YEŞIM SAĞLAM: Good morning, good afternoon, and good evening to everyone. Welcome to the At-Large Consolidated Policy Working Group Call taking place on the Wednesday the 1st of June 2022 at 13:00 UTC.

We will not be doing the roll call due to the increased number of attendees, as well as for the sake of time. However, all attendees both on the Zoom room and on the phone bridge will be recorded after the call.

Just to cover our apologies, we have received apologies from Marita Moll, Christopher Wilkinson, Vanda Scartezini, Holly Raiche, Mouloud Khelif, Judith Hellerstein, and from Roberto Gaetano.

Before we get started, just a kind reminder to please state to your name for the transcription purposes because it's the ICANN74 Prep Week. We do not have interpretation provided for this call, unfortunately.

And with all these reminders, I think I'm good to leave the floor back over to Alan. Thanks so much.

ALAN GREENBERG: Thank you very much, Yeşim. This is a rather different meeting than normal. First of all, without interpretation. It's only an hour long. And the bulk of the meeting will be taken up with a presentation on a rather interesting potential SSAD implementation. We have one short report prior to that from Steinar on, I presume, the Transfer Policy, but I'm not sure. And Steinar, why don't we go to you first? And then we'll go back to Mike Palage.

STEINAR GRØTTERØD: Yeah. Hi. A very short update on the Transfer Policy Review PDP. There was no meeting yesterday. We all were free to join the Prep Week. There was a presentation by [inaudible], the chair of the group on the GNSO Policy Update. And the essence here is that we plan to initiate the initial report for Phase 1A for public comment on June 20 this year.

And this phase-in includes recommendation on form authorization, Auth-Codes, denial of transfer, and additional security measurements. And they will be some sessions at the ICANN74, and they will be another work group meeting next week in front of the ICANN74. So next week, hopefully ICANN come back to more details or we'll see each other in the Hague. That's all. Thank you.

ALAN GREENBERG: And thank you very much for that brief comment. Mike, are you ready to take it over?

MICHAEL PALAGE: I am, Alan. Thank you. If we can just make Frank the presenter, he will share the deck. And this deck will be provided to ALAC, be uploaded on the Wiki after the call.

YEŞIM SAĞLAM: Frank, you have co-host rights now.

FRANK CONA: Great.

YEŞIM SAĞLAM: And I'm going to stop sharing so you can share your screen, please.

FRANK CONA: Excellent. Thank you. And you guys can hear me okay?

MICHAEL PALAGE: Correct.

YEŞIM SAĞLAM: Yes, we do. And we can see your screen. Thanks so much.

FRANK CONA: Excellent. And I'm going to hide the controls here.

MICHAEL PALAGE: So first, as Frank's doing that, we just want to thank everyone for allowing us to present today to ALAC on what we think is a potential SSAD option or solution to the current quandary that ICANN find itself into.

Joining me on today's call as part of the Info Networks Team is myself, Mike Palage, Frank Cona, and Tim Mesker. We are also joined today by Tomofumi Okuboto from DigiCert and Brian King from Clarivate.

Unfortunately, there were apologies from Mark SV from Microsoft. And with that, Frank, if you could go to the next slide.

Just a little bit of background here. What you see here today is actually kind of a culmination of approximately four years' worth of work as we have tried to undertake a holistic approach to addressing the RDDS problem. Three of the companies that had been working on this solution—Info Networks, Microsoft, and DigiCert—all three companies actually submitted RFIs to ICANN as part of the SSAD RFI last year.

And it was a result of that process afterwards where we sort of came together and decided to go, if you will, old school ICANN multistakeholder in our approach, and try to sit there to work together to come up with a solution. I think we went public with this public SSAD Sandbox at ICANN73. Since then we have welcomed Clarivate, and we've integrated with them. And hopefully within the next couple of weeks, we'll be able to announce additional people that are joining the coalition.

So one other important thing here is that this solution, the Sandbox solution that you see here, was originally based upon a solution that Info Networks had built for .music. So, .music is a community TLD. They will be launching, we believe, later this year. And as a result of their community obligations, there were certain requirements that they needed to build into the registry operation—Trusted Notifier, takedown mechanisms, verified registrants.

