ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 06 July 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/WgTpCQ

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, everyone. Welcome to the Transfer Policy Review PDP Working Group call taking place on Tuesday, 6 July 2021, at 16:00 UTC.

In the interest of time, there will be no roll call. Attendance will be taken by the Zoom room. If you're only on the telephone, could you please let yourself be known now?

All right, for today's call, we have apologies from Kristian Ormen and Tom Keller, both with RrSG. They have formally assigned Volker Greimann (RrSG) and Jody Kolker (RrSG) as their alternates 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 Panelists and Attendees in order for everyone 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 Zs before your name and add in parentheses "alternate" after your name which will drop 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 emails.

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 email 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. Hello, everyone. I don't have anything big to share to get us going here except for, I don't know, some of you may have noticed that it appears that the SSAD ODP webinar is scheduled at the same time our meeting is next week. So I want you to think about if that's going to be a conflict, if you're planning to attend that and won't be able to attend this. We don't need to know now, but when we talk about the next meeting at the end of the call just be thinking about that and let us know if that's going to be a problem. And if we need to move this meeting or look for a different arrangement to account for that SSAD webinar, we'll do that. So we'll talk about that at the end. Just wanted everybody to get that in their head to think about it.

Let's go ahead and jump into the work plan, Berry, if you want to go ahead.

BERRY COBB: Thank you, Roger. Before I get started, I see Jim has his hand raised and should be migrated to a panelist. Jim, did you want to opine on that last comment, or was that just you trying to get in to be a panelist? Okay, good. Right, and I also need to be a co-host, please. Thank you.

All right, so you've seen my email or should have seen my email after the agenda was sent last week. And just as a reminder for new working groups moving forward as part of PDP 3.0 we are tasked with developing a work plan and submitting that plan to the

GNSO Council for which we'll be held to account for delivering to our committed to dates.

And so the task really before us here is to commit to a plan that is reasonable, attainable, and of course predictable not only to just keep us into account to delivering to those dates, but this is really into the larger context of all of the other policy work that is going on. And it helps in terms of the GNSO Council to be able to plan for its pipeline of future work as well as work that is in [flight] here today.

So I know that what I'm sharing on my screen is going to be difficult for you to see. If you want, you can maximize your screen a little bit or refer to the PDF that I had attached. But in short, our key delivery dates that are proposed at this point in time are that by 16 June of next year, 2022, we'll deliver our Phase 1A initial report for public comment. We basically immediately pick up on the Phase 1B topics which deal with change of registrant. By the middle of September of next year we will have concluded the review of the Phase 1A comments and then solely focused on Phase 1B type of topics. By 30 March is when we would deliver our Phase 1B initial report for public comment and conclude the review of those by June. And as it's shown here, then basically the target would be mid-August 2023 to deliver a final report of both phases to the GNSO Council.

And of course I'd note that there's also a Phase 2 that is part of our charter, but we'll repeat this exercise when the Phase 2 group spins up. So for the current aspect it's out of scope.

So this plan has a couple of assumptions. It assumes that this group will only meet once per week at our typical duration of 1.5 hours of meeting time per week. The plan does not account for down times, such as holidays for American holidays, for example, as Thanksgiving or Christmas that's typically global. There is slack or padding, so to speak, that is built into this plan, but some of that slack is accounted for as I noted that holidays aren't necessarily factored into here.

And then further, which is I think something important to note and you can kind of see on the screen, in this section over here to the left are all the Phase 1A policy topics that we need to review. And within each one of those you've heard me reference before what is kind of the [crank] or approach where we'll deliberate the policy topics and charter questions, we'll get to some sort of draft document, we'll go through an initial reading, a secondary reading, get to some form of a stable draft, and then move on to the next topic. And rinse and repeat until we complete all of the topics that we've been chartered to do.

Now based on our initial review of the policy topics that are part of our charter, there wasn't an indication that any of these could really be discussed in parallel. Now that doesn't mean that we can strive to maybe do some of that, but the way this is laid out now and you can see over here on the right for what is considered a Gantt chart, we're starting here in Topic 4, then we move to Topic 3 on additional security measures, then we go to losing FOA/gaining FOA, bulk use of auth info codes, and then conclude with the Wave 1 Recommendation 27 report from the EPDP.

So all of these are set up iteratively. That ultimately gets us into building the initial report for both phases and then concluding to a final report that's down here on the lower bottom right.

So a couple of takeaways here. Two years and three months from now appears to be a long time, and it's probably scary to think about that this group could be meeting for that long. When we first started, once we reviewed through the issue report and the charter, my desire was I was hopeful that we would be able to conclude this within 18 months which is much more aggressive than what we have here by about 9 extra months.

But what I want you to put into context here is to not fall into a common trap of thinking that this is a plan based solely on calendar date. And also, don't be fooled—and we've got plenty of veterans here—but the deliverable dates for these things can creep up to us pretty quickly. And given our less than aggressive meeting schedule, that creep can appear before you know it.

Another way to think about this is our Phase 1A initial report is scheduled, as I mentioned earlier, to be opened for public comment mid-June of next year. So if we really put that into context, what that really means is that we have less than 80 hours of call time between now and June of next year to get to that delivery of the report. Or if you could compact everything down into two business weeks or five business days per week, that's essentially just shy of two full, solid, 40-hour work weeks to discuss through all of these issues and come up with consensus recommendations for change.

So while it may appear like a long time on the calendar, in fact from an hourly perspective and where most productivity occurs is on calls, that is not a lot of time. So that also suggests that even with this kind of extended timeline that we're still going to be looking to really produce work on lists outside of calls and those kinds of things.

So the last few things I'll say before I turn it over to Roger, committing to this particular timeline is kind of an under promise but over deliver. There's nothing that prevents us from working more aggressively and delivering earlier than what we commit to. There's no harm in that. Conversely though, there is harm if we can't meet to this committed schedule. Now there's always a relief valve. The last course of action is going through a project change request and asking for more time, but there needs to be appropriate rationale for doing so and we're probably better served to be more aggressive upfront and deliver earlier than what we planned to do.

