COPENHAGEN – Emerging Identifiers Technology
Tuesday, March 14, 2017 – 11:00 to 12:30 CET
ICANN58 | Copenhagen, Denmark

UNKNOWN SPEAKER: Audio test, one, two, three, four.

UNKNOWN SPEAKER: Welcome everybody. Have a seat.

There are still few chair around the table, so if you are at the back and you want to join us on our only table, feel free to do so.

So, welcome, again, to this session, which is a panel on emerging identifiers technology. Before I start, a few logistic announcements. Unfortunately, the chat for the remote participation is not working for this session. We have to close it for some technical reason.

So, unfortunately remote question to the chat room won't work. But the rest of the session is being streamed on Adobe Connect channel. So, our session today is mainly an awareness session. It's follows some constant and continual requests we get from the community about some of these technology, about what we know about it.

So, we feel like it's may be interesting to hold a session here, and invite a key actor of those technologies to come and explain to

the community a little bit how it works. And we have organized in the way that we have time as well to interact with you, so we will have a Q&A session after the presentation.

So, with me on the panel today, we have Jeremy Rand from NameCoin. We have Alexis Tamas from Frogans Technology. Christophe Blanchi from DONA Foundation, and Alain Duran from ICANN, the research team at ICANN.

Each of them are going to give us a brief presentation, 10 minutes, and then we will move to the Q&A session.

Steve is helping us from a presentation. So, the first presentation will be from [inaudible]. So, we will start with Jeremy Rand from NameCoin. Jeremy, the floor is yours.

JEREMY RAND: Okay. I'm Jeremy Rand from NameCoin. This presentation was co-written with Hugo [inaudible]. So, let's get started.

So, the underlying motivation of NameCoin is that humans behave non-deterministically, and that means the systems they operate behave non-deterministically as well. And this includes things like the DNS. Maybe your registrar makes a mistake and lets someone else change your records, or maybe the government who owns your ccTLD. Maybe 10 years from now, they get overthrown and the new government decides to seize

your name, or maybe in the future political pressure causes ICANN to implement a new policy, in the future, that you didn't really agree to.

And any of these could happen and poses a risk. And so, if DNS weren't run by humans, it would be a lot easier to make reliable predictions about the DNS's future behavior. So, the underlying motivation of NameCoin is basically an experiment to find out, can we make something that's similar to the DNS, but with as little human involvement as possible?

And the hope is that behaving more deterministically then the DNS, this might be more reliable and secure against a lot of security issues that are caused by humans. So, let's look at some existing identifier systems so we can see how NameCoin differs. Manually naming at a site, things like Host Files, they don't have a global name space, so the names are only meaningful locally, but they are safe from non-deterministic human third parties, and they have human meaningful names.

So, that's good. Hierarchical naming, such the DNS, has a global name space, but it's not safe from non-deterministic human third parties. It does have human meaningful names. It's very good usability, but it's risky as a route of trust. So, in addition, there are identifier systems where the name is the public key. These are things like the dot onion domains that Tor uses.

These have a global name space and they're safe from non-deterministic human third-parties, but they don't have human meaningful names. So, they are safe as a root of trust, but the usability is very poor. When a user types [inaudible], they see something like this. Actually, I'm lying. Tor is doing a security upgrade. When they're finished, it's actually going to look more like this.

So, yeah. You might have noticed, in the slides I just presented, there are two checks and one X. This is something called [inaudible] triangle. [Inaudible] Wilcox conjectured many years ago, that it was impossible to achieve all three of these at once. So, NameCoin is a pluck chain for name registrations and updates. And it's a counterexample to [inaudible] triangle, it actually does achieve all of these properties at once.

Global name space, safe from non-deterministic human third parties, and human meaningful names. Shifting gears slightly, a related problem is the TLS public key infrastructure, which is used whenever you're accessing a HTTPS website, for example. The certificate authority used right now is problematic, even with certificate transparency.

And this is fundamentally because there are way too many non-deterministic humans involved, who might make mistakes. There is a proposed solution called DANE, which validates TLS

certificates using DNS. This could be an improvement. The problem is that the DNS root and the TLD operators are still non-deterministic humans.

So, this still isn't ideal. And NameCoin could provide the advantages that DANE provides, without relying on those non-deterministic humans. NameCoin is designed to interoperate with DNS as much as possible. It has a DNS compatibility layer that can translate DNS requests into NameCoin requests, and this means that in theory, at least, installation is relatively simple.

You can just install NameCoin and the compatibility layer on your machine, and the applications that you have that speak the DNS protocol, will work with NameCoin mostly out of the box. So, this means that you don't need to change all of your applications to be able to use NameCoin.

And NameCoin is using the dot bit top level domain. This is not registered with ICANN or IETF right now. And we realize this is a problem, and we would like to find a workable way to get it registered, for example, as a special use name, the way dot onion was registered by TOR.

So, what are some real world use cases, where NameCoin's deterministic behavior can help? Well, let's say that you're trying to buy or sell a name. In the DNS, buying or selling a name

usually involves some counter-party risk, and you may have to rely on some third-party escrow agent in order to mitigate that counter-party risk. In NameCoin, the buyer and the seller can jointly construct a single transaction, that automatically pays the seller and transfers the name to the buyer.

And this means there is no counter-party risk, and you don't need some third-party escrow agent services. Another very interesting use case is two-factor authentication for updating your DNS records, without needing to fully trust the two-factor authentication service. And for example, you could set a policy sort of like this, making arbitrary name updates requires two [inaudible] verification, however, you can revoke your TLS certificate records, TLSA records, even if the 2FA service is down.

So, the 2FA service can't force you to keep using a compromised certificate. If the 2FA service vanishes, you can still recover your name by just waiting a given period of time, after which the 2FA service's signature becomes not required anymore. And in addition, the 2FA service can't issue any updates whatsoever, without your consent. And this is all cryptographically verified, and the policies are specified in a reasonably flexible scripting language, so you can customize things according to your needs.

Unfortunately, in order to have this determinism, we need to make some trade-offs. For example, if a name is transferred to a

new owner, the old owner can't get it back without the new owner's signature. And this means that NameCoin names are somewhat more vulnerable to hostile takeover by malware.

Some workarounds would include storing your private keys on a [inaudible] machine, or just use two-factor authentication, as described earlier. Another tradeoff, is that deterministic systems like NameCoin, don't have a way to detect trademark infringement. And that means, if you have rightful ownership of some trademark, someone else can register the name for it, and you'll have to negotiate with them.

As a work around to disincentive this, users could opt into black lists such as fish tank, to detect fraudulent websites. Another tradeoff is privacy. NameCoin transactions are public. That means anyone in the world can easily see whether multiple names have common ownership. And this could be very problematic for privacy.

In addition, the person who sold you your NameCoin tokens that you use to register names, they know which names you registered with them. We don't have any good workarounds right now, but for future workarounds, we are collaborating with [inaudible] privacy projects, like [inaudible], to give better privacy in the future. But for now, if you really need good privacy, you shouldn't use NameCoin.

The last tradeoff is something called a 51% name attack. If you're already familiar with Bitcoin, then you already know what this is. If you're not familiar with Bitcoin, you can picture NameCoin as a voting system, where instead of one person, one vote, it's one CPU, one vote. As a result, if an attacker somehow manages to hold a majority of all of the computing power, on the NameCoin network, for a long time, something like months, then they can use that to steal names. This is a very expensive attack to pull off, but it's much cheaper than directly attacking the elliptic curve cryptography that NameCoin uses for the rest of its security.

A workaround here is that the attack is easily detectable in real-time. So, users could blacklist the hijacked name automatically, if a name ever did get hijacked this way, which would decrease the incentive to do it in the first place. And we are also investigating other ways to raise the costs of such an attack.

In terms of direction of development, we're focusing again on making NameCoin easier to use, because for average people, the installation is not sufficiently automated, especially if you want TLS to work, which you should because HTTPS is more secure than HTTP. We just received funding from the [inaudible] Foundation, and the Internet Hardening Fund, with budget from the Netherlands Administrative Economic Affairs.

And this funding will be used to improve usability and application support for NameCoin's usage as a TLS public key infrastructure. And the four people doing most of the work on this, are me, Hugo [inaudible], Brandan Roberts, and Joseph [inaudible].