So based upon that code that we were working with, we decided to expand and turn this into a full SSAD Sandbox. What you will be seeing

here today when Frank runs through the demo is a full ecosystem. We're actually running a full version of FRED. That is the open source registry that is was written by cz.nic and is run by nine other ccTLD operators. There are multiple registrars and, as I said, we have the integration with Microsoft Authenticator, with Clarivate, as well as with DigiCert.

Because .music is a [separate]-based company, we submitted a very detailed Data Privacy Impact Assessment. We've received verbal non-objection to move forward. And right now, as we are considering other partners joining the coalition, it is our intention to actually submit a revised Data Privacy Impact Assessment to additional Data Protection Authorities.

And one of the things that we are hoping to do here is to show the broader ICANN community that there perhaps is a path to move forward on the original recommendations that were approved in EPDP Phase 2. Next slide, Frank.

So not be intimidated by that very detailed graphic on the right-hand portion of your screen. Again, these slides will be made available after the call, and you can go through and read through them in more detail. The key point here ...

And for those that may be involved in OpenIDConnect or OWA, this kind of represents a modified IDP in which there are relying parties and issuing parties. But the key thing that I really want to stress here, and I think it will be ... They say, a picture's worth 1000 words. We think a demo is probably worth 10,000. So what I really want to focus on here is

that the way that we have designed this, the key is about verified credentials.

And for .music, not only did there have to be verified credentials for the registrants, but for purposes of SSAD, there are the verified credentials of the requesters. And the reason that that, obviously, is very important is we do not want to be giving access to PII to non-vetted parties. One of the things that is also very important here—and this was one of the things that was vetted with the Cypriot DPA—is a rather established governance framework. And we'll get to that in one of the next slides.

And one of the things that we have done here and I think was key in the original envisionment of the SSAD was to provide predictability. That's what everyone's looking for here. Not only the contracting parties, but also the requesters. So what was part of our Data Privacy Impact Assessment was very detailed templates that set forth a number of criteria that hopefully would provide a predictable basis to automate if the contracting parties so choose. Frank, can you go to the next slide, please.

So one of the other things that we'll be walking through here today is the actual requestor accreditation. And as Alan may know, or others that have read the SSAD report, the accreditation is something that ICANN really struggled with, and it's one of the reasons why Info Networks, DigiCert, and Microsoft really focused on this aspect of the approach. And one of the things that you'll do and what you will see here is that we have come up with a number of implementations. There's a web base. There's an API. We've done an integration with Microsoft Authenticator.

So what has been very key is providing flexibility and modularity to the overall system design. So as you can see on the left-hand side, we are looking to work with a number of third-party verification services. Clarivate, as you will see, will be providing the verification of the underlying trademark rights of the SSAD requesters. In the case of .music, they will be using Shufti Pro to do the identity proofing of their .music registrants.

So again, we want to sit there, and we view this as a marketplace where there should be the opportunity for a number of parties to participate. Franks, thanks.

So going to the governance slide here, what you see here—and this is part of the modular approach—we designed this to be very modular. So, much like the Internet is a network of networks, we have designed these identity ecosystems to be spun up one at a time. So while we are doing this first with .music, there is the potential to roll this out in other ecosystems.

The other thing that is really important to note here, particularly when it comes to registrant verification, that can be an option. So for those TLDs that do not have a registrant verification, unlike a .bank or a .music or a .pharmacy, you can have that. It's an option.

And the other thing that we have really focused on here is how to allow this to be phased in over a period of time. So this is not a Thanos, snap-of-the-minute, all registrants are going to become verified. We haven't done that. But we do recognize in light of NIS 2 and other potential legislative initiatives that the landscape and legal obligations of

registration authorities are going to be changing. And again, the key here is to focus on policies and predictable due process rules.

One thing that you will see here is that in the governing body or, if you will, the network, we've approached this like the traditional credit card processing network, like a Visa or MasterCard, where we are focused on moving that tokenized data. We are not involved in the merchant banking or anything like that. We allow that PII to sit in those respective data sources. And what we are doing is just providing a trusted network to move and, should there be a conflict or an issue where someone needs to be, if you will, identified providing a predictable means.

