ICANN75 | AGM – Updates on the Root Zone Management System (RZMS) by IANA
Tuesday, September 20, 2022 – 10:30 to 12:00 KUL

MARILIA HIRANO: Hello and welcome to the Root Zone Management System Updates. My name is Marilia Hirano, and I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in the chat will be read out loud if put in the proper form, as noted in the chat.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will unmute in Zoom. On-site participants will use a physical microphone to speak and should leave their Zoom microphone disconnected.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for the session in the Zoom toolbar.

And with that, I will hand the floor over to Kim Davies.

KIM DAVIES: Thanks, Marilia. Welcome, everyone, to this session. We're really happy to be able to talk to you today about a project we've been

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

working on for a number of years. As you heard, my name is Kim Davies. With me, I have Amy Creamer. She is our Operations Director in IANA. As well as George Sarkisyan, who is a Senior IANA Specialist. Both Amy and George are part of our Project Team working on this system.

I also wanted to call out a colleague behind me, Simon Raveh. He is the ICANN Vice President of Engineering, and he's responsible for the team that develops the Root Zone Management System. So, let's see the next slide.

So for those that aren't familiar, the Root Zone Management System is a tool that we use, one of the fundamental tools we use to deliver the IANA Services to manage the DNS root zone. It's been in operation for over a decade. The current system has served us well, but we've been investing in improving the system in recent years to better cater for evolving and future needs.

I talked a little bit about this yesterday in another session, but the previous system was really showing its age. It was limited in the capability to evolve to our new requirements, so improving the system to better cater for that was essential.

Now, we've been working on this project for a number of years, but the first significant upgrade we intend to release into production is planned for later this year. And there are some changes for our customers, so we wanted today to preview those changes, discuss them, and also answer any questions that you might have. And also possibly stir up some thinking that you might have. And you can ask us questions later or set up a time with us to walk through those issues.

So the IANA Team, I just introduced. We're on site all this week, so if you do have questions or something specific to your TLD you want to discuss, we're happy to try and make time for you to do that. But if not, we can always meet up virtually at a later date. Next slide, please.

So just some brief history on root zone management. When ICANN was created, and indeed before ICANN had this role, when it was with the IANA Team under Jon Postel, root zone changes were essentially manually processed. There was e-mails going back and forth. But the fundamental business model involved printed out checklists and very old-school staff with would write notes on paper. But, you know, by the early 2000s, there was a recognition that that was not a scalable or indeed a desirable approach.

And at the same time both ICANN Org but also the TLD community recognized that there was a benefit to increased automation at the root zone. And this led to a number of different parallel activities to realize it in day-to-day operations. Next slide, please.

So in 2006, ICANN kicked off the implementation of a new Root Zone Management System. The purpose of this system, and indeed what it delivers today, is end-to-end management of the workflow of root zone changes. So that's capturing or receiving the submission of a change request from TLD through all of the different phases of processing that is done within the IANA Team and then transmittal to Verisign who plays an important role in disseminating updates to the Root Zone Operators.

And so this system resides that ICANN with the IANA Functions, but at the same time Verisign developed their own system to handle their component and the two systems are integrated. So the ICANN system speaks to the Verisign system, and that Verisign system was launched at the same time as the ICANN system.

The ICANN system itself is an iteration upon a Proof of Concept that was developed by the community I think, if memory serves, around 2003-2004. There was an initiative at CENTR, the European ccTLD organization, to explore/experiment with the concept of an automated root zone. And they commissioned NASK, the .pl registry to build that Proof of Concept. Once ICANN kicked off its project in 2006, NASK donated that source code to ICANN and, in fact, worked closely. NASK developers and ICANN developers work together to build the very first Version 1 of the ICANN Root Zone Management System.

And so it took a few years to build it out. I think, as someone involved at the time deeply, I'd say that there was a lot more complexity behind the scenes in implementing such a system than was perhaps evident in the community. So that Proof of Concept needed a lot of work to bring it to a level where it could be put into production. So the actual launch of RZMS was 2011, and it's been in place ever since.

So what does RZMS do today? All TLD managers can use it to perform common operations. They log into a self-service portal with a username and password. Common operations include submitting change requests, approving change requests, monitoring the progress of a change request. If the change request identifies an issue, they can go in and see what the issue is, and in other account maintenance tasks.

Also, it streamlined processing. Prior to RZMS, as I mentioned, it was all manual. And this even meant that, let's say, the technical tests that we do were performed manually by our staff. They did use tools to do this. They ran those tools, but they ran them manually. Today it's all automatically conducted. When a TLD manager submits a change request, the execution of the associated technical test is all done without any human intervention.

The system as deployed in 2011 is not the system we have deployed today because it's evolved with new requirements over time. What's happened since then? Well, we've signed the root zone, for one, in 2016 with the IANA Transition. NTIA, the U.S. government department who was indelibly involved in root zone management, their role was removed which changed business operations. And the system was updated accordingly.