So, thank you for inviting me. I'm happy to take questions when the Q&A rolls around, which if I understand correctly, is after all of the other talks. So, thank you.

[APPLAUSE]

UNKNOWN SPEAKER: Thank you very much. Wonderful. We will move directly to the next presentation. Keep your question handy, and we'll come back to this a little bit later. So, the next presenter is Alexis Tamas from Frogans Technology. So, Alex is one of the co-founder of the technology and everything around it. So, Alexis.

ALEXIS TAMAS: Okay, thank you. Hello. So, my name is Alexis Tamas. I'm a co-founder of the Frogans project, which is an initiative to develop a new software layer on the internet, to publish content. And I'm here to talk about Frogans' addresses, because this system requires new kind of identifiers, and we are going to tell you more about that.

And the fact also, that this new identifiers enable a new security model for publishing content. Well, so… Okay. So, the Frogans' technology, is a secure technology for the publishing of content on the internet. It enables the implementation of a new software layer on the internet, called Frogans' layer alongside the other existing software layer such as, email [inaudible].

Frogans' technology comes with a new type of online content, called Frogans Sites. They are not websites as you can see later on. And the new software, and there is also a new software to navigate [inaudible] Frogans player.

And as I said earlier, there are new identifiers, [inaudible] identifier for those sites called Frogans addresses. Frogans addresses were designed at the very beginning of the project. It was 17 years ago, with the following goals. They had to be short and simple. They could not contain any technical information. They had to clearly stand out in various contexts, and they had to be original so that user could easily distinguish them from other internet addresses.

At that time, we did not choose domain names and URIs for as the naming system, because we could not directly achieve these goals, without changing or modifying some schemes or syntax in that. So, moreover, the GNS technically could not be used to resolve Frogans' addresses, given that the size of the data that

we had to look up was bigger that what we could, what the GNS could afford.

So, and that site could increase also in the future. However, I would mention that right now, Frogans' layer requires DNS to function in order to address two kinds of servers. The first one is the resolvers, the Frogans' address resolvers. So, the computers that are used to resolve Frogans' addresses, and actually, I will tell you later, they are running, they are named using the dot Frogans TLD.

I will go back on this later on. And we also need the GNS for addressing the computers that hosts Frogans' sites. And that comes with any gTLD or any ccTLD for that. So, as I told you, the [inaudible] the non-profit organizations, which holds, promotes, protects, and show the progress of Frogans Technology, to apply to operate the dot Frogans' TLD. The objective for this TLD was to ensure, and is to ensure the security, stability, and reliability of the Frogans layer for the benefits of all internet users.

And the dot Frogans TLD domain names are only used to address a computer, as I mentioned. And two extra websites, one for [inaudible] and one for accessing the addressing services. The key benefit in using a TLD instead of a second level domain, is to again, maximum control over the registration

process and resolution of these critical domain names, because the whole system, the whole new layer relies on that TLD.

So, on that domain. So, it was really important to have maximum control there. Then, why bringing that kind of addresses, we could also enable, by this means, enable a new security model for online publishing, which is based on five inter-related components. First, I will mention quickly the Frogans' address pattern, then the existence of a registry for Frogans' addresses, then the resolution process, and after that, we can discuss a bit on what kind of settings are related to the address, and how it can help and benefit for the security of end users.

Of course, this security model was developed by taking into account extensive work done by the community, and especially IDNs, and DNSSEC, and DANE, there are many concepts there, that were very help to design the solution.

Well, so that my last two slides before the demo, because I want to show you some Frogans sites. So, from the… About the Frogans' address pattern, the pattern is written here. It's a network star nigh, network name star site name. It's a two level name space. The asterisk separator or character is used, so there are no dots. The only specific character is the asterisk

character. It supports Unicode, so you can also have right to left writing systems.

We have developed within the pattern specific rules for ensuring security, but identifiers especially from the IETF and the Unicode consortium. And all this is written down in technical specification at the international Frogans' address pattern, which is available online at Frogans dot org.

Concerning the Frogans' registry, it's called the Frogans' Core Registry, or FCR. It's delegated by a [inaudible] by a NTT called the FCR operator. Registrations are made by FCR [economy structures?], they play the role of registrars. And they're using APIs or [inaudible] email interface, depending on the volumes and concerns.

It's a first come, first serve registry. We are running UDRP for Frogans' addresses. It's an adaption of the UDRP. It's implemented by [Forum] in the US, and [inaudible] in Asia. There are dealing with categories that you can register addresses in, and we have specific composition rules and [inaudible] characters for each linguistic category, that are enforced to registration time to avoid confusion by end users.

And this, all of this is specified in the Frogans' address technical specification, which is also available online, on Frogans dot org. And then the system, the resolution system is operated by the

[inaudible], it's called the [FNS], Frogans Network System. FNS server is deployed worldwide. We are currently running in six locations in the US and in Europe.

And we expect to be deployed in China and Russia by the end of the year. These servers run IPv4 and IPv6, domain names rely on the dot Frogans TLD, that's a very strong piece of the security. And FNS records are signed on the fly, using this [inaudible].

So, we can benefit from the authenticated [inaudible] of existence, and everything is specified in the FNS specification. And the last slide is about the Frogans' [inaudible] and the [inaudible] from it. [Inaudible] settings are the information that comes with DNS requests, so the contents, both administrative and technical information on the Frogans' side.

For example, as in, and this information is set by the Frogans' [inaudible], which is the publisher of the [inaudible]. So, this information [inaudible] with the intended audience, which is managed before the end user accesses to the Frogans' site content. So, it relates, for example, to the age category, all the countries where the Frogans' site might be disallowed or allowed.

And the publisher also, that is a key point, I guess, from end user security, publisher has precise control over the network protocol that is used by Frogans' player to access the server hosting the

Frogans' site. So, for example, when using TLS protocol for hosting the Frogans site, the publisher can tell, can set its address saying, this is the [inaudible] I want to use.

[Inaudible] I want to use, this is my certificate, the [hash?] for my certificate, etc. And that is enforced when connecting, when [inaudible] player, when the end user connects a server, this information is checked. And moreover, there are also information on the way the Frogans' site has been developed, for example, the version of the [inaudible] language used to develop Frogans' site. So, there is no need for Frogans' player to guess what's wrong potentially.

And so it's easier to develop and you get less [inaudible]. The Frogans' site format, lastly, is something important, as you can see in my next demo. It's based on descriptive language called [FSDL?], based on [inaudible] itself. [FSDL] documents and auxiliary files are hosted in a single directory, so you know exactly where all the content comes from, it comes from the publisher, on a single server.

It can be generated dynamically, or it can be static, of course. Every technology is possible, and the existing web technologies can be used to host Frogans' sites, of course. And [inaudible] is really is in the form of [inaudible] for all, anyone can build any tools, and services upon that. And as you can see in my next

demo, the Frogans' site offers a complimentary and visual way to publish and broadcast content online.

And this content is actually rendered identically on all end user devices, so you can be sure that your content is the same everywhere. You don't have to adapt anything. So I'm trying to switch now to my computer, so I'm sorry for the online audience. I wish display…

Oh, yes, for the audience, I just to show this, okay?

But I need to load this one first.

Okay. So, back to my computer. What you can see here, on the screen, are some Frogans site. So you can see that they're not similar to websites. Those are, okay let me put that away so you can see a bit better. So, each one of them is associated, or is identified, by an address, Frogans star here, [inaudible], and this address is, if I close it. This [inaudible] here, this [inaudible] is Frogans' player. Frogans' player is not complete full screen software, it's just something very discrete on the screen.

And so, I can enter a Frogans' address here. What was it? [Inaudible]

And now, Frogans' player has resolved the Frogans' address on servers, and has been loading content, this content, from the Frogans' site server. So, it goes very fast. Those little things, you

see, you can recite them on screen very easily. They can take different appearances depending on the site the end user chooses.

You can navigate inside this site. See? And can have dynamic information. For example, here, you have something about the weather, looks like a small widget on the screen. And so, you can do very creative things with this, but this is met through using just this simple language. You can use this here, and this language is completely descriptive language.

You see, this one has been met with 76 lines of code. And so, it's very easy for developers to create these sites. It's very fun, actually. Well, so I think I can go back to this later on, if you want. But that's all I wanted to say right now.

You can test that, you can go to Frogans dot org, and you have the complete technology available for testing. And currently, it's released for developer, but it's quite… You can use it this way, it's very simple.