One of the other things that was very key in the Data Privacy Impact Assessment that we submitted to the Cypriot DPA was this concept of a dispute resolution mechanism so that if a data subject felt that there was an inappropriate disclosure, there was a mechanism for that individual subject to challenge that. So again, this is all part of a really detailed governance framework. But in the interest of time, if I could go to the next slide, please, Frank.

So here is an example of one of these rules templates, and the idea of these templates were to provide the contracting parties with predictability.

And in building out these templates, there were basically three accesses that we were looking at from a data point. One was what were the attributes of the requestor? Was this a trademark attorney? Law enforcement? So, who was the person asking for the data? The next

was the request attributes. Was this in connection with fraud? Litigation?

And the final access that we looked at was the data attributes. What specific data elements were they asking for? And by combining these three sets of variables together, we put forth a way that the DPA would be able to say, “Yes. In this scenario, this would be an appropriate balancing test for disclosure of the data.”

As I mentioned and as Frank will show in the demo, the system can either be done in an auto or manual process. So in talking with registrars, there were a number of registrars. The original alpha. Not even the Alpha. If you will, beta. The original design was to automatically have the default to be disclosure, but the registrars were like, “No. We want the default to be manual. And only after we gain confidence with the system do we want to sit there and elect to automate the processing.”

So again, very detailed and really provides the ability for the registrar or the IDP to make the appropriate determinations of whether or not that data will be disclosed. Next slide, Frank.

So what we have done here ... And this is why we're trying to educate the broader ICANN community, particularly in light of some of the small team Phase 2 deliberations that are going on right now. As some may be aware from some of the previous ALAC briefings, there have been discussions of a pilot, perhaps a scaled-down ticketing system. And what we wanted to do here is just show the community what a group of

companies have done and just have that entered into the overall equation.

Next slide, Frank. And I think we're going to be turning it over to you real quick.

So the key benefits here, and I'll keep this real high level. This is all about enhancing privacy. Not only does this solution, do we think, scale and address the concerns of the GDPR. We actually believe that this would be suitable for those countries with even more stringent data localization requirements.

We believe that this lowers the cost for both registries and registrars that choose to implement this, and perhaps most importantly for them, also lowers their risk because it really is minimizing the data and providing a level of predictability that has been vetted with appropriate Data Protection Authorities. Next slide.

So the demo today that Frank's going to walk you through is literally the cradle-to-grave, if you will, of this ecosystem. We'll start off with how a domain name would be registered, then how a third party would go about requesting access to the underlying WHOIS information. We also will just touch upon the ...

I know Trusted Notifier has been a concept that has been discussed within the community, particularly within Europe. So we are going to show you how we have implemented Trusted Notifier for purposes of .music and their original community obligations. And we also want to show how these credentials have the ability to be ported into multiple DNS abuse complaint providers.

And finally, we will walk through how an SSAD requestor would be credentialed and onboarded. So with that, I'm going to turn this over to Frank. You have the floor.

FRANK CONA: Thank you, Mike. Let me close out of here. So on my screen here, as Mike mentioned, our Sandbox is the complete domain name ecosystem, obviously including this SSAD solution as well.

So on the left-hand side of my screen, you have a one of our test phones which is hopefully visible to everybody. On the right I have a number of windows open for various aspects of the system. So what we'll do, as Mike noted, we'll start with the registration process. So you can see here on the right is one of our registrars that we have in the test system. And if I'm a registrant, I have my credentials.

Now again, as Mike mentioned, we have a verified registrant approach here, as well, that we did for .music and obviously can carry over as registrant verification—incentivized or mandated or whatever the rules are—come into play. But the SSAD aspect of this can work independently of that as well for accredited requesters.

But if you have a domain name such as .music that requires the use of verified credentials, the process could be very similar to what you do today. I'll do alacdemo.music to see if that name is available. Surprisingly, it is available. I'm going to add that to my cart, go to purchase that name. Now because the .music domains require the use of verified credentials, what I'm going to do is present the credentials that I have in my credential manager over here on the left.

