ICANN79 | CF – At-Large Plenary Session 2: Building Trust on the Internet through Registrant Verification
Wednesday, March 6, 2024 – 4:15 to 5:30 SJU

MICHELLE DESMYTER: Hello, and welcome to the At-Large Plenary Session 2, Building Trust on the Internet through Registrant Verification. My name is Michelle DeSmyter and I am a participation manager for the session. Please know that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod, which is located at the bottom of your Zoom screen. If you would like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. Onsite participants will use a physical microphone to speak. Interpretation for this session will include English, French, and Spanish. Please state your name for the record and the language you will speak if speaking a language other than English. Please speak at a reasonable pace. And with this, I will hand the floor over to Michael Palage and Avri Doria.

MICHAEL PALAGE: Thank you. My name is Michael Palage, and I am the co-moderator of this session with Avri Doria. The way we'll be handling this is we are intending to make this a very interactive session between both in-person participants, as well as those participating online. While I will be primarily coordinating the activities of those within the room, Avri

will be, if you will, quarterbacking the activities and discussions through the Q&A pod as well as the chat.

Just a quick level set, as you can see the way we have decided to break down this session is into two panels. The first panel will be about level setting on the concept of trust. And again, we have three very distinguished speakers. The second portion of the session will be sort of a tour de table for those that are familiar with how center operates. And this is going to be the opportunity for the participants to hear brief vignettes of how individual registry operators are tackling registrant verification, as well as how they are integrating different aspects of digital credentials to enhance that.

So again this is the potential roadmap, and in the interest of time and to maximize the time for our speakers, I would like to hand over to Finn Petersen, who is the director of International ICT Relations Agency for Digital Government, and he will speak to NIS2. Finn, over to you.

FINN PETERSEN: Thank you. And can I have my slide to be presented? Thank you for inviting me beside my job in the Danish agency. Here I am also chair of two EU working group under the NIS directive. The one is on digital or security measures for digital infrastructure and services, and also chairing the work stream on WHOIS, and in this capacity, I will talk about Article 28. Next slide, please.

Here's a short overview on what is the most important things in this directive concerning WHOIS in Article 28. I will encourage everybody to read it, but I have tried in short to summarize it. The instances which are under these obligations are registries and entities providing domain name registration services which we'll see registrar, resellers, proxy, and private providers in this respect.

I've listed certain requirements which those will be under, and they will be under if they are targeted customers, private, or entities within the EU no matter whether they are based outside EU. First of all, there is a requirement to collect with data that have been questioned before, whether on the GDPI, you are allowed to collect data if you have no use for them, but it is clearly stated in NIS2 directive that you must collect it in order to secure and have a reliable and stable internet. So it's legitimate to have it.

The NIS2 directive also specified which data you must collect and you must collect the domain name, the date of registration, the name of the registrant, contact, email address, and telephone number. And if you have somebody you have entrusted to do this, that person's address and names and telephone numbers must also be collected. Those data, they must be accurate, they must be up to date, and they must be verified. So all of this data are supposed to be accurate, complete, and verified. There's also an obligation to publish on the website the old WHOIS information which are of non-personal nature, and especially also to publish information for legal entities.

Also, the name of the legal entities even if it's contained personal name is if I have a company called Finn Peterson Incorporated, that they must be in the open WHOIS. There's also an obligation to give access to the WHOIS data, let's say in the close part of the WHOIS to legitimate access seekers for lawful and dually substantiated request. Next slide.

This is a provision in the directive. The directives are going to be transposed or implemented in national legislation in all EU countries in seven and a half months' time. It is up to member states to implement it, they have certain freedoms to implement it. The directive is a minimum requirements they put at additional provisions on top of it. Within the NIS directive, there is a cooperation group. It consists of all member states and the commission are present and the European security agency are participating there. They have a certain task, altogether, I think is 27. I have listed some of them among others, provide guidance and exchange practices when implementing the NIS directive.

Next slide, please. In this respect, they have created a work stream, and that is the one that I'm among others, sharing on WHOIS. And the purpose of this work stream is to draw guidelines for the Article 28 in the NIS directive in order to have a harmonized approach when implementing and using the provision in the directive. The member states have certain freedoms, but we hope that with this guidelines, we can have a harmonized approach. In Europe, we know that there's many entities under this obligation, and it is the aim that they are not

having two different conditions depending on which member states that jurisdictions will be in. Next slide, please.

We have created within the work stream two task forces, and the one is what we call the task force on verification. And they will or seek to draw up guidelines on how to verify WHOIS data and also what should be done, how to verify already existing data. The NIS directive does not distinguish between new and old [00:09:55 - inaudible] data. All of them should be accurate and verified. So we will try to issue guidelines there. We know, of course, it's a major task also to look through already existing data that you have collected. But anyway, it's a requirement under the NIS2. The other task force will especially look at legitimate access seekers who should be considered as legitimate access seekers.

And there is certain provision of responding to request for access to the so-called close part of the WHOIS things and we will specify what kind of information should be delivered within the 32 hours. And we are also seeing to see whether there should be certain guidelines on urgent request, it has something which have been up in this community here, but it is still pending.

So in light of any guidelines or any movements in this community, it'll be something which might be addressed by member states, and if it's addressed, our aim is to have it in a harmonized way. As I said, the NIS2 directive on this paragraph is up to member states to implement. And you can read the text and you can have different interpretation,

and that might also be in member states and still be within the scope of the NIS, but the devil is always in the details.

And if we can try to, so-called, have the same devils and each member states will try to to seek that. Whether member states will follow the guidelines, that is, of course, not something I know, but at least if we issue guidelines, it will go through the corporation group where all member states are present and they have to agree upon, and they can only be valid if nobody post them.

So the aim is try to have a harmonized approach there. So that is the Article 28. There's other provisions in the NIS2 directive with, of course, TLDs and DNS providers and other digital providers CDNs, ISPs, and so on, and that is the security measures here that will come more rules from the EU commission in so-called Implementing Act.