UNKNOWN SPEAKER: Fantastic. Thank you very much, Alexis.

[Applause]

And for the demo as well, it makes it more concrete. We will now move to the next presentation, which will be from Christophe Blanchi, from DONA Foundation. And welcome our friend from ISPCP, just on time. So, the floor is yours, Christophe.

CHRISTOPHE BLANCHI: Hello. Good afternoon. My name is Christophe Blanchi, the executive director of the DONA Foundation. Thank you for inviting us, and I'm going to talk about the handle system and the global handle registry. Next slide please.

So, this is part of something we call the digital object architecture, which is an architecture that seeks to find an uniform operable access to heterogenous information systems, resources, and other entities. So, this is a big mouthful, but the idea is that we would want to make information a first-class citizen on the internet. And there are a few things that this entails.

One is you have to have a common way to talk about things on the internet. And so the model here is digital objects. You have to have identifiers that can allow you to point to systems and physical things. You need uniform description systems, allow you for searching and retrievable capabilities. And a lot of this is tied to the notion of sensible typing of data and services, so that

you can dynamically figure out what these digital objects are, and how to interact with them.

They also, the point of the digital object architecture is to be sort of system independent. Hardware will change, some technologies will evolve. But the model itself, will still remain valid because it's independent of that layer of systems.

It has integrated security, and is highly scalable. So, the piece of the digital object architecture that I'm going to talk about specifically is the identifier system. Oh, sorry. I added this slide and I forgot about it. A little bit of background. The digital object architecture is something that's been around for a while. Bob [inaudible] and Vince [Surf?] at CNR, where I used to work for, where I used to work, developed the notion in the 80s when they were talking about mobile programs, called no bots.

They were evolved and funded by DARPA funded effort called the computer science technical report project. Then there are various efforts to develop it, the cross industry working team wrote about it, and other entities also evolved views on it, and the architecture, digital object, digital ID award in 2003 for balancing innovation with reality.

So, that's a little bit of a background. DONA has been statute, has the goal of evolving the architecture. But the thing that is actually running at the moment and used by many

organizations, is the handle system. So, it's the key component of the digital object architecture, and it's defined by a protocol in a data model.

It's a basic identifier resolution system for the internet, and can be used in all sorts of computing environments. You can resolve… The notion here is simple. You take a handle, that's what we call an identifier in the handle system, and you resolve it into a digital object's current state information.

Now, the definition of a digital object can include things that are non-digital. So, for instance, you can have a digital object pointing to a piece of paper, and that's a way for you to link an identifier back to a physical thing, or an IOT device. The identifier persists, and when the handle system, the handle service changes, it does not the effect the identifier, the handle identifier itself. And this is, for instance, one of the problems that this was resolving is if you had a URN, a URI, sorry, and you change your DNS name because the resource was reallocated to another company, those references will break because the DNS name will change.

In the case of a handle, you don't have this association of identifier to a service. The name of the handle is independent of the service that resolves it. The handle system is logically single system, but it's physically and organizationally distributed. It's

highly scalable. We've had people have a billion handles in their own service. At the moment, there are 100s of millions of handles used in China for doing counterfeit prevention on some of their products.

Another well known users of the handle system is the DOI's, the digital object identifiers, for identifying genuine article data sets and such things. Typical use of handle is to associate an ID, a handle in this case, with an IP address, a public key, an URL, meta data, anything that the handle owner wants to pretty much.

There is secure resolution, administration using an integrated PKI capability. In some cases, it's obligatory if you're using a LHS, but if you're using just to handle client libraries on top of an existing service, maybe you don't have administration. It's optimized for resolution and speed and reliability.

So, a little bit of comparison between the handle system and DNS. They're both resolution systems. They both work in the internet, and they have extensive collections of data. Oh, sorry, can you switch? Sorry, I apologize. I keep driving it from my laptop and I forget it's over there.

The handle system in a way is compatible with DNS. You could very well have a handle system pointing to DNS resolver, and have the handle system, but behind the scenes, query the DNS

system get the record, return it as a handle. The handle system is very generic in the way it formats its handle records.

A local handle service could resolve DNS requests in native form, by reaching out to traditional DNS servers, and it would cache the results. The client software could access the handle system directly from an application, if you want. And then, the interesting part is if DNSSEC is not available, the handle system has a built in security, and the ability to sign individual records, so you could use the handle system to sign the values in a record, and then have those records be resolvable, either through the handle system, or through your DNS resolver.

There were experiments were people implemented bind on top of the handle system, so they could manage the, in effect, the DNS records, using the handle protocol in a secure fashion, and then providing resolution through DNS.

So, a few key features of the handle system. Authentication. There is an optional PKI capability built into the system. There is a bi-directional handle service and client authentication. Authorization. Handles have administration capabilities, but you have to have the proper authentication and permissions in order to be able to do so.

Handles also have the ability to restrict who can see what in the handle record. There is confidentiality, the protocol is

encrypted, [inaudible], because the servers have to do a public private, sorry, child's response requests, so that a client can verify the server they're talking to is indeed the one that they want to, and also, the handle records can be signed by other certificate authorities to establish these trusted records.

And there is an audit log that goes along with it. So, what's a handle? There is a prefix, and there is a suffix. Handles are global unique. The prefix are allotted by MPAs, multi, suddenly blank. I think I'm going ahead of myself.

So, the prefixes are allotted by, or are contained at the global handle registry. And the typical, the first part of the prefix is resolvable at the GHR, and the second part may or may not be in the GHR, depending on how the MPA, the Multi-Primary Administrator decided to setup their prefixes.

But this handle is… This is a handle. The full handle is resolvable at the local handle server, which is managed by the entity that is minting the handles themselves. It's encoded in Unicode 2.0. I mean, the character set is Unicode 2.0, the encoding is UTF-8.

The prefixes nowadays are numeric, and the suffix is pretty much anything that you would like. Handle resolves to typed value pairs. There is no restriction as to what these typed value pairs can contain. There are certain types that are registered,

part of the infrastructure, like SSH admin, URL. There are things that are known.

But you can create any type that you would like. HS Pub Key is something that is recognized by the system for doing public private key [inaudible] response, and the signature is another thing that is known by the system.

So, the resolution system works as such. You have the global handle registry at the top. And then you have a bunch of local handle servers. And the way it works, is each handle service can consist of one authoritative service, or multiple authoritative service mirror setups. And each service can, in itself, contain multiple servers. So you could have, for instance, a primary local handle service site with 10 servers, or you could have a mirror site with just one.

It's up to you to figure out what you want. When you resolve, when a client resolves, you first go to the global handle registry, which picks any of these multi-primary administrators, returns the service administration, back to the client saying, your prefix is held in that particular handle service, and the client then will get the service information for all of the primary and mirror sets, and they will pick, in this case, many authoritative and because of the way that service is setup, they would go to the fourth

server and then the client would directly talk to that fourth server to resolve the handle, and get the results.

So, it sort of looks like this. You issue a request to the global handle registry. You get a service set of information back, all that of is encrypted. This is probably something you don't see, but it's describing all of the security features that you have at that point. Here is what the service information looks like.

You pick a mirror service too, and the service too within it, and then your device talks directly to that server, to issue the request. And that's how the handle system works. So, the evolution of the global handle registry, originally the global handle registry was developed by [inaudible] and operated by [inaudible], until last year.

[Inaudible] decided to further enhance and develop the GHR functionality. And especially to, or allow multiple organizations to be multistakeholders, and become what we call multi-primary. It May 2014, CNR transferred the rights to administer the [inaudible] DONA Foundation. And the multi-primary GHR became operational 9th of December last year.

So, the way it works is you have these MPAs in the global handle registry. If, for instance, CNRI, who is now MPA, wants to create, or is asked to create a new prefix by an organization, they push it to their MPA GHR service, and that service then pushes updates

to all of the other MPA GHR service, and each service verifies the signatures and the key chain on each of them to make sure that these are valid per policy.

And if there is anything that happens that either the signature doesn't work, the keys are outdated, or the policy is not the proper one, then the transaction is rejected. So, same thing. And if another MPA does that, it adds new, the right prefixes, they get replicated to all of the other MPAs.