So I'm going to select that credential. I'm going to click Present. I'm going to scan this QR code. And by doing that, the relying party here—in this case, the registrar—is connected to my identity provider, this MyIdP, in my credential manager in order to prompt me to consent to send, in this case, proxy data. Because what we're doing for .music is providing domains registered using proxy data. So the credentials are verified, but you can register the domain names pseudonymously. Right?

So if I go into this particular credential itself, all of my actual registrant data is stored with my IDP in an escrow. Right? So my name, all of my contact information, etc. But when I actually register the domain name, what my identity service provides from this credential is actually the pseudonymized data.

So if I go to alacdemo and I pull up what we call enhanced RDDS, you can see there's general registration data for that domain. And then there's enhanced data regarding verified registrant. And this is part of what we did specifically for .music.

But what it illustrates here is that the domain names could be registered pseudonymously but using verified credentials where the data is stored with the identity service. And what can be placed into the registry and available for WHOIS is the information about the verification, the level of [inaudible] to which the person was verified identity wise, who the identity provider is, what trust framework was used, etc. Right?

And in the network, the trusted credential network, what we maintain is a ledger of those registrations. And you can see that there's a

transaction-specific identifier that's used in the ledger to represent that transaction. Even though these registrations, for example, may have been registered by the same registrant with the same credential, each one has a unique transaction identifier, so they cannot be inherently correlated.

But this does come into play for SSAD requests. So if even if the domain name has been registered using this proxy data—and this identity provider framework is akin to a privacy proxy service with certain changes under the governance model—this can be used when there isn't an SSAD request for providing access to that data under the due process rules that Mike had had mentioned previously.

So if I come back here for a moment and I pull up this site, if I assume now ... Now I'm going to demonstrate the SSAD process. This a live site. It's live at the third level—fourth level, technically. And so if I find this site ... Let's assume I think this is infringing on my intellectual property, for example, and so I want to submit an SSAD request to find out who owns this particular domain name.

So I'm going to come to the request gateway. This request gateway can be hosted by ICANN if it's a centralized model. This could also be hosted by registrars or registries. Under the approach it's not particularly limited because the request will get routed to the appropriate party who has to make the determination. If that's a registrar, for example, or a registry, or if it's an identity service.

SÉBASTIEN BACHOLLET: Be calm. You are in an international setup. You are not in a U.S. or English-speaking only people here. You are talking about things who are new for us in a language which is not our mother language. Please take care of us.

FRANK CONA: Thank you. I will try to speak more slowly. I appreciate that. I have a tendency to speak quickly. So to repeat, then, what I was saying. On the right here is the request gateway. And this can be hosted by ICANN. This could be hosted by a registrar or a registry. It's not limited because the system can send the request to the appropriate party to determine whether to release that data.

So in our example, that appropriate party would be this identity provider who is holding the actual registrant data because the domain name was registered using a pseudonymized credential. But the registrant data is actually held by the identity service which is akin to a privacy proxy service that exists today except that it's subject to the governance framework that we've created for this approach.

So now as a requestor, I wish to submit an SSAD request. You can see on the gateway we have a process for domain abuse, for SSAD, and separately for Trusted Notifier. But we've also included that with the SSAD process as well.

So if I click on SSAD, I have a choice now to submit a request based on intellectual property, law enforcement. And we can add other categories as well. And we've outlined a number of these in our Data Privacy Impact Assessment. I'm going to choose intellectual property

here. And similar to before, as the requestor who wishes the disclosure under SSAD, I need to present my accredited credentials to the system.

So for this example, I'm going to use a version of the credential that we have in Microsoft Authenticator. So when I registered the domain name, I used our reference implementation of the identity provider wallet. But here I'm going to go into Authenticator where you see I have a credential for SSAD that has been issued by DigiCert. And then all my relevant information, similar to the other one, is included in this credential as well.

So now what I'm going to do is scan the QR code as I did before. And now it's prompting me to provide my relevant data. And again, the network is able to connect the request gateway with the credential service. I'm going to choose the IP rights that I wish to assert. And here it also provides certain information about me to the gateway, and I'm going to click Consent to send that information. Oh, I can't see. Hold on. This is not going.

MICHAEL PALAGE: Frank, is it because you use the camera in Authenticator instead of the ...?

FRANK CONA: I'm not sure. Let me try it again. It might be Authenticator, so what I'll do is use the relevant one from our credential manager. Just refresh this for sure. Sometimes there are glitches with the Authenticator network.