That said, even before we get to any kind of PCR should we ever need one, we do have tools at our disposal, such as doubling up on meetings or extending meeting time, as I noted, trying to increase our productivity of working over the list or in between calls intersessionally.

And perhaps we can even contemplate working some topics in parallel. As a loose example, and I'm not presupposing this, but could we in fact talk about the losing and gaining FOA in parallel, or do they indeed need to be discussed and considered separately and iteratively?

So these are the committed dates. We need to send this to the GNSO Council by next Monday the 12th. Right now I believe it's just target as an any other business item to basically just inform and have the council acknowledge that this is the plan we're working to.

And the final thing I'll say is, as I noted in the email, I don't have any expectations that any of the working group members here need to dive into the details of a Gantt chart project plan. This is a tool mostly for myself and the leadership team to gauge our progress and being able to more effectively show what we're working on now, what we've completed, and what we plan to work on in the coming days and times.

Which takes us to the other link that I included which everyone should have access to. We have a dedicated Google shared drive. This is a work product that is our work plan and action items. Some of you are already familiar with it, but essentially this is a more tactical view of what it is that we're working on. It will have the meeting schedule set out for the next few months ahead of us as we continue to work along the calendar. And as we get more involved and deeper into some of our work, there of course will be action items that will be assigned to either the leadership team or the represented groups here.

So this will probably be your more go-to resource for understanding what we're doing now and what we're going to be doing in the coming weeks ahead.

So with that, I'll turn it back to Roger and happy to answer any questions. Thank you.

ROGER CARNEY: Thanks, Berry. That was great. Again, I just want to add on to what Berry was saying. It does look like a long time and many of you probably signed up for this not expecting it to be that long of a time. My expectation is that we will hit earlier than what this shows. I know that we have identified our work plan as being very sequential. We're going to work on this and then work on that.

But even through the first few meetings you can see that it's not that simple that you isolate these things one-to-one. We cover them and as we iterate we cover several items at a time which hopefully later down the line when we get to gaining or losing or whatever is next, we've already covered a lot of that and discussed it and there's a general understanding of what's going on so that will actually speed that up.

So I'm not too worried about that long timeframe because I think we will be able to shorten that up as we go along. But I open it up to any questions, comments from the group before we move into our topics today. Okay, and as Berry mentioned, we'll get that sent off to the council by next week so they can have it for their next meeting.

All right, so let's go ahead and jump into our continuing discussion on AuthInfo, or as we're calling it now Transfer Authorization Code (TAC). Okay, last week we ended on and had a brief discussion about b3 and the SLA around the five calendar days. We briefly talked about it and introduced it. So I wanted everybody to have a chance to speak to it today if they had any other additional comments, questions on it.

It sounded like from last week people thought that there should be a timeframe given. What that timeframe was sounded a little more undefined. The current five days seemed like it was good for some people. Others thought maybe that was too long. Others thought maybe it could be longer.

Again, I think one of the big things that came out of last week was this was the maximum time, not the standard time or anything like that. What I heard last week, the potential would be that we could look at a fairly quick transfer and it not take five days just to initiate the first part. It could be hours or whatever, but allowing for the five day window was something that was said it was preferrable.

Theo, please go ahead.

THEO GEURTS: Yeah, thanks, Roger. Why did we have five days in the first place? Does anybody remember? I don't. Thanks.

ROGER CARNEY: Good question. I don't know. Anyone have thoughts of why the five day, five calendar day was requested? And I'll recognize that the transfer policy is pretty specific and throughout it, it mostly talks about calendar days not business days. And I think the goal would be to stick with that, but that's up for discussion as well. Keiron, please go ahead.

KEIRON TOBIN: Yeah, thank you. I do agree. I think five days is right, but I think maybe we should change the language preferably. So rather than saying "within five calendar days" maybe "up to five calendar days" or "up to five days." And then that way if people want to do it sooner, that's fine. But I think the words "up to" would allow everyone on both sides who want to extend it have their say but also those who want it less. So it's kind of an equilibrium for everyone, essentially. So I think that would be a good way to just change the wording slightly, just "up to." But I'm happy to have other opinions on that as well.

ROGER CARNEY: Great, thanks, Keiron. Thoughts on that? "Up to," is that clear for everyone? I guess more clear as a statement instead of "within five" but using "up to"? Okay, and if anybody can think of why the five days was there, I assume it was more of probably a dart deal. Someone just threw it at the dart board and that's what came up, but I don't know. There may have been some discussion around it. I have no idea. Okay, so I think that let's leave it as "up to five days," and we can obviously revisit this, but it sounds like that's general agreement. Okay.

All right, let's go ahead and move on then to b4. The transfer policy does not currently require a standard time to live (TTL) for the AuthInfo Code. Should there be a standard time to live for the transfer code? In other words, should the transfer code expire after a certain amount of time?

I think on this one not just should there be a TTL but should there be bounds on that TTL? Should there be policy state the maximum is this or the minimum is this? And along with that, does it make sense to have a TTL? Thinking about it from a security aspect, does it add security to have the TTL? It seems like it would, but I'll leave that open to discussion. Theo, please go ahead.

THEO GEURTS: I think there are a couple of tracks and approaches here we can approach. We could quickly set a TTL for this segment here, but I think or I suspect when we go back to the stuff which we discussed last week about perhaps improving the end user experience and make sure that registrants have access to a one-time token or one-time authorization code or whatever you want to call it, if we circle back to that, then maybe this becomes no longer required.

So I wouldn't spend too much time on it. Just follow standard security practices on how long a TTL is normally required for a password or an AuthInfo code. And of course, [inaudible] policies within a company but if you look at passwords, some companies you have to change your password each month, sometimes at 90 days.

So I would just go down that road and not spend too much time on it. I think any number we set on a TTL now would be good security anyway because we don't have a TTL currently. So anything we throw out of here as a number would be an increase to security of the AuthCode. Thanks.

ROGER CARNEY: Great, thanks, Theo. And I'll note that in the TechOps discussions 14 days was suggested and discussed, and it seemed like a lot of people were behind that 14 days. If that's the right number or not, again, that's what this group should be able to decide. Jim, please go ahead.

