HYDERABAD – How It Works: Introduction to Registry Operations Workshop (ROW) Topics
Friday, November 04, 2016 – 13:45 to 15:00 IST
ICANN57 | Hyderabad, India

[GENERAL CHATTER]

UNKNOWN SPEAKER: Would you look at the time? It's 1:45 and time to start. Welcome. I hope you're all well fed and still awake. So if I see nodding heads, it means you've eaten too much, and I'm going to come and bang the table.

We are in session three of the How It Works today. This is on registry operations workshop topics. The registry operation workshop, the ROW, as we call it, is an informal industry group and discussion forum for the technical aspects of registration operations of the DNS ecosystem.

It's formed from the people, from the techy people who are involved with registries or with ICANN process, and are trying to do technical work through that. So, a lot of the registries are involved, there are some other entities involved as well. And we're trying to generate interest.

There is… I might be jumping ahead. We published, ICANN published a version one of the RDAP gTLD profile in July of this

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

year. And we have a crucial need to pursue registration operations, discussions, and solve shared technical problems. So we're going to be talking today about RDAP and EPP specifically. And discussing how to take next steps, or looking to ways to take next steps.

There is a session on Monday, November 7, here in hall 2, which is somewhere out that way, about RDAP implementation next steps. So if you find this session interesting, I suggest looking up on Monday at 5:00 PM, in hall 2, and join that discussion. We can always use more voices, especially in technical discussions. We don't have…

We could use more technicians and technical people at the ICANN meeting, so I welcome that. And then we're looking to do a workshop, registry operator workshop, in the spring. We haven't landed on a date or a venue yet, but if you have any interest, there is a link here. [Regy] OPS dot net is a mailing list. It will also be at the end of the presentation.

If you have any interest in what's happening after today's discussion, which I hope you will, please join the mailing list and add your voice to the discussion, and hopefully, you know, we can see you at the workshop as well. So the purpose of the forum, though, is to raise interest with a broader global audience, and to open it to all interested parties.

So, like I've been saying. We want more voices in this process. We want people who can implement, people who can design and develop, more registries, as many technical people as we can, that are leading to, and contributing to, the discussion would be helpful. And with that, I'm going to pass it over to Joe Waldron. You get the magic clicker.

Joe is from VeriSign, and I'm going to pass it there, and then from there, we go to Francisco Arias from ICANN, both will be talking about RDAP and the EPP, or just RDAP for you?

JOE WALDRON: RDAP.

UNKNOWN SPEAKER: RDAP. Okay. Joe, thanks.

JOE WALDRON: Thanks. So, my name is Joe Waldron. I am responsible for the product management of our domain name registries at VeriSign. So, we operate dot com, dot net, dot name, and a number of other top level domains. So, just so I get an idea of the level of interest and awareness, how many people here would say that they have a familiarity with RDAP?

How many have ever heard the term? Okay. How many are familiar with something else called WHOIS? Okay. So we have some people who have never heard of WHOIS as well. All right. So, we're going to go through a little bit of the basics, I think, to help understand what this session is all about.

So, I'll start with WHOIS. And this is part of something that has been referred to as registration data services, and this goes back more than 30 years, where at the beginning of the registration of domain names on the internet, this was all done through a centralized system. Originally, the defense data network, and later this thing called the Internic, which is an organization that was created.

And if you wanted to register a domain name, and wanted to find out any information about that, you would go to a single organization for domain names in dot com, dot net, dot org, and other TLDs that were managed by the Internic. CcTLDs would have been handled within each of the country jurisdictions. So that process worked for quite a few years, but then around 1999, there was something that was essentially coincidental with the creation of ICANN in separation of two key functions in this registration process, which we refer to as the separation of the registry and registrar functions.

So where previously, you would go to network solutions and they were kind of a one stop shop that did the customer facing piece, as well as all of the technical backend, infrastructure operations, those functions were separated.

So, every top level domain has a single authoritative registry. So VeriSign in the registry for dot com, New Star is the registry for dot biz, and so on. So each registry has a single entity, or each TLD has a single entity responsible for that top level domain. But then you could have, instead of that just same entity, also as the consumer facing storefront, you could have multiple registrars.

So this created a new model that expanded the number of registrars that were serving the needs of registrants, the people who were registering domain names, as opposed to just having this one single entity, such as the Internic that was doing it previously. And then in 2000, in accordance with one of the early mandates to create competition within ICANN, there was the first introduction of new generic top level domains.

So, dot biz, dot info, and a handful of other top level domains were introduced. There was an additional introduction of new top level domains in 2003 and 2004, and then more recently, there was an application process that began in 2012, and we've been seeing an explosion of the introduction of new top level domains, at a rate that's just unprecedented in any of the history of the domain name system. So we currently have over 1000 generic top level domain names that are delegated and available. So that created some changes when you think of where all of this data exists for the domain names that are registered within each of those top level domains.