When we did the new gTLD round in 2012, we've set up integrations with what is today the NSP portal so that TLD delegations from that program are neatly integrated into the system.

So today, many of the common operations are maintained within RZMS, but not all. Particularly complex tasks are still done out of [band], as in manually. The most obvious one is a ccTLD transfer. For those that are not familiar, when a ccTLD is transferred from one organization to another, there's a lot of due diligence performed that is analysis-style work. So in those instances, our team works with the applicant, with a ticketing system separate to this system. Next slide, please.

So why do we need to change what we have today? Our customers today, at least some of them—not all, but some—have usage patterns that just weren't imagined in the early 2000s and mid 2000s when we built this system. Remember, back then there was 320 TLDs. Most of them were ccTLDs with about 25 gTLDs. And with a few exceptions, each organization ran one TLD. That's not the case today.

So today, there are companies that run tens if not hundreds of TLDs, and our interface is not optimal for that use case. Further, with DNSSEC, it's a very common pattern that our customers do frequent key rollovers. Married with having a large portfolio, hose key rollovers can be quite complicated to coordinate with the IANA Functions.

Further, the technical architectural choices that went into the original design kind of limited the flexibility that the system had. So when we started to look at what we wanted in terms of future functionality, the software development team that Simon leads recommended that we essentially rebuild it from the ground up with a modular architecture that was better suited for evolving into the future. So in brief, the current system kind of reached its limit and we needed something designed with modern needs in mind.

At the same time, we had strong ideas about how to increase customer utility. Not just that the model didn't work for people with large portfolios, but there were other changes to the way customers worked. Again, in the early 2000s, whilst there were some registry operators, there was a lot of TLDs that were essentially operated by single people at that time. And that has clearly evolved as well. Next slide, please.

So with that, I'm going to hand over to my colleague, Amy, who will talk more about the new Root Zone Management System. Amy.

AMY CREAMER: There we go, okay. Thank you. So one of the feature upgrades that we're doing that we're most excited about is changes to the TLD authorization model. Currently, we're combining the public facing person with the approver, but we know that, logistically, this isn't always the same person for every TLD. So now we're going to be separating these two roles out. You can provide separate details for your public contact which would be going into WHOIS and RDAP, such as using a role account, if you'd like. And then you'll have your RZMS user who will be credentialed to enter change requests and approve it.

So your administrative contact and your technical contact will be retained as your public information only in WHOIS and RDAP. And your users will be tied to individuals not roles.

And we're going to see some increased flexibility. Part of the authorization model changes will now be allowing you to add more users versus just the administrative contact and technical contact who you're currently restricted to. So we're going to be giving you more flexibility to tailor your operational needs. And I'll be explaining in some of the future slides how you'll be able to just set up a configuration for each user’s privilege that you add to the system.

So with each new user added, IANA will be validating that it's associated with an individual, not a role account. This will limit password sharing, which can become an issue if you have an individual leave your organization. And then for password recovery purposes, we're going to be asking that each user please complete their profile information.

Also, currently, you receive an e-mail with a token in order to confirm a request. So you receive an e-mail. You click on a link. And that's how you approve the request. But now you'll still be receiving an e-mail, but it will give you a reminder to please log in directly to RZMS and approve the request through the system. We feel that this is a more secure method than having a lot of e-mails out there with links for requests approval.

So earlier I referred to giving you the ability to create a configuration for each user's privileges. and within RZMS we have kept categorized four request types which we're going to refer to as:

Change of control. And this is such changes as making changes to the registry operator. This would be like a transfer.

Non-technical changes such as changing public contact information.

Technical changes, adding or removing NS or DS records.

And then we have a category we're calling authorization policy. This is adding or removing users and changing approval thresholds, which I'll be discussing. So you're able to add these privileges to the user, one or all four, as you would like.

Then we combine this with the configuration setting for approval thresholds. So now you can determine how many users need to approve which type of change request by setting the threshold. So previously, you had just the administrative contact and the technical contact, and they had to both approve every change request.

Now you can select to have all users who are designated for that change type be required to approve it. You can select to have a majority of the users designated for that change type be required to approve it. That would mean 50%. Or you can select a preset number. So you can select one on up of how many users you want to approve that request before it moves forward. And let's take a look at an example that I think will help illustrate this.

So let's say you have five users that you've given permission to approve technical changes. So when you have a technical change requests submitted, the thresholds that you've set determine how many of those users must approve the request. So if you had set All, then all five of those users would need to approve it. If you had selected Majority, as soon as three of those users approve it, the request will move forward. And if you had selected Minimum, you would have had to have entered a number. So whichever number you've entered—which would have been some number between one and five, in this case—as soon as those number of users have approved it, it will move forward.

So besides the TLD authorization model, we do have some other features that we're releasing. Currently, you can only have one change request be active per TLD at the same time. Now, you may have multiple change requests be active per TLD as long as they are not overlapping. So you cannot have two change requests simultaneously trying to change, say, contact information for the administrative contact. But if you have one change request for contact information for the administrative contact, you can then enter a separate change request, maybe a technical change request. And that will be fine.

