ICANN75 | AGM – Emerging Identifier Technologies
Wednesday, September 21, 2022 – 15:00 to 16:00 KUL

ADIEL AKPLOGAN: The session today was originally planned to be a session dedicated to a new type of name system, particularly those based on a ledger-based naming system. We have had, already, an emerging identifier session in the past—a session dedicated to that—and this is a follow up on that, noting that those technologies have evolved in between. And Octo has also produced a document that kind of looks at those alternative names systems and the challenges that they pose.

So today we're going to hear from Alain. Alain Durand is part of our research team at ICANN, and he's the author of OCTO-034, which gives an overview of the challenges that we are talking about. And he will start with setting the scene a little bit for us.

Then we will hear from Luc van Kampen from ENS. He will tell us a little bit about the Ethereum Naming System. And we'll have some questions and interaction with them.

And the last presentation is not directly an alternative naming system but is aligned with the title of this session which is emerging identifier, but in this case within the DNS will be presented by Jacques Latour from CR.

So if there is no further announcement, we'll move on with the presentation. And I will give the floor to Alain. Alain, if you're online you can go ahead.

ALAIN DURAND: Good morning. Or good afternoon, I should say. It's morning where I am, but it's late afternoon in Kuala Lumpur. So I wish I would have been able to join you physically, but life made it differently. So I hope you can hear me okay. If you can give me some feedback on that.

ADIEL AKPLOGAN: Yes, we can hear you.

ALAIN DURAND: Perfect. Thank you very much. So today I'm going to make a presentation about a document that I published earlier this year called OCTO-034, Challenges with Alternative Name Systems. Next slide, please.

So the goal of the document was to look at alternative name systems and not alternate ones. "Alternate" means you have one and then another, and then one and then another. That's not the same as alternative which means "something different."

So look at the technical challenges that somebody would face in deploying those alternative naming systems. [inaudible] alternate. Anyway. So our goal is to go in depth into how the underlying technology supporting with other name systems work. We're not going to go even into the policy-making processes of each of those alternative systems. So we will focus, really, on the technical challenges deploying this.

There is a link here if you want to download the document. Next, please.

So alternative naming systems are really nothing new. Some alternate roots have existed in the past, and some even predate ICANN. And that led to some not very clear situations. And in 2001, the ICANN document called ICP-3 was published, making a statement saying that these alternative roots will actually be somewhat problematic.

So I was slightly torn on ICP-3. But keep in mind that this is nothing new. Twenty-something years ago, we have been there. The reason why this is coming back to the limelight is that the popularity of blockchain in general is bringing attention to blockchain-based naming systems.

So there are three popular alternative naming systems today. There's Handshake which is from a derivative of Bitcoin. There's ENS. It's based on Ethereum. There's Unstoppable Domains that is from a derivative of ENS.

The first thing to notice that there was no requirement, actually, to use a blockchain-based naming system to create a naming system for blockchains. You could use DNS to do that. But for some reasons, the developers of blockchain system decided to create their own. So that's the first observation about this. Next slide, please.

Another thing that is new is that there are ICANN accredited registrars that are selling some of those blockchain-based names. [I want you to] remember is that blockchain-based domains are not bound by ICANN policies. They are their own independent policies. That's neither a good thing or a bad thing. It's just a statement of fact. Next slide, please.

So, here you go. Deploying those alternative naming systems. The question is, how can Internet users resolve a name from such an alternative name system? Because if you simply want to deploy it, buy a name. It's easy to buy a name. If you want to create your own servers using that time, it's easy to. Very easy.

The real question is, how do normal, regular Internet users access those names? How do they resolve those names from those alternative naming system? So, there are different ways of doing this. Essentially, if you use a native application you can use some dedicated libraries. And some exist for all of the various programming languages that are popular today. So it's not really a problem. So if you create something new, you just use the correct library and you're good.

Now if you have a legacy application ... And legacy applications, think about e-mail. Think about simply browsing the web from a regular web browser. It's a little bit more complicated and there are bridging techniques that exist. So you can use some kind of a URL bridge to reach those domains. You can put something in your local resolver or in a resolver operated—[a recursive resolver] operated by your ISP. Or you can use some dedicated browsers or dedicated browser extensions.

But all of those techniques have some issues, especially if you're telling people to use a specific browser or to put an extension to a browser. Some kind of manual intervention is required by the user. So that works well for early adopters or enthusiasts. But it doesn't really scale much past that.

So now the challenge becomes not only to communicate to your potential [inaudible] customers, to communicate to them the name. But you also might need to communicate to them the instructions on what to do in order to resolve that name to apply, for example, “Okay, use this particular browser if you want to connect to me. But don't use that one.” So that's a little bit of a challenge. Next slide, please.