Previously, if you wanted to look that up, you would go to an Internic server, a WHOIS server, and you could get information that was available publicly, and determine all of the technical information about that domain name, when it was registered, when it is expiring, the DNS servers that are authoritative for it, contact information about who the registrant is, or the technical contact, or the administrative contact.

So that really, if you think of the management of the data, created new challenges. And we wind up with a WHOIS service that goes from being managed by a single entity to multiple WHOIS services run by multiple organizations.

Along the way, in the 90s, there was a recognition that the WHOIS protocol was a little bit out of date and didn't necessarily meet all of the needs of the community, and there were a couple of attempts, and I won't go into the details of WHOIS plus plus, and this thing called referral WHOIS, they were attempted, but I think the key point here is that, there was recognition very early that there was a need to develop a replacement system to move that public access of registration data into something that was more current.

In 2005, there was something called Iris that was done within the Internet Engineering Taskforce, and there were standards documents that were created for Iris in the CRISP working group, and again, that never really got a lot of traction for various reasons, but that, essentially, leaves us at a point where we know that we have a problem in terms of an old protocol that's not meeting the needs of the community, or hasn't evolved with the evolution that we've seen in the rest of the ecosystem.

This button, let's see. Very good. Okay, so we moved from WHOIS, into some key areas that we've identified as what we really need in a new RDDS, or Registration Directory Data Service. As I talked about on the last slide, we've moved from kind of a single data model to a distributed model, and we need a system that recognizes and is able to handle that. Authoritative data is another key, I believe, because sometimes data for a single domain name is distributed across multiple entities.

And I'll go into that in a little bit more detail to show what that looks like, but if you think of the registry and registrar model, the registry is the one that receives the information from the registrar when somebody is trying to create a new domain name, so they know the name, they know the create date, they know what the term is, so they know when the domain name expires, they know the technical information that's needed by the registry to make the name resolve.

And then there may be additional data that's passed to them, but they're not necessarily authoritative for who the contact is, because the registrar is the one that has that relationship that can validate that information. So we need to be able to address that source of authoritative data in a new service model. Data protection and privacy is another area that we've seen a great deal of interest in a lot of change over the recent years.

Privacy laws within the EU, rulings from other legal jurisdictions, have defined certain data that we have had in WHOIS for many years, like IP addresses, or email addresses, street addresses. And there currently aren't mechanisms within WHOIS to be able to provide those types of data protections and address those PII concerns. And scalability is always something that I look at from the registries that VeriSign operates, just because of the scale of having 100 million domain names in dot com, you know, that's one scalability issue.

But this model needs to handle also the scalability of the number of registries where we now have over 1,000 gTLDs, over

200 ccTLDs, we've got over 2,000 accredited registrars that operate with those registries. Resellers, there is just a lot of scalability issues that we haven't necessarily addressed in a coordinated manner. It's evolved as kind of a patchwork quilt over the years.

And then finally, we need something that is a standards based solution. So while Iris was a standards based solution that was developed within the IETF, I think what we're looking for here is something that is coordinated across the entire ecosystem, so it's a technical standard that engineers understand and could coordinate on, but it also has to meet the needs of the people who operate daily.

It has to meet the needs within this community of the current and whatever we could expect would be future policies. So as we create new policies, we want a service that will evolve and continue to support that so we don't have to continually replace a protocol every time some new policy is developed.

So if I just try to show that as a graphical model of how this works today, you can see an internet user on the left hand side who can be a registrant, somebody that just wants to go out and look up information about domain names that she owns, and she may have to go to multiple registries if she just has a dot com, a dot net, and a dot org, you're going to go to three different registries, find out information about where that domain, when that domain name was registered, when it expires, is all of the data correct? Or the status is correct?

You may also have to go to the registrar. Dot com is a thin registry so we don't collect and store all of that, all of the contact information for the domain name, so you may go to the dot com registry, you could go to the registrar that registered the name.

It may not have even been registered by that entity that we have listed as an ICANN accredited registrar. It could be through a reseller, or a partner of the registrar. So it could be another organization. And then we have something that's also in discussion this week while we're here in India, about privacy and proxy services. So, even though I go registrar a domain name through my chosen registrar, one of the options that many registrars offer today is a privacy or proxy service, where my information wouldn't be displayed publicly in WHOIS.

The proxy information would be displayed, and then under whatever the conditions are of that proxy agreement, that data would be released upon request, but again, that's a lot of heavy lifting that we're expecting this poor internet user over on the left to figure out how to navigate all of that environment, because the typical registrant or end user that's doing a WHOIS lookup, isn't an expert in all of these systems and knowing where to go to get this information.

So, what this RDAP solution, one implementation of this is a proposed model where, if I start on the right hand side of the slide, I collect up all of those authoritative data sources. So that could be registries, registrars, resellers, proxy service providers, other new services that evolve, that have certain types of data.