JIM GALVIN: Thanks, Roger. Since you mentioned Security, Roger, Theo touched on something, and I want to highlight some questions for the group to think about. As you decide whether or not 14 days is enough or is the right number rather, if we go back to thinking about security principles and that's what we want to apply to the use of the AuthInfo code, consider the overall business process and what's going on here.

I would observe for you that there's a relationship between the five-day grace period for the transfer to take place and this 14 days and the notion that this is a unique, one-time password code, a unique code of some sort. I would expect that in the grand scheme of things if the code gets used at all if a registrant attempts to use it at a gaining registrar and it goes up to the registry, I would expect that part of the system to the extent this is a unique code the registry would clear that code out and not allow it to be used a second time.

And so what that suggests is that the 14 days being longer than five days is probably not the right thing. So it calls into question the five-day grace period too which is probably less likely to change as part of all of this. So really what I'm highlighting here is that there's a relationship among these parts that we are going to have to discuss and decide what we want things to look like at some point down the road. So I'm cautioning whether 14 days is too long given the one-time use principle that might come to bear here. Thanks.

ROGER CARNEY: Thanks, Jim. And I'll just add a little onto that in that I think you touched on it was if the code gets used at all, and I think that we've seen numbers not specifically but that many transfers are initiated that never go through. And I mean many by a factor, multiple factors of the ones that actually do go through. So I think that is somewhat something to think about is if that AuthCode is ever created and given to somebody, right now the majority of the time it does not get used.

But to your thought, Jim, on the five days versus 14, yeah, I think that's something to think about. And I think you have to start mapping that out as to, okay, it's up to five days from request to get that one-time code and then X time to use that code. So, yeah, I think that's right, Jim. You have to start thinking about those things together and how that works.

VOLKER GREIMANN: [inaudible]

ROGER CARNEY: Volker, please go ahead.

VOLKER GREIMANN: Yes, sorry.

ROGER CARNEY: No problem.

VOLKER GREIMANN: I'm just wondering if TTL adds any real-world benefits. Do we have any cases where an older AuthCode was abused after maybe a year or a month that suddenly caused a domain to be hijacked? I mean, if we are changing anything to our existing implementation, that means implementation work and that should be something that's considered as worthwhile and adding additional security and benefit to the customer.

In most cases today, the AuthCode is generated when the domain is either created or transferred into the registrar and resides in the system to be requested by the customer at any time he chooses. And I don't think that having to rotate those AuthCodes or generate them upon request adds any additional benefits to that. Unless we have any evidence of cases where either the AuthCodes have been hacked out of the registrar's database, therefore that may be something that requires to have it rotating. Or where really someone is requesting AuthCodes in bulk and then aging them and transferring the domains out against the will of the registrant that way.

So while it might add some theoretical security benefits, I think we should look at the real-world benefits first. And if we do not have any real-world benefits, then we leave it as is. That should always be the default. Thank you.

ROGER CARNEY: Great, thanks, Volker. Steinar, please go ahead.

STEINAR GROTTEROD: Hi. I'm just wondering, the TTL, if it's being deleted immediately after the transfer has been initiated and approved by the gaining and losing registrar. Then it can't be used, so why do we have to stick to some number of days before it's being deleted? I don't get it. Thank you.

ROGER CARNEY: Thanks, Steinar. Yeah, and I think that's kind of what Volker was hitting on. Obviously, once the registrant has the code—and if you look at it today, the code's probably sitting in their email somewhere—so if they don't use it and today obviously even if they do use it, that's kind of an issue. But if we're looking at it as a one-time password going forward, but if the registrant does not use it and decides I don't want to move it and if that code's still sitting in their email, their email could be hacked at some point three months, six months from now and someone finds that code. Again, I think what Volker asked is valid. Are there real-world scenarios of this. Obviously, it is an additional layer of security but, as Volker points out, is it required? Is it necessary? Jody, please go ahead.

JODY KOLKER: Thanks, Roger. Can you hear me?

ROGER CARNEY: Yes. Please.

JODY KOLKER: I think there are some assumptions here that Volker and Steinar are assuming that I think need to be played out. But I think what Volker is saying is that in the current world that we have an AuthInfo Code is set at the registry when the domain is created.

I think what Volker is assuming is that this policy is telling us that every 14 days that that password needs to be changed. I had not been assuming that reading this. What my assumptions are is that once the password is given—I'm sorry, once…what did we call it? The TAC is given to the customer, that's when the 14-day TTL starts. It doesn't start when the domain is created and an AuthInfo Code is set. It only starts when the customer has actually been given the TAC. That's when the 14 days starts and that's when it should be changed.

I fully expected not to be having to update AuthCodes on all of the domains that have been registered by the registrar every 14 days. It would only happen when the TAC was delivered to the customer. I'll leave it at that, but I'm curious if that's what Volker was expecting. Thanks. Bye.

ROGER CARNEY: Thanks, Jody. I'll just add onto that. The TechOps was under the thought of what Jody was describing. There would not be an AuthCode on a domain until a transfer is requested. And then an

AuthCode would be created and associated to that domain. And then the TTL would drive how long that AuthCode would be valid for. And then that AuthCode would be eliminated after that time on that domain. So that was the principle, I think, from the TechOps. Steinar, please go ahead.

STEINAR GROTTEROD: The understanding is that if we set the TTL for the TAC to be 14 days, the registrant has 14 days to actually initiate the transfer. If it's past the [14] days, the transfer will not succeed. Is that the correct understanding?

ROGER CARNEY: Steinar, I think that would be the correct understanding. And then the fallback wd be the registrant would have to request an additional or a new AuthInfo Code or transfer authorization code. I think that's kind of why it's important on the [days], if this goes down, I think that the number of days is important because again I think if you look at it statistically, most transfers do happen within a certain amount of time. What that time is, is I think the important part. Steinar, please go ahead.

STEINAR GROTTEROD: But the way I understand Jim is that this 14 days TTL is kind of a security risk. And if that's correct, I'd really like to understand why. The obvious reason is, of course, the email or whatever can be hacked and the TAC is being seen by nonauthoritative persons, etc. But the combination of the five days and the 14 days TTL, that was a security issue. Thank you.