So as I mentioned earlier, this bridging could be done in a recursive resolver. And while, typically, the idea that was floated around was, okay, maybe your ISP can do that or maybe the public resolvers can do that. But you have to be very careful when you go that route because it can lead to instability because the result of a resolution will really depend on which resolver is being used because some may do something and some of them may do something else. So you will face consistency issues.

A simple example. Let's say you at home and you have a cellular network and you have your Wi-Fi network. And maybe your cellular operator is not the same as your fiber or DSL operator that you have connecting your Wi-Fi network. So depending on if your cell phone is connected to cellular or to Wi-Fi, while you may have one resolver or another meaning that you have potentially two different answers if those resolvers are not configured the same way.

So in my house, in some parts of the house I have a Wi-Fi signal. In some other parts, the Wi-Fi signal is very weak and I switch off to cellular. So depending on where I will be in the house, I will see some of those domains or I will not see them, which is somewhat a serious consistency issue. How to explain to regular users? Next slide, please.

Okay, so this was about deploying one alternative naming system, but what about multiple? I mentioned at the beginning of my presentation that there were three major ones, but nothing stops a fourth or fifth or sixth one to come. The issue is that there is no community-driven coordination—neither between those alternative naming system nor between those naming systems and the DNS.

As a result, name collisions are unavoidable. And we know that name collisions are problematic. There have been a number of papers, a number of SSAC papers and others talking about issues and the problems that arise from that.

So the naïve approach to this is, oh, more naming system to choose from is great because if I cannot get the name I want in one naming system, I'll just get it in another one. Great, I have more choice. But that's a naïve approach. It doesn't answer the question, how do people reach you? Because the naïve answer is, "Well, I'll just tell them to use this app." But applications can connect to only one name system at a time. If not, it's unstable.

So you will need to have a specific app for the specific namespace on which you have decided to connect your name. So that gets really, really complicated now. If not, we really have an unstable and unpredictable resolution. Just like I explained the situation in my house where I can switch between Wi-Fi and cellular. But now it really depends on how things are configured on different places. And it's very difficult to debug. End users who are not absolutely technology savvy will have a hard time to navigate those issues. Next slide, please.

Really, the risk here is a fragmentation, again, of the Internet by creating some separate ecosystem, one for each naming system, because that's really the solution here. You say, “Oh, I am in this family of alternative naming system. I'm using this family of applications. And in the other one, I'm using this other family of application.” But neither one will work with the other. And they also never shall talk to each other. That’s not necessarily the outcome we would like, but that's what it is. Next slide, please.

So this really reminds us of the early 2000s, late 1990s that led to the creation of this ICP-3 document. And here, you can go and read it. But I've put a few sentences extracted from ICP-3. It was a document reaffirming ICANN’s commitment to a single root. And really, the reason was that alternate roots, some are substitute insular concerns in place of the community-based processes. And that's really what is at stake here. This is exactly the same issues. Not the same technical issues because it was an alternative naming system not based necessarily on the DNS protocol. But all of the other issues of name collisions are exactly the same.

So I'm not saying that ICP-3 should apply to this situation. I'm saying that we should get inspired by this and add this as a driving lesson to shed some light in this discussion. Next slide, please.

So I guess some time people say, “Oh, name collisions. That's not really a big deal.” So I have a little cartoon here that is going to drive you through a scenario of how end users can be impacted by name collisions. Next slide, please.

So there are two characters in this story. There's John. He's a techie. He's a geek. And there's a Sally, his girlfriend. She's also a bit of a geek, but not as much. And there's a third player, of course. It's called Market.

So John says, "Oh, I want a new domain name. I want to impress Sally. Maybe I can use a blockchain name. Market, do you have something cool to sell me?" And Market says, "John, I can sell you this domain john.cryptonite. Do you want it?" So John's buys it. Next slide, please.

And it goes to Sally. "Sally, connect with me. Here's a new name, john.cryptonite." And Sally tries it, of course, and it does not work. Next, please.

And John explain, "Oh, I forgot to tell you, Sally. You first need to install this very cool web browser." And Sally says, "I've never heard of it. Is it safe?" Next.

A little bit later, John the geek says, "Oh, I found this other blockchain. There's a lot of cool stuff there. Wow, cool. Maybe I can ask Market if I can get a new domain over there, too." And Market says, "Sure, John. I can sell you john.superblockchain." Next, please.