One of those is called RIR. So these are the Regional Internet Registries. There are five of them worldwide, and they are responsible for IP address allocation. They also run a WHOIS service. Many of them are also running RDAP services today. But each of those are authoritative for different types of data, different information that an end user may want to look up.

So, under this proposed model, the… What's listed here as RDDS service, is a directory service that will build a system that would know how to go do that navigation. So in the previous slide, the end user was figuring out where to go to get each piece of information that they were interested in, this would be a service that would have the information to go navigate through all of those authoritative data sources.

It could only be one, but sometimes even finding that one may be a challenge. So what we have in this model is above the RDDS service box is something called data source directory. And this is actually a directory that exists today, run by IANA, that is essentially a listing of all of the authoritative sources.

So every registry that is delegated within the root zone, has a record in a file that the service can look up, and know where to go. So if you think of a new top level domain being delegated, if I get dot Joe, I don't know, is dot Joe delegated? So if I get dot Joe, and I create a new registry, it gets put in the root zone, you probably wouldn't know where to go find my WHOIS server.

That's not something that is intuitive to an average user, but this RDDS service, would have the ability to go to a single repository of all of that information that know how to go navigate those registrars, registries, resellers and so on. We also included a new component here called authentication provider, or an identity provider. We've got, again, looking at some of the privacy concerns, some of the recommendations that came out of many of the working groups that ICANN has had going on for years.

That there is a concept of tiered access. There are different terms for that. But if you think of the average end user that's looking up a WHOIS query, what are they looking for? Are they looking to just determine whether a domain name is registered? Is it available? What's the expiration date? Or do you need to know who the registrant is? Or do you need to know who the technical contact is?

Maybe there is a technical issue that you're trying to help get resolved. But if you want to get information about PII, any private information that's very sensitive in some jurisdictions, maybe you have to meet certain thresholds. You know, maybe you need to be a law enforcement officer, or a trademark attorney, or meet some other qualifications. So this model enables that type of authentication, so there is a way to get the information to the right request, to respond to the right request, and not provide information that is unauthorized to go.

Now that system doesn't exist today, but it is one of the weaknesses that has been identified of the current WHOIS service, so again, that is part of the design of the model. So I'm going to shift quickly from kind of a functional model, into, I don't know what you call this, a system behavior diagram.

This is something that an engineer would write, at least, that's where I got it from. So these boxes are very similar to what you saw in the previous slide. So I still have an internet end user, or RDAP user in this case, that's what is labeled, who has a request, a query. So you may be looking up information about a domain name. You could also look up information about a registrar.

You could look up information that a RIR would have, but we're just going to talk about the domain name piece here. And that RDAP user would access a RDAP client, and that client then has a relationship with this RDAP bootstrap service, which is the service that is run, or the listing of authoritative sources that's run by IANA.

It's one of the registries that IANA maintains. So that would inform the RDAP client of where to go find authoritative information. So this, I would draw an analogy to the way the DNS works, when a resolver or a recursive name server is doing a look up, one of the first places you go is to a root server, and that will tell you where to go find dot com, or dot jobs, or dot museum, or whatever the top level domain is.

And that's exactly what that service provides. That level of authoritative information, back to the client, so then the client knows to go to the registry, and be able to query that registry client that is there as a proxy service, which in this model, we have called a virtual thick RDAP service, because the authoritative information that the registry provides is only the data that they're authoritative for.

If there is additional data that's required for contact information that a registrar would provide, RDAP has a referral mechanism that allows that query to be referred, again, to the appropriate source, so that you can continue to navigate through the RDAP service providers for each of the different authoritative data sources.

So then finally, I'm going to add into that same diagram, one additional component which is this authentication piece. So it really is something that does need to be there from day one, it's not there today, but we want to build a model and build a system that isn't trying to figure out how to bolt this on after the fact. It's available and is part of the design that the client could negotiate with the authentication provider, and obtain a token for a certain client that met a qualification level, and then that would authorize the appropriate level of information to be released.

So you may have some clients that only have a basic level of access requirement, and they would get that basic level of information. You may have other clients that would be able to authenticate higher levels of users, and then be able to obtain and deliver the more detailed information that user would be authorized to have.

So, what I've described briefly here is, really the problem that we're trying to solve in a lookup service that has been in place for many years, and how that service works today, and how we're trying to evolve that into a system that will meet some of those limitations that we've seen over the years, as well as prepare us for any future policies that come up, such as some of these authentication systems, or other considerations for new services that would be added into the overall ecosystem.

And then what Francisco is going to talk about next is the provisioning side, or the frontend side, of the data collection and some more of the detail of the RDAP specification.

[SPEAKER OFF MICROPHONE]

Sure.

UNKNOWN SPEAKER: Thank you, sir. I have small query regarding the privacy service. [Inaudible] privacy from the perspective of the registrant. For example, [inaudible] look at the type [inaudible] someone has registered it [inaudible] and doing [inaudible] activities. [Inaudible]. So how to identify those persons?