ROGER CARNEY: Thanks, Steinar. Jody, please go ahead.

JODY KOLKER: Steinar, yes, I mean, the obvious reason is the email could be hacked or if we decide that we can deliver this by any other way of email—whether it's by phone, by WhatsApp, by texting, anything like that, I mean any number of ways that the password could be hacked—from a security perspective I'm just nervous about giving out a passcode that the registrant can accidentally leave anywhere and it's now open in the wild and this domain name could be transferred immediately with that. And that just makes me very nervous from a registrar perspective. I'm curious if anyone else is nervous about that or thinks that this is too long, the 14 days. Thanks.

ROGER CARNEY: Thanks, Jody. I'll just add I think last meeting or the meeting before someone brought up the idea of a shortened TTL for either important registrants or important domains themselves. So I think, think about TTL in the sense of Facebook.com wants to transfer or whatever. Is there an issue with TTL being important in that case? So, Volker, okay. I'll call on you in a couple then. Keiron, please go ahead.

KEIRON TOBIN: Hello. Yeah, I agree with Jody. I do think a time limit is definitely required rather than being indefinite. I think for a security feature, it's definitely right. So I do definitely agree on that side. Although, I'm just thinking in terms of the 14-day [inaudible] to put a lock on it. If the registrar was to cancel it maybe because they didn't support the gTLD or something like that, would the registrant be required to request a new passcode or would they still be able to use it elsewhere even if it was rejected?

ROGER CARNEY: Thanks, Keiron. Jim, please go ahead.

JIM GALVIN: Thanks, Roger. I want to respond somewhat directly to Steinar who asked a question about why setting the TTL is good or bad. I want to offer another example of a way that this might play out. I think that having a TTL of some sort is a good security principle. It's a good security practice.

But my main point in my comment was that there's a relationship between the TTL and the security principle of one-time usage and it being a unique value and only being allowed to be used one time. So there's a fuller picture of the overall business process that we have to map out and understand before we can speak quite deliberately about whether or not there should be a TTL and what it's value ought to be.

So I'll offer an alternate view here. Right now we're talking about a maximum TTL value. I actually offer that you could also be thinking about a minimum TTL value, not a maximum. Different security properties but different reasons why that's valid. For example, you might just say that it has to be valid for at least five days because that's the five-day grace period that you get for the transfer to happen. Maybe it should be a little more than that to give the registrant some time to get to the gaining registrar and use it.

But I say that because who controls the TTL? That becomes a critical question here. Whether you're going to do at the registrar or you're going to try and say you want to change the system and have the registries do it. What I think is the registrars—I mean, now my particular comment here, specific comment is—the registrars should own that and have it for themselves. But that means how does the registry know that there's a TTL at all? What do you expect them to do about that?

I think the registrars are going to have different models, different ideas, different delivery mechanisms. They're kind of going to want different TTLs for different reasons. Probably different length TTLs for different reasons. But you probably need to have a minimum on behalf of the registrant. And then what that means is when that expires, the registrar would then delete it from the registry so that it can't be used anymore. That would be an overall business [process] consideration.

So there's a larger mapping that has to happen here. Sorry to talk so long. I just want to make sure I'm putting questions in front of you to think about in the overall picture of what security you're trying to apply to the system here because there are choices to be made. Thanks.

ROGER CARNEY: Thanks, Jim. And I appreciate that, Jim, because you kind of hit on something Sarah mentioned in chat a while ago is about the one-time use. And I think that's correct. If we go down that path where it's a one-time use, the TTL is the maximum time that they would get to use that one-time use. Once it's used, it's done and cannot be used again. Even if there was a 14-day TTL, once they've used it the TTL no longer matters. And to your point, and again Sarah brought that up earlier, so I just wanted to touch on that.

Volker, please go ahead.

VOLKER GREIMANN: Yes. I mean, being one-time use is kind of implicit in the process of a transfer code because once it's transferred it's used. Then basically, a new one has to be generated at the new registrar already. But I wanted to look at another point here. I mean, in many cases the interaction between the registrar and the registrant is not a direct one. There are resellers. There are agents. There are law firms that manage domain portfolios for their customers. And in such cases it may very well also be the agents that receive the AuthCode.

In many implementations that I've seen so far, the registrar does not even see when an AuthCode has been requested because that request is not made to the registrar directly but it's made to his wholesaler, the agent that manages the domain name and they manage that process for him. So in many cases, registrars outsource part of the registrar services to other providers.

And having to then accommodate a feedback loop where the third party that provides that registrar service now has to notify the registrar that the AuthCode has been provided to the registrant or to another party that might be in between there, I mean, the chain of resellers might be very long and can become very opaque for the registrar at a certain point.

So the point I'm making is that the registrar need not necessarily know when an AuthCode has been requested by the registrant or when it has been provided to the registrant because of the way that the business relation is set up. And therefore, attaching a TTL to that request might become very, very difficult to implement through certain business models that are currently present in the registrar space and that I don't see any reason to change at the moment. Thank you.

ROGER CARNEY: Thanks, Volker. Yeah, and I think that's important that we have to remember the different models. And I'll just throw in, Volker, as you described it the reseller of the reseller of a reseller of a reseller, however far you go, the one issue is normally—and this may not be true everywhere—but I would say that normally whoever is doing the EPP, I'm guessing that's going to be the actual registrar that does the EPP, would know that the AuthCode is being set because they're the ones that are having to do it. But I still think we have to think through all those scenarios. Thanks, Volker. Jody, please go ahead.

JODY KOLKER: Thanks, Roger. First of all, I'll address Volker's point. I agree with him to a point that there may be times it may take, if you have a reseller or a reseller of a reseller of a reseller, well, that's a good reason to have a TTL because now you've just given it out to at least six different people that have it probably in their logs or they've had somebody watch it go through their system that have the AuthCode now.