Currently, you can make multiple changes on a single request and you will be able to continue to do that. But now that we have the threshold levels in the user privilege categories, if you have a change request with different types of requests ...

So let's say, in my example, on one request you ask to change information on the administrative contact and you asked to add or drop a DS record, you're going to have to have the users who are privileged for technical contacts approve it, according to the threshold level you set, and the users who are approved for non-technical contact requests, approve it according to the threshold you set for non-technical requests before the entire request can move forward.

Another feature that we're going to be launching that you'll see is that you'll now see an activity log in this system. So this activity log will show which of your users submitted the request, which users approved the request at what date and time, when your technical checks were run. And you may see, if the technical check didn't pass, you may see it being rerun every six hours until it does pass. So you'll be able to track the different phases that your request goes through. It gives you more visibility into the history of your request.

We're also excited because we're making some changes to the technical check service. So first, you're going to see just a new visual for the technical checks. We put it into more of a report card looking format where you'll just seeing a pass or fail, but you can still click on it to dig down into the details of the technical checks. That's available now, but it's in a slightly different format that we think is more visually appealing.

But the real change that we're excited about is that we have separated the technical check process into its own independent infrastructure which will give us benefits of being able to scale the technical checks to increase throughput and optimize performance. And we can continue to evolve the technical checks.

This is a big topic for us, and we want to invite you to come to ... If you're at the ICANN DNS Symposium which is happening in Belgium in November, on that Thursday, the 17th of November, we have IANA Community Day. And we'll be having a session on the evolution of technical checks. If you're able to, we'd love to have you attend so that we can engage in a discussion with you about the future of technical checks and get your input.

Another new tool that we'll be introducing is an API. These are for TLD managers to build or use tools to [programmically] communicate with RZMS. Our initial feature focuses on bulk updates by registry operators who manage multiple TLDs—tens to even a hundred—and need to perform change operations efficiently. Kim mentioned this earlier in his slides about the history and evolution of RZMS, and this is definitely one of the reasons, for the large registry operators, why we've been doing this evolution.

And I'm now going to hand this off to my colleague, George Sarkisyan who is going to be doing a demo of this system. I think that if you see some of the features that I've talked about—the users, the thresholds, etc.—it will make a lot more sense when you see it in the system. So I'm going to be passing this off to you, George.

GEORGE SARKISYAN: Thank you, Amy. Hello, guys. Let me just share my screen so you guys can see. All right. So when you do log in, the first thing you'll see is the homepage, the dashboard. It may look similar to what you're used to now, but it's upgraded.

So I'm logged in as Amy. She's sitting right next to me, but for this purpose I'll be Amy. So the top section, you'll see the TLDs that you have access to. Just for the example we have three, but if you're a registry operator that manages 30, 40, up to 100, 200 TLDs, you'll see the first 20 up in this section. And then you'll see a link right underneath it that says View All Domains. You can go ahead and click on that to view the list of all of them. You'll also see a search option to search for a particular one that you're looking for.

Below that will be the change request section. Here you can filter if you want to look at open, closed, or all of your past requests and current requests, as well as searching for these as well if you want to look at a specific TLD request. Or if you already know the ticket number you can search that way.

Something new you'll see is that it summarizes what the change requests is as well as what state the request is in. So this will be helpful if you want to know that there's two requests that are pending contact confirmation. So there's an action to be taken there, as well as two requests that are in technical check remedy. So it definitely requires your attention there.

Having looked at this, I will just go ahead and jump in and start with submitting a change request. So you'll click on the TLD. The information here should be similar to what you're already used to. You have the registry operator followed by the public contacts. These will be your administrative and technical contacts. And then the technical information—the name servers, the delegation signer records, as well as the additional information which will have your servers and URLs.

You'll notice this over here for the name servers is grayed out. That's because there's an open request for that. And you can see that summarized right on the top. Here's the ticket number, and there's a request to add a name server. So you can't edit that section. But as you can see, all of the other sections are blue. You can click to modify and submit additional changes.

You'll also see that there's actually two tabs up top. The roots zone data that usually will go into the WHOIS record in the RDAP and now the [newly authorizer] section. Important to keep in mind that you don't have to submit separate requests because it's separate tabs. If you have changes for both, you can make the changes, save, and then complete the request in one ticket instead of multiple, if that's what you want to do.

So in this section, we will go ahead and add a user. And before I do that, you see that we have Kim and Amy as our users. And they are set to approve all types of requests. And this will carry over for everyone who is a credentialed user right now when we launched the new system. As well as the thresholds, it's set to All. So Kim and Amy will are set to approve all of the requests, and it's set that they both have to approve. We will start by adding a new user. This will be me. And let's just make me ... Okay.

And when you do add a new user, it does say that there isn't a record found. So that's a new user being added. If it is someone that already has an RZMS account, the message will say that this user already exists. So you're just giving them access to the TLD once the request is completed.