So, and DONA is sort of a special MPA in that it creates prefixes for MPAs. So, what is one of these MPAs? It's an organization that is credentialed and authorized by DONA to create the right prefixes [inaudible] credential prefix. These organizations get one prefix, and they are allowed, and they've delegated the permission to create as many derived prefixes from that one allotted prefix as they like.

DONA makes sure that they have that credential, that their keys worked, that their system operates. DONA does not tell them how to derive their prefix, or how they should derive their prefix. All the GHR, all the MPAs within GHR, validate all of these derived prefix creations.

So, what is the role of the DONA foundation? It's based in Geneva, Switzerland. It provides coordination, software and other strategic service for the development, evolution,

application of the [inaudible] architecture. But it also makes sure that the GHR is up and running, and that the MPAs are all doing their jobs at maintaining the integrity of the GHR.

DONA also promotes [inaudible] recommendation, X12 55, which is a standard base in the DOA across many countries and industries. And will try to develop pilot projects in public interests. And of course, the credentials, new MPA candidates. They make standards, because DONA has, for prime interest, to manage the standards of the handle system in the DOA, and welcomes external inputs to try to steer it to new features, or performance requirements that it needs to update itself with.

And the point of the DONA Foundation is to foster community interest and development, work with others to develop the availability of relevant standards, reference software. Industries that we're working with at the moment, or areas that we're working on, is the IOT, issues of device typing.

How do you interact with devices? Big data. Again, identification of data sets. Data typing. Of course, there is the issue, there is the capability of identification of distributed resources. So, there are certain models that keep appearing back and forth between IOT and big data that we would like to standardize.

And then the big thing is, we like to use the handle system, maybe as a way to bridge other identifier resolution systems, like IOD, or any other, Orchids. Because, I think, the point of the handle system is not to be the system for all identifiers, but a system that can bring interoperability across identifier systems.

I'm done. Thank you.

UNKNOWN SPEAKER: Thank you very much, Christophe. So, we will move to the last presentation, which will be from Alain Duran. Alain Duran is part of the research team at ICANN, and his presentation will mainly focus on what we have done to explore a little bit how DOI work from the research perspective, and what we have found, and this will probably help educate that aspect of the discussion later on. Alain?

ALAIN DURAN: My name is Alain Duran. I work in the Office of the CTO, and am part of the research group over there. And, a while ago, about two years ago, [inaudible] interesting work happening in the space of new identifiers, why don't you look at it? So, I started to explore it, that space, and I would like to present some of the observations that I've made during my [inaudible] observing this. Next slide please.

So, we started with in 2015, Dr. [inaudible] technology, as his team of CNR in Western Virginia, lives just like a mile away from there, so I met with him several times. And we had some very good exchange, explained to me how this thing worked.

We obtained a prefix from [CNRI] at the end of 2015, and we have been running an experimental server since then. Last year, there was a new version of the code, so we updated to a new version of the code. [Inaudible] we are put all of our experimentation was number of memos we sent to management and to the ICANN Board. Next slide please.

So, caveat before I go on our observation is, a complete and up to date documentation of DOA data format, protocol, wire, security protocols, etc. I'm not, do not appear as being publicly available, don't necessarily have access to everything, of course, but several of us try to find some reference document, and we found some older documents but not up to date ones.

So that, it has been an issue. We have access to the [CNRI] implementation with reference of implementations within the available, the [inaudible] of implementation but we have not access to. So, it's bit difficult sometimes to [inaudible] what this protocol description from what is actually an implementation choice from reference implementation.

And our observation, our best understanding of this work, there might be errors, so I'm sure that my colleague would correct me if I'm making some mistakes here. And I apologize in advance for those errors. Next slide please. So, we DOI, DOA, DONA, and it was an alphabet soup. It was difficult to understand. Is it the same thing or not? So, our understanding is, the technology that binds us all is the handle system. DOI is an implementation of it, that has been used by the publishing industry for quite a while.

DOA is the architecture about this. And DONA is a Foundation that is essentially promoting the technology, and doing all of the governance around the technology. So, we have seniority of a bunch of prefixes, so maybe we can simply look at the next slide please.

All right. So, prefix is a left part of a handle, so prefix slash name. So, as of today, in most cases, it's only digits. There is one case where it could be letters. It's for dot NA, so [inaudible] purposes. But it's mostly digit. However, from what we have seen, it could be anything else. There is no technical limitation to say it cannot be letters at some point of time.

So, even types of prefix, depending on the number of dots, but varies in that. So, when there is no doubt, it's called a zero

[inaudible] prefix, when there is one dot it's a one [inaudible] prefix, and there are two dots, two [inaudible] prefix.

As of today, we understand that the new NPA system, we can only register one [inaudible] prefix or more. For prefix we have one, one, seven, three, eight, was allocated by [inaudible] before the new regime. It has been [inaudible], so that's why we have [inaudible] prefix. Next slide.

MPA, so my colleague talk about that, we do not… Not sure exactly how can somebody become a MPA, what exactly the responsibility of a MPA are, so we are doing some inference about that. We haven't seen actually the documentation that explains that, it may be to exist simply haven't found it.

So, we dealt with the [inaudible] which is the [inaudible] system and the main MPA, so just to give you an idea of the cost, as of last year, we just renew the prefix. When you want to prefix something, it's a one time cost of $50, and then every year you pay $50.

So, now relationship with [inaudible] they explain to you as if we want to have a sub-prefix of this prefix, for example, if you wanted the prefix one, nine, three, five, which is a department number for the research team, so one, seven, three, eight for ICANN dot one, seven, three, five, four of [inaudible] group, then

we would have to register that prefix directly back to [CNRI] and pay a second-time.

So, we cannot [inaudible] a prefix. Apparently, from what I understand, that technologies that would enable that, but the response we got from [CNRI] is they don't have the business model to actually enable this. Next slide, please.

So, from a governance perspective, so that's the DONA Foundation we talked about this in Geneva, our understanding is that the DONA Foundation does three things. The evolution of a protocol, which is somehow, if we try to map this into internet space, that's what the IETF does for the DNS, if all of the protocol. Also, there is a policy development, we are keen to the world that ICANN does for DNS. And also the operation of a GHR, which is what the root server operators do for the DNS.

So, those three roles are actually taken by the DONA Foundation. And there is a MOU between the DONA Foundation and the ITU. From what we understand, the ITU provides a secretariat function for the DONA Foundation. And we provide reconstruction in case of the failure of the DONA Foundation. Next slide please.

So, how it works, that's what we really try to figure out. So, there is a client, a client asks for a global handle registry. We have the prefixes, and then ask a local handle registry for more

details about the object. So, this can be done over UDP or TCP, specific protocol, or it could [inaudible] API using a [JSON] format over HTTP or HTTPS.

So, [inaudible] global handles registry, well, the client is seated with the IP address of a global handle registry. So, this is very similar to DNS. You have hint file that helps you to find your root servers. Next slide.

Scaling, well all of the prefixes are in the GHR. So, there was a question, how does this [scale]? So, next slide please. Well, the way it scales is through a hash table. So, the GHR are actually sliced into a number of servers through a hash function. The client-side, has knowledge of that hash function. So, it can apply this hash function before it actually go and ask question to the GHR, so apply the hash function, find the actual IP address of the proper GHR, and [inaudible].

So, that's a way this thing can actually scale. For this to work, the client has to be aware of a hash function [inaudible] change in the choice of hash function the client would have to be able to [inaudible]. Next slide, please.

While, replication we talk about [inaudible] in this presentation, we can skip this one. Next slide. Security, so there is a security model with essentially the PKI, which was explained. This is a model that is very similar to DNSSEC. There is a key which is the

same as a key signing key that we use in the DNS. The one that you are going to rollover in later part of this year.

So, this is a signal model. The client must have the knowledge of this master key, which is a key's key. So, if that key were to change, some of it we have to make to the client. Next slide please. So, how do these things really work? Well, there are very few native DOA clients that we have found.

There is a plug-in we found for Firefox, so you can download the plugin in Firefox, and then you can type in the browser window, [HTL], short for handle, colon, slash, slash, my prefix, one, one, seven, three, eight, slash and one of my objects, or [inaudible] projects at ICANN. So, I've created an object for this.

You type this, you actually go to the ICANN website that talks about [HTL]. But plugin not the best way to [inaudible] and so, many applications use proxies. So, there is a proxy service, that is available. Handle dot net, as HTTP handle dot net, operate such a proxy.

