go ahead.

KEIRON TOBIN: And thank. Yes, Kristian’s point was kind of along the lines that I was thinking of. There definitely needs to be something in there in terms of that if something is hacked or anything like that, that there is a possible way in order to kind of ensure that we can fix that, like you said, in terms of maybe if something is hacked or X, Y, and Z, then we definitely need something in there. And let's not have that minimum as a requirement unless there's something in there in terms of security breaches.

ROGER CARNEY: Right. Okay, that makes sense. Thanks, Keiron.

All right, let's go ahead. That was the last poll question, so thanks everyone. That was a great discussion and I think, again, just trying to iron out and get closer to the details on these. And it sounds like we’re getting there, so that's good.

Let's jump to just a couple of things here at the end. There are two recommendations in the Auth-Info Working Document and I’m not sure if there have been any comments on either one of them. Yeah, so no comments on these two.

I just want to get everyone to take a look at them. These are draft recommendations from our current discussion so far, so I think that any comments on either one of these would be great if we can get those. And actually, any comments over the next week. Again, I think we're going to transition over to talking about the FOA starting at the next meeting.

Obviously, we're going to revisit this, but we'd like to put this working document behind us and revisit it when needed. But any comments on these two? Otherwise, we'll think that they're perfect and we'll move forward with them.

Theo, please go ahead.

THEO GEURTS: Yeah. I think the recommendations are okay, but I do not think they will be … There will always be an issue with it. Let me phrase it that way. I mean, you have different languages. So you can talk about the TAC all you want, but still registrars will need to translate it. And then you will get [a bit] other acronyms. So I'm not sure how feasible it is. I think it's a good goal, but I think eventually it is not something that will be universally applied across the globe. Perhaps the English-speaking countries, but that's about it.

ROGER CARNEY: Thanks, Theo. Yeah, and I think it was getting to just a common agreement. And as you said, in practice we hope it gets used, but in practice it'll probably be supplemented with whatever they're using there. But it's at least common language between parties within all the communities it can use to reference the same thing. Great.

And again, any comments on these two recommendations but also in the whole working document, especially focused on any of the straw man things that we talked about today and last week that need a little more clarification or more discussion on them? And again, we're going to circle back on a lot of these things as we go through the remaining items, so we're just trying to move on from this document into our next discussion of the losing FOA which hopefully is a fairly quick discussion.

It’s the losing FOA. You begin an interesting concept of name, but talk about that. And for homework, obviously I want any comments that you have on the working document here, the Auth-Info Working Document. But also, read up on the losing FOA questions, charter questions; and familiarize yourself with the process of the losing FOA so we can start those discussions next week.

Thanks, Julie, for posting that. Yes, call next Tuesday. Same time. Any comments, questions from the group? Okay. Any comments/questions from staff.

Kristian, please go ahead.

KRISTIAN ØRMEN: Just a question on the meeting schedule. My calendar shows stopping August 31st, but I’m assuming that we just continue Tuesdays. Or is that just me assuming or hoping?

ROGER CARNEY: No, that is the goal, to continue through at the same time moving forward.

KRISTIAN ØRMEN: Thanks.

ROGER CARNEY: We'll get the other one scheduled as we get closer. Okay? All right, well I'll give everyone five minutes back. Thanks, everybody, for the great discussion today.

JULIE BISLAND: Thank you, Roger. This meeting is adjourned. You can all disconnect your lines and have a good rest of your day.

[END OF TRANSCRIPT]