Of course, John goes back to Sally and says, "Hey, Sally. I have yet another name and very cool stuff there for you to try. Look, john.superblockchain." Sally says, "John, I installed your special browser that you told me last time, but now it doesn't work with your john.superblockchain. I'm not happy." Next.

“Sally, oh, I forgot again. This is a different blockchain. You need to have this other browser and there's also a plugin that you need to download.”

“Oh, go away,” said Sally. Next, please.

A little bit later, Sally goes back to John and says, “John, I eventually followed all of the steps you gave me and now I can reach you at this john.superblockchain. But when I go back to the first one that you gave me, this john.cryptonite, I don’t see you. I see my ex-boyfriend’s profile.”

“What! I have not done anything,” said John. “Look, look.” He shows his phone. “This is my profile.” So the two of them see different things.

And John goes back to Market. He says, “Sally is unhappy. How come she and I see different things when we type john.cryptonite?”

“Well, this is called name collision,” says Market. “Cryptonite is popular. There are three different blockchains that are using it. And your computer and hers are not set up the same way, so you look in one namespace and she looks in another. No wonder you see different things.” Next, please.

“But how come john.cryptonite is not unique?” And Market says, “You see, nobody guarantees those names are unique. And by the way, there's also john.cryptonite in a third blockchain naming system. Do you want to or should I offer it to Sally's ex-boyfriend?” Next.

And, of course, John is very unhappy. “This is stupid. I'm going back to my old john.icann TLD domain name. At least this one was unique.”

And Market says, “You cannot escape name collisions. See? .icann TLD is now available in five alternative naming systems. Maybe you should create your own naming system.” And John says, “Market, you’re a monster. The Internet is not broken.”

Thank you for indulging me with this cartoon with some light humor. I tried to show what can happen to regular users when they are faced with name collisions.

ADIEL AKPLOGAN: Thank you very much, Alain. And for ending on that nice note of the cartoon. I think this sets the scene a little bit. And from your presentation, I can highlight three key point. The challenge of resolution interoperability. This is not guaranteed with what we're seeing today. We have the user confusion that is well-illustrated by your cartoon. And all of that, the underlining elements that can drive us to fragmentation of the DNS at first, and the Internet globally.

So that being said, we'll move to the next presentation before we take the questions around this for the first part of the session.

So Luc, I will give you the floor. You are from ENS. ENS is one of the alternative namespaces, of course. And I’ll give you the opportunity to share with us what you are doing there. Thanks.

LUC VAN KAMPEN: Okay. Can everybody see me? Hear me? See my screen? Cool. All right, let's see if I can do this. Good morning, afternoon, and evening, whenever and wherever you are. Whether you're joining us in person

here—and, my, we have a turnout—in Kuala Lumpur or virtually through Zoom. Thank you for being here and thank you for your time.

As stated, my name is Luc van Kampen. I'm here today to talk to you about the Ethereum Name Service. The Internet is evolving every day. We are here, after all, maintaining it. In 1989, ICANN was founded to bring clarity, order, and logic to the fragmented, chaotic Internet.

In 2004, we had the breakthrough of social media centralization. An estimated 80 million websites were live, serving to a total of 1 billion different users. Later, we decided to coin this the Web 2.0 era. Today, we see 5 billion users on the Internet, approximately 63% of the total population. And with that, the world is changing rapidly. And with that, authentication is as well.

Slowly we're seeing a shift—actually, rather rapidly—we're seeing a shift from password-based authentication towards public key authentication. Public key authentication is not something new. We already see it happening in technologies you use every single day—HTTPS, SSL, PGP, and most importantly of all, DNSSEC. There's obviously many more.

So how does this affect authentication? Authentication and public key authentication aims to solve a lot of issues. Here's a couple. Insecure passwords, password leaks, mass account hacks, and name availability are issues that, using public of public key authentication, their days are limited.

So let's look at that last slide from the previous presentation with the ICANN social media on it. Right. Here are just some of them. We have

@icann, @icann, @icannorg—because the ICANN Facebook is taken by a person called [Ican N]. The @icann Instagram because the ICANN Instagram is an empty profile. The @icannnews YouTube channel because the ICANN YouTube channel is videos of dogs. ICANN photos on Flickr and ICANN on SoundCloud. And most importantly of all, the source of truth, the ICANN website.

So public key authentication solves a lot of these issues. Most notably, users have a public key and private key key-pair. The public key is used to identify them on the Internet. It looks about like this one. This is mine, in case you were wondering.

And the private key is stored on their local device. It never leaves the local device. The beautiful thing about this is that users can now use their local device to sign in. It's one tap. To confirm a message, one tap. Confirm an action, a bank transaction, a message—something along those lines—or sign a message and prove that they were the original author using their favorite biometrics, face ID, PIN code, password, or OTP which is completely on their device and local.