And it seems that we see a lot of applications really using this. For example, the DOI used to reference in the publication something that looked like DOI column, then dot, here is an example, 10 37 slash RMH zero, zero, zero, zero, eight. So, that was a publication from the American Psychological Association, pointing to one of the scientific paper.

In 2014, that American Psychological Association changed their recommendation of their cross-reference syntax, and moved from this to a proxy. And a proxy is using the HTTP form, so everything goes through a proxy, and then is resolved by [inaudible] client over there. Next slide please.

So, bunch of objects, I'm going to skip over this slides, because we're running out of time. Next slide, next slide. This is interface on how you actually contribute things, a bunch of keys, the file is not necessarily important for here. Next slide.

As I mentioned, the [inaudible] API, the [JSON] API, so you can do put, get, delete, and all of this could be associated with [inaudible] head to have security. Next slide. And this is a slide where I tried to compare the different elements in the [inaudible] architecture and the DNS architecture. For syntax, it's dot separated UTF-8 card, so you can put anything you like, it's UTF-8 and just separated by dots.

DNS, you have a format for things on the wire. There is a restriction on actually what character you can put in there. In two others, there is no [inaudible]. When you want to do a registration in the DNS, you use registration, registrars, you have to talk to a MPA. The elements of the resolution system, GHR for the Global Handle Registry, essentially that maps to the root servers.

The LHR, that maps to the [inaudible] service. The [replication?] system in [inaudible] DOA maps to secondary servers. Caching server map to caching resolver. This hash function that I was mentioning earlier is something specific to DOA, but doesn't exist in DNS.

Based on the wire, [inaudible] for back to [TCP?] on port number 53. There is a similar thing on port 26 41, UDP fall back to TCP, or as I mentioned earlier, the [JSON] API on HTTP or HTTPS. Data objects. So, in the DNS we have defined [inaudible], defined by ITF and [inaudible] process to define some new ones.

In [inaudible], you don't have static [inaudible], you can do essentially what you want, indexed, so you have to know what the data is, but [inaudible] type. And that's interesting because server in the client, have to know what it is, but nobody else does. So, that's the difference between the two.

And I mentioned the other three before. So, in terms of protocol extension, this is done in IETF over DNS. This is done by the DONA Foundation. Although, in terms of governance, this is done by ICANN for DNS, by DONA for the DONA Foundation. And from an operation perspective, [inaudible] we have a root server, TLD server, top level domain servers, resolver, operators, service providers, registries, registrars, all of this essentially done by the DONA Foundation in the set of MPAs.

And I think that is my last slide.

UNKNOWN SPEAKER: Thank you very much. [Applause]

And thank you all of the panelists for those brilliant, very detailed presentations. Now, we'll move to the second part of this session, which is questions, Q&A [inaudible]. Feel free to ask questions to any of the panelists. The panelists as well will participate into this discussion if there is any interaction.

So, back to the audience. Question, I will be managing…

UNKNOWN SPEAKER: Please raise your hand and I'll bring the microphone to you.

Go ahead and use the mic at the table, please.

JAY DALY: Hi. I'm Jay Daly. So, if you look at the global DNS, on a daily basis, it handles in the order of billions of queries per day, hundreds of thousands of registry transactions. That's, you know, the creation of new things or the change of ownership or something. And then millions of technical changes as well, per day, on a simple basis.

I'd be interested to know whether any of these three technologies can come anywhere close to that. And if not, what your estimates of the total, global capacity is for those technologies.

JEREMY RAND: So, in NameCoin's case, I actually did some informal calculations about how well this will scale up to the amount of usage that the DNS has. These are not absolutely figures, but it's just estimates. But basically, the estimate I did was, if 100% of the domain names that are currently under the TLDs that are issued by ICANN switched to NameCoin, then what's called the block size, in NameCoin terminology, which is how much transaction that goes through every 10 minutes.

The block size would, on average, be similar to three and four megabytes. Now, for reference, NameCoin currently has a block size limit of one megabyte. So, it wouldn't scale up exactly to the level DNS can handle, but it could actually come reasonably close within an order of attitude.

And we are planning on doing some upgrades to the NameCoin network, that would get it closer to there. There is a proposal that is implemented by Bitcoin very soon, called [inaudible] which we plan to adopt as well. That would almost double it up

to roughly two megabytes, and Bitcoin is planning on doing some upgrades to their network that we'll inherit as well.

So, I think we could scale up to a level that is reasonably close to what the DNS has, but again, we can't prove that that will work as well until we actually change. But we're close to being able to scale that high.

JAY DALY: Sorry. Could you explain that in non-coin terminology, as to what a megabyte means in that regard? Because as far as I understand it, the global Bitcoin network can handle about 21 transactions per second.

JEREMY RAND: Yeah, that's correct. Right. So, in the number that is restricting the [inaudible] of Bitcoin right now, is a number called the block size. And basically, this is the total number of bytes of transactions that are allowed to go through the Bitcoin network every 10 minutes. So, if the block size is limited to one megabyte, that means that every 10 minutes, at most, one megabyte of transactions can get through the system.

So, in NameCoin, if NameCoin were to scale up to the level of usage that the DNS has right now, we would need a block size of

somewhere around three to four megabytes. And right now, our limit is one megabyte, which is the same as what Bitcoin has.

How many transactions? Let's see, I think… I don't have an exact number of transactions handy, but the number I was using to calculate this was, let's see, I was assuming that 100 to 200 million domain names would need to be, have a transaction at least once per year to renew, and in addition, I'm assuming that IP address changes are relatively negligible so those don't need to change very often.

And I'm also assuming, I think that what? 10% of the names will need to revoke keys early per year, and so that adds an extra transaction. So, I think, that's the map I used. This is not exact math, if you like I'm happy to redo the math after this panel. I can get you some more exact info, if you like.

JAY DALY: Thank you.

ALEXIS TAMAS: At Frogans, your concern is our concern for a long time. Of course, we know that this application, I've just demonstrated, is to be used by many people. So, from the beginning, we tried not to reinvent everything, and especially we're working on top of DNS, not for any reason, just because…

And we are using the same kind of technologies for hosting these resolvers. For example, we are connecting our server on the backbone, we are using internet carriers, major internet carriers. We are testing DDOS mitigation on those servers. So, we know perfectly that we have many issues that we will be facing, but I think the main thing is that we have tried to use the industry existing solutions, and not try to rephrase everything.

So, we are building on top of things that can scale.

CHRISTOPHE BLANCHI: So, I think the handle system, again, does not have the level of scalability that you would be thinking in terms of DNS, but to give you an idea, a server can resolve 50,000 records per second. And that's a medium sized Amazon record, a medium sized Amazon image. So, if you bump this up, you can imagine optimizing it to maybe, you know, a little bit more.

Then you can optimize the storage, because your storage is very little. You have very few prefixes in the GHR. I'd like to correct my colleague here, is the idea of the prefix, the GHR to contain one [inaudible] prefixes, and the other thing is we don't, we recommend that the MPAs don't put their derived prefixes that they allot to organizations at the GHR, because the point of this is to allow them to do whatever they want without telling anybody else.

And so, when the moment you put something in the GHR is globally known, and the other MPAs well know, wow, this guy just created a million prefixes this month, they're doing great, we need to change our policies. So, we expect to have very few records in the GHR, and if we don't, the current GHR with the way it's setup, so about 50,000 records per second, four hours a day.

So, we're talking about tens of billions of resolutions per day. So, that's before hashing, because we have six and seven and eight, we're going to have 10 MPAs this year, and we anticipate more. So, I think, from a scalable point of view, I think there are ways to deal with it, and I'm sure that we'll have to change some of the underlying technologies that goes on, but I'm not too pessimistic at our ability to scale.

And this is, of course, an element of prefixes. If a MPA decides they want to have 10 million prefixes [inaudible], clearly that would not be conducive to optimized resolution, right? And then you have to think that there is caching involved as well. I mean, it's very unlikely that typical clients go to GHR one, so then they resolve to a bunch of hundreds of records afterwards.

So, I'm not saying that we have the perfect solution, but I think we have some technology that we can apply to help.