Important to note that the invitation that the new user gets has a link that's good for 72 hours. So we want the new user to set up their account as soon as possible. And the link is a one-time use, so if you do click on it and you decide you don't want to do it at the time, you want to come back to it, you're going to need a new e-mail with the new invitation link.

So let's go ahead and set up George. Let's just say I'm just going to approve non-technical requests and authorization policy requests, so I only have access to those two. And Kim and Amy want me ... Or maybe here. We'll do non-technical requests. We'll set this to one approver. And what this really just means is that there's three of them that can approve. And all three of the users for subsequent requests will get a notification that there's a request, but only one of us needs to approve. So whoever gets to the system first and approves that request. But it's not a race, guys.

And let's say for the authorization policy, even though all three people can approve, we just still want to. So you can make those changes and submit the request. If you have any other requests, you can definitely go ahead and submit them at this time before you finalize it. But you can see my name is highlighted as a new user, as well as the changes to the thresholds.

So we'll go ahead and finalize. It'll summarize here for you. I'll just move this so I can see that, and we'll proceed to launch it. Okay.

Now what happens if that new user, George, is on vacation and that ICANN72-hour period has passed and he didn't create his account? So what you can actually do is, as the TLD authorizer, go to the request ... Actually, let me go back to ... We've just launched campus. So we have George, here, invited. And if that ICANN72-hour period passes, it will actually say “expired.”

And if you do need to resend a new link, there's the option right here under the Actions tab. Click Resend. I'm already selected, and you can go ahead and resend me a new invitation link that will work. And if this did say “expired,” it'll go back to “invited.” Okay.

So next, I'll go ahead and show you the technical remedy screen so you guys are familiar with that as well. We'll take a look at this request. We're adding a name server. And you can actually see in the activity log, as Amy mentioned, that it shows the test results that we run every six hours until it's remedied or until the request expires. So if you have taken care of the issue ...

Well, first let's view it. There was a screenshot of this. Here's a closer look at all of the tests and what passed and what failed as well as ... If you want a full technical log of that, you can click this link and get a readout of that as well.

I'll go back one screen. And let's say it's all taken care of. You just want the request to pass now. You can go ahead and click Retest. And it is scheduled, so that will hopefully run and complete it. In this example, of course, it's still going to fail. So let's say it completed.

And then finally, of course, let's go ahead and actually approve a request. We haven't done that yet. We can use this example. In this example, we're just updating an administrative context. So this is just the public contact information, not the users. You can see in the authorizer section ...

Here's Amy and Kim. They have received their notification to login and confirm. I, as Amy, am already logged in, so I'll go ahead and confirm the request. And that'll be in the Action section as well. I can either withdraw if I need to make additional changes, or if maybe there's an error, or go to Go to Form to approve or reject.

So here's the summary of the changes again for one last review. You can either approve and submit or, let's say you don't agree. Go ahead and ... Wait, I’m sorry. And then if you need to reject it, go ahead and put a reason. It is required. And then go ahead and submit that. We won't do that. We'll just go with Approve.

Sorry. I didn’t mean to move the Zoom link around. There we go. If I scroll down, you can see I, as Amy, has approved the request. And we're still waiting for Kim, but he's a little busy at the moment. So there's that.

I think I'll stop there and turn it over. Back to you guys. Thank you.

AMY CREAMER: Thank you, George. Our goal with RZMS is one of continual improvement. So after this first upgrade, we will be doing future releases with improvements. And yesterday at the ccNSO Tech Day during the last block which was [inaudible], Kim Davies gave a talk on this system. Some of it overlapped, but he actually went into a lot more details that we did not cover today. So I would encourage you to listen to that recording if you're able to.

And the next set of future releases on TLD Manager, API, multi-factor authentication, and technical check warnings, he went into a little bit more detail than I'm going to go into here. But on the horizon, we're going to be making enhancements to the API including use of secure API token for authentication.

Multi-factor authentication has been talked about a lot, and we do recognize that it is not a one size fits all. I think Kim did an excellent job of discussing the future of that and how we're trying to navigate it.

And then for technical checks, right now you just have a pass or fail. And so we're going to be introducing a warning which will allow for certain technical checks that have been determined in advance for the TLD manager to review the information to determine, for those particular ones under the warning, if they would like to proceed with the request and move it forward on their own.

So that is the end of what we wanted to present to you. And now we're going to open it up for questions. And also, we would like to receive just general feedback/comments. Because this is a discussion with the community about where you would like to see RZMS go. Again, we're planning for constant incremental improvements so please, by all means, share your vision with us, too. Thank you.

KRUPA SHAH: Krupa Shah from Identity Digital, for the record. Thank you for sharing that. That was very helpful. I have a number of clarification questions. Can I just go one by one?

AMY CREAMER: Yes.

KRUPA SHAH: Okay. In terms of rollout, I believe you said you're rolling out some changes over the remainder of the year.