So public encryption from a security perspective is awesome because it provides practically unbreakable security. We would need infinite computing resources for an infinite amount of time to take over a message.

Public encryption, scalability wise, is amazing because we don't need servers anymore to keep track of usernames and passwords. It is simply done on device and we use the public key as the user identifier. From a machine readability perspective, it's amazing as well because the

length is set. We use a fixed character count. The character set is exactly set, predefined, etc., as well as more information.

And last but not least, human readability. This is human readable, but I'm going to be dead serious with you. I might enter this into a website once and then I'm never going to want to do that again. It's too long. It's 64 characters. So from a human readability perspective, it's a bit meh.

And this is where ENS comes in. ENS is the Ethereum Naming Service. ENS aims to integrate public key authentication with the already existing Domain Name System. This means that anyone with an existing DNS could use their domain as their identifier anywhere across the web.

Remember this slide from a few seconds ago with the different ICANN ones? That could simply be this—icann.org—everywhere. And that little lock I added, little cute lock emoji, to signify that every single message, every action ICANN will take will be signed off and authorized. This could be by a single user with a single device or multisig, meaning that multiple people will have to approve any action ICANN takes publicly on the Internet. It adds security.

So who am I? This is me, as I stated before. Actually, this is me—luc.computer. A domain that I registered with a registrar. And I've set it as my primary name using ENS. Any of the websites that I visit will have this available. Provided they support ENS, I can see luc.computer.

If you look it up—you go to a search bar, you type in “luc.computer”—you will find me. You'll find 0x225 ... and the whole shebang. What does that look like? It looks like this. This is the top right corner, the user

profile section—or the top left corner if you use an RTL layout—on the ENS website. Like this on the Uniswap website. And like this on the 1inch website. And on edge server. And obviously, many, many more.

Actually, at this very moment, 2.4 million names have already been connected through ENS, spread out across 600,000 different users and available and usable on over 1,000 different websites.

So how does this exactly work? Seeing as I only have 10 minutes and my time, thereby, is limited, I'll try and keep it short. ENS, the Ethereum Name Service, is built on top of the Ethereum blockchain, a public ledger that allows us to store information and keep track of information and the history thereof in a decentralized and permissionless manner.

Ethereum utilizes smart contracts. ENS is a set of smart contracts which are essentially code and logic stored on the blockchain, written once, that are a set of predefined rules that decide how data should be handled, what actions should be allowed, and what we should do with it. This allows us to store all of the information on the blockchain.

So what does that look like? Super simple. This is one of the smart contracts. It could store my name (my domain name), my public address which is what I use anywhere across the web for authentication, and obviously extra information: a pointer to another resolver, other place where I could host my information—my name, my avatar, my banner, my bio, or maybe my Telegram or my LinkedIn or my Twitter. And obviously much more.

But this is the core essence. We at ENS envision a world where everyone can use their domain as a universal identifier. Any valid DNS domain ...

Okay, any valid DNS domain, provided that it supports DNSSEC is a valid ENS domain. That means that you can go to any of our smart contracts and submit your DNS domain as well as a claim proving that you own it, and the smart contract will then reach out to the DNS server, provided it supports DNSSEC, do a TXT record verification, and say, "Okay, yes. Luc does, in fact, own luc.computer." This then gives me permission to edit my records.

Ownership transfers, as well, are handled similarly. If I decide for some reason to sell luc.computer to another individual and I make the change in my registrar accordingly, then the new individual who now owns luc.computer can go out there, reached out to the ENS contract and say, "Hey, I'd like to claim this name. Here's my proof." The ENS contract will do the validation, and the new owner will be set.

So in addition to the above and as previously mentioned, we do provide an on-chain registry. This is done on the chain itself, and this is provided for blockchain users. Specifically, this is done under the .eth TLD. This is the only—[and limits thereof]—TLD we provide. This TLD enables us to do more things than ICANN simply can.

It allows us to host decentralized websites. A whole other story. Essentially, website users can visit without needing to contact a single data server, a single web server centralized somewhere. No more DNS routing and localization and doing all sorts of fancy infrastructure and running entire data centers. Simply host your website, and any device that loads it will immediately become a cache and load it for other users. Data locality, worth a whole other talk.

In addition to this, .eth domains have registration fees. This is obviously done to prevent spamming, prevent hoarding of all of the names, and make sure names are still available. These are set to $5 a year. This is a reasonable amount. As per defined, the Dow has control over this. A reasonable amount so it's not enough for somebody to suddenly purchase all of the names available.