So, similar process, though. I'm going to present that credential. Just as I was doing before, I'm going to select the IP that I wish to assert. And you can see now that it logged me into the system and it provided my verified requestor information from my credential.

And if you remember from what Mike was showing under the rule templates, we make the rule decisions based on the attributes relevant to the requestor—who the requestor is, the nature of the request, and then attributes of the data itself, the registrant data. Is it personal information? Is it commercial or business information? Is it a natural person? Is it a legal person? Etc.

So here, you can see all of my credential information that was provided. Here I'm going to choose the relevant policy-based reasons for the request. And obviously, I'm just picking these at random for purposes of this. I can also upload any relevant evidence such as a subpoena or a court order.

The domain name that I'm interested in is alacdemo.music. In this case I'm going to choose the registrant name, phone, and e-mail. But obviously we can designate particular attributes/data elements that can be requested, and the rules can be applied to each of these attributes and elements individually. And I'll show you that in a minute. I will also just request suspension of this domain, similar to the Trusted Notifier program as well.

And as Mike alluded to, all of these requests are subject to the governance framework that he touched on, including a code of conduct

as well as the dispute resolution policies to which all of these requests and the requestor credentials are subject.

So then I'm going to submit that request. Now that request, as I mentioned before, that request was sent to the identity provider who has to make the decision whether to disclose the registrant data. So now I'm going to switch over to a dashboard for the party that is reviewing the requests that came in. In this case it's a privacy proxy or identity service as well. I just have to log back in.

So now you can see on this dashboard ... And this just represents a generic reference [implementation] of a ticketing system or a dashboard or a delivery where the request would go so that that identity provider can review it manually and make that request. So if I pull up Review Request, you can see ... All of the information about me as a requestor is here. All of the request details are here. And importantly, there are a number of reports here.

So Mike mentioned the rule templates, and I was saying before that they consider all of these attributes. And I'll pull up an example of one. So for the registrant name, in this example there are four templates to decide whether the nature of the requestor, the request, and the data that's being requested fit a category where there's a legitimate interest for disclosure

Under Template 1, you can see that the legal right is a sufficient legal right. The specific lawful purpose was sufficient. There was no evidentiary support provided. Etc. And these are all criteria. We also do

a comparison of the trademark. In this case, obviously very different from the one that I registered.

So those reports can be used to either provide an automated review and disclosure, as Mike mentioned, or obviously they can assist a party who has to manually make that decision. So a big part of what we are proposing as part of a pilot is to vet, is to consider a number of situations where there may be a legitimate interest and establish rules and these templates for those situations so that we can build some consistency, as also reduce the risk of liability for a disclosure because there's an established legitimate interest and lawful basis for making that disclosure. And then that's all wrapped into the governance process where there's also a dispute resolution mechanism for the data subjects as well.

So in this case, though, first I'm going to agree to suspend the domain. And I'll show you that. So if I come back to here and I refresh this page, now you can see that the page has been suspended. It's no longer live, and there's a notice that it was taken down due to an intellectual property-based Trusted Notifier request.

If I come back here to this, I also want to approve the release of that data. So now as the identity service who's holding the registrar data ... Like I said, that could be a registrar. That could be a privacy proxy service. I've now agreed or approved the release of the requested information to that requestor.

And so now as the requestor, if I come back, you can see that I now have an e-mail that says I have a new SSAD request. And then I have

one that it's been approved. I'm going to click here to access that report. And you can see it's for the ALAC demo domain name. And here is the registrant name, all of the information that I requested.

Now we provided this output via this authenticated link to a web page. We could also provide that output in any format. It could be in a spreadsheet. It could be in a watermark PDF or other document. The system isn't particularly limited.

So that illustrates the request process, the registration process, the SSAD request process, and Trusted Notifier.

The last part of the system that we wanted to illustrate for the demo is the actual accreditation process for a requestor. So if I come back here—

BRIAN KING: Hey, Frank?

FRANK CONA: Yes.

BRIAN KING: Before we jump into that, I just wanted to note that Hadia has her hand up in case it's related to your previous point before we move on from it. If you don't mind.