And when it's requested from the registrar, that's when the registrar will know that it's been given out and can put that TTL on it. And now it's gone through a bunch of hands to get to the registrant, and that's more of a reason to have a short TTL on this because now it's just been looked at by many people instead of just the registrant, the person who wants to do it.

I also wanted to comment on Jim's comment regarding how the TTL will be set up. I think that we have to think about how long it's going to take to implement something like this. If a TTL is to be set up by the registry, it can either be a standard where it's always 14 days no matter what. It is never less than nor more than that, it's always that. Then this could be set up easily by the registry. But then we are very constrained as to how long it can be because it will be a policy and this is what the registry says it is or this is what the policy says it is and the registry just implements it.

But if we want to be more flexible, then the flexibility depends on who is setting it or who is controlling the TTL. If the registry is to control the TTL based on what the registrar has sent it, then we have to change EPP which will have to go through the IETF and we're probably talking about years before that is done. I'm exaggerating a little bit, but it could be years before we actually have a TTL that can be set by the registrar, sent to the registry to be able to implement.

Whereas if the registry does it or the registrar does it, well, the registrars can implement it as they have time. which I know everyone is busy and has a lot of things on their plate, but the registrar then has the flexibility to decide when it's important for them to set that TTL. They would obviously have to do one according to policy.

But then the importance of setting lower TTLs, some of these domains are worth millions of dollars. If they're going to be transferred from a registrar to another registrar, I would imagine that the losing registrar in order to avoid liability would want to make that TTL about 30 minutes long or even less to say, "Oh, you're going to transfer? All right, let's put a 30-minute TTL on it. Here's the AuthInfo. Go ahead and transfer it now. It's being unlocked. We've got 30 minutes to get this done." Which shouldn't be a problem, but then that AuthCode is only out there for 30 minutes and there are only 30 minutes of problems that you have to worry about. Thanks.

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

THEO GEURTS: Thanks. Maybe we should move on from this topic for now. I mean, we will get back to this regardless when we move to bulk transfers and go back to the stuff which we discussed last week. They're all intertwined, so to speak. They're all connected and at some point one of these discussions we are having now, one of these topics will have to drop in favor of one of the other solutions that will come out of there. So we are not totally dependent on this very heavily at the moment, I think. Like I said, we will get back to this one way or another. Thanks.

ROGER CARNEY: Thanks, Theo. Yeah, and I think that Volker put in the chat obviously a TTL was probably—and any security features we add—are probably going to cause additional support items. And again, I think it's one of the important things we look at is if it's standard, it's easy to explain across. The more flexible it is the harder it is to explain across registrars and the entire ecosystem.

But I think that one of the issues is that maybe—and again I'm just throwing it out here—TTL is not a topic that's even addressed by the policy. But registrars could still do their own TTL unless we forbid it in policy. We wouldn't even have to write policy. Registrars could just create it, and it's their responsibility to explain that to their customers. But just throwing that out there. Maybe we don't need it.

And as Theo mentioned, a lot of these topics are intertwined. We keep hitting slightly on the fact that the other day we talked about who is going to manage this transfer authorization code, registry or registrar. Obviously, that topic is being talked about here sort of. So again, I think Theo's right. We will come back to it, and I just wanted to make sure this was all discussed as we can.

So I liked one comment. I saw this in chat. John made some suggestions, but I'm not sure anybody responded to John's last question about a possible manual revocation of the transfer authorization code. I assume John is talking about the registrant going back in and saying, hey, I don't want to transfer this anymore. So something else to think about.

Okay, any other comments on TTL? Again, good discussion. And like Theo said, it does get intertwined into other topics, and I think where the management gets done will directly tie into this and how difficult that is. And again, I think we need to think about policy versus strictly saying, yes, you can do this or strictly forbidding, [no], you cannot do this. So just thoughts.

Okay, well, good. Good discussion. Again, I think we'll go ahead and move on, and we'll obviously tie back to this as we continue. Once we get through all these AuthCodes, we'll have a more general discussion as we try to tie all these pieces together. So good.

All right, let's go on to b5. Should the ability for registrants to request AuthCodes or transfer authorization codes in bulk be streamlined and codified? If so, should additional security measures be considered?

This specific charter question came out from some comments actually on the transfer report survey. So throwing it out there. I think we've already kind of talked about this a couple times, at least briefly, and delayed a more thorough discussion until now. So bulk transfer of domains and how AuthInfos or transfer authorization codes relate to those. I'll open it up. Theo, please go ahead.

THEO GEURTS: Yeah, it's actually a good question if there is such a need for it. I haven't heard of…I didn't hear any information over the years that there is an issue with it, but it's good to discuss it. Also, keep in mind if we would go for a one-time pass for the one-time AuthCode in possession of the registrant as discussed last week, it would nullify this question because then the registrant would always have already the AuthCodes regardless of how many in his or her possession. Thanks.

ROGER CARNEY: So, Theo, on that topic what if the AuthCode was a single AuthCode that allowed the registrant to transfer 10 domains at one time?

THEO GEURTS: I would think that it's going to be bad practice to have one.

ROGER CARNEY: Okay.

THEO GEURTS: But that's also an interesting topic to discuss. I mean, it would be very handy if you need to transfer 10,000 domain names and do it with one AuthCode. That would be very, very productive, of course. Especially, resellers would like such an option to have just one code to transfer a lot of domain names, because under the current transfer policy bulk transfers are completely broken. Thanks.

ROGER CARNEY: Okay, thanks, Theo. Keiron, please go ahead.

KEIRON TOBIN: Thank you. I think coming from a registrar where a lot of [inaudible] are domain investors and things like this, definitely a bulk transfer is definitely something to consider. However, what you find is that with a lot of domainers and stuff like that, they are much more aligned to security. So for example, a lot of them have two-step authenticator already on their domains. They tend to be a lot more security conscious in regards to this matter.

So I think if it was something that we should look at in terms of bulk, I think we could easily look at potentially adding additional security stuff on and that would also enhance domain investors and stuff like that but also protect us as registrars as well as registries. Because I think it definitely needs a higher level of security because if someone was to transfer 10,000 domains and there were issues going across, that could be detrimental to a lot of us. Thank you.