All of the registration fees from .eth domains go directly to the ENS Dow, a non-profit organization that utilizes these funds to fund public goods and other open-source systems. The Dow, by the way, is a decentralized autonomous organization, an organization run in a very similar model to ICANN's multistakeholder model. We are completely transparent, publicly governed, have working groups, requests for proposals, stewards, and much, much more. And most importantly, anyone can participate.

So, why? I hear you asking. What is the motivation behind this? Allow me to explain. We are a collective of open-source, public good developers and contributors who care to make a difference in the world. We're funded ... Development on ENS, specifically, is funded by the ENS Dow and done through proposals.

Every year, we put in a proposal stating the amount we need, the amounts that will go to salaries, the amount that will go to transport or those kinds of things, marketing, accounting, etc. And the ENS Dow then votes on this proposal and decides whether or not it will happen. In the event that we, as the ENS development team turn malicious or have other means or have a dispute, the Dow can step in and make other decisions or appoint other people.

So in contrary to any other naming system or the naming systems previously mentioned, we aim to extend and improve the current DNS's functionality with today and tomorrow in mind.

I think in a minute, after the next talk, we'll have some time for questions. If you have a question or your question does not get answered or you have a question afterwards, you can always reach out to me at luc.contact—another domain. Thank you for your time, and I look forward to the great things we can accomplish together.

ADIEL AKPLOGAN: Thank you very much, luc.computer. So this is an interesting presentation, indeed, and shows us what ENS is doing. And in fact, what is interesting there is the use case of this alternative naming system that is different from the DNS as we know it today.

So before we move to the last presentation, I will make a pause and actually go out for questions on these two presentations that are very related for about 15 minutes before we move to the next presentation. So I will open the floor.

Do we have any question online? Maybe we'll start from people following this online?

DAVID HUBERMAN: Yes, Adiel. We do have one question online. The question is from Ajith Francis. It is for Luc. It is a two-part question. Luc, the first part is, "Does .eth's switch from proof-of-work to proof-of-stake model have any impact on the accessibility and decentralization for ENS?" And the

second question is from an end user perspective. “When can seamless integration between name servers and ENS domain names be possible or expected? Or is this is not an objective?"

ADIEL AKPLOGAN: Thank you very much, David. Luc.

LUC VAN KAMPEN: To address the first question, it is not in relation to ENS. It's in relation to the Ethereum system as a whole. Recently, Ethereum swapped from proof-of-work to proof-of-stake, reducing energy usage by about 98%.

This means that with the community push and the requirement for a consensus for changes to be made to the Ethereum network, many new updates from the Ethereum core team can be pushed out in the future improving gas fees, registration costs, etc. Although this only minorly affects and can improve the lives of those using ENS, this does not really affect the ecosystem too much as a whole. We were running smoothly before and we're still running smoothly after.

To address your second question, when we can expect seamless integration? It's a bit of a tough call. Currently, we're seeing thousands of websites being developed in the Web3 ecosystem, utilizing public key authentication, and all of these great wallet apps you can use to connect to websites.

As previously mentioned in the presentation before, there are still a lot of issues. The major ones are integration, obviously. As long as ENS does not get implemented at a DNS level or at a root zone level,

seamless integration does require user manual interaction. This means that you'll have to install an extension, use a compatible browser, or use one of our public resolvers hosted by us or by the community.

I hope that answers your question.

ADIEL AKPLOGAN: Thank you, Luc. Any questions in the room? Yes.

BEN MCILWAIN: Hello. Ben McElwaine, Google registry. What would happen if, in the next round of the TLDs released by ICANN, somebody applied for and got .eth for real, like in the DNS root zone? Doesn't that kind of ruin everything? Like, it would cause unimaginable levels of collisions.

LUC VAN KAMPEN: Yeah. So as previously mentioned, name collision is a very difficult situation. There are currently other parties out there that are trying to register an enormous amount, or even auction off TLDs which does not really match with the ENS philosophy.

In the event that ICANN would give out the .eth TLD to another party that is not Ethereum Name Service, that would and could be detrimental to the ENS ecosystem. Yeah, for sure.

But we hope to obviously make sure that doesn't happen and that we can do as much to support and make sure that everything stays available and working, for sure.

ADIEL AKPLOGAN: So should I understand that you're planning to apply for that TLD?

LUC VAN KAMPEN: That is something I cannot say for certain, so you'd have to ask the core team.