AMY CREAMER: We have one launch with the majority of what I showed you on the slides. And then in the future, we'll be rolling out some future incremental changes, which was the last slide.

KRUPA SHAH: Right. In terms of in terms of rollout, will there be some sort of a test or a UAT period where interested registries can participate and provide feedback?

AMY CREAMER: We're not doing a beta test with our users. We are doing [the rollout UAT] internally. But we decided not to do that.

I don't know if you want to elaborate. Is there anything you want to say about that?

KIM DAVIES: Yeah. As Amy noted, we don't have a plan for a customer focus testing period. I know it was the discussion within the team. I think some of the complexities around mirroring production data and so forth made it difficult. But we're happy to take feedback on the rollout. And if there's other things we can do to educate you, involve you ...

And indeed, I think our primary focus has been to sit down with key customers that use our system a lot—I think you're one of them—over the coming few months and set up time. I think we can work through your concerns, and if you have specific things in mind that drive this question, maybe we can come to some accommodation with you. Thanks.

AMY CREAMER: Thank you.

MARILIA HIRANO: Amy, Kim, are I would like to ... There have been questions in the chat, so once we are ... Do you still have questions? I'm sorry. I can’t see you.

AMY CREAMER: I think Krupa had an adjoining question.

KRUPA SHAH: Yeah, thank you. I'll make one last question and then we can chat afterwards. My understanding is that e-mail acknowledgments are not going to be accepted in the future. Right? It's all going to come in through the RZM, and if it comes through e-mail it's not going to be accepted anymore.

AMY CREAMER: You'll receive an e-mail asking you to sign into the system and do approvals directly to the system. Correct.

KRUPA SHAH: Right, okay. Got it. Thank you.

KIM DAVIES: I'll just add to that. If you're a credential user then, yes, you must log in with your credentials to submit your approval. We do have workflows outside of the system like, if it's a ccTLD transfer, the gaining party, if you will, is not a credentialed user. So there's some minor use cases where we will still use e-mail. But the current methodology where an e-mail is sent and you receive a unique token and you need to use that token to act upon it, that's going away. There'll be no more sharing tokens in e-mails.

KRUPA SHAH: Thank you.

MARILIA HIRANO: I'm going to read one question in the chat, and then I'll go back to the room if that's okay. Because they've asked a while ago. The question is from Dirk from the .eu. “Can you confirm that if you have five users defined, you could define a policy that only one user is needed to approve the change?” Shouldn't root zone changes have at least two pairs of eyes for any change to be approved from a security perspective?”

KIM DAVIES: So it's true that you can configure your TLD to just require one approval. Personally, I would not recommend it for that very reason. I think it'd be good practice, if not best practice that you have multiple reviewers. And indeed, if you have more than two, if you like, that's part of the flexibility we're granting you.

However, we have had requests in the past from TLD managers who just want one approval for certain kinds of change requests. So we're giving you the flexibility. How you use it is up to you. We're not mandating specifically two anymore. You can configure it in a way that meets your business needs.

GEORGE SARKISYAN: And if I can just add. Currently, you can have the same administrative and technical contact with the same e-mail. It's taking out that redundancy of that same e-mail confirming twice if it's still the one person confirming.

MARILIA HIRANO: And there's a follow up, also. Another question from Dirk on feature requests. “From a compliance view, it would be interesting to have an additional audit compliance role who receives all changes and/or can request a report of all changes." So it sounds more like a comment than a question. Dirk, if you want to comment or unmute yourself to be more specific on what the question is. Thank you.

AMY CREAMER: It sounds like a suggestion, so we'll take that down.

MARILIA HIRANO: The next person in the room that has a question? Yes, go ahead.

YUDHO SUCAHYO: Thank you. Yudho, chairman of pandi.id registry for the record. I have several questions. Number one, when are you going to implement this? Because currently, in PANDI we are updating our constitution, and some of the clauses essentially depends on how are you going to manage this [inaudible] context. That's question number one.

Question number two, other than this application and framework that is fantastic, is there any plan to have guidance or policy written that we can just simply follow or use as our guidance? Because what happens is that some of us may still refer to the old RFC 1591 which was actually published in 1991. And as you know, in some policies scattered then the Internet or on the IANA website, sometimes the use of sponsoring organizations or managers are still interchangeable. So it is better if there is one policy or one guidance that we can just follow, and we can say that this is what we are going to prefer.

Question number three. I still prefer that changing the admin and technical contact is still not [inaudible] delegation which requires so many rigid procedures asking for supporting letters from government and the communities. So is it still that changing the administrative and technical contact are adding credentialed users is simply the authority of the ccTLD managers? Thank you very much.

KIM DAVIES: Thank you for those questions. Let me hope I caught that all. So terms of your first question, when will this be launched? We're not sure of a precise date yet. What we're sharing today is that we expect it to be before the end of this year. I think in reality, we're looking towards late November, possibly early December. That's the kind of time frame we're working to.