And our groups, the one that I'm also responsible, have given the technical input to that. And those Implementing Act, they do not have to be transposed into national legislation, but are directly applicable to the operators who are within the scope of the NIS directive. Thank you.

MICHAEL PALAGE: Thank you, Finn. And Finn has to get back to the GAC and communique drafting, so if there are any questions, please put them in the Q&A pod and we will work with Finn to answer them and post them online for everyone.

FINN PETERSEN: Sorry not to be here, I think this is much more interesting than communique drafting, but I'm paid to be there.

MICHAEL PALAGE: Thank you. The next speaker, I would like to introduce is Karla McKenna. She's the Managing Director and Head of Standards at the Global Legal Entity Identifier Foundation, or GLEIF. This actually has become one of my favorite international organizations. For those of my colleagues that know me, I mention it very often. I will now turn it over to Karla to explain the history of GLEIF, what they do, and how I think it potentially provide a roadmap for what we in the domain name community are trying to do. Karla, over to you.

KARLA MCKENNA: Oh, thank you very much, Michael, and it's a pleasure to be here in order to be able to present these topics to you today. So next slide please. Just to confirm the agenda, I'll give a brief overview of the Global LEI System, some that Michael has said that tie back to the financial crisis back in 2008, and then go into how the LEI formed the basis for the digital strategy that GLEIF has been working on for the last several years.

Next slide please. And then the next one. So the Global LEI System was called for by the G20 leaders in 2011 post-financial crisis in order to be able to create a global level international identifier that identifies parties to financial transactions. This does not necessarily mean that

the LEI itself, the Legal Entity Identifier, only can identify financial institutions.

It means that it can be assigned to a very, very broad environment and a very, very broad list of legal entities that are out there internationally who participate in financial transactions, even a corporate treasury department, for example, in a corporation.

So the Legal Entity Identifier Foundation was put together under regulatory oversight because of this call by the G20 and because of the fact that we have our history that is tied to the 2008 financial crisis and helping to be able to the regulators and business and private sector alike of being able to understand those who are legally responsible for different roles within different transactions within financial transactions, and those also responsible for transparency, exposure, supervision, et cetera.

So we were created as GLEIF under regulatory oversight, and you can see our regulatory oversight committee. The GLEIF is the operator and the operational integrity of the Global LEI System. And then we employ partners, a network of partners that actually validate that the legal entities actually exist and validate information about them that then is transported to GLEIF and is published without any restrictions under Creative Commons and under no licensing agreements to users in the global LEI repository, which is what we call the Global LEI System. Next slide please.

So, a little bit on GLEIF, a little bit of statistics. We have both the rock and the board and we are a Swiss not-for-profit foundation. And we

have a little bit more than 2.5 million LEIs that have been issued to date. And then the next slide, please. I think that it's important to note that the legal entity identifier is actually an ISO standard.

So this is what the regulators called for back when they were trying to be able to sort out what happened. They wanted to be able to communicate across boundaries, and in some particular cases, even within the same jurisdiction, across agencies using a common identifier because nothing existed at the international level.

That's when I entered my involvement with what became the GLEIF because I was part of the development at ISO in order to be able to come up with the LEI standard as an international standard that was developed by ISO. So the next slide please.

So based on what I said, the partners that we have in the Global LEI System that actually validate the existence of legal entities and certain information about, these that led GLEIF to be able to think that we had a very, very strong footing or foundation with the LEI in order to be able to think about how to be able to make the LEI more useful outside of it being just a dumb code that is tied to a set of standardized reference data.

And we started to be able to think about what could we do in order to be able to also make it relevant from a digital identity perspective. Next slide, please. And so we thought that what we had was the basis for providing with what we're calling now the verifiable LEI, which is a digital equivalent using the LEI, that what we were really offering here was the possibility of organizational identity for the ability for a person

or a thing to be able to prove that they had authority to represent the organization, which was represented by its LEI, either externally or even inside the boundaries of organizations, because some organizations are very large and not everybody knows each other and what the authority of everybody carries with their roles.

And so this started us on the journey in order to be able to create what we're calling the verifiable LEI and to create organizational credentials that could prove organizational identity with security certainty and verifiability. Next slide, please.

So what we're really offering here with what we've put together for the verifiable LEI is a zero trust architecture for organizational identity using what we're calling organizational credentials. And what we want to be able to do is to support the movement in order to change the behavior of users that receive documents, files and other artifacts, other pieces of information, or even when they engage in financial transactions or other kinds of transactions or decide to engage business to business, business to consumer, et cetera.

We want to be able to be part of that movement in order to offer features for the VLEI that offer multisignature weighted threshold requirements and also the pre-rotation of the cryptographic keys so that we keep security for the VLEI and the use of the VLEI and the organizational identity first always. So the next slide actually depicts what we call a role credential. Sorry, please.

The next slide, please. I keep forgetting that we have the section breaks in here. So what we've created here is the ability for an

organization to go to a VLEI issuer who GLEIF has qualified through a structured program and would requalify every year to be able to give the organization a credential with its LEI, and then to allow that organization to request additional credentials that we call role credentials that represent the connection among organizations, persons, and the roles that they carry out either within or for or on behalf of the organization. Putting the real world and the digital world next to each other, representing the organization by the LEI being able to identify the person by some identification credentials that they have, and the role.

And so we've done this in two particular flavors. We first started to think of how we could be able to do this from an officer or an official role perspective. But then with the use cases and the conversations that we've had with people in the industry and those in the technology area supporting the VLEI, we felt that we could also use these change credentials that we have in order to be able to support functional roles or defined roles for particular use cases in order to be able to broaden the value of the VLEI. And the next slide, please.

I'm going to bring you through the chain of trust for the VLEI. So we've established ourselves as GLEIF as the foundation and the root of trust for the VLEI. And I mentioned briefly before that these credentials are actually chained to each other. So with this new kind of technology and protocols that we're using, we can actually create a chain of trust not only for the issuance of credentials, but also to form as the basis and the foundation for the cryptographic verification of the credentials later on when the credentials are used and presented.