WARREN KUMARI: Hi. Warren Kumari, SSAC. I will just note that according to the last Applicant Guidebook, there is no way that Ethereum could apply for .eth because there's a whole bunch of requirements that simply cannot be met, like be able to escrow your zone file. If you don't have a zone file, you can't do that. That's obviously according to the last Applicant Guidebook. I don't know what the next one might be like.

LUC VAN KAMPEN: Yeah. So I think in the event that we do get the .eth TLD, it is very possible that we set up a separate service because, to some extent, the DNS and the ICANN naming system requires a central IP to be available. And we cannot simply start messing with BGP zones and cause global outages.

So what would happen there is we could, in such a hypothetical situation, set up services ourselves that users can opt into to make their domain available over the DNS. This would require manual user intervention on the domain owner's side. So if I register [inaudible].eth and I would like that available over DNS, you would have to go through

the ENS website, opt into that. And that way, we can make sure that they can still comply with all of ICANN's requirements to that extent.

ADIEL AKPLOGAN: Thank you. John.

JOHN CRAIN: John crane, ICANN CTO. So technology is really cool, really interesting. No doubt about that. So ICANN, the organization I work for and what everybody is, here with the multistakeholder community, discussing is as much about policy as technology. So I was wondering what kind of safeguards and norms you are putting in place to deal with, shall we say, misbehavior and harm that are used within these names? What are you doing about security threats that would use the namespace?

LUC VAN KAMPEN: So essentially, within the current implementation of the Ethereum Naming Service and the extensions that implement us and the integrations we have, domains are unable to be revoked or removed under any circumstance. However, if we were to run a gateway, that would forward the DNS records for the .eth TLD. Then we can definitely implement those things and we can make sure that they happen, as well as to direct it to [where, with] the previous question, make sure WHOIS records are available—although deprecation—etc. So, ICANN compliance.

JOHN CRAIN: So if I understand correctly, under the current solution, if I'm a criminal and I register a name and then I get one in your space, I'm pretty secure today. I'm not going to lose my name.

LUC VAN KAMPEN: Under the current system, everything under the Ethereum Name Service and any domains registered through the .eth TLD are completely censorship resistant to the extent that it would require a 51% consensus on either the ENS or the Ethereum level to be able to revert changes.

ADIEL AKPLOGAN: Thank you. Well, we'll move to the next presentation, and if we have more time at the end of the session, we'll come back to further questions. So Jacques, I'm going to give you the floor so you can share your presentation with us, which is about digital identity and emerging identifier technology.

JACQUES LATOUR: Hello, everybody. Can you hear me okay? All right. So I'll try to do this quickly. My name is Jacques Latour. I'm the CTO at CIRA. We run the .ca registry. And over the last year or so, I've been working with DIACC here in Canada—the Digital Authentication and Identification Council of Canada—working with Digital Lab of Canada and trying to work with the digital identity community in Canada to understand more about the challenges that we're facing. And it's about trust.

But today, that's the topic of my talk. In the world of issuers—digital identity—it's a driver's license that's digital, that goes in the wallet. I'm not going to talk about anything today about wallets and all of the naming in the back-end on wallets. I want to talk about the ecosystem. So we have issuers that issue verifiable credentials. Those are digital credential that are sent to a wallet. The wallets store those just like your physical driver's license, except they're digital and they're signed by the issuer. And then there's verifiers.

That's how the ecosystem works. And it's all digital and people selectively present parts of their verifiable credentials, and then it gets verified. So this could be from a driver's license, university diploma, and all of that.

So if we look at a real case scenario, CIRA. We have a Canadian presence requirement process, for example. So for some domains, we need to verify that the nationality of the registrant is Canadian or they live in Canada. That's all we need to check to meet that requirement. And today in the real world, they send us copies of passports and driver's licenses and birth certificates. And we don't want that.

So in the digital world, you would have the Canadian government that would issue a digital, verifiable credential for driver's license, birth certificate, passport, for example. Each one of those are signed by the issuer, and the issuer has a .ca domain name. All of the issuers have a .ca domain name that people know and trust in Canada, or they think they trust.

So, verifiable credentials are signed. They go into a digital wallet. And then part of the process would be ... We have CIRA. We're a verifier. And the registrant would just provide us enough information to prove that they're Canadian or they live in Canada.

But the big question is, how do we know the issuer is trusted to issue those verifiable credentials? How do we know it's the Quebec driver's license and not a fake driver's license ? How do we know the wallet is trusted to hold credential? So a passport shouldn't go in every wallet. The passport would go in certain wallet. And then the verifier. Is CIRA really CIRA? And are we allowed to ask for certain information?

So there's a lot of trust issue around that ecosystem that needs to exist and needs to be verifiable so that people can actually make this ecosystem work.

