Transcription ICANN Toronto Meeting

Registrar DNSSEC Meeting

Tuesday 16 October 2012 at 15:30 local time

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

Matt Serlin: Let's go ahead and get the recording started. Okay so we are going to get started; it's about 3:30 local time. We've got a 30-minute - oh, yeah, sorry. Hang on one second.

((Crosstalk))

Matt Serlin: Okay. We'll hold off on the recording. Sorry, (Tim), don't run; don't hurry. It's fine, slow down. Not worth it. So I will turn it over. We've got a DNSSEC briefing from the SSAC, Steve and others as well so over to you.

Olafur Gudmundsson: Thank you. Thank you. Bring it up. My name is Olafur Gudmundsson. I am from the technical side of things working on the DNS protocol. I've been the Chair of the DNS Extensions Working Group for a little while. And I'm here talking about some observed issues that the DNS community sees and how possibly Registrars can help us get things to be a little bit better in the DNS.

So this is based on work that Steve Crocker and I were doing to facilitate DNSSEC enabled transfers. But we realized that to get things like that to

work there were a few other things that had to be fixed first. And this is the baby step.

Okay so I'm going to give you this presentation in the beginning from the view from the DNS world. And then (unintelligible) into the world that you might be slightly more used to. And then we are going to talk about issues and finally I'm going to talk about some possible solutions.

Okay when I'm talking about DNS we are talking about what does the resolver see when it gets a request to resolve a name? And it gets a name that it doesn't know and has a (go to) so first thing it sees is it gets to - (unintelligible) the server that says I am the parent of this delegation so I'm going to give you a referral to the actual operated server for. This is the so-called (MS record).

So the resolver gets that back. It gets back information from the child servers and deals with that. And these child servers is operated by an entity that I call a DNS operator. And if something is wrong I want to complain to them if things don't work. And if things work right then everything is fine.

But in the ICANN RRR world we have registrar, registrants and registry. And where does the DNS operator fit? Well it could be the registrar, commonly the case; it could be the registrant or it can be some other party.

And what are the implications when it is in each one of these cases? That's what we do in the next. Now there is information (unintelligible) flow from the DNS operator through the registration system into the registry that updates the information that the parent name servers give out.

If the registrant operates the DNS, like I do for myself, then I go into my user interface with my registrar, type in the information and it gets through the registration system shows up there.

If the registrar is operating the DNS on the customer's behalf it's even easier. They just go ahead do it when they have to and nobody is involved. But if it is an external party that is operating the DNS we have a problem.

They have to - any changes they have to do has to flow through the registrant because they don't have access to the registrant's account. And so the DNS operator has to beg the customer to do it. And the customer may not know what it means, it doesn't pass it on right, it doesn't do it so things just fall off the edge and things start deteriorate.

So when the external operator takes over it basically has to make some choices. I'm going to - while I operate this I cannot make any changes or I will try to make changes. The technical consequences are that it is hard to rename the name servers. It's hard to bring in new services. It is hard to do many things.

And if there is a DNSSEC in use key changes may be almost impossible because the child - the information cannot go through the system. So can we make things better for everybody involved? Yes.

The next slides are going to be some ideas. This is not firm; this is just to start a discussion. And we have to realize that there are - in the ICANN world there are three things we need to worry about; there is the contacts that everybody has for their registration, there is - that we all know. There are roles and then there is what is the account.

Normally when I - any of us goes and buys a domain name it - you have one account with a registrar. And all the contacts go through that. So if I, for example, or an organization has decided that some technical person can do the - maintain so things work but then suddenly they have been delegated the authority to do anything including to transfer the domain away, which may not have been the intent.

So first idea, can we create what I call sub accounts, i.e. a limited role accounts that are attached to the domain name registrations. Each one of this can only do the specified operations. The DNS operator can change the DNS records, go in there and its own contact information period.

The billing contact, if they get a sub account, they can only deal with what is for them. But the administrative account can do everything for everybody. The - how this gets implemented I don't know. It will probably depend on how you have implemented your systems, what you want to support, what your customers want and how close a relationship you want with the various DNS operators that are out there.

There is also another possible solution space. We can go into the technology and go into having the registrar scan what is the information currently in the child's zone and if it is different from what is currently in its database pull that information into the registry's system and store it there, i.e. go - this could be done on schedule, it could be done up on requests or when it is convenient.