So GLEIF, from our root of trust, we qualify VLEI issuers and issue them a VLEI credential. When they issue credentials to organizations, it lengthens the chain in order to be able to link all of the organizational credentials that qualified VLEI issues on behalf of its clients.

And then all of the role credentials that we just spoke about also are able to be linked back cryptographically both to the organization that authorized the issuance of that credential. So the legal entity itself, who owns the LEI, and then also back to its issuer, the qualified VLEI issuer. This verification chain on the zero trust principle can allow a verifier or recipient of a credential to verify all the way back that the LEI is actually existing and active in the global LEI system. So the next slide, please.

We're gonna spend the last couple of minutes on how VLEIs can be used. So in using VLEIs, I have tried to be able to give a couple of examples of how the identity verification could be used for businesses, for the public sector, and for people in three different areas.

We see use cases come to us wanting to be able to support HR functions including employee onboarding and authorization within a firm and representing outside of a firm, client onboarding, submitting and signing reports, forms, and taxonomies. We see a large potential in being able to use VLEI in order to be able to sign documents as they go through the physical supply chain into the trade finance area. And then we also see a huge opportunity in order to be able for access to public services as well in order to be able to use VLEIs. And I'll give just a couple of examples. Can we go to the next slide?

So one of the use cases that I wanted to leave you with is digital signing with VLEIs. This is something that we're working on quite actively now. The digital signing use case is a very, very strong one, both for mandatory and voluntary submissions. So starting at the left, a reporting entity could submit a regulatory, a filing to a regulatory authority signed with the VLEI. The receiving entity would be able to verify the cryptographic validity of the credential and the signature, and also could check that the organization through taking its LEI and comparing to a white list, for example, that this was an organization that the authority planned to hear from before letting the submission actually into their production system.

So kind of like a front end type of check along with the verification. And then the receiving entity could accept the filing upon the successful verification. We have actively on the next slide, a pilot that we're working on, and the pilot is pillar three reporting to the European Banking Authority. So the overall general use case is private sector reporting to the public sector, but the EBA has secured the participation of 17 banks, they have announced this in a discussion paper that they published just recently, and they're looking for feedback by the end of March.

After the conclusion of a successful pilot using VLEIs, the EBA would announce a decision whether to use the VLEI for pillar three reporting, and then implement pillar three reporting for a total of the 600 banks that would need to report directly to the EBA, replacing the 27 reports from the National Competent Authorities from which the EBA now receives pillar three reports. And this would cover the identification,

authentication, authorization, security, and the management of users in charge of submitting these frameworks to the EBA. And so I think that's all I have. Well, one more slide before I close.

I wanted to be able to bring up that a large part of our VLEI ecosystem and infrastructure was putting together a governance framework. It's something that I was actively involved in preparing and am responsible for. It's 24 documents in total. It covers everything from the issuance and the revocation of credentials, the rotation of the keys, the requirements for our qualified VLEI issuer, pretty much focuses on guiding GLEIF, the qualified VLEI issuers and the users of VLEIs to fill all of the operational and governance requirements required for the VLEI system. And a lot of these requirements we see are being baked in both to the software that we have developed as GLEIF and by providers who want to be able to support the VLEI.

MICHAEL PALAGE: Thank you, Karla. And if you could stay online in case there are any questions, I would appreciate that. Thank you. I would now like to turn to the next speaker who is also the co-coordinator and co-moderator of today's session, Avri Doria, a research consultant and a friend of many in the ICANN community, including myself. If we can have the Avri slide. And Avri, you have the floor.

AVRI DORIA: Thank you very much, Michael. And thank you for the introduction. So basically, I'm gonna try and talk through a question of why is it so hard

to find a solution space for identities for digital identities, and bringing it kind of back to ICANN and looking at what is our responsibility to trust, to a multi-stakeholder trust?

For years, I've been part of discussions that have focused on the ability to establish or verify identity and various processes, some of the latest examples being RDAP, SSAD, et cetera. At the end of every discussion, it was determined that the problem was too hard. We had difficulty finding a consensus point in longstanding stakeholder policy oppositions. We did not have a clear view of our data protection and human rights responsibilities when dealing with the privacy, access, and security of information.

And this is whether it was about individuals or organizations that need protection or any organization. So among the things we need to do is we need to keep working on our consensus issues and discussing them, and we need to develop further skill and use with our impact assessments for human rights and for data protection.

But most haltingly is that we really did not believe that there was an architecture or set of protocols that could be used to do the job. It was too hard. Collectively, we did not seem to believe that there was a technical solution. Some thought differently, but most of us looked at it and said, I don't see the solution. Being unable to solve a problem does not do much to bring about trust, and that's what makes it very important for us to look at it. It is troubling that we cannot find a solution at this point.

So earlier today, I listened to a discussion about the number of registrars who are thinking about the problem and thinking about it hard and genuinely and honestly, but are finding the problem intractable. And many of the possible solutions that they come up with are operationally untenable.

I expect that handing 100% of the problem using a single set of tools probably is intractable at this point. But the question I have is stepwise refinement at solving the problem possible. Is it possible to use a combination of tools and policies to get a result that is good enough now and will improve over time? Is there a role for ICANN to help with the collaboration and cooperation necessary for a path to solution? As the availability of protocols and architecture seemed to be the one gating issue to the hard questions, I started looking at these protocol issues and started talking to people like Michael about them.

And we got to this beautiful galaxy of digital identity solutions. And so I started to look at that, I looked around, I saw many of these protocols, and it really is a richness of choices. I mean, the examples include protocols for electronic signatures from [00:33:50 - inaudible] client to authenticator protocols, Fido Ctech, legal entity ideas, the GLEIF that we just heard about, trustless frameworks for Pantera, standards for identity from NIS, and NIS Security Assertion Markup Language, the SAML from Oasis among many others, they all figure into this chart.