So the answer is trust registry. So a key component in the picture, there's a trust registry. And in there, it can be used to verify that the issuer is authentic. Luc was talking about public keys. So the public key is actually from the Canadian government. It actually matches what's in the registry. And then the registry has rules to say, you know, this issuer is allowed to issue that kind of credential. So with the trust registry, the participant in the ecosystem can verify that the parties are who they are.

So that's the framework that's architecture for the system. The challenge is, the trust registry has not been well defined so far. So Trust Over IP, as a definition of a trust registry, is like a repository or a

directory or a hub of registration that are alike within a governing authority and a framework.

So an example of a trust registry is academia or Canadian universities. That would be all of the universities in Canada that are allowed or accredited to issue certificates and diplomas. So trust registry would have maybe 75 entries in Canada, and these would be all of the entities that you would trust to be in that registry. In Canada you would have, for example, hundreds of trust registries.

And that's the challenge we're having right now in the digital identity community. Do we have one trust registry? Do we have tons of trust registries? How do we know which trust registry is what? How do you trust other trust registries? And then if I'm in Canada, how do you trust the Poland academia trust registry? How do you know they are who they say they are?

So today, a lot of people are building walled garden digital identity ecosystems and it makes it hard for government participants to trust this trust registry because they're missing something from a hierarchy here.

So when I first started looking and reading on self-sovereign digital identity, all of these things, the first thing that came to mind is, there's no unique identifier. So we just saw in all of the discussion that people can create their own domain, their own identity. You could have the Quebec government, presumably, in a different blockchain. So there needs to be a global, interoperable, identifier structure in Canada. You

need to have unique identifiers for credential. Otherwise, if credentials are not unique, then you can't verify them. It doesn't work.

So I think at a start, we could use the DNS for fundamental, verifiable credential issuers. So national ID card, driver's license, passport, health card. That could be the fundamental layer. All of these entities today have domain names in place.

And then we have DNSSEC today. So DNSSEC [inaudible] trust from the root all of the way to pretty much every ccTLD around the planet. And then so we could have unique DNS. So if we have a global trust anchor, we have global trust registries, country code national, we end up with a structure that looks like this. So we could have ... Wait. My little Zoom window's in the way.

So you could have a global trust anchor in the root zone. From there, you could have, inside ICANN/IANA, a global country code trust registry. So that registry would have all of the ccTLDs or all of the country code trust registries in the country. And then in there, you can have the Canada trust registry.

And then inside the Canada trust registry, you could have what I call national trust registries. Those would be the university, the plumber's association, all of the different organizations that need to have their ecosystem. And then every country could have their own structure. And you can have same thing on the commercial side.

So what that provides is a unique identifier structure. Something that is missing in all of the stuff I see when people issue credentials in a sovereign blockchain somewhere, there can be multiple blockchains

and ledgers. And you don't really know where to go to verify these things. That's everything aligned. [And, look, what we're] talking about is the proliferation of blockchain and ledger. It makes the unique identifier not unique in the digital identity world.

So this is not for wallets. This is for issuers to have their credential in a way that can be unique. And it allows the verifier and the wallet holder to verify the information according to a unique structure.

So there's maybe more to this is in DNSSEC. With DNS and DNSSEC, we're looking at building mechanisms in the ENS to find the trust registries that are associated to an issuer, a verifiable credential issuer. And then we can find if that issuer is registered with a trust registry. And then you can find digital identity document (DIDs) from a domain name.

So the DNS is distributed, decentralized, and scalable. I think it's the right platform to register... It's the right platform to map the digital identity identifier in a unique way to ensure uniqueness and global interoperability.

So at the DNSSEC session earlier, there was a presentation that was done about an hour ago or two on the DNS/DNSSEC. More technical on the details on how to make this work. So that's it.

ADIEL AKPLOGAN: Thank you very much, Jacques. And this is an example of bringing digital identity using the DNS and a decentralized feature to manage this. This is complimentary to the topic we talked about before, but using the DNS.

We still have a few minutes, so I will open the floor for a few questions, if there are, for Jacques, on this interesting application of digital identity to the DNS.

GABRIEL KARSAN: Hello, question. My name is Karsan, Gabriel from Tanzania. I'm an ICANN Fellow. These are emerging technologies, but from a global [inaudible] perspective, I want to know what is the inclusion strategy? Because I'm hearing a lot of user confusion, and we come from regions where even operators do not have a lot of resources or the knowledge base to understand DNSSEC. And it's a mandatory prerequisite for you to access digital ID.