Because you are giving the protection under the privacy, that person registered [inaudible] pornography or [inaudible] activity. He would do it under the cover of privacy protection service. So, how do you, how do as a user, should approach that [inaudible]? This guy is doing this type of thing, basically abusing the…

Is there a mechanism in this flow, where we can complain, report about that abuse of the domains? Thank you.

JOE WALDRON: So, that's an excellent question. I think you're helping to highlight some of the issues that are going on, that RDAP and WHOIS intersect many other areas of abuse, you know, privacy, proxy services. There are separate sessions going on about proxy services, I'm not trying to propose what the policies or implementation of those services should be, nearly recognizing the fact that those services do exist today, and there should be some standard mechanism for how you negotiate to those services and obtain that information.

And right now, I would say, not standardized. The system that we're talking about here is also designed to support the policies that come out of some of those other discussions, in terms of, is there going to be an accreditation on how to privacy proxy services work? Who gets access to them?

We're not answering questions of, what are the different levels of access that users should have? Who is going to determine who is an appropriate law enforcement agency? Right? So, we're not trying to solve that problem from this perspective. I think there are other discussions, but we're trying to make sure that we put a system in place that enables us to address those concerns.

FRANCISCO ARIAS: Thank you Joe. This is Francisco Arias from ICANN staff. I work on the technical side of gTLDs within ICANN. So, I'm going to talk about two topics. One is EPP, the other RDAP. So, let's start with the first one. EPP, or full name, Extensible Provision and Protocol, this is a protocol that is used for the communication between the registers and the registrars.

Here is high level diagram on the, I guess a little bit simplified version of what Joe showed before. And that shows how the interaction between the parties that are involved in the domain name. So to the… So we have the registrant on one side, that is the person that is trying to obtain a domain name, and they will usually go to registrar, who is a party that is offering these domain names to the registrants.

And in turn, the registrants will interact with the registry to raise the, or manage the domain name for the registrant. So the registry, the box there, they offer a few services. For example, the top with CDNS, DNS is the service that is used behind pretty much any internet service, and allows for, for example, to do the mapping from domain name, to an IPR so that you can access a website, or send email, or pretty much anything else on the internet.

And that's a public service that anyone in the internet can access, by necessity. RDS, that's Registration Directory Services, are not deployed here because there may be a number of them, excuse me. And that's another public service, and that is what Joe was referring to before, where the information of who the domain name holder is, or information related to the domain name is published.

And again, this is available publicly. There is another service, and this is the subject of this first presentation, it's EPP, the Extensible Provision and Protocol. That's not a public service. That's a private service that the registry offers to the registrars that have been accredited to offer registrations, their TLD. So this is the service that we are going to be talking here.

As before, this is a protocol, EPP is a protocol that manage, that is used to manage the domain names and other related objects, like contacts that's the person's that are identified as being responsible for a given domain name. And this is used by the registers, they send the comments to the registry to effect certain actions on the objects.

The EPP protocol uses XML behind it. Also uses TLS's standard that allows for providing encryption in the communication between the registry and the registrar to avoid, or minimize, attacks in that channel. And the EPP protocol, it's a protocol that has been around for quite some time, since 2004, when it was first published as a standard by the IETF.

IETF is the organization in which most of the internet protocols are standardized. So the first version of the protocol [inaudible] policy in 2004, went through a subsequent revision in 2007, and the final version in 2009. And it has been around for several years, and it's used by probably the majority of the TLDs in the domain name industry.

In the domain name industry, there are three objects that are the ones that is most raised is managed. And that's the domain name itself, domain name that has been raised, for example, the contacts and host. Host being, for example, the name servers that are related to the domain name, and that eventually make it work in the DNS.

EPP supports three types of comments, that's the actions that are to be acted. The first type are the session management comments. This are very simple. Just allow to open a session, or to close a session, with a registry. As I mentioned before, the EPP protocol is a private service that is offered by a registry to a set of registrars.

So it has to be some change of setting up, for example, a user password, or some other indication mechanics to allow a register to access an EPP service on a registry. The second type of comments are read only comments. These are comments to discover the information about the domain name, or the contact, or a host.

The first type there is, comment there is the check comment. This comment is used to discover if a domain name exists, if a domain name has been already registered, for example. And it's all it does, not anymore. Then we have the info comment, that is the one that is used to discover all of the information related to a domain name.

For example, the status creation date, and modification date. If the registry supports comments, contacts, sorry, the contacts that are related to it, like initial contact, technical contact, registrant, etc. We have a couple of more comments, I'm not going to go into details there.

The transform comments, we have the create, which is when you create or register a domain name or a contact, etc. Delete, to remove an object in the registry. Renew, for example, in the case of domain names, that is usually a payment that has to happen for the register to the registry to keep a domain name. So renew is the comment that is used once a domain name has been created to the register, for the register to say to registry, I want to keep this domain name for one more year, or two years, or whatever the registry allows as extending the ability of the domain name.