UNKNOWN SPEAKER: Yeah, [inaudible]. So the following question, or the conclusion is that there hasn't been real life testing of the capacity of all of those things. So…

ALEXIS TAMAS: Excuse me, we have been testing some kind of load on our servers. And we had, for example, for the resolution of Frogans' addresses based on the, a number of 100 million names, addresses. We had some kind of 30 with the signature, [inaudible] the signature on the fly. We had the, some kind of 30,000 requests person.

[SPEAKER OFF MICROPHONE]

Available for people to look up? Yeah. We have had a demonstration, [light] demonstration during one of the Frogans' conference earlier. Then we access them… Yeah, I can… Sure.

UNKNOWN SPEAKER: Yes. I'm interested in DONA Foundation. And your statutes state that you're a multistakeholder organization, but I want to know, why you decided to create these top down organizations, I suppose say, bottom up organization. So, can you define what you mean by top down organization?

CHRISTOPHE BLANCHI: Yes. It's just that one of the functions of the Board of the DONA Foundation, besides the operational of the organizations, is setting of policies and procedures to… I mean, it is not only the operational part, but also the policies that define the operational of this identifiers. Am I correct?

UNKNOWN SPEAKER: So, I would say the policies apply to the way GHR itself operates, which is not the same as the policies that the MPAs will use when they [inaudible] their own prefixes to their own customers. This is the piece that is totally outside of the realm of DONA.

DONA is only concerned with the management of the GHR, and the policies only have to do with, how do the MPAs do their proper replication? Are they following the rules so that we can have a proper performance, security, and the scalability of the GHR? So, certain policies would have to be, you know, the restrictions on the sort of hardware you run, the sort of environment that you have, the software restrictions, maybe the security level of their keys, things of that nature.

But when it comes to prefixes themselves, as soon as you exit from the top level prefixes, like 10, or 21, DONA has nothing to say as to what you do with these prefixes. If they're one [inaudible] prefixes, if you have one [inaudible] prefixes, they would be in the GHR. But not all of them. You could actually

have one [inaudible] prefixes be in a local handle system, outside of the GHR.

And in that case, DONA wouldn't even see what these prefixes are doing at the GHR level. We can resolve them, but we're only responsible for the GHR. Don't have policies for those.

UNKNOWN SPEAKER: So, it's not clear for me. Who defines the policies that apply for the whole identifier system?

UNKNOWN SPEAKER: So, the way the Board is setup is about a third of the Board members are made up of MPAs. And they rotate in. And the actual number of MPAs that we have, there is some calculations but it's like, I'm afraid if I try to reconstruct them I might get them wrong, but the point is there will always be about a third MPA representation, and they are MPA or industry guests at the Board meeting that are invited to forge the policies.

So, that was my initial point. If policies are defined by the Board, that's a top down organization. That was my question. Why do you decided that this is a better definition, better organization versus a bottom up?

UNKNOWN SPEAKER: Well, I mean, you do have to have consensus as to what the policies are. If it's from the bottom up, somebody has to agree as to what these policies end up being.

UNKNOWN SPEAKER: Yeah, somebody has to agree, but not the same has to define those policies.

UNKNOWN SPEAKER: So, I would push to you, who has more interest in making sure that the system operates properly?

UNKNOWN SPEAKER: Yeah, I don't know. I don't know your system, but I would invite you to go to ICANN meetings, where most of the discussions are bottom up.

UNKNOWN SPEAKER: So, again, the DONA Foundation is a fairly new organization. The Board is definitely open to listening to any users or MPA concerns, with the idea of improving the operational persistence, I mean, performance and security of the system. So, maybe you get the sense that it's a top down, and you know, you're welcome to your opinions.

And if this becomes a problem, we will have to address it at the Board to make sure that the community senses that this is, their concerns are understood, and acted upon. And I think the proof will be in the pudding. If the community feels that the Board is responsive to their demands, then I think it will answer your issues.

PAT: Hi, this is Pat [inaudible] with VeriSign. I've got a question for ICANN staff. What risks or opportunities do these global unique identifiers that rely upon the DNS, present for ICANN?

UNKNOWN SPEAKER: So, I will take that question. I mean, I think, this is the first step of looking at this from our perspective. So, as Alain has shown in his presentation, we have taken this from purely technical perspective, and provide to the management some memo about what it is, and I think the next step internally will be to look at that, and involve the community where needed, but as you have seen, what we have done at this stage, is purely from the research perspective, understanding the technology, looking at how it works, and then reporting that back to the [inaudible].

UNKNOWN SPEAKER: I understand, thank you. But when I walked in, it felt like we kind of invited the foxes into the hen house, and I'm just curious as to what ICANN sees as their role here, or their next steps in terms of, do we look at this as a risk to what we've developed here, or do we look at this as an opportunity to manage other identifiers so that ICANN space.

So, that's kind of where my question is coming from.

UNKNOWN SPEAKER: Okay. As I introduced the panel, at the beginning, this is just an awareness session. It's not about defining a strategy, defining what ICANN should do. This is an awareness, purely awareness for the technical perspective. Letting the community know, these things are happening. This is what we are looking at, and then, from then again we can look.

I will let Alain add, if you have any…

ALAIN DURAN: That was really spirit of the work we did, try to figure out what it is technically. That's step one. If the community wants us to do second step, which is a risk analysis, then we will respond to the community.

UNKNOWN SPEAKER: The queue is growing, so we'll try to manage it a little bit. Yeah, I have Tony, right? And then, okay. So, one, two, three, four, five.

UNKNOWN SPEAKER: Thank you. I have a couple of comments, and a request, and finally a question. The comments are, having listened to the previous question, it's really difficult to adopt any other view, other than this is top down, when you look at the website, DONA dot net, and from that, you cannot even find who are the DONA members. You cannot find who the Board members are. And it doesn't even list the MPA.

So, it's very difficult to take any other perspective with that. Sorry, did you want to answer that?

UNKNOWN SPEAKER: I just want to make a strong… The Board directors are listed on the website, the MPAs are listed on the website.

UNKNOWN SPEAKER: When I looked, I couldn't find them. So, that may be my mistake.

UNKNOWN SPEAKER: I'll gladly show it to you.

UNKNOWN SPEAKER: Okay. That's fine. It certainly isn't clear the way that it works from the website, that you mentioned the rotation of the MPAs, and that clearly isn't set out there. I'd also like to make another comment. You referred to an ITU recommendation, X 12 55. DOA is not mentioned in that recommendation, at all, so it's a very lose connection with that recommendation.

The request I have is, and this isn't my request. I'm make this on behalf, formally on behalf of the ISP constituency in ICANN, we would request that you continue the work in the CTO. That you do look at the risk analysis from this. I think it has been very helpful, the work that's been done so far in understanding that.

So, we certainly support that that work is done. And my final question, if we could go back to the slide that Elaine had with the table, in the last presentation. Certainly, Christophe, you did answer one of the questions that were raised. My question, if we look at that the table, that the other analysis that's been produced in that table, is there anything else in there that you would consider is an inaccurate reflection of the situation currently?

Yes, this one, thank you.

UNKNOWN SPEAKER: So, I think this is actually, I don't have any fundamental issues with what is discussed here. The data objects, the [inaudible] types, I would have some issues with, because the whole point of the typing system is to be handle types that can be resolved to figure out what they are. And the idea is to have a system that can bootstrap its own understanding of types.

But, you know, things like, you know, the protocol extension, the element, DONA is overseeing the process. The idea is to get the community involved through the MPAs and their constituents. To make recommendation as to how this needs to be involved.

And indeed, the operation is DONA and the MBAs. I don't have any issues with this table.

UNKNOWN SPEAKER: Thank you.

UNKNOWN SPEAKER: Thanks. Then next, yeah.

UNKNOWN SPEAKER: So, two requests. Number one, could all of these presentations be uploaded to the ICANN website as shortly thereafter? There was a lot of information, so it would be helpful.

[SPEAKER OFF MICROPHONE]

Yup.

UNKNOWN SPEAKER: They'll be uploaded… They'll be on the schedule itself. They'll be uploaded very soon, if they're not their already.

UNKNOWN SPEAKER: Perfect. Second request, with regard to the memos that ICANN prepared for ICANN staff or senior management, would it be possible to get access through that, either through a [inaudible] request, or if you could make them available? It would be helpful to see what that internal discussion is.