So in this case if the child updates its name server list then it can be assumed that within X number of days, weeks, months the registrar will look at this and say, hmm, this has changed. Let me change what's in the registrar system and then it will flow up to the (unintelligible) end and we have DNSSEC in sync again.

If there's a DNSSEC in use and the DNS keys have changed then the registrar could calculate what the DSs are or if we get the new proposal for the child's DS record published at the child then they can pull that and translate that in the DS records. These are relatively simple operations.

And, yes, if the registry - the DNS operator has access then they can possibly even have a bulk interfaces. There are some DNS operators that may be operating tens of thousands of domains that are under registration with each one of you. And they may want to do a bulk operations.

So it is totally up to you how you want to do it. But it is something that we want to see done in the future. And hopefully we can get rid of some of these annoying problems that the DNS suffers from once in a while. Thank you.

Matt Serlin: Olafur, thanks for that. This is obviously the first time that we've seen this so I think we're all just kind of digesting. Can you back up a couple slides maybe? You had a slide in there that talked about levels of access. And I just wanted to - oh, yeah, no that's...

Olafur Gudmundsson: Yeah, sorry.

Matt Serlin: No it's fine.

Olafur Gudmundsson: Yes.

Matt Serlin: Anyway so maybe can you just walk me through that again? You're essentially proposing that a registrar would have to provide different levels of access to update certain information related to a domain name. Did I...

((Crosstalk))

Olafur Gudmundsson: This one, yes. In this one it could - right now there is one domain is one account. The account can't do everything.

((Crosstalk))

Steve Crocker: Let me intercede here just a minute.

Matt Serlin: Oh, Steve, I didn't even see you come in.

Steve Crocker: I sneak in. So Olafur and I have been working together on this. Let me cast it - I understand your question and given the flow of this let me try to untangle this slightly.

What's up on that slide there is a possible approach to a mechanism to solve a problem. Hold that aside for a second, let's just talk about what the problem is and you guys may be in a far better position to say oh if that's your problem here's how we think about it, which would be fine. I'd be happy - we're eager to listen to that.

So the problem is that the DNS operator of the child - of the registrant - will sometimes need to change some parameters that have to be sent upwards to the registry. In a pre-DNSSEC world that didn't happen very often. The only common thing that happened - the only time that was normally triggered is if a third-party DNS operator who wanted to make a wholesale change to the set of name servers that they were using. That's rare; that's an extremely rare event. It happens occasionally but it's very rare.

But if it ever happens it's quite awkward because every single one of the registrants would have to communicate that information up through the registrar interface to the parent and - which is one of the reasons why a third-party DNS operator would be very slow to ever have to go down that path.

However in a DNSSEC world key rollovers are regular occurrence. They don't have to be super frequent but they generally have to happen. You can pick your parameter - let's say it's just once a year.

So imagine that you have a third-party DNS operator, you know, UltraDNS is one of the more common ones. And let's suppose that - but there's plenty of others - who are providing signed DNS service for their customers. And the time to change the key comes along and therefore they have to cause a new DS record to be sent up to the parent. How is that done?

Well the only mechanism that exists today is for the registrant to manually send that up through the registrar interface. And that's a awkward situation because, first of all, the DNS operator has to make that information available to its customer somehow and then the customer has to send that up through the registrar interface.

Typically two manual operations involving a long string of bits that better be exactly right on a regular schedule. And for large numbers of these transactions this is just disjointed.

Conversely if the DNS service to the customer is being provided by the registrar then this is an internal transaction and it's just handled automatically. And so that puts the registrar, who's operating DNS service for his customers, in a qualitatively smoother position than DNS service provided by third party or provided internally by the customer.

That's the problem. This is a noodling about a possible kind of solution, which is postulating a kind of interface. But the big part of what we have to say is there's a problem. And the smaller part is and here's some thoughts about the - but you can view that as a provocation that you can push back on and say oh don't do it that way; do it this way.

Matt Serlin: Okay thanks. That seems then because without - without first hearing what the problem was I was kind of lost. Steve, did you say the problem was that there was this qualitative difference or that it's complicated?

Steve Crocker: It's both of those in that a third party DNS operator serving a customer has no path to send the necessary information up and so it becomes complicated because they have to engage their customer in a manual operation that has to engage the registrar so that's the complicated part.

And it is also a disparity in the relative...

((Crosstalk))

Steve Crocker: ...status.