FRANK CONA: Sure, yes. Absolutely. I'd be happy to answer a question if there's a question.

ALAN GREENBERG: Just to note, we have a little over 15 minutes left. Unfortunately, it's a very tight meeting today.

FRANK CONA: Understood. And I won't go through the entire actual accreditation process. We'll just take you through the high points. So now, if I go here ... If I can get this—

MICHAEL PALAGE: Frank. Are you going to take the question before?

FRANK CONA: Oh, was there ... I'm sorry. What was the question?

MICHAEL PALAGE: Hadia has her hand up. So, Hadia, do you do you want to go first? And then Lütz, I think you had a question in the chat, so perhaps you can go after Hadia.

HADIA ELMINIAWI: My question is in relation to the identity service provider. So, how do identity service providers participate to this or join this program? I do

understand that identity service providers get the registrants or registries. How do they become part of this? Thank you.

FRANK CONA: Yes. Under the governance framework that Mike had outlined earlier ... And that can be run, in the case of .music, they're running their own ecosystem that obviously can be done at the ICANN level as well. Right? There would be a set of accreditation agreements and requirements/ policies, similar again to what exists today for parties to become identity providers. And that's why I said it's akin to privacy proxy services, if you think about it in that vein.

Different registrars today have privacy proxy services. There could be independent privacy proxy services. The identity service is very similar. They would be accredited under the governance framework to hold that registrant data, similar to the way a privacy proxy service does today. A significant difference being providing access and disclosure of that data if it meets the requirements for disclosure under the rule templates that we mentioned earlier.

MICHAEL PALAGE: And just to follow up on that, Hadia, right now I think there's generally an overall transformative thing taking place right now with postal operators, telco operators, banks getting into the identity space. So while we initially have viewed this focused specifically on registries and registrars, as the broader identity eco space matures, the ability to take verified credentials from other sources is one such possibility. So we view this as a much larger opportunity in this space.

And then I think, Lütz, you had a question regarding the QR code. Can you perhaps repeat that?

LÜTZ DONNERHACKE: No, I do not want to repeat the silly question. I have a different one. If I understand correctly, this is a wonderful framework for having [a list] of people who are able to take down domains, to have access to domains. So I have to [inaudible]. Which is the applicable local law which is in place here if the requestor comes from a different country than the domain owner or the authority who authorized the request?

And the second one. If I'm a domain owner, how do I protect from the censorship framework here? Thanks.

MICHAEL PALAGE: Sure. So let me take this. And Frank, maybe if you could go back to the request because one of the things was the jurisdiction from Point A to B.

FRANK CONA: Right.

MICHAEL PALAGE: So what happened here, Lütz, the importance here is in the registrant choosing who is their IDP because that IDP will be the trustee of determining whether that data gets disclosed or not. So, Frank was just showing you the rules. Frank, I'll let you explain it on the jurisdictional.

FRANK CONA: Right. So in terms of the data protection laws and data localization. Under this framework, my identity service could be in my home country. For example, even though the registration and the other data may be elsewhere, under the governance framework that Mike had shown earlier, we can layer in local policies that may apply to that identity provider in that country around data localization and disclosure as well as layering that in with any ICANN consensus policies or any policies for the registry in that TLD, etc.

So the data itself can be localized and stored by an identity service in country, and then any rules around cross-border transfers—and we had that behind this process—is a whole set of rules that take the attributes of the registrant and where their data is located, as well as the requestor who's making the request, and can determine if that cross-border transfer is allowed, for example.

And so jurisdiction can be taken into account, and data localization can be taken into account as both part of the technical setup where the data can be localized as well as part of the governance framework and the rules. It can be considered as part of that process.

MICHAEL PALAGE: So in this example, Lütz, you can see data transfer from U.S. to U.S. So it's not leaving the U.S. This is both a U.S. requestor and a U.S. registrant. And because of that, the rules engine has said, “That's green. That's acceptable.”

Now to your—

LÜTZ DONNERHACKE: Sorry. Do I understand correctly that an option to follow the local law?