Transfer, that's a comment that is used to move a domain name from a register to another. And in this case, you can see there is a transfer comment on the query section. That is because on the query section, the comment transfer can be used to know the status of transfer. So, to know, for example, if the domain, if the transfer has been, or not, accepted by the lucent registrar.

And finally, on the transfer comments, we have the update comment that's used to update the, give an object, for example, to change the status of a domain name, to update the name or the address of a given contact, etc.

So those are the comments, the base comments, that EPP supports. This is an example of how the information looks into EPP. This is an example of an info comment sent by a registrar. I highlighted in blue the important bits. For example, to identify that this is a comment, that this is an info comment, and that this is an info comment on a domain name, and that that domain name is example dot com.

So this is what a registrar would send to a registry, and the registry would reply providing the information related to this domain, and this [inaudible] in the registry allowed by the registry to see this information. If you recall the name of the protocol, EPP stands for Extensible Provision and Protocol, so the E, it's a very important thing that was put in the design of the protocol to allow it to extend it.

We have approximately 1500 TLDs in the public DNS. And as you can imagine, we have different policies, different ways of doing things in the registries. So what the technical community did with EPPs, they put it in the base EPP protocol, the objects and the comments that are most of the registered use, but by making it extensible by design, allows for registries to add their own extensions, to add their own comments, their own objects, or extend the existing objects to sweet their needs.

For example, in some registries, in some TLDs, they are four contacts, they document idea. They require the content provider, a document ID, and there is [inaudible] extensions, there is some registry of EPP extensions within IANA, that leaves the extensions that have been registered there.

There is no automatic registrations of EPP extensions. That means someone has to go there and register the extensions, and this has been around for a year or two. I don't remember exactly when it was created, but it wasn't a long time ago. There is a working group in the IETF, that coordinates the development of EPP extensions. That doesn't mean that all the EPP extensions have to go through the IETF.

However, and many go there at least to get some feedback from the technical community. So who uses EPP? In the [inaudible] space, that's all of them. They are required by contract to use it. On the ccTLD world, as you can see, there is a big number of them that are using it. And there is, there are also other registries that deal with domain names. The [inaudible] registries. [Inaudible] is a mapping of four numbers to domain names, that are mapped into a specific domain name.

They, some of these [inaudible] are using EPP to provision these domain names into the DNS. And another use that we know about is in the RIR. RIRs are the regional IP registries that provision IPRs. And at least one of them, LACNIC, uses EPP to communicate with national IP registries within the region.

So that's another use for EPP. You can extend to use it pretty much anything you want. So that's about it for EPP. Now, I'm going to talk about RDAP, or the Registration Data Access Protocol. So going back to the diagram describing a high level the services on the interactions between the entities involved in the domain name industry.

Now we're talking about RDS, or one of the RDS services. As you can see, it can be offered by the registry and the registrar. So, why are we working on RDAP? And here, there are two parallel tracks that happen one within ICANN, and the other in the IETF.

Within ICANN, things started in 2011, or at least formally, when the publication of the security and stability advisory committee, they publish a document called SAC 51.

And in that one, they were recommending the ICANN community to adopt RDAP replacement protocol for WHOIS. And, the Board adopted that resolution shortly after, adopting the [inaudible] was created in 2012, and in parallel, in the IETF, a working group was created to work on this protocol that eventually was called RDAP.

And the work in the IETF finalized in 2015, or should I say, the work on the core protocol, because like EPP, RDAP is also an extension, Extensible Protocol, so you can have RDAP extensions, and they are also, there are some of them that are being discussed in the same working group that deals with EPP.

So, coming back to the ICANN [inaudible], there were conducted provisions that were added, negotiated with the gTLDs, and as of today, most of the registries and registrars in the TLD space, have contractor provisions that, under certain conditions, require implementation of what is now called RDAP.

And the last bit on the ICANN side, we work with the community for, about a year I want to say, probably more than a year, on developing what we call the gTLD RDAP profile. The first version was published last July.

I think I have more on the profile later. I'm going to explain what it is. But that's our general sense of the timeline in the, in replacing the WHOIS protocol. So why do we want to replace the WHOIS protocol? Has a series of drawbacks, lack of [inaudible], it's a very old protocol. It was designed in the 80s, early 80s, and it's very simple.

It basically says, some [inaudible] to the server, and the server return some bites, and that's it. There is no standardized format for the [inaudible] return, for example. And as you can see in this, just three examples, the output that you get from the registry or the registrar, can vary very widely.

There is no support for internationalization, there is an ability to have your contact data in Chinese, Arabic, or [inaudible] or any other language. As a matter of fact, the problem with WHOIS is even more basic. There is no support to say, what [inaudible] you're using. Again, this, this protocol was assigned in the early 80s, when mostly only US ASCII was used. And so, it's kind of a hidden assumption, of course it's not stated in the protocol, that everything would be ASCII.