ROGER CARNEY: Thanks, Keiron. Volker, please go ahead.

VOLKER GREIMANN: Yes, thank you. In the past, the AuthCode has always been unique for each domain name, and I think there are important security considerations that make that interesting to keep. However, I think as Keiron said there are certain types of registrants that value their mobility of registrations from one registrar to the next, and that would be very ill-served if they would receive the AuthCodes by a single email per domain name. So in the past, this has always been a service that many registrars provided, even if not in an automated fashion but through their support. If we introduce that as an automated feature, then that might introduce security issues. So I think I come down again on the side of why fix something that isn't broken at this point. Thank you.

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

THEO GEURTS: Yeah, I'm going back to my original point. Is there an issue with the request of authorization codes in bulk? I think you can boil it down to if you want to say something about it, the request of AuthCodes in bulk should be permitted and how that is done, that is up to the registrar on how to decide. Like Volker mentioned, our support sometimes gets these requests and then we just give them an Excel sheet with all the AuthCodes. So I think it's up to the registrar. If we need to do this, something in bulk, just keep it simple and leave the solutions to the registrars on how that will be delivered. Thanks.

ROGER CARNEY: Great, thanks, Theo. Other comments? Theo had a nice elegant proposal at least to answer this. And it's, yes, that bulk transfers should be allowed and again that implementation is registrar dependent. And again, I think when you look at the scenarios of where bulk would be applied, certain registrants obviously some of the domainers or, I don't remember if it was Theo [or Volker] who said something about resellers doing it. I think that those are probably two of the bigger ones that would take advantage of that. And do we get an advantage of trying to standardize that across all registrars or, as Theo mentioned, let that be a registrar implementation issue and even fit into their own business model that way. So something to think about. Keiron, please go ahead.

KEIRON TOBIN: Thank you. I would probably say though if it was in a bulk transfer such as a large one or something like that, we should probably deter just regular users using this tool. So for example, what we could state is that—without jumping the gun—if you were to use this tool, you couldn't expedite domains as such as fast and it would need to go through the full process. Just something along those lines to deter people from using it and just make sure that it's kept to the larger customers.

ROGER CARNEY: Thanks, Keiron. Okay, any other comments on b5? Okay, great. Let's move on to b6 then. So b6 is does the CPH TechOps research provide a logical starting point for future work on transfer authorization codes or should other options be considered?

I think that the group at least sounds like they have already assumed that it was a good starting spot for this work. I think the important part of this question is the last piece. What other options should be considered that aren't considered in the TechOps papers? Again, we can debate which one of those options is good out of the TechOps papers, but what's missing that we should be considering is probably the bigger question here.

Thoughts from the group? Anything come to mind? Okay, again, we can come back to that. I think that, again, we've already started using a lot of what the TechOps provided, and I think that once we get through b7 here, we can probably start pulling the pieces that we think make sense together when we look at transfer authorization codes more holistically and solve these security problems. Taking a look at it from the aspect of does this lead us into solving the FOA questions as well. Okay, just give that thought. And again, anything that is missing out of the TechOps paper, please bring up for discussion so we can roll that in and get a good discussion around it.

All right, let's move on to b7, and b7 is should required differentiated control panel access also be considered, i.e., the registered name holder is given greater access (including access to the [AuthCode] transfer authorization code) and additional users such as web developers would be given lower grade access in order to prevent domain hijacking?

Again, this question was prompted by comments out of the survey. So, Theo, please go ahead.

THEO GEURTS: It’s a good question, of course, and from a security perspective I would be all for it. But it is quite unworkable if we go down that route. That will be a) a lot of work and b) I am of the opinion that if we would make it a policy, that it would derail a lot of business practices among registrars and resellers. Plus, I am of the opinion that when it comes to security of accounts we already have enough requirements, be it through law or regulations already.

I mean, the GDPR has something really, really broad. It says you must provide adequate protection, which means that you need to make sure that everything, regardless of what it is—your backend, your database, your user accounts—must be protected very, very well. They must be very, very secure. There are several security [acts] out there which we need to comply with.

So there are already those requirements. We must already put in our best effort to make sure that the data of the registrant, the domains of the registrant are already super well protected. So that is a given for us anyway. And I think if we would go down the road to put something in like differentiation through an ICANN policy, that usually ends up very, very bad. It could even conflict with certain cybersecurity laws and data protection laws. Thanks.

ROGER CARNEY: Thanks, Theo. It looked like Sarah and Keiron kind of agreed with you there in chat. Jody, please go ahead.

JODY KOLKER: Thanks, Roger. Yeah, I agree completely with Theo and with Sarah and Keiron on this. I think that this is a business practice and just a huge overstep by ICANN on this. It should be just a policy of the registrar and how they want to give out the AuthCode. Thanks.

ROGER CARNEY: So I'll throw it out there then as not a recommendation that this is done, but would it be useful for this group to suggest or comment that other security measurements are a great idea to implement or something to that effect? Again, just throwing it out there just rolled off the top of my head. So not a recommendation that, hey, you have to this or you have to have two-factor, but maybe it's just a comment that we place that, hey, these security measures are out there and people are using them. Something to that effect. Greg, please go ahead.

GREG DIBIASE: Sure. I think Roger and Jody said it, but I agree. Just from a workability perspective like control panels and how registrars define different users within their ecosystem are all different, so I just think even working out the definitions for such a requirement would be completely unworkable.

ROGER CARNEY: Great, thanks, Greg. Okay, so it sounded pretty resounding that, no, we don't want to step into this work here. Again, maybe it's—

Sarah put in there—maybe we just keep a list of things, other good ideas, practices, security items and realize and let people know that we thought about these and they're good ideas. We're just not going to make policy out of them. Okay? Okay, any other comments on b7?

Okay, so I think we made it to the end of all the transfer authorization code charter questions. I think from here what I want to do is maybe work through maybe multiple scenarios of now looking at it more holistically. How do we see all the pieces that we've talked about fitting together to create a secure mechanism to improve the transfer authorization code from what it is today to what it could be and should be in the future?