We'd really hope to have an exact date to share with you this week, but we're not quite there in terms of our internal planning. But that’s the kind of time frame. And as soon as we do know the cutover date, there'll be announcements because there will be a period of cutting over. And for a short period of time, the service will be unavailable, etc. So we will be giving notifications when we're confident in the date.

In terms of the second question with respect to documentation, I think there's two parts to the answer there. I think it's fair to say that we have sparse documentation from IANA, and that's something we're seeking to improve. There's historical reasons why that's the case, but at this time there's no prohibition on us expanding the wealth of our documentation.

So I think in the context of the things that we can control, we’re looking to do that. We had a similar ask yesterday in a session. I think better user documentation for the Root Zone Management System is definitely something we'd see as desirable. Separate to that, as we evolve the technical checks we kind of touched upon, we expected the evolved set will have much more thorough documentation. Like for each check, exactly how we test it, how a TLD can remediate it, why we test it, things like that.

But you did mention RFC 5091, and I did want to respond to that. That is a community policy in effect, and that's not something we as staff have the authority to change or replace. So there is a bit of a fragmentation of the policies. The short answer is that that's in the purview of the ccNSO to evolve beyond the current status quo.

But I think as staff, again, we have an opportunity to perhaps wrangle some of those outside sources—RFC 5091, GAC principles, the Framework of Interpretation, etc.—and perhaps recast it in a user friendly sort of way that if you're an outsider to this community, you don't know the nuance of those different things that we can help you along there.

And then apologies. Your third question has escaped my mind. Can you repeat it?

YUDHO SUCAHYO: So is changing the admin and technical contact simply the authority of the ccTLD manager? Or is it like a delegation who requires rigid procedures, supporting letters, etc.? Thank you.

UNIDENTIFIED MALE: Yes. So, it depends. I mean normally a public point of contact change is straightforward and it's just a routine change. There's some nuance to our policy. The way we do it today is that there is a manual inspection of those kinds of changes. And in accordance with our implementation of the policies, if we have reason to believe that the contact changes are surreptitiously trying to change the TLD manager, then we will make further inquiries and possibly treat that as a transfer redelegation request.

Our basic objective is, if we think that there is a fundamental change of control happening by virtue of the change ... And to be clear, that's not just the context. Hypothetical, if we get a request where all of the name servers are being changed to a new operator and we have reason to believe that that is indirectly trying to move the TLD to a new manager, we're going to make further inquiries to understand the situation.

And if it crosses that threshold where we need to do due diligence to accord with the ccTLD policies, we will do that. So that's part of why there is still manual review for some of these changes, is to look for some of those aspects of the change and, if necessary, dig in.

But in the general case, if you're just changing a contact person, it should be relatively straightforward.

YUDHO SUCAHYO: Thanks, Kim.

MARILIA HIRANO: Okay. I'm going to go to Rick. He has his hands raised in the Zoom room. Rick, if you want to unmute yourself. I know you have questions in the chat, too. I don't know if you want to ask.

RICK WILHELM: Sure, thanks. Rick Wilhelm, PIR, for the record. So I came to the table after Krupa's question about the ... I guess, technically she was talking about a beta period or something like that. And I understand that you might not want to do a beta period on the initial rollout and stuff like that.

I would encourage you to—and offer—that, assuming that you're heading down the path of an API, you're going to need an OT&E environment for the API. When you get an OT&E environment, you're going to end up with needing the GUI attached to the OT&E environment, which is going to essentially be the same kit and context that you'll need to do a beta rollout.

And so that investment in infrastructure, process, set up to be able to set up an OT&E environment is coming. And so you it's your decision to do so. And I understand, having done innumerable rollouts over my career that beta feedback is both of ... They say you normally say, "Feedback is a gift" through gritted teeth as you're biting your tongue.

But from a from a technical and operational perspective, you're going to get there anyway because you're doing this API. And you're going to need a place to integrate everybody when you do releases this because now you're almost like a TLD operator where you've got an EPDP integration and in that sort of a thing.

So conceptually, you're kind of in that same spot. Even though it's not an EPDP integration, it's an API integration.

So I would just give that some thought. Now whether that timing works out for [4Q] rollout, I get it. And probably most people here would not trade the beta experience if it's going to cause a delay in the rollout. But I think for future versions, you're going to end up there anyway. Right? So I would just offer that.

I have a couple of other questions, but I'll stop there so you can comment on that one.

KIM DAVIES: Yeah. Just to acknowledge and agree. I mean, I'm a long-retired software developer, and I think it's essential, particularly with an API, to have a proving ground—I think I said as much yesterday—where our customers who want to use this integration can build that without touching the production system.

So I'm fully agreed. I’m sure we will get there. And as you said, it's just a matter of priorities in terms of ... I mean, the other thing that underlies this is that we do have a very small team running this project. It's taken us a while. So we’re sort of just picking our battles and choosing our priorities as we navigate forward. But I think we share a common vision for the end goal there.

RICK WILHELM: Yeah, understood. Understood and agreed, entirely. I get where you're kind of coming from.