So when you don't have a way to flag [inaudible], then you get things like that. That, the box that I'm showing there, it's a real example, when caught in a registry in WHOIS. Since there is now way for the client that is doing the query to know [inaudible], so there are assumptions that are made sometimes, that are [inaudible] assumptions, they don't allow you to even know what it is that you're getting there.

In this case, I think it was Japanese. And I don't think that you can see that there is any Japanese in there. There are other issues with WHOIS. There is no way to authenticate users, so you cannot provide differential access. There is no support for encryption in the passing of the information, or authentication of the server.

So, there is no way to know if you are quoting who you think you're quoting, and getting the information in a secure way. As Joe mentioned before, there is also no bootstrapping mechanism. This is the way to know who to query to get the information, you need to know the WHOIS server of the registry, the registrar, in order to obtain the information you are looking for.

And there is also a lack of standardized way to [inaudible], or reference. This is, for example, Joe was mentioning before, they have dot com, dot net, and those are what are called thin registries. They don't store information about contacts, and so if someone is interested in knowing who the registrant is for a dot com domain name, they need to query the registrar service in order to obtain that information.

So in WHOIS, there is no standardized way to discover the, in this case, the WHOIS server for the register. So, what are the features that RDAP offers? Not surprisingly, it's basically all of the drawbacks that you have in WHOIS, they are solved, and you have a standardized query response and the message.

You have secure access to data. It runs over ACTPS, extensible, and it has some bootstrapping mechanisms. There is support for redirection and reference mechanisms. It builds on top of a very well-known protocol, HTTP. This is a protocol that is used for, in the web, and as you can imagine, most organizations will not hope to deal with HTTP. They most likely have a webpage, and so they can leverage their expertise, and ICANN can have a RDAP service easily built.

And this is actually one of the key elements that some people say, why Iris didn't get traction when it was available. Iris was one of the previous attempts to replace WHOIS, that Joe mentioned before. Iris was designed to use transport protocol called [inaudible], and not many people know what it is. And it's not exactly very well, very used.

So, getting back to the features that RDAP has. It has support for internationalization, and of course, enables differentiated access. This is, these are some examples. On the top of how the queries for RDAP would look like, as you can see, they are HTTP

URLs. The kinds, the same kind you will see when looking at a browser address bar.

And they can indeed be shown by a browser, since it's using HTTP. On the second part of the slide, you can see the response. This is not the full response, the full response can be very long. This is just to give you an idea what it is, and how it will look like.

So, going a little bit more into detail on internationalization, or some of the key features in RDAP. Internationalization, in this case, is referred to two things. One is the support for internationalized domain names. So now that you can query for internationalized domain name, and also take information about internationalized domain name without an issue.

The other part is the internationalization of the contact information. So, for example, the domain name can be in the language that the person writes their name, or they [inaudible] the language of the [inaudible] where this person lives. And so this is something that is supported [inaudible] in RDAP.

There is also support for, optional support for the language stacks that can be used to identify what's the language for a script of the data. RDAP uses Jason, just like EPP uses EPP, sorry, EPP uses XML to define the structures within the protocol. RDAP in this case uses Jason. And Jason, by default, supports

UTF-8. UTF-8 is one of the encoders and probably the most common encoding for Unicode.

Unicode is the mapping that intends to include all of the characters of all of the languages in the world. So it's by that virtue, makes RDAP naturally, to support internet association naturally. And it also is using HTTP, as you might remember, as the transport protocol, and HTTP also supports UTF-8, and pretty much any encoding that exists out there.

As a matter of fact, in HTTP you can do the negotiation of the encoding, so you don't necessary have use UTF-8, you can use encoding. Bootstrapping, as I mentioned before, in RDAP, you have this feature. So when you are query, doing a query in RDAP, you don't need to know the name of the server… You don't need to know what server to ask to, you just put the query in the client, and the client has a way to find what server is the authoritative source of the information, and obtain that information for you.

In WHOIS, at least in the case of the new TLDs, since we didn't have that feature, there was no RDAP back then, we did what can be called a hack, or a patch. It's not a very elegant solution, but at least we've got something there. And there is a naming convention for the WHOIS server, but this only applies to new

TLDs, and it's not necessarily true for legacy TLDs, and certainly not for many ccTLDs.

In the last bullet, you can see, to Joe's point earlier, that's the list of the sources of, authoritative sources for information, for domain name TLDs in RDAP, IANA keeps a registry of that, and that's what it is used in RDAP to discover the RDAP server.

Differential access. So this is the ability to give differences of information depending who is asking. So for example, one possible way to implement this, and there are, of course, multiple ways to do this, is to say that when authenticated users only get information without the contact data, and authenticated users, get the full data. And I believe this is what, there are three gTLDs that have contractual provisions that allow them to do this.