Even though it's brilliant, good security and everything, but connecting the next billion will really come from the Global South where people do not have the literacy of understanding decentralization or DAOs. And I think it is within the Ethereum philosophy to bring more people, to bring the new vibe of young people who actually understand and can leverage this decentralized, or rather emerging technologies to bring change because it's more of a democratic way of representation.

So my question is, rather, are you really catered to only a particular type of stakeholder? And how would you really improve inclusion and diversity to actually include the people from my region? Thank you.

LUC VAN KAMPEN: Thank you. I think it's very important to note that the ENS Dow votes and is in control of the ENS ecosystem. And with that, that means that

any and all participants, thereby shareholders of ENS Dow, anybody could join in and participate depending on absolutely nothing. There's no prerequisite—no race, no religion. There is no discrimination to that extent. No income, no origin, no nothing.

What that means is that our token distribution at this point in time, are those who have governance rights, has been a small percentage, is the core founders. A large percentage is given to the Dow itself to distribute to community projects. So if a project builds on top of ENS or promotes the ecosystem or works on the ecosystem, the Dow can vote to allocate tokens to that project and give them more governance rights.

And we have a large portion of our tokens were initially distributed across early ENS registrants. So late last year, essentially what we did was we took everybody who registered a domain and we distributed the tokens among them. Which means that currently, I think our largest stakeholder is 8%. And then after that, it's all 6%, 4%, 4%, 4%, 4%, 4%. Which means that, essentially, there is distribution of representation.

And anybody, regardless of any form of discrimination, can participate—regardless of what country you're from or what its GDP might be, etc.

GABRIEL KARSAN: Okay. This is a simple question. But for me to get an account, I need to have an operator or a domain name that is signed by DNSSEC. Is that correct? What if I come from a region where I have partially signed or I haven't really had the compliance to have DNSSEC?

And the other question, are you doing any engagement or outreach program at a very low level where you can include more people who don't have an understanding of these emerging technologies?

LUC VAN KAMPEN: Yeah, thank you for your question. So what we're doing is ... Obviously, the Dow token distribution, etc., and governance rights. If the domain does not support DNSSEC, users can always register a .eth directly on-chain. And that is without requirements of registering under a DNSSEC-supported TLD.

In the event that a domain does not support DNSSEC ... Which currently an amount of TLDs definitely don't because they are not bound to ICANN gTLD policies, for example, because they're ccTLDs, etc. That means that a user would have to register under another TLD that does support DNSSEC or they are not able to use the ENS system.

But they can still participate in all of the technologies that are out there. However, instead of showing the domain of their choice because they do not have one, their account would simply show their wallet address—so their public address, their public key.

When it comes to outreach, the Dow tries to allocate a certain percentage of funds every year to outreach programs to making sure that everybody is properly educated. And part of my function as well at ENS is to essentially go to all of the regions out there that are interested in these technologies and where we could aid.

An example of this is about two weeks from now, I will be present at the Ethereum Foundation's Devcon event in Bogota, Colombia, to talk to the local community there and to talk about the state of the union of the ENS network and what ENS can do and how that affects the people there.

I hope that answers your question. If it doesn't, then you can always reach out to me.

ADIEL AKPLOGAN: Yep. Thank you very much, Luc. Interesting. We are running out of time. Usually this emerging identifier session at the beginning of the discussion around this topic, the topic are usually very, very burning and interesting. But we would like to encourage you all to go to ... Yeah, we are running out of time. I'm not sure if we can still take a question.

But what I want to say is that we have received the special interest forum online. And one of the reasons we have them is to be able to take the discussion that we have during the Emerging Identifier Technology session at ICANN and continue them online so that we can dig further into the presentation exchange with the presenters that are on the mailing list so that we can have more discussion beyond the one hour or one hour and a half that are usually assigned to this session.

Carlos [inaudible].

[CARLOS ALVAREZ DEL PINO]: Thank you so much, Adiel. Really quickly. ICANN's public safety engagement, a very specific question. How do you deal with legitimate

and fully-legal requests from law enforcement regarding [inaudible] information behind the people that register malicious ENS domains?

ADIEL AKPLOGAN: Can I suggest that we talk to you, Carlos, right after the session? Because we have to close and wrap up this session? Thank you very much, Carlos, for the question.

[CARLOS ALVAREZ DEL PINO]: Right. Thank you.

ADIEL AKPLOGAN: And there are a few other question on the chat room as well about intellectual property and squatting names on ENS, etc. So thank you very much. Very interesting and informative session. And I'll see you all on the [inaudible] mailing list. You can have information about the [inaudible] on the ICANN Wiki. Thank you.

[END OF TRANSCRIPTION]