But there really was no one tool, which seemed to solve the overall problem. Fortuitously, at an outstanding tech day presentation, I saw plenty of ccTLDs and others using a combination of these tools to build systems that provide a degree of the basic functionality that is needed. I recommend that session for later enjoyment to anyone that didn't have a chance to see it. There are gaps, and on listening to some of the possible solutions, I have questions about scalability. But when taking a look at the galaxy of possible digital identity solution, it looks like there may be a tool for just about every issue. They just do not necessarily work with each other easily.

For example, my latest fascination is with ITFs WHIMSE, and that's Workload Identity in Multi Service Environments, I love it. An aspiring new working group, which wants to tackle the interoperability and combination of the many tools and architectures that have been used for a long time in their own silos. It may offer a path. I have started collecting information. Can we go to the next slide, please?

I have started collecting information on many of the protocols in this galaxy, and I'm trying to understand which are used and to what purpose to better understand the combinatory power and their sensitivity to data protection and human rights concerns.

I have a table in a [00:36:00 - inaudible] file that I will keep editing and updating while doing this individual research. It is open for comment, correction, and augmentation. Finally, I have begun to trust that a technical solution is possible. That still leaves the other two areas

needing a lot of work, but I really do look at this and think a technical solution is possible.

The rest of this session, when we go into the next panel, takes a deeper look into some of the ways that the pieces are being put together operationally today and doing so hopefully in adherence of their data protection and human rights concerns. So thank you and I pass it back to you, Michael, for the next panel.

MICHAEL PALAGE: Thank you, Avri. Now we are going to move on to the second panel of today's session. And this again is going to be the tour de table where we are going to move quickly, basically three-to-four-minute presentations by a number of TLD operators that have implemented registrant verification and digital credentialing at different levels. First speaker will be Lucas Prêtre, a telecommunication engineer at the Federal Office of Communication, OFCOM, and he's going to tell us about the .swiss gTLD. Lucas, you have the floor.

LUCAS PRÊTRE: Thank you, Michael, and thank you for giving me the opportunity to present to you, to the community what we do at for the verification of registrant at .swiss gTLD.

Next slide, please. So, .swiss domain names are allocated to specific entities based in Switzerland. In general, the ones entered in the Swiss commercial registra, but there are some exceptions. The criteria are defined in the ordinance on internet domains, OID, and the register

application contains, what we call an eID, it is the enterprise identification number in Switzerland. And this number, this ID, allows to carry a national database for the record. So we get data or not.

And when not, it could be several things that eID has been mistyped, doesn't exist, or was randomly failed to overpass the system. And when we have such cases, the application is rejected with an application code. And if it's found, we get the entity details and its legal form populate our evolution tool. This tool has been developed specifically for the .swiss gTLD. In this tool, some automation is made to check if the name associated to the eID is equal or looks like to the registrant organization, and the tool will visually flag it so we can see what we do. Next slide, please.

And some of the legal form are specific to Switzerland. It's different in each country, and not all of them are obligated to be entered in the Swiss commercial register, but the registration in this register is mandatory for the eligibility. I will skip the extract of the low, the ID, and if the result is decisive, so it's true false. If it's false, we don't go further. And when it's okay, the application is eligible, we make, I would say, we make an evaluation about the relationship between what the domain name is requested and the applicant or it will do with the domain name, it's a project, a product. I will go next slide, please. Sorry.

So we have four type of objective link or relationship. If it is a trademark in the Swiss register, if it is name based, it is the same name, the company and the domain name. General recognition is like

if it's an abbreviation of the company name or it's a product or project in this company. And if not, could be two things or we see no link between the domain name requested and the applicant, or if it is a generic term, this causes the rejection too. Next slide, please.

As you've seen before in the slide, we have a change in this eligibility on April 24th, 2024. We open the .swiss gTLD to natural persons, and this person will have to provide a number. The name is UPI, Unique Person Identification, sorry. And this ID is the Swiss Social Security number, the applicant should provide that. So I think I'm out of time, I'm sorry. And I don't know if you want to hear about the RDAP, it's quick.

MICHAEL PALAGE: If you could keep it to 30 seconds. I do think this is an important protocol aspect, so 30 seconds, please.

LUCAS PRÊTRE: I will do it. So our next slide, please. Sorry, next slide. Our technical partner has made a lookup of RDAP of a domain name. It's a eID, the ID is not published, you cannot see it, but if you use other- next slide, please- if you use other client, it depends on the client, you can see this ID, and it use the public IDs in the database. Thank you. So I'll stop here. Thank you.

MICHAEL PALAGE: Thank you. And the slides are available online, so I would encourage everyone to go and look at this, particularly with the RDAP. In the interest of time, I now want to move to our next speaker, Niamh Lewis. She's the Senior Digital Health and Policy Expert at the National Association of Board of Pharmacies, NABP. Niamh, are you online?

NIAMH LEWIS: I am.

MICHAEL PALAGE: There you go. You have the four.

NIAMH LEWIS: Great. I will be quick because I am at another conference right now, and so have to-- I don't even think I'll take my four minutes. So your 30 extra seconds were fine. So we wanted to start with-- NABP operates the .pharmacy TLD, so tell you something about NABP. The National Association of Boards of Pharmacy, we're 120 years old. It's a US-based nonprofit organization whose members are the 50 state regulators of pharmacy practice in the United States.

So our members are the government regulators, as well as pharmacy regulators in a number of other jurisdictions, including 10 Canadian provinces. So NABP has been around a long time, and the .pharmacy is only part of what we do. So we're a mission driven organization. Our goal is to protect public health.

We have a large staff of over 180 people that includes more than a dozen pharmacists just on staff, nevermind contractors and regulatory professionals, lots of lawyers, myself included. NABP offers, like I said, a number of other programs that are designed to protect public health. A lot of what we do is every pharmacist that is licensed in the United States, the NABP creates that exam, we do other accreditation programs and inspections, and we do license transfer if a pharmacist is moving from one state to another. So, next slide.