I had a question in the chat about MFA, but that's more about when MFA comes. I was not quite apprehending that it's not there yet. I put another question in there about the approval page printing nicely, which is kind of a question but more like a suggestion. Because when you're doing browser stuff, as you know, getting stuff to print nicely is not a given. Right? You hit Print and it's like, “Oh, my God. What would that do?” So that's just something to think about because it can help you out with Dirk’s thing.

And then lastly, what are the password requirements, initially, since MFA isn't required? And then after MFA is required, I think the password requirements should are probably going to change. And so I’d just urge you to keep that in mind. Thank you.

KIM DAVIES: Thanks for those questions. I mean, to speak to the audit log concept, I think that's something we've discussed internally [inaudible]. We made some improvements in terms of what's logged, but I think the full vision is to have the ability to download comprehensive audit logs with a view to compliance. I mean, I think that's the nature of Dirk’s question. So I think we have a view to that, as well. Again, a matter of prioritization. But that certainly makes sense.

In terms of password complexity, we do enforce password complexity rules. Off the top my head, I can’t recall exactly what the logic is but it was informed by our [inaudible] audit. And so we adopted good practices there. Some users might recall that we reset passwords to enforce that a few years back.

But that continues to evolve. I mean, irrespective of multi-factor or not, we want to better adhere, moving forward, to industry best practices. So we'll continue to monitor risk, and if there's an opportunity to mitigate risk in RZMS, we will seek to do that.

MARILIA HIRANO: I'll go to the gentleman on the left here. He was raising his hand. Yes, go ahead.

KRISTIAN ØRMEN: Thank you, Kristian Ørmen from .se. First, a short question, and then probably a future request. Is it correctly understood that the users are just users with special rights for each action and they don't have an admin or tech role?

KIM DAVIES: So in the beginning during the migration, what we're doing is taking the existing admin and tech contact and essentially creating two users that map one-to-one to that. That's the starting point. That's the migration. But you're free to depart from that right away. So if you no longer want that configuration, you can create new users, delete those users, etc. So over time, they can continue to be correlated or they can be completely separate. It's really up to you. We give you that flexibility.

KRISTIAN ØRMEN: So as a future requests or idea is that you also put roles to the contacts because instead of just saying like a minimum two approvers, if you basically have two admin contacts and two tech contacts, it would be great to say, “I would like minimum one admin minimum and minimum one tech to approve a request.” Because then always have an overlap. If one admin contact is not present and one tech contact is not present. But to do that, you need to assign roles to the contacts as well, instead of just what they can approve.

KIM DAVIES: I think on that, definitely in the early design phase of this, we actually envisaged a much more elaborate and flexible authorization model with the potential not quite the same, but creating, like, groups of users. And you could label them how you like. If you wanted admin and tech [concepts], but you could have a management group or however you wanted to construct it.

But as we developed this, we realized it was too flexible and the UI was infinitely complex. So we scaled that back. And I think our thinking was, “Let's add some flexibility that we know will help for many of the use cases we've heard about, and over time we'll reassess.” So I think what we’d like to do is roll this out. If there's more flexibility needed or there's opportunities in the future, we can evaluate that and continue to evolve the concept. But that was kind of why we scaled back our ambition on that front.

MARILIA HIRANO: I have another question here in the chat, Kim, from Raymond at GoDaddy registry. "As a registry service provider with a large number of TLDs under management, we will need to guide and assist many of our clients through the process of setting up access and approvals. Will training sessions be provided? And then will IANA consider working with registry services providers and portfolio holders in setting up each TLD?"

AMY CREAMER: Do you want me to answer? I'll answer that. Hi, Raymond. Yes, we will be happy to work with you and provide any training sessions that you need and support you in whatever manner that you require. So we're flexible at meeting the requirements of each registry. And if that's what you need, we will set that up for you. Absolutely.

MARILIA HIRANO: Okay. Is there any question in the room? Okay, go ahead.

ASHLEY ROBERTS: Thank you. Ashley Roberts from Com Laude. It's a question on permissions. Say I'm one of the original users for a given TLD. If I then give a user permissions to make and approve technical changes, can that user then add or remove other users for that TLD and adjust their permission? I'm trying to get a grip of how these permissions work.

KIM DAVIES: In short, no. There was the four categories in one of the slides. I think Amy's pulling it up now. To add and create users, you must have the authorization policy entitlement. So if you give them the technical entitlement, they can only change NS/DS records. And I think WHOIS and RDAP as well. Is that ...

AMY CREAMER: Yes.

KIM DAVIES: Yes. So those four fields. But they cannot add or remove users.

ASHLEY ROBERTS: Right. Thank you.

[EDUARDO DUARTE]: [Eduardo] from .pt registry. Yesterday on the presentation, you talked that you are going to change all glue records, or change in the database. Do you have any other glue records for the TLDs?

KIM DAVIES: Sorry, I'm not ... What kind of records? Sorry?

[EDUARDO DUARTE]: The glue records.