And again, taking into account, obviously, the different business models, the impact on registrants and everything. So I think when we look at the discussions we've had across all of these, is there one multiple solution scenario that we can create? Hey, this piece of what TechOps said, this piece of what we came up with here, this piece of the TechOps, and pull it together and make a maybe not complete but close to complete idea of what the new transfer authorization code should be modeled on.

And then maybe supply two or three of those scenarios to TechOps. And again, just thinking maybe supply two or three of those scenarios that we draw up. Hey, this seems like a good path. This seems like it. And see what the technical operations group thinks about that. Comments on that? Thoughts on progressing this overall discussion into a more cohesive multiple recommendations that we can pull out of it? Theo, please go ahead.

THEO GEURTS: Yeah, I think we can definitely pull some stuff from here and post it to TechOps. My only reservation about it is that it might end up when we progress more and more into the other talking points that we will conclude that those questions which we posted to TechOps to think about, that at some point in time we made a different decision, took another direction, and those questions are no longer relevant. But I don't think that is a major problem.

Of course, I'm not diminishing the value of the work from TechOps, and I don't want to burden those guys—probably myself because I'm still part of it in some shape or form. So I don't want to waste volunteers time, but I think the benefit to make progression and move along with the TechOps to pose them several questions is beneficial, even though there is a risk that it might be that we move into different directions.

That's just the way it is. I think these things are very complex. I mean, we already touched upon different scenarios where another scenario would be completely excluded if you would go right or left. So I think that's just a little bit how it goes, business as usual. So that's a little bit of my thinking here. Thanks.

ROGER CARNEY: Great, thanks, Theo. John, please go ahead.

JOHN WOODWORTH: Sorry, I was double muted there. I would like to bring up the potential of having a proof of ownership field as part of this. And I don't know exactly if that fits into the b7 category or where it would fit because there's some overlap with DNS and domain here as well.

I'll give you an example. With a, let's just say, web hosting or a DNS hosting for a domain one thing that you would want to do is validate that the person requesting this is indeed the owner of the domain or at least has some sort of authority over the domain.

And there are ways to prove that if you currently have a hosted DNS or web hosting service where you can, for example, make them create a DNS record. But that requires a bit of a paid service in some instances where you add a burden to that registrar. Whereas if we could have a field that you could change, the service provider could request that you put a certain string in that field just to prove that you have edit capability for the registration of that domain rather than trying to probe around and figure out and how can I determine if this individual has access or should be making this kind of request.

ROGER CARNEY: So, John, you're thinking proof of ownership on the gaining side?

JOHN WOODWORTH: So this—apologies, go ahead.

ROGER CARNEY: I was just going to say on the losing side proof of ownership is kind of already conducted through login and two-factor or whatever, right?

JOHN WOODWORTH: Right. And again, this is kind of an overlap of where DNS and where the actual domain ownership, they are intertwined even though they're not the same. But for example, the gaining DNS provider, in order to make sure that whoever is requesting record changes or not necessarily registration changes but just other DNS service-related changes, that you're authorized to make that request. So you want, for example, those records hosted by this DNS authority.

Right now, you want to follow the ownership chain back to make sure that you have the right or the authority to actually make changes to DNS. And even if, for example, and I don't want to get too off track here, but even if you're not delegated to because you still have to go through that part of DNS. If you're on an authoritative server, you could impact services for other people that are hitting that authoritative server even though you're not necessarily going to be delegated to. So there could be some impact, especially if they're doing a hybrid authoritative recursive solution where you may have an impact on a domain that you really shouldn't have any authority over.

And we can take this offline. I don't want to, again, take this too far off track. But I would like to at least suggest a user defined field where the registrant can make an edit to data at the registration level, similar to this AuthCode or the AuthInfo Code.

ROGER CARNEY: Yeah, I think you're right. Let's take it off and put it on the list. John, if you can put it together and just send out an email to the group, we can spur the conversation on the list there.

JOHN WOODWORTH: Definitely.

ROGER CARNEY: Thank you.

JOHN WOODWORTH: Thank you.

ROGER CARNEY: All right, Theo had a comment, but I think he's done now.

THEO GEURTS: That is correct. What John is describing is, of course, very important. But the way the discussion was going, we were at some point talking about parts of the DNS which I as a wholesale registrar am not even part of. So that would be very, very complicated to accommodate that. So if we can take this on the list, great. Thanks.

ROGER CARNEY: Thanks, Theo. Okay, again, I think the goal out of this is to start coming up with recommendations on each of these questions. So I think now that we've talked through—and again I know that we'll still come back to these as we talk through other security measures and the gaining and losing, we'll still hit on some of these—but I'd like to start coming up with recommendations for the transfer AuthInfo. And I don't know if the best way may be just to spin off a group of three, four, six people that can come up with, okay, this is how AuthInfo should look or would the group rather just walk through all that on the calls together?

I don't know if it seems maybe like it would be more productive if a smaller group got together and said, okay, if AuthInfo transfer authorization code was this way, the registrar does this, the registry does that. Answering all these charter questions basically going through and provides that feedback to the group, maybe next week even, next time we meet, that may be the more efficient way to spur discussions. Thoughts? Does everybody want to try to work those in the large group or maybe isolate five or six people to do it independently before the next meeting? Greg, please go ahead.

GREG DIBIASE: So I think either of those make sense. I'm just wondering, do we have a threshold question on whether the AuthCode is controlled by the registry or the registrar that we need to determine before handing over this work to TechOps? Or are we envisioning that they be basically putting together parallel proposals? Here's what happens at the registry controls, here's what happens at the registrar controls.

ROBERTO GAETANO: Yeah, good question, Greg. I was thinking that we would come up with that saying this and then ask the technical people and even the security people what's wrong with this. We've gone through and we've seen what TechOps has suggested already in their paper. And some of it makes sense to us, and some of it maybe doesn't make sense to us. But if we put together a scenario or two that this group thinks, hey, this makes sense and ask TechOps to tell us why it doesn't make sense more so than that and how can you improve this kind of thing.

Okay, other thoughts? Sarah, please go ahead.