And I believe [inaudible] until do something like that for registrations that are related to individuals. So not companies. So individuals in those two TLDs have the option to opt out for that, and name has a little bit more complex access they define four types of access, I believe.

So, there are different… The point here, I guess, is that there are different implementations for differential access. And only three gTLDs have these provisions. There is a policy development process that is ongoing right now in the GNSO, it started earlier this year. They are working on, among other things, on the, potentially the finding requirement for all of the gTLDs to support differential access.

And perhaps, they could also define a standardized way to, how this differential access should work. But this is in the early stages, and it's probably going to take some time for the community to reach agreement on how these things should work.

So, [inaudible] data, Joe mentioned before com, net, and jobs, complete the three, the list of three gTLDs that are thin. The rest of the TLDs are thick, meaning they store all the data related to the registration, including the contact data. So when you have thin registries, then you need a way to discover the RDS server of the registrar, if you are trying to get the information of the contacts.

So with RDAP, you can have this information, either by [inaudible] or reference, [inaudible] is the standard in which EPP, sorry, HTTP works. In HTTP when you access a given URL, you can configure your HTP server, your web server, to return a response saying, I don't have the information, but the information is in this other URL. And then the client, for example, the browser, can go automatically and obtain the information in this new URL, where it's being redirected.

So that's one potential mechanism to handle this. Another mechanism that is also available in RDAP is to provide a reference. This is for example, a thin registry could reply with the information they know about a given domain name, so that does not include the contact data, and also include a reference to the RDAP service for the registrar where the RDAP client can go and obtain the rest of the information.

And this is about the RDAP profile, so we covered the main features for RDAP. Now, going back to the status of RDAP in the [inaudible] space. We work with the community for a year or so in agreeing on what we call the gTLD RDAP profile. The ccTLD are the profile maps, existing, contractual, and policy requirements regarding the RDAP service, two features in RDAP.

RDAP, you can think of it as a menu. You have a menu of features that, it tells you, you want to do this thing, this is how you do it. But it doesn't tell you have to do that thing. The profile, the gTLD profile in this case, tells you these are the features you have to turn on. So, from this menu, selecting the things that have to be turned on for gTLDs.

I should say that this profile, so the status of the discussion of turning on the RDAP service on gTLDs, it's in the final stages, but still pending. If you are interested on that topic, there is a session on Monday at 5 PM. Where you can learn the status in more detail, and see the different points of view from the community on what should be done there.

And the, as you may remember, I mentioned before that RDAP DS is plural services, there are different services, at least in the gTLD space. Currently, both registries and registrars in the gTLD space are required to offer two RDAP services. One is WHOIS, the portfolio service it's also called, and the other is web based WHOIS.

We envision that once we issue the RDAP service requirement, then we will have temporarily three services, and eventually, at some point, we are going to turn off WHOIS, the portfolio service, but we envision that we will keep the web service, together with RDAP. As you may remember, when I showed an example of the output in RDAP, RDAP was not designed to be the most human friendly protocol.

It was designed to be stripped or standardized [inaudible] etc. But by the reason of being stripped, it allows for easy transformation to something that is more user friendly, or privy to the [inaudible] of humans, you know, so that you can easily understand the information that is out there.

So that's the reason why we envision that we are going to stick with web base RDS for a long time. And of course, in order to be able to turn off portfolio WHOIS, there has to be discussions in the community to agree when this makes sense. And since we're talking about internet wide migration, my guess, and this is only a guess, it would take a couple of years before we can, after we turn RDAP, before we can turn off WHOIS.

And with that, that's all I have. Thank you. One more slide.

UNKNOWN SPEAKER: Thanks. Do we have any questions or comments to either of the speakers or either of the topics?

UNKNOWN SPEAKER: In the RDAP model, you talked about differential access, one is only for the anonymous, is only restricted. Another is about the full access. Can you elaborate on who will get that full access? And who will authenticate that user? Or is there [inaudible] repository which will say, okay, these are the agencies or the users who have got the full access to that information? Thank you.

FRANCISCO ARIAS: Thank you for that question. So, on RDAP you have options on how you can do these things, and how those things should work, how differential access should work, and it's the subject of a quorum policy discussion. The RDS PDP, I can't remember what it stand for, but there is a policy description that is going on within the community, and one of the things that they have in the scope is to define differential access where there should be differential access, and if so, how it should be.

So, for example, to define who will authenticate the users, or who gets to see everything, and who gets only a limited view. However, there are three gTLDs, I think it was in an earlier slide, that already have provisions in their contracts that allow them to offer this service.

And, I believe what they do, at least in the case of [inaudible] is, you are an authenticated user, you get everything. If you are not, you get only pretty much [inaudible] data for domain names that are related to an individual.

UNKNOWN SPEAKER: Okay. We have a couple of questions. I have three.