[MICHAEL PALAGE]: No. It's not an option. You have to follow the law. Yeah. You have two lawyers, so—

LUTZ DONNERHACKE: [inaudible] which local law? I have my domain name and I choose [inaudible] the domain name. And if the registrar's an international one because he has to operate with some special top-level domains which is not accessible for a private, small company here—for instance, in Germany—that means that I depend on the identity providers which are chosen by the registrar not by reseller or not by myself because I'm the domain owner.

So what's the real advantage to store data outside of the registrar? If the data was stored at the registrar or at the reseller itself, none of these problems would exist.

MICHAEL PALAGE: So, just mindful of time, and we can discuss this afterwards, the registrant chooses their identity provider. The registrar doesn't choose it. The registry doesn't. It is the registrant that chooses who it wants to hold it data. So you as the registrant choose that, and that allows pseudonymized credential to be used cross-border in a trusted manner. And only if there is an issue where your disclosure needs to be

unmasked does someone then come back to your IDP. Assuming, obviously, that privacy is very important, you would most likely choose a German IDP that would then be determining how your data would be disclosed.

And then just one ... I will answer your other question regarding how is a registrant protected. You'll recall that we specifically have a challenge mechanism so that if you do believe that the data has been in improperly closed, you can challenge it.

Also as part of the Data Privacy Impact Assessment, we recognize that some requesters that may be dealing in large-volume transactions may in fact be required to post a financial instrument in the case of a breach. So these were all part of the detailed analysis that we set forth in the Data Privacy Impact Assessment to protect registrants.

So Frank, with that I'm going to turn it over to you to perhaps run through the ... If you could run through the request or onboarding just briefly because I do want to show the integration with Clarivate and their trademark data, if possible.

FRANK CONA: Sure, absolutely. And so now, here, I'm at a reference dashboard for DigiCert in this example. If you remember when I showed you the credential in our system, it was actually issued by DigiCert. If we assume for a minute I did not have this credential, there are two ways I can get a credential.

There is a bulk invite process that we can use where an organization can request accreditation and provide information to be verified in bulk and send out those invites to people. And then there's a manual, individual process as well, if I wanted to apply.

So for example, if I wanted to just add this credential, there's a various set of applications. If I went into the requestor one, you can see that it requests information about me, about my identity, how I want to do that. We're providing both manual, and we're also working towards some of the automated identity proofing solutions as well, such as the work that's being done with mobile driver's license and others.

But if I want to manually provide my info—and I won't walk through the whole process—but then I would provide, obviously, my information. I would then provide proof of my identity. And that information would get submitted as well. If I wanted to do e-mail verification, I could put in my e-mail, my IDP, and click Verify. And you can see it's pending.

And just very quickly, if I go here to my requestor e-mail account, you can see there's a verification request. And I click to verify that e-mail. And then my e-mail it's verified. I could do the same thing with my phone. In the interest of time, I won't do that now.

As Mike had mentioned, in addition to am I a legal professional, I could provide proof of the fact that I'm an attorney because that could be one of the criteria for requestors that's considered. In regard to IP rights, similar process. There are different ways that we're providing to actually validate your IP rights. One of them is working with Clarivate, as Mike mentioned.

So if I click Clarivate and I continue, I can now import those rights. I want to import my trademarks. It now links me with Clarivate. This is some of our demo registration data that I'm now going to import. And those are the ones that you saw that I used when I actually did the SSAD request. All of that registration data gets important. And again, I can provide a manual proof of my right as, for example, attorney of record, or whatever, or use an automated process that will work as well.

And if I represent a particular organization, I can go through that same whole process. And I would provide that information and submit the application which, in the interest of time, I won't do. But I will show you one of the prior requests.

So when I submit that, it would come here and, obviously, all of the information can get reviewed by DigiCert in this example. And then they can approve the credential for issuance. And that credential would then be provided to the user in their credential manager. That could be a credential manager for my identity provider. As Mike said, I may have the ability to choose my identity provider as a registrant or a requestor. Or I could store them in Authenticator, as I was showing you, with those credentials as well. The system isn't limited.

As Mike mentioned, we've tried very hard to be technology agnostic in approach. Really, our focus has been on that governance framework, making sure we protect the rights of data subjects while also trying to drive consistency in disclosure decisions and minimize the risk for making a disclosure if there is, in fact, a legitimate interest under those rules.