KIM DAVIES: Oh, the glue records. Okay. Yes, we're changing our operational practice there. So the current operational practice is that glue records ... Which, for everyone's benefit, is when one name server is shared by multiple TLDs. Our current practice is that when there is an IP re-numbering event—changing the IPv4 or IPv6 address for that host name—we require every single TLD that relies upon that name server to consent.

Historically, if we go back some years, I know ns.ripe.net was used by something like 60 or 70 TLDs. So if that changed, there was a big effort to get all 70 TLDs to agree. This is less common today, but nonetheless we recognize an opportunity to streamline that. So our new approach is that when we receive a shared glue change, only the submitting TLD needs to consent, much like a regular change that only impacts themselves.

But then all of the other TLDs are notified of this pending change request and we give them an opportunity to object. And essentially, if any of the TLDs object then we will explore the situation more and seek to understand what the objection is.

Truth is, it would be highly unusual for a TLD to object to a glue record change which already is part of our technical checks. It's already changes being made, but the authoritative A and AAAA records for that host have already been changed and we're merely seeking to reflect that in the root zone. So it's a safeguard to allow them to object in case there's some issue that we're not aware of, but we're not expecting that to be a normal thing that happens. I don't know if that answers your question.

[EDUARDO DUARTE]: The question is, if the change in the root zone only goes ahead after the das that they have to object ...

KIM DAVIES: Correct.

[EDUARDO DUARTE]: There is no way to expedite that process? So ...

KIM DAVIES: I mean, there's a hack way to expedite it which is to rename the host. I'm trying to recall the conversations. I mean, we could have retained the current methodology and done both, but I think for simplicity this is the new approach that we've taken. I mean, is there a particular use case you have in mind where you think that this will [inaudible]?

[EDUARDO DUARTE]: No. I thought to said that it's 15 days to object. So if I made the change and only after 15 days, she will be visible on the root zone.

KIM DAVIES: Only if it's shared glue.

[EDUARDO DUARTE]: Yeah, if it's shared.

KIM DAVIES: If it's not shared, then it will go straight forward.

[EDUARDO DUARTE]: Okay.

KIM DAVIES: Again, shared glue is much less common today than it has been in the past. I wouldn't quite call it a corner case, but it's relatively rare.

MARILIA HIRANO: Let me go back to the chat here. Question from John [inaudible]. Is it already on production? Can we use it now?"

AMY CREAMER: No. We're going to be launching it late this year, we think late November. And all of our TLD managers and any user within RZMS will be receiving plenty of communication from us about that. So don't worry. It won't be a surprise.

And I see that there already is a question about, "Is there a dedicated website to this?" We do have some FAQs out and we'll be building out a dedicated website about the upgrade. And we'll be advertising that in the e-mails out to you as we add more documents to that in the user documentation.

We know that the community requires that. We're working on getting that written and establishing that as well. So there will be a website where you can access it, and plenty of e-mails with links to that will be going out to everybody directly. Thank you.

MARILIA HIRANO: Okay, thank you. And that was the question by Dirk in the chat that Amy just answered. Are there any other questions in the room before I move to the next question in the chat? If not, I'm going to read this question. It's from Rohan Durrant of GoDaddy. "Was it mentioned that there is an API available or coming, in particular to assist with more automated submission of DS record updates (remove cut and paste errors)?"

KIM DAVIES: I think, to answer that, yes. An API is coming, and I think that use case is probably Use Case #1. I mean, that is the perfect application of an API where we know some registry service providers basically have a list of DS records that they wish to switch to pre-populated in CSV or some other structured form. And we expect to provide sample code and illustrative examples of how to exactly plug that in so that a bulk update of DS records with RZMS is possible. Thanks.

MARILIA HIRANO: There are no more questions in the chat. No hands raised. Anybody else in the room? No.

GEORGE SARKISYAN: Maybe I can just add a little bit of clarification since we talked about the use of the token. So the authorizers don't use that. But if you are updating the public contacts, the e-mail change for a public contact, they will receive a notice that that e-mail will not be listed in the public record. And we just ask that they use that token to acknowledge that they're okay with that e-mail being used in the public record. So that will be done via token, but it's only for the public contacts to publish that e-mail. But that's it.

KIM DAVIES: Thanks for the clarification, George. Well, I guess with no more questions, that kind of brings this session to a close. But, again, our team is on site. We're happy to sit down one on one with customers who wish to discuss it in more depth, particularly for your individual use cases. And beyond that, if we can talk to your teams on Zoom or whatever down the road, answer any e-mail questions that you have, and so forth.

But also, Amy implored you to provide us advice on further evolution of this. We think we've hit the key pain points that we know from customers, but we hope to continue to evolve this service to better meet needs into the future. So whatever you can do to share with us what you'd like to see will be very helpful in informing us for those future plans. With that, thank you for attending. The session is closed.

MARILIA HIRANO: You can stop the recording. Thank you.

[END OF TRANSCRIPTION]