So what do we do with .pharmacy? So the .pharmacy TLD is available to healthcare merchants and merchants that are considered healthcare adjacent who have obtained NABP Healthcare Merchant accreditation or another recognized program. No one's applied to us be recognized, so right now it's healthcare Merchant accreditation. The TLD is also available to pharmacy regulators.

So Healthcare Merchant accreditation is a global program, they have to meet our eligibility criteria in order to apply, they have to comply with our 10 program standards, which include things like, are they properly licensed, are they in legal compliance, both where they're located and where the patient's located, do they meet privacy standards?

Those are just a few. If we are reviewing applications outside of the US or even in the US, we collaborate with regulators, Health Canada, MHRA in the UK, NAPRA is the sort of equivalent of NABP in Canada.

The reviewers for healthcare merchant accreditation include attorneys and pharmacist and pharmacist attorneys. So how do people use the

.pharmacy TLD, sort of how do third parties use it? That I thought Michael mentioned people might be interested. Well, essentially, the idea is that it serves as a fraud proof seal.

So in the online pharmacy space, there's a lot of seals, a lot of people have seals that aren't actually accredited by the organization who seal they have on their website, and the TLD is a fraud proof seal. And it is recognized, there are third party stakeholders who require certain accreditations, one of which is ours.

There are other accreditations that are recognized, but those stakeholders include if you wanna advertise on lots of e-advertising platforms like Google or Bing or TikTok or whatever. Visa and MasterCard also recognize our accreditation. They have certain requirements in their programs for what they refer to as card-not-present pharmacies, people who is a pharmacy that does business where you're not physically swiping the credit card. And they consider that high risk, they require certain accreditations or other things, and our accreditation is recognized by theirs, but it's certainly not the only one. So right now, there are currently over 600 .pharmacy domain names under registration.

MICHAEL PALAGE: Thank you very much for coming in on time, and I will let you get back to your other conference.

NIAMH LEWIS: Thank you very much. I'm sorry.

MICHAEL PALAGE: Thank you. I'd now like to turn to our next speaker, Craig Schwartz, the Managing Director at fTLD Registry Services. Craig, over to you.

CRAIG SCHWARTZ: Thanks, Mike. If we can go to the next slide. So thanks for giving me an opportunity to talk about what we're doing with .bank and .insurance. The TLDs are globally available community based, and are restricted to chartered retail banks, licensed insurance distributors and producers, as well as their trade associations and regulators. So because of these restrictions, the pool of potential registrants is small, you can see our DUMs under management or domains under management are low. However, DUMs is not the only metric of success. And in fact, as of this week, about 17% of the banks in the US are now actively using their .bank domain for their consumer website, so we're super proud of that.

As it relates to Karla's presentation earlier today on LEIs, we've determined that about 80% of our registrants in the US already have LEIs. So we're looking to how we might ultimately incorporate that into our verification process. We are one of the very few registrations, excuse me gTLDs, that's always conducted pre-registration verification, and I'll speak to this in a moment. What makes us also more secure is that we require various security technologies and protocols for domains in our zone. For example, DNSSEC, strong TLS encryption, and email authentication.

And not only do we have these requirements in place, we actively monitor them for compliance on a daily basis. I'm proud to say that in our nearly 10 years of operations, we've only had 18 alleged reports of abuse, and they've all turned out to be false positive, so it's been clean since day one. So in addition to security requirements for second level domains, we also look at how we can do things hierarchically for our TLDs.

So in 2018, we became the first non-Google TLDs to be added to the HSTS preload list, which means if you are properly secured with a TLS certificate, you'll resolve in the DNS and with an HTTPS connection. And then more recently, after a five-year journey, including the IETF RFC process, we've implemented what's called Public Suffolk Domain, DMAC, which adds a layer of protection from phishing and spoofing for non-existent domains, so if anybody's interested in learning more about this, you can certainly approach me. Next slide, please.

So we have always operated what's called a pending create and registry, which means we manually approve every new registration. This is to ensure that the registration data matches that which we verified, and also to ensure that nothing ever inadvertently slips through the cracks and gets registered.

For verification, which we rely heavily upon publicly available regulatory databases, we're confirming, for example, the eligibility of the organization, the eligibility for name selection, the address, the email address, are they on any blacklists based on the US Treasury's OFAC and STN lists that could prohibit registrations. And we also

ensure that the registrant contact has authority from the organization to register and maintain the name. Verification happens prior to the initial registration annually thereafter.

And when certain registration data changes, such as the registrant organization, the registrant contact, or the registrant email address. And then finally, we used to outsource this to Symantec, it was super complicated for us for registrars and very expensive. In 2017, we submitted an RSEP to ICANN to create what's called DRV or Dynamic Registration Verification to bring this in-house, which we have successfully been doing now for five years. It's still largely manual, but it's worth the pain for the trust and verification of our TLDs. And then, in closing the next evolution is going to involve increased levels of automation, possibly the inclusion of LEIs and AI, if possible. Thanks. Mike.

MICHAEL PALAGE: Thank you, Craig. And if I can ask one follow up question. Alan Greenberg in the pod asked, what is the cost of LEIs from I believe the thing? fTLD does have an LEI, can you just say what it costs per year?

CRAIG SCHWARTZ: Yeah, I think we paid 60 or $80 to Bloomberg for the LEI.

MICHAEL PALAGE: If I could now turn to our next speaker Tom Keller, Executive Board Member DENIC. Tom, you have the floor.

THOMAS KELLER: Thank you, Mike, for having me, and thank you for giving me the time to actually show what we are trying to do now that we are the subject to DNS2, which will go effect sometime this year. So just to help few words about DENIC, it's a nonprofit organization based in Frankfurt and Germany. We are owned by our members, that's a very unique setup.