And then I guess the third point that I would like is with regard to Tony. I do think this is something important, and in my personal opinion, would be for ICANN technical staff to not only inform management, but as well as the community regarding these developments. And finally, although I have had some concerns about what I heard here today.

As someone who is attending his 54th ICANN meeting, when I attended my first, I had a lot of concerns then, so to me, let's keep an open mind, and as I said, perhaps this is what staff can do in keeping abreast of what the risks and opportunities are with these technologies.

UNKNOWN SPEAKER: Yeah, thank you, if I may comment on that. Exactly. The memo that have been produced internally, have nothing more than what is here. This is just a report on the research that was done, an explanation of what we understand from DONA, and that's why we are bringing it to the community now, and then from there, we take it up.

There has not been any decision or, you know, analysis on that.

UNKNOWN SPEAKER: Is it just [inaudible] or is it…? As I said, instead of just picking on [inaudible], but all of these different identifiers would be helpful.

UNKNOWN SPEAKER: Yes, exactly. Right now, we started with [inaudible] as one of the research project, with the report coming out. We will do for the… I mean, there is also result limitation. We try to navigate the thing.

UNKNOWN SPEAKER: I would like to go on further. I spent most of my time in this space, looking at DOA. I've spent a little bit of time looking at the others, but not as much. If a community would like us to do

something now, analysis of the other technologies, that's feedback we would like to get.

RACHEL POLLOCK: Yeah, hi. My name is Rachel Pollock. I work at UNESCO, and I'm a relative newcomer. So, apologies if these questions are basic. But in the first presentation, from NameCoin, it came up that the privacy aspects were not completely resolved at this point, and I wondered, for the other two technologies discussed, specifically DOA, the idea of the world handle registry, and being linked to individual identifiers, what the privacy implications of that might be?

Especially in light of the discussion that we had yesterday with the European data commissions and the UN special rapporteur on privacy, about continuing issues with the WHOIS database, and any parallels there.

And then secondly, I wonder if the exercise that ICANN as a community has gone through in the last few years with the IANA stewardship transition, and enhancing accountability and transparency within ICANN, might be, if there are any points from that that maybe could be drawn to some of the other initiatives? Thank you.

UNKNOWN SPEAKER: Thank you. You want to take that?

ALEXIS TAMAS: Okay. Just about privacy in the Frogans' layer. We are, in the technology itself, we take a lot of care of trying not to leak data from the end user to servers, but actually, as you could see, it's a publishing system. So, you have a publisher on one side and an end user on the other side.

So, we never know what's happening between them. So, when end user give data to the publisher, it's [inaudible] on the technology itself. But inside the technology, many things are predicted, for example, the publisher does not know the type of device that the end user is using. It only knows the IP address, of course.

UNKNOWN SPEAKER: So, yeah, privacy is something that DONA is very concerned about. We have a particular perspective, because we don't actually resolve any of the handles, we just resolve prefixes. So, you know, and DONA's servers are actually not publicly accessible. They're accessible to the MPAs, but not to the public. To the MPAs, but the MPAs have the same data that DONA has, because that's the whole point.

But the MPAs do have logs of who is resolving what prefix, and they are very concerned about what to do with these logs. I mean, they typically are, this IP address requested this handle. And they are doing what needs to be done under their legislative regulations, to deal with that. But DONA is making them aware that they have to be extremely careful about this.

When it comes to local handle servers, they're the ones to actually see who is resolving what handle. And that is, at the level of the LHS operator, and they could be all around the world, and they are all around the world, and again, we always tell them to be careful as to what they do with their logs.

But again, they're subject to their own country's laws, and they have to think about that. And it's not so easy, because if they get resolutions from the US, so that's one anticipation, or if they get some from Europe, it's another, but if they get some from Russia, what is the operating privacy laws that they have to follow?

So, it's the same thing with DNS. I think you guys have the same issues. So, we're not going to reinvent the wheel here. We're going to do what other people have been doing successfully all of this time.

UNKNOWN SPEAKER: As a follow-up question to this part of the DONA architecture, as I mentioned in my slide, there is increased reliance on proxy, and I will look at the privacy implication of using proxies.

UNKNOWN SPEAKER: So, proxies again, they are a resolution system that accumulates logs, and they are subject to the same sort of concerns. One note I would like to say about the proxy is, this is because until this time, we could never get a URI standard for the handle system.

Now, we've sort of given up because getting URI standard doesn't mean that the browsers are going to implement URI standards, so what's the point of having URI standard really, if it doesn't buy you resolutions to the browsers?

Now, the idea is simpler, maybe just a sign of the times, but using JavaScript resolution libraries, you can resolve handles natively within your webpage. Not the most, best solution, but it's a solution, so I mean, as much as we would like to have a URI standard, again, it's not going to get what we're looking for, which is browser resolution. And the only way we can get browser resolution is if the community asks for it, because we've asked for it, it doesn't…

A small organization is not going to get Google to put a new resolution system in their browsers.

JEREMY RAND: So, about the privacy issue with NameCoin. My opinion is that privacy is a fundamental human right. I totally agree with the UN on this. And from my point of view, the privacy issues with NameCoin are a bug that needs to be fixed, and those issues need to be fixed before NameCoin sees any kind of mass adoption, because if NameCoin got any kind of mass adoption, before those issues are fixed, my guess is that people would end up causing harm to themselves inadvertently by leaving data lying around, that other people could see that they didn't intend.

It's a difficult problem to solve, but we actually do have a fairly detailed plan to have much better privacy. I just was at a conference last week, and I met with up with Ricardo [inaudible] from [inaudible], which is a block chain privacy project, and he and I had a fairly extensive meeting there, talking about how we can work together to try and improve the privacy issues that NameCoin has.

So, yeah. I hope no one here got the impression that we're okay with privacy having problems in NameCoin. We are not okay with NameCoin's privacy being bad, we want to fix it as soon as

we can. We're actively working to get it fixed. And yeah, so I'm with you on that. Thanks.

UNKNOWN SPEAKER: Thank you. We will take question here. Please state your name [CROSSTALK] remote participant.

UNKNOWN SPEAKER: My name is [inaudible]. I'm also a newcomer, so bear with me if the [inaudible]. I was interested in learning whether there were any patents, IPRs on these systems, [inaudible] obviously by the organizations that would seem to promote those systems. They could be IPRs for anyone on anything, including on standards.

But it's generally transparent with standards, whilst in this case, they might not be. So, thank you.

JEREMY RAND: So, in terms of patents, NameCoin's code base is very similar to Bitcoin, so by far, the widest extent of potentially paten code would be whatever is in Bitcoin. And this has been a fairly well-studied. My understanding is that some of the elliptic curved math that is used in Bitcoin has a slightly uncertain patent situation, to the point that, for a while, the Fedora Linux

distribution was refusing to package the libraries that Bitcoin needed.

Now, my understanding is that those issues are resolving themselves, but I'm not a lawyer, so I can't comment for certain on that. I can say that the NameCoin developers ourselves, we definitely do not have any patients on any of that NameCoin technology. We don't plan to file for any, and yeah.

In addition, NameCoin is not even a formal organization. It's a group of mostly volunteers, at the moment, who released our code under open sourced licenses. So, in many cases, filing patents would be actively against the goals that we have for the project. So yeah, as far as I know, there aren't any patent issues with NameCoin, except possibly the elliptic curve math that's used in Bitcoin. But, I'm not a lawyer.

UNKNOWN SPEAKER: Yes, I would like to make a statement about this one, because this comes and hits us on the head all of the time. We have no intellectual property rights any more on the handle system or the DOA. There was a patent filed October 24th 2000, on systems of [inaudible] and persistently identify managing and tracking digital objects, which covered the handle system and the DOA.

That patent has expired. There are no pending patents, so this makes that the source code that is freely available under an Apache license, would get you into no legal trouble when it comes to IPR. And the other thing I would like to say is that we don't have a licensing issue either, because you are free to get the code from handle dot net, the local handle system code, including the client.

There is no license fee. There is no license agreement other than you need to go find a MPA to give you a prefix. And those MPAs can do whatever they want, and if you don't like one, you'll go to the next one.

UNKNOWN SPEAKER: Thank you. Because we are running out of time, I am closing the queue, but we already have three questions in the queue. So, I will go to you, and the next one, and [inaudible]. Okay.