SARAH WYLD: Thank you. In general, I like the idea of we have all provided input as to what we think the answers to these questions would be, and then a small group can take that and work with it and come back with a proposal and then we all look at it. I think that's a really good way to consolidate these ideas that we have all discussed. But unfortunately, I can't commit to doing that this week myself personally. So if it's something that has a longer turnaround time than just one week, that might make it easier. If I did understand the proposal correctly. Okay, thank you.

ROGER CARNEY: Great, thanks, Sarah. I appreciate that. Okay, other comments on moving forward with these? Berry, please go ahead.

BERRY COBB: Thank you, Roger. Staff will be here to support helping to schedule a call for a small group and those kinds of things. Whatever the next steps that this group agrees with and whether this technical proposal or dual proposals are shared with the TechOps, I think what's going to be important about this next phase of the exercise is that it's kept in the context of what the current requirements are in the transfer policy around AuthCodes. So really, the top of this document.

At least my initial reaction to this is, do any of the current policy requirements need to change? If so, what do they need to change to? Based on the set of proposals that this more technical group will look at, what are additional policy requirements that may need to be added that we don't see there? So I think it will be very important to keep that attached at the hip, for lack of a better phrase, in terms of progressing the work and getting to ultimate consensus recommendations that update or change the policy. Thank you.

ROGER CARNEY: Great, thanks, Berry. Okay, any other comments? Okay, I think we'll go ahead and move forward then with trying to pull together a small team. If you want to volunteer for that small team—and again as Sarah said it may not be possible in a week's time to begin with to get all that together—but if you want to volunteer for that small team, please let us know on the list here. You can raise your hand now, or you can email me directly. However you want to do that. You're looking to identify and work on this small group to provide…and as Berry mentioned, basically answering the questions to this whole document here.

[Jothan], I see that. Is the small team available to alternates? Good question. I don't see why not. Again, a small team just to be productive. So five, six people I think can be productive and should be able to provide the scenarios back. Okay, sounds like a good idea for allowing alternates as well. So, okay, again I would say let us know by the end of the week so we can schedule a time to meet up and get to work on that.

Keiron, please go ahead.

KEIRON TOBIN: Sorry if I'm just missing something. Do you want us to choose by the end of the week, or are you expecting us to meet by the end of the week? Sorry, I'm a little confused.

ROGER CARNEY: No. Yes, a good question. I want you to make the decision that you want to work on that small team by the end of the week. And the sooner the better, and we can get a call scheduled together with the group as soon as everybody volunteers. Again, you can volunteer now. Let us know in chat or let us know on the list that you want to be participating. Or you can email me directly if you want to.

Yes, Sarah, that is correct. So Sarah asked in chat, understand that the small team is consolidating all the input that we've had over the past few weeks and coming up with a proposal. And again as Berry mentioned, not just the charter questions but also taking into account the current policy and what would need to change or stay the same. So again, yes.

So we have a few volunteers. [Jothan], Volker, Jody. Again, just think about it. Let us know, and we'll try to get the group pulled together as soon as we can and get to talking about it. I assume it will take a few meetings for the small group to get it done, but good. Emily, please go ahead.

EMILY BARABAS: Thanks, Roger. So one possibility to think about is that given the conflict for next week's meeting on Tuesday and the fact that the small group might need some time to work, one possibility is that we cancel next week's meeting and use that time slot for the small group if the small group members do not feel that they need to attend the webinar. So that's just one possibility. We could, of course, talk about it offline and see what makes sense. Alternately, we could keep the meeting and schedule another one for the small team. So different options, and we're certainly available to assist with whatever makes the most sense. Thanks.

ROGER CARNEY: Yeah, Emily, thanks. I was thinking the same thing. We still haven't decided on meeting next week or not. I know Volker already has the preference of not meeting next week in lieu of him wanting to attend the SSAD webinar. So good transition, I think. Let's go ahead and talk about that and see what people think as far as meeting next week or not.

Just as a reminder, we won't be meeting in two weeks. So if we don't meet next week, that's going to be three weeks from now before we meet again. So just to give everybody that extra knowledge there so they can make the decision. Emily, please go ahead.

EMILY BARABAS: Sorry, old hand.

ROGER CARNEY: Okay, thank you. So Volker said that he would prefer not to meet next week so that he could attend the SSAD webinar. Anyone else have concerns about next week? About the conflict with the SSAD webinar? Owen as well. So Volker and Owen. Volker, please go ahead.

VOLKER GREIMANN: Yes, I think it's unfortunate that ICANN scheduled the SSAD webinar against us because they probably should have known that many people that worked on the SSAD plans and that are interested in its continuations would also be on the transfer PDP. So that's unfortunate. I don't think it necessarily means we can't meet next week. Just not at that time slot. But I agree that probably rescheduling might be difficult for many members. So with the availabilities being already limited, postponing by a week might be the only choice. I'd prefer to have both, but yeah.

ROGER CARNEY: Okay, thanks, Volker. And it looks like several people…yeah, exactly, Theo. It looks like several people are commenting that the SSAD is something they want to attend and participate in. So I think that we'll go ahead and plan to cancel next week's full working group session and, as Emily mentioned, maybe use that same time for the small group. But we'll see with that group, who is participating, if that makes sense or not anyway.

Jim, yes. So we'll be cancelling next week due to the SSAD. The following week on the 20th—Emily can keep me straight—the following week on the 20th is already canceled. I won't be around, so we've already canceled that one. So it would be the 27th would be the next one, next meeting for us. That would be our next meeting.

Okay, concerns from anybody on that? I mean, that will give the small team a couple weeks to come up with a scenario or multiple scenarios to provide to us that we can then review on the 27th, actually. Okay, I think that's the plan. We'll not meet for the next two weeks. Plan on reviewing small team when we get back together and continuing our discussions.

All right, with a whole extra two minutes left, I will turn it back over to staff.

JULIE BISLAND: Great, thank you, Roger. Thanks, everyone, for joining. This concludes today's call. You can disconnect your lines and have a good rest of your day.

ROGER CARNEY: Thanks, everybody.

[END OF TRANSCRIPT]