So once we learned about that we are subject to the new regulation, we reached out to our members and went through a very far reaching process to decide on what we're gonna do. And I can show you today what our current thinking is. Of course, the term regulation hasn't been passed, so we will wait until we do any of the implementation until we see whether this will be a good idea or not, but at least I can show our thinking. So next slide, please.

So DENIC has almost 18 million domain registrations currently, which makes us the second largest TLD in the world. We have 290 members and we have one of the lowest records of measurable views of all TLDs in the world. So I think there's a very good record, but as you can see with 18 million domain names, this is quite a sizeable operation, so we have to be very careful in what we do.

That means that we have a lot of registrations that are already there. So we're not starting from the beginning, it's not like 500 or anything, but this is very complicated for us. Next slide, please. So when we convene the group to deliver on what we wanna do, so first thing we did is we came up with a couple of principles, and the principle has to

be future orientated. We don't want to come up with a process where we might be stuck, where we might have to change it at some point of time or maybe do something completely new.

So it has to be scalable and flexible, and it should be a risk-based approach. Risk-Based means that we do mandatory checks for new, updated, and transferred domain names, but that we only check on registered domaining on the complaint base. So if someone's coming to us and say, okay, this doesn't seem right, then we would actually go through that process again. We will offer X posts and X under verification possibilities. And one of the ideas we're having, and I don't know whether we really ended up with that, is that verification can be used again, even for other TLDs. That's one of the concepts we're trying to implement, and yeah, let's see whether we get there.

Next slide, please. So what are we going to verify? Very briefly, the name, the address, whether existing or fake, the email address with every holder, and the phone number.

Next slide, please. But the process we will implement as we're thinking currently is that if a request comes in, it can be a new registration, can be compliant, can be anything, we will be conducting syntax, incompleteness checks, is all the data there, is all the data something we can actually work with, if not, the request is rejected.

And then we go in a validation phase and a risk assessment. This is including some magic AI sourcing. All the data we have from the registrar and the registration data, is there anything that looks like it's not a good idea to actually register the domain name or not. In the

case we come to a very high risk identification, we will quarantine the domain name, we will not delegate it, and it needs to be verified in a different manner. We would just see it as a high risk to domain is delegated and verification is required in the time of two weeks.

And if there's a low risk, the domain is delegated and the verification process is necessary. Next slide, please. Who will do the verification? That was a long debate with us and the members, whether we should be doing that or the members should be doing that, and it went to the registrars. So the registrar has the obligation by contract to actually do the verification, and we will offer a wide variety of allowed verification methodology. So this is ranging from ID card checks to photo ID processes to having a look at the credit card data, all that sort of things. And we are very open to actually experiment with stuff that is working. So thank you for giving me the time, and let's move on.

MICHAEL PALAGE: Thank you, Tom. And again, I really do appreciate the outreach and engagement with registrars to come up with a forward-facing solution. Our next speaker is Dr. Bruce Tonkin, Chief Operating Officer at .au. Bruce, you have the floor.

BRUCE TONKIN: Thank you, Michael. If we can go to the next slide. One more slide. So this is sort of the requirements for .au. So the requirement essentially is that the registrant must have an Australian presence. And so that typically means they're a citizen of Australia. There's some form of

registered company, or they can be a foreign company, but they need to have an Australian trademark.

In addition to that basic requirement, we have individual namespace. So we have .au direct, so for example, .au that just requires the Australian presence. For com.au and net.au, you need to be a registered commercial entity. So to do business in Australia, and there's a sort of a fairly involved tax system where everything gets taxed. You basically need to have a tax number and be registered with the government to do business.

For not-for-profit organizations, we have a separate organization that registers not-for-profit entities. And then we also have government entities and education providers. So these are all backed basically by government databases that we can check. So the next slide. So registrars need to validate the information the registrant provides against the information on one of those databases.

And I stress here, it's not verify. So it's not, I think one of the early presenters was talking about a verified global identifier, and there's some sort of password required to provide the identifier. So we just basically collect the information, check it against the government databases, shows that that company exists or that person exists, and that's sufficient for registration. Most registrars, well, effectively what you need to check is that the name, address, and the identifier is real.

And most registrars in Australia are using the government's business register. And the good thing about this is it's free to do lookups, this is a very reliable service. You can search by the name of the person or

company or search by the identifier. It returns a record, it's structured information, and you can compare that with the information the registrant has provided.

And if it checks, then you can register the domain name. The other service that's possible is if a person doesn't have a business identifier, so it's literally just a citizen, and that's a low percentage of registrants. They can verify using a identity document such as a passport or driver's license. The government has a service for validating that information. The only problem with that is they charge multiple dollars per check, and one of the sort of user issues here is that if a user's typing in information for their driver's license, sometimes they need their middle name, sometimes they don't. So the check can get rejected, or sometimes they get the wrong number.

So a driver's license has got a card number and a driver's license number, so people put the wrong number in. So every time a registrar is given the wrong information by the registrant, it costs them several dollars, and it might be reject, reject, and eventually the user gets it right. So that's one of the challenges, and hence something that registrars are not that keen on using. But it is available as a method of validation. The key here though also is that although registrants can use a driver's license or a passport to register a name, there's no requirement for the registrar to collect that passport, and especially not to store it.

The only thing is that they're collecting the number that's on the passport, running that through the validation service. It gives you a

yes or no answer. And all they need to do is store whether they validated a timestamp basically. But the idea here is you don't actually store any of the identifier that's personally attached to the person, like a driver's license.

The end result of this system, if you like, is we have very few, what we call malicious registrations. So it's somebody registering a domain name for the purposes of doing some sort of crime. And in the cases where they do, it's usually stolen identities. So you can have the best validation system you like, but if the identity's stolen, if you find someone's driver's license, it's a real driver's license, it will pass the validation checks.

Much the same as if you find someone's credit card on the floor, you can go and buy something because you've got everything you need for that transaction. What we do see though, is while we don't get many malicious registrations, we do get DNS abuse, and mostly it's compromised websites that are more than five years old, so nothing to do with validation at all, but really just that organizations don't maintain and patch their websites. They get hacked and phishing and other illegal content gets put on those websites. That's all from me.