But that's the accreditation process. Again, it could be through automated verification or manual as well. And so I'm going to hit stop there because I know we're running short on time. And if there were any other questions or comments.

MICHAEL PALAGE: I see Siva and Brian have exchanged some there. But, yes. And just one other thanks. I also want to thank At-Large as well. I mentioned ALAC at the top, but At-Large as well since this is a combined meeting.

So Alan, hopefully this has provided you, as a small team member to this issue, some additional tools that are potentially out there. And as I said, in light of ongoing NIS 2 discussions and deliberations as we potentially move to a verified registrant world, these show you some of the tools that we think could help provide more security and stability to the Internet and the broader DNS infrastructure space.

So with that, back to you, Alan.

ALAN GREENBERG: Thank you very much. I do want to note that Michael offered to do this presentation, I guess, about a week and a half ago. And the last CPWG meeting on last Wednesday agreed we would hear it. However, this meeting scheduling was a bit unusual, and Michael and his team were asked whether you could actually give this presentation about 15 hours ago. And Michael's in Europe, so most of that time was overnight. So I do thank Mike and his team for pulling this together so quickly.

I don't know if there are any other questions or if Olivier has any other wrap-up information, but hopefully this will have been illuminating. And we may hear from this again sometime. I will note that this has been presented in a number of ways to a few ICANN bodies, and they have universally said, “Oh, that's interesting. Let's go on to something else.” So we'll see where this goes.

Olivier.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Alan. I hope you can hear me, but it doesn’t look like you can.

ALAN GREENBERG: [inaudible] Olivier is with us or not.

OLIVIER CRÉPIN-LEBLOND: He cannot hear me. Okay.

ALAN GREENBERG: We didn’t get to the Clarivate stuff. Is there something that can be done in a minute or two which may be illuminating? Nothing from anyone.

OLIVIER CRÉPIN-LEBLOND: Hi, everyone. I hope you can hear me now.

ALAN GREENBERG: We can.

OLIVIER CRÉPIN-LEBLOND: You can hear me now. Okay. Well, I could hear everyone on the whole call, but no one can hear me because the Adigo line doesn't seem to be properly connected to the Zoom meeting. So that's a problem that will have to be fixed alter.

Anyway, thank you so much for this presentation, Michael and colleagues. I think we can ... Well, well we just have a few minutes for the policy comment update with Jonathan Zuck and Claudia Ruiz, hopefully.

SÉBASTIEN BACHOLLET: We don't have time. We are supposed to go to another meeting now.

CLAUDIA RUIZ: Yes. Hi, everyone. This is Claudia Ruiz. And we [inaudible] report.

OLIVIER CRÉPIN-LEBLOND: Go ahead.

CLAUDIA RUIZ: Hi, everyone. Apologies. Yes, we really don't have much to report or any updates. We can go on to the next call.

OLIVIER CRÉPIN-LEBLOND: Okay, thank you. Then we have Any Other Business. Not seeing anyone put their hand up. Okay, that's pretty quick. So swiftly, we have to find out when our next call will take place. And it seems to be next week. There's some traveling involved, but the next call will be at 19:00 UTC. I haven't checked with my colleagues whether we should have a call next week or not. Is there a conflict with any topic? Because I don't believe that there is. It's just the week before the ICANN meeting, so I believe there won't be any interpretation. But everything else will be in order.

ALAN GREENBERG: Olivier, it's not clear we're going to have a lot of topics either, so maybe we should look offline and see whether there really is any content before scheduling.

OLIVIER CRÉPIN-LEBLOND: Yah. Thanks very much, Alan. So let's just say that if there is one, it will be at 19:00 UTC. But you will receive further details in the mailing list. We will check if we can populate and enter an agenda for that time.

So thanks very much to everyone for having been on this rather shorter call than usual. I know that there's something else immediately afterwards, so have a very good morning, afternoon, evening, or night. And thanks to our interpreters and to the real-time text transcription service. Thank you and goodbye.

JONATHAN ZUCK: Thank you.

YEŞIM SAĞLAM: Thank you all. This meeting is now adjourned. Have a great rest of the day. Bye-bye.

[END OF TRANSCRIPTION]