MALCOLM: Thank you. Malcolm [inaudible] from London Internet Exchange for the records, speaking personally. If a technology is to be widely adopted in the market, it is usually helpful if the technology is useful to the users, and for that reason, I would like thank the gentleman from NameCoin for starting his presentation with a statement of the design goals, expressed

from a user perspective as it was seeking to achieve for the benefit of the user.

Now, the question from scalability that we'll put to you, believe me, and the answers you gave and the assumptions that you made, leave me deeply skeptical that NameCoin is ever going to likely be interesting as a replacement for the DNS.

But because you started with an explanation of the purposes, I do think it might be interesting, as a potential complimentary alternative for particular use cases, where those design goals are the priority for the user.

However, I'm completely mystified, at the moment, as to what the benefits for the user of the DOA structure is. As a registrant, in DNS terms, or as the publisher of information that wishes to attach meta data to the digital objects that I've got, what is the benefit to me as the producer of that to seek to bind that to a surface that is outside my control, rather than to bind it to the document or to the other digital object that I've created?

Why is that beneficial to me? The whole presentation of this has been structured in this sense, in a top down sense, it has been structured from the perspective of the registry, and how the system is organized, rather than from the benefit of the user and why I would want to actually use this technology.

So, if you could say some more about the design goals from a user perspective are, I would be very interested.

JEREMY RAND: So, from a user's perspective, the handle system the advantage, one, is that you can run your local handle server if you like, and hold your data in a place that you control. So, that's not a bad thing. And the other thing is, you can put whatever you want in the record. So, then the other part that's very useful for a user's standpoint is the persistency of the record.

So, one of our biggest adopters is the International DOI Foundation, which creates registration agencies, that then mint DOIs for identifying journal articles. And as you well know, if you make a reference in journal articles, the reference breaks, then you are really out of luck.

So, the point of DOIs is that they persist independently of the service that they're residing on. So, you can swap the services around or you can swap the location of your article, whatever you like. You update your DOI, you don't break the reference. So, it's a simple thing.

You can do it in different ways, but it just so happens that the handle system was one of the first ones to provide an infrastructure to let them do that. The ability to manage your

records, in the way that you like, for instance, the Chinese are creating identifiers for keeping track of physical devices, so they can figure out whether this is the device that they wanted, at the place that they wanted, to keep track of counterfeit.

They can mint hundreds of thousands of them per day. My little device with my native handle library, scan the device, get state the meta data about the box. That information is signed by the manufacturer of the box. The owner of the box holds the local handle system, so they have the advantage to manage your data. As a user, I can get to their data. And new statements can be made and validated cryptography so I can make sure who made that statement.

And where does the data come from? So, that's another application that has been used to deal with the [inaudible] laced baby formula, that's how they solved it. So, there are lots of applications. Again, the handle system, the first big adopters were the publishing community, and then more recently, there have been were called the idle registry, which is to register multi-media movies.

So, most of the Hollywood, like, I think it's, MGM, Sony, are registering their movie assets using the system, so that they can have persistence of their references, and start [inaudible]

models based on those. The DOI are evolving identifiers for things, so building materials.

Again, it's the association and the ability to de-reference what is being resolved to, from what you actually, what is the resource that… So, I have a piece of data, and I want a handle to be able to talk about the data without talking about the, without accessing the data directly.

So, from an identifier, I can get some description about the stuff I'm really interested in. In the case of big data, we have several [inaudible] of data, you don't want to start looking at the data [inaudible], that's what you want. You want [inaudible] interoperable record to be able to tell you that.

And you want it to be interoperable, so the big data organizations there, can figure out what that big data organization is doing, and whether they want to exchange the data sets. So, the point is, to try and describe your information into simple ways. And I would argue that a type value pair is about as generic as you can get, and if you have globally unique types, that are registered with descriptions, and resolvable using the same resolver, you can figure out what that data set.

Whereas before, you just had to get some information to hopefully make sense of it.

UNKNOWN SPEAKER: If I may. All those examples do sound like…

[SPEAKER OFF MICROPHONE]

UNKNOWN SPEAKER: We are running out of time. We still have two in the que, I think that, Christophe, you'll be around, right? Yeah. So, please, if I can ask you, you can have the discussion, and I think, as I said, this is the first of this kind of session we are having, and we'll probably have more time to, you know, dig into this more research. But thank you very much for your question. Next.

GEORGE: Thank you, I'll make it quick. George [inaudible] from dot [inaudible] registry. I'm stepping out from behind the column. I want to give a lot of credit to ICANN for researching some new technologies. I think we need to innovate on the DNS. I've been watching NameCoin for a while, I think block chain is a great opportunity.

Question for the digital object architecture. Could you respond to the overview of the digital object architecture paper from the Internet Society? Particularly on the aspects of governance. I'm

finding it hard to get any kind of transparency into the management of these MPAs.

Is there a PDP, a police development process, an open multistakeholder model, something I've come to now cherish? And then, what element is there for protection of capture being that MOU states that this is a partnership with the ITU?

JEREMY RAND: Thank you for the question. So, as far as the governance, so I agree with some statement that was made, which was that it's difficult to find out what a MPA, how do you become a MPA, and part of it is because we just started having, you know, we started our system, first [inaudible] is maintaining it. We had some multistakeholder that were part of that system, that we then brought back to this new architecture, and now we're out and looking for new MPAs.

And finding a MPA is something that is a mutual thing. They show interest in understanding in what the architecture allows them to do, and DONA, through its Board, reviews their interests and their application. And I agree that the process needs to be made more open.

So, DONA will write some documentation and put it up for review, for the public to be able to understand how do you

become a MPA. So I agree, that this is something that we need to make more clear, but it's clarity more because we're actually working through the process of, you know, how do you become a MPA?

Because you know, it's a little bit like [inaudible] talking about trying to ask people whether they wanted IP addresses at the beginning. Everybody was like, why do I need that? But here, it's not this case. People are actually coming to us and wanting to become a MPA. So, it's a question that, are you doing this for a public good? Are you doing this in an open way? So these are the questions.

So, when we figure these questions out, we'll write a paper sooner than later, and put it up for review. As far as the reconstruction of DONA, last thing. So, there is a MOU that says that in case DONA fails, the ITU will continue operation and recreate a MPA, I mean a replacement DONA Foundation.

So that's all there. The thing that it doesn't tell you, is the ITU would never get the cryptographic keys to make new MPAs, or make any modification to the system. Those keys will be transferred to the new organization. So, DONA, so ITU will never be able to change the system. They'll just keep the lights on the server, which is very nice feature to have, because this way, you

have some people can take questions, you can maybe organize some MPA meetings.

But until the recreation happens, nothing can happen to the GHR. And that's the idea. So, we're not, I just wanted to clarify that.

UNKNOWN SPEAKER: Yeah. Thank you very much. Last, brief, question. If it's a long one, Tony, you want to…? Thank you very much. Is it a question or a comment?

TONY: Last one, I'll get to the heart of it. Okay. You must know that most of us in the community think of the ITU as snake oil. So, why are you in any way engaged with them if you expect any credibility at all from us?

UNKNOWN SPEAKER: I'm sorry you feel that way. I mean, I can't make you change your mind. You know, ITU has its own good and bad. I mean, they brought USMS, maybe you should stop using it, snake oil. You know, it's a damned if you do, damned if you don't. I mean, when we recreated… When the idea was to go from [inaudible] managed THR, to a multistakeholder GHR, a lot of people in the

community came and said, maybe, you know, the ITU should do this.

And we're like, well, you know, why is this such a good idea? So, some people in the community don't share your feelings. Now, I understand that a lot of people see ITU as, you know, the end, an evil entity, but if the community sees ITU as playing a vital role to determining what standards you should be believing in, and what standards they should be trying to focus their energies on, my only recommendation is, you know, keep pushing at your ITU membership to make your dissatisfaction known.

UNKNOWN SPEAKER: Okay. Thank you. You used a completely contradictory phrase, the word multistakeholder and ITU in the same thing. That's the essence of the issue.

UNKNOWN SPEAKER: Okay. Thank you very much all. I think the discussion was very interesting. I would like to thank my panelists, thank you very much for being on the spot. And addressing all of the questions. Thank you for all of your comments. Staff, we take note of all of your recommendations and requests, we'll work on them.

And probably this is not the last, this kind of session addressing other emerging other technology in this area. Thank you very much.

[END OF TRANSCRIPTION]