MICHAEL PALAGE: Thank you, Bruce. I'm now going to turn to good a friend and colleague Jaromir Talíř, a Technical Fellow at CZ.NIC. Jaromir, you have the floor.

JAROMIR TALÍŘ: Thank you, Michael. Next slide. So .cz registries is one of those registries that actually cared about the domain verification for many, many years, maybe almost 20 years, or at least since 2006 when we deployed our new registry system. So this sort of global panic about NIS2 and Article 28 keeps us quite calm. And we actually started with simple sending the registered letter to the registrant which we received some complaints about incorrect data or that was selected by, by scanner that there are some suspicious information. And when we haven't received the response about the reception, we just delete the domain.

But of course, we cannot verify this by the whole zone, so in 2010, we actually decided to try to convince people to do the voluntary validation of the data, and we introduced the Digital Identity Service, more ID on top of the registry, the contact database. And actually, it's possible to verify on the level that you can actually link the contact data with the citizen registry. So we receive even updates when the person move or change the name or something like that. And this service was at the end recognized by governments for the access to governmental services and it's notified according to the eID, so it's possible to use it around whole EU.

So this way we solved the Czech citizens, let's say. But we, of course, need to verify also the registrants from foreign countries, so we tried to join with four other ccTLDs in 2019, took advantage of the eID network to verify also holders of the eID of other countries. So this way we linked our history with also eID. And last year, the last change that we did is that we rewrote our verification system to introduce

some source service portal where the party that is expected to be verified will just select some method. So this is just to scale up and handle more cases. Next slide.

And so what we plan to do in upcoming years, of course, we are looking into integration with the online registries in Czech Republic. We have Public Street Address Registry which we can query. There is the public component registry that we can use, or we are thinking about, also about to use GLEIF for the verification of organizations. We are also part of the large-scale powers for European Digital Identity Wallets, where we would like to explore some ways how use this wallet to also for the registrant verification and maybe for some other things. And of course, we still need to keep an eye on the people that don't have eID. So we are thinking about other methods, how to verify these people.

And of course, there is a big question whether the complete verification, it should be mandatory at the end or some incentivized voluntary, for example, like to provide the cheaper domains for verified contact or to provide them some additional value if they will verify themselves like maybe giving them some domain ownership certificate that they could provide and get some value by using that certificate in some other services. So that's it.

MICHAEL PALAGE: Thank you, Jaromir. Our next speaker Timo who's Head of development at .ee. Timo, you have the floor.

TIMO VÕHMAR: Hello. Next slide please. So I'm from Estonian Internet Foundation, we are private, not-for-profit foundation. So founded for managing Estonian County-Code Top Level Domain .ee. We have been doing strong contact identification since 2010, and like most ccs, we use registry-registrar-registrant model. So that puts actually the obligation of identification of contacts on the registrar.

So we have dealt with two challenges throughout these years. First, how to identify foreign contacts. This is not a problem in Estonia because we have very well-established eID infrastructure. And secondly, how to help and enable our registrars to identify, authenticate registrants and contacts. So far, we have used what I call Caveman BankID. So this means that if bank transfer has the same details as a domain registration application, then the contact is authenticated. But this solution can be very expensive in case of international payments from outside of EU. Next slide please. Next slide.

Yes, but now we have a better solution for all these problems. We call it EUID because it's better than eID. Gateway, it is basically gateway to a long list of available EUID options. For example, government provided solutions like from Estonia, Latvia, Sweden, Belgium, Spain, but also private solutions like my ID from check registry or bank IDs from Nordics.

So with this, our registrars do not need to integrate with all these options directly and save a lot of time and hassle from managing all

these contracts, and integrations directly. But for cases where contacts don't have access to EUID, we provide our own eID. We use video identification for that, we have partnered up with service provider Brief for this, but there are number of different service providers like them around the world. Their main clientele are banks and financial institutions with their KYC operations. So they know what they do and they are very good at it.

And we use Open Standard called Feed ID to hold identity data. That is standards created by Feed Alliance. Feed Alliance consists of all big names in the internet business. So Amazon, Google, Visa, Mastercard, you name them, they're probably in there. And if you have not heard of Fido, then maybe you have heard of Passkeys. This is a solution for passwordless authentication. So registrant is actually directed to EUID platform for identification.

And using this great EUID, they can then now dedicate themselves to registrars to register the domain. So it's simple, secure, and efficient. Next slide, please. Very quickly. I'm running out of time anyway. So I believe we have come up with killer solution for contact identification issue, and now we are focused on making it available and accessible by bringing down the cost of identification. And if this EUID topic is interesting to you, and if it's not, it'll be soon enough, then don't hesitate to contact, we got you.

MICHAEL PALAGE: Thank you, Timo. And I would encourage everyone to look at Timo's presentation during tech day, where he actually got into some of the

cost elements. Mindful of time, I'll like to turn to our last speaker Jacques Latour, the CTO at CIRA. Jacques, you have the floor.

JACQUES LATOUR: Yeah, and I'm between you and beer, so I'll do this quickly. No beer. So I'll talk about the .ca Registrant Information Validation Process. So next slide. So today, the process that we have for verifying a registrant information is based on the Canadian Presence Challenge. So to get a .ca, you need to be Canadian basically.

So right now, when a domain, there's a report of abuse for a domain, we execute the challenge and then we ask the registrant to give us a digital copy, a scan of their proof of citizenship, so passport, driver's license, birth certificate. There's two problems with that. One is it's not privacy preserving, meaning they upload a passport, a web server somewhere, and then we do all our best to delete the data and get rid of it after verification. That's the first issue. We don't need all that information.

And second, there's no human that can detect fraud today with all the deep fake stuff happening. And so it's very difficult to do that part. So, the document we get are not signed, we can't verify them, and we can't trust them. Next slide.