UNKNOWN SPEAKER: Hi, good evening everybody. I'm [inaudible]. And I work for National Internet Exchange of India, which also manages India's ccTLD dot IN. So I have this specific query to Joe. We know that ccTLDs have their own privacy proxy policies. They differ among the ccTLDs themselves, so if RDAP becomes the standard, how do they ensure that ccTLDs maintain, how can it mandated [inaudible] ccTLDs so that uniformity of information is maintained?

Because different ccTLDs might have different privacy proxy policies. So how do we ensure?

JOE WALDRON: Thanks for the question. I think that's appropriate for discussion within the ccNSO, but the policies that come out of the GNSO really are geared toward the gTLD registries. And I think that ccTLDs oftentimes will adopt those, but it's really a choice of each of the ccTLDs. When Francisco talked about EPP, while that's required for gTLDs, some ccTLDs have chosen to do that, and some have obviously chosen to use other protocols or other mechanisms.

So, I don't think that we're prescribing that ccTLDs must implement this, but it's something that I'm looking at it more from the gTLD perspective, but I think it's important to share with ccTLDs who may want to participate in the same standards.

UNKNOWN SPEAKER: Good evening. Is there any plan to provide domain names in local languages, like [inaudible] or whatever? Can they register for a domain name in a local language?

JOE WALDRON: Absolutely. Many registries today run internationalized domain name programs. So I know in dot com, we first launched IDNs back in 2000. So you can register at the second level label. We now also have internationalized domain names at the top level, so are a number of those that have deployed, so you can register in local languages that are operated as new gTLDs, ccTLDs, and again, the RDAP protocol will support that look up of those names in the local language, which is another limitation of WHOIS.

UNKNOWN SPEAKER: Yes. [Inaudible] of Egypt ccTLD. I just… You said [inaudible] proxy for RDAP. Is this other phase of [inaudible] and EPP, or RDAP support also [inaudible]?

JOE WALDRON: Can you restate that? I'm not sure I followed your question.

UNKNOWN SPEAKER: You said there is contact proxy to for the privacy of the contact, in WHOIS data. So, is this other face of contact disclosure that is in EPP?

JOE WALDRON: Maybe I won't go back on the slides. So, when we were talking about privacy and proxy services. So, today the way that operates is really with that proxy service, which often… Go back just a couple of more.

So if I go back to say, this slide, so where you can see where there are proxy services, and that may be operated by a registrar, it may be operated by a third party, and what we're showing here in this diagram is that, the data that the proxy service would have, they would have the mapping of the identity of the proxy service, that may be passed out as part of the WHOIS response today, or passed to the registrar, passed to the registry, and ultimately past to the registrant.

Only the proxy service would have that mapping of that data of, you know, this domain is protected by a proxy service, with who the actual registrant contact is behind that. So that's why the proxy service is a source of authoritative data that you know, may be an entity that would operate a RDAP service that could be queried as part of an authenticated query, that said, you know, I am a valid law enforcement agent, who has the authority to get the information.

So rather than trying to navigate across all of these different boxes in this diagram, that one client on the next slide, that one client that the internet user, or the law enforcement officer is using, would go to a RDDS service, receive the appropriate authentication, and then all of that authoritative data that is appropriate for that level of authentication, as a user, would be provided.

UNKNOWN SPEAKER: Is contact [inaudible] is separate from RDAP? Or integrated with RDAP package?

JOE WALDRON: So, we're showing a framework of a model that would enable it to be included in the overall ecosystem. Right now, there is no policy or standards for how proxy services would be included. And I think there are discussions going on about privacy and proxy services, even today.

UNKNOWN SPEAKER: Is there a good guide to help through this, help to remove [inaudible] from our function and add RDAP function?

FRANCISCO ARIAS: This is Francisco. So, RDAP, to be clear, is not a replacement for EPP. EPP is the way to, for the registrar to communicate with the registry. So, you can think of from the point of view of the registry, that's the input point to get the data. And RDAP is one of the ways to output that data, so that internet users can see it.

So, they are complimentary. They are not, one is not a replacement of the other.

UNKNOWN SPEAKER: Any other questions in the room here? Anything online? Okay. Thank you all. Thank you Joe and Francisco for coming back today and doing this. Can you bounce to slide 44 really quick? Last slide? Yeah.

If you have any, found this interesting at all, I see that many of you are still awake and your eyes are open, or you're sleeping really well, please consider joining the mailing list and getting involved with the ROW, the Registry Operators Workshop stuff, and contribute your voice to this discussion about RDAP and the EPP.

We would certainly appreciate it. So thank you Joe, thank you Francisco, thank you guys. We're going to have a short break of about 15 minutes, and we will have members of the SSAC and the Root-OPS community come and talk about root server operations and any cast and other fun stuff.

So, I hope to see you all back in about 15 minutes. Thanks.

[END OF TRANSCRIPTION]