So what we're looking at is digital credential presentation. So this is privacy preserving, this is important. In the process, we'll ask the registrant to use a wallet to use existing digital credential. Like in British Columbia, citizens can have a verified person credentialed

that's issued by the government. That document is signed and we can actually verify it with the signature.

So the goal is to request the registrant to send through a wallet and digital credential, claims, not the document themselves, but a claim that they are Canadian. So it says I am Canadian and it's signed by the issuing entity. And then we get the information, that can be verified. So digital claims are privacy preserving in ma manner. Next slide.

So now we have digital credential, we have a claim, we know that this document is signed by this entity, but how do we trust that the document is actually signed by a trustworthy entity? So today at the DNSSEC workshop, we had a panel that we spent an hour talking on digital trust on trust registries, so you can look it up there.

But basically, we're building a fabric of trust registries and that an infrastructure of digital trust with trust registries to be able to verify that the entity is who they say they are, and they're authorized to issue the credential that they did. So when we get that signed credential from the BC government, we can go in the trust registry and see that it's actually trusted in Canada to issue these credential, then we can trust that the information we get is authentic. So everything has to be signed, everything has to be verified, and then we need trust to check all of this. That's it.

MICHAEL PALAGE: Thank you. And literally on time, the end of the session. If I could ask ICANN Org colleagues, can we go a couple of minutes over to see if there are any questions from the room? Is that possible?

MICHELLE DESMYTER: Five minutes? Yes.

MICHAEL PALAGE: Excellent. I guess my question is, are there any questions either online or in the room, please come to the table and pose your question. And if there is anyone online or in the room that has a question that comes to them afterwards, please submit any questions that you may have to staff@atlarge.icann.org and we will take it upon ourselves to speak with the panelists and get those answers to you.

AVRI DORIA: If I can, I wanted to come back to Alan Greenberg's question in the QA pod because he was actually asking that of GLEIF itself and not necessarily how much was someone paying. So it basically said, what are the costs associated with VLEI? Not necessarily exact, but at least order of magnitude. So I don't know whether there's someone who could still answer that question here. Ah, yes, Karla.

KARLA MCKENNA: VLEI or LEI? Can you hear me?

MICHAEL PALAGE: Perhaps you could do both because obviously you could explain with LEIs, there's a cost recovery mechanism, hard coded, so I will let you articulate that.

KARLA MCKENNA: Sure. So we have over 30, almost 40 LEI issuers, and one of the statutes under which GLEIF was founded was that the system needs to operate for issuance and registration of LEIs under a cost recovery principle. So each of the LEI issuers actually submit every year their cost recovery numbers, and that drives the amount that they're able to charge in order to be able to do the validation and then to issue and maintain the LEIs. The range is anywhere from very, very low in bulk registration for some of our LEI issuers in the twenties.

Very, very common around the $50 mark, and also upwards into the hundreds of dollars depending on the type of organization that needs to be researched because organizations such as Trust Pools and others, not just your Garden Variety Corpse and LLCs are eligible to get LEIs. VLEIs at this particular point in time, we have one qualified VLEI issuer, and they're charging around $200 for VLEI issuance.

AVRI DORIA: Thank you very much for the complete answer. Had one other thing, I don't have any other questions in the Q&A pod. At one point during the discussion, Hadia, you had your hand, up and I want to make sure that it didn't go away in frustration, but that if you still had a question, you had a chance to jump in. I guess not. Okay. Back to you, Michael.

MICHAEL PALAGE: Thank you, Avri. Ah, Jonathan.

JONATHAN ZUCK: Thanks. Jonathan Zuck here for the record, I'm the ALAC Chair. And this is a very interesting presentation. I enjoyed all of these. I'm curious what the level of integration to date has been with registrars. Because obviously in the gTLD space, there are an integral part and multiple registrars per TLD. And so they would need to integrate this kind of technology as well if they were trying to implement this verification, or is it black box and it just gets rejected. How does the interaction with registrars happen? And I don't know who to direct that to, but that's what I kept thinking as I was watching.

MICHAEL PALAGE: Sure. I will let Jacques and Jaromir and then perhaps Timo.

JACQUES LATOUR: For the stuff you just saw for .ca, the feedback from the registrar is make it work, build the standard, make it low cost, and then we'll look at it. So what we're doing right now, that's why you're seeing registries working on this and making it work is, we gotta start somewhere and then they can just replicate now, they don't have to engineer all of this.

TIMO VÕHMAR: Yeah, we have similar approach. Our registrars actually are happy if they don't need to do anything. So if we told them that we will take care of that, they will super happy.

JAROMIR TALÍŘ: I guess the basics are the same for us as well. The EUID platform is new still, so we haven't started forcing it on registrars yet.

JONATHAN ZUCK: So it's all hypothetical so far with respect to registrars then? They're hopeful, but they haven't engaged yet.

TIMO VÕHMAR: Yes, yes. We are in discussion for a long time, so they are prepared, they know what's coming, and our job is basically we make the integration as simple and cheap for them as possible.

AVRI DORIA: Jonathan, one thing is you might want to check out that tech day presentation because in that, several of the ccTLDs did discuss the extent to which they've incorporated this protocol or that architecture or were working on it. But it really does seem like it's a thing that's just sort of starting to gather a little bit of momentum. And it is one of the things I was hoping to start collecting in that table I started building of who is using what, where. I don't know how much

information I'll be able to get, but it is something that I'm interested in trying to understand.

MICHAEL PALAGE: Bruce.

BRUCE TONKIN: Yeah, just a bit of contrast and maturity, I guess. The business identification checks have been running for 20 years in Australia, so it's fully integrated. And the registrant verification's been running for about two years, fully integrated.

MICHAEL PALAGE: And with that, I think we have exceeded our extended time. Thank you everyone, panelists, attendees and ICANN Org for a very good, constructive and engaging discussion. Thank you.

AVRI DORIA: Thank you.

MICHELLE DESMYTER: Thank you, Michael.

[END OF TRANSCRIPTION]