Matt Serlin: Just to maybe, you know, to simplify it a bit then I think that complicated part you can look at it no more or less complicated than it is today. I mean, it's always easier for a customer to get DNS service from their registrar just straight out of the box and people...

Steve Crocker: Sorry, sorry, the - with the introduction of DNSSEC the requirement for changes that have to be propagated upward is on a regular basis whereas - that is it will happen - whereas pre-DNSSEC once you set that information in place it's good indefinitely until the customer chooses to make a change. So there is an added flow of information that has to flow from the DNS operator up to the registry...

Matt Serlin: I get that. So - but let me just try it like this and...

Steve Crocker: Yeah.

Matt Serlin: ...then you tell me if this helps and that's all I'm, you know, trying to do with this. That qualitative - it's a complicated and then a qualitative difference...

Steve Crocker: Yeah.

Matt Serlin: ...with the qualitative difference, I think you've just said the qualitative difference is more important today because it's complicated but there is that difference today anyway so I don't think that's new. I don't think it's new in the...

Steve Crocker: Yeah.

Matt Serlin: ...supply chain.

Steve Crocker: Fair enough.

Matt Serlin: And on the complicated side can it be handled just with delegation? In other words if I delegate - if I'm going to - I was a registrar, right, and I have my - and I'm supporting DNSSEC and I have my DNSSEC-enabled domains delegated to, you know, to a certain place - when I say delegated - DNS is delegated to a certain place.

Steve Crocker: Yes.

Matt Serlin: Then that might allow me to just have this, you know, added account complexity for those DNSSEC domains instead of requiring me to add that complexity to my whole platform. So I don't know if that delegation would be sufficient or not, that first delegation...

((Crosstalk))

Steve Crocker: I missed - you began by saying a registrar has delegations but that's not actually what happens, right? The delegations are from the registry and they're either delegated to the internal DNS service of the registrar or they're delegated to external name servers of some sort that the registrar is not running.

Matt Serlin: But we're writing them up. We're taking the record and publishing it up to the registry.

Steve Crocker: Right.

Matt Serlin: So...

((Crosstalk))

Matt Serlin: ...we're the ones who are - we're talking to the registry to make it authoritative. And I'm just saying...

Steve Crocker: Where - you're talking to the...

((Crosstalk))

Steve Crocker: ...send it up; where are you getting it from?

Matt Serlin: Right. We're getting it from the registrants or we're getting it from...

((Crosstalk))

Matt Serlin: ...the reseller or we're getting it from...

Steve Crocker: Right. And the issue is that you typically will do it essentially once at the beginning and then whenever...

((Crosstalk))

Steve Crocker: ...registrant needs to make a...

((Crosstalk))

Matt Serlin: I'm in a different place though...

Steve Crocker: Yeah.

Matt Serlin: ...so I get that. So I'm saying if I can - let's say I just point all of my DNSSEC domains to a certain set of name servers that are my - let's call them my DNSSEC name servers. And now I can just introduce this added account complexity to that set of...

((Crosstalk))

Steve Crocker: You're choosing the name servers for those?

Matt Serlin: Yes.

Steve Crocker: But that's an interesting idea. In essence you're saying if a customer wants to run his own set of name servers...

((Crosstalk))

Steve Crocker: ...zones...

Matt Serlin: No.

Steve Crocker: ...who are outsourced to somebody else who's going to - you're not providing...

Matt Serlin: No.

((Crosstalk))

Matt Serlin: I'm saying they need me in any event to talk up to the registry.

Steve Crocker: Yeah.

Matt Serlin: So if what I do is I (unintelligible) whether I'm providing the DNS or not for names that I'm supporting DNSSEC with if I point those down to a set of name servers that now are essentially my, let me just call them for lack of a better term, DNSSEC administrative name servers now those can either be DNS provided by me, DNSSEC, DNS provided by me, or by third parties but I've now just narrowed the place that I've got to introduce this added complexity to.

Steve Crocker: I'm...

((Crosstalk))

Steve Crocker: ...I apologize for being slow on the uptake but let me see if I've got this...

((Crosstalk))

Matt Serlin: ...white board this separately...

((Crosstalk))

Steve Crocker: No doubt.

Matt Serlin: I apologize.

Steve Crocker: But you're suggesting that there be a - I'll use some terms that you didn't introduce but that I sense you may be that there is a defined qualified set of DNSSEC name servers that you've got that relationship with.

Matt Serlin: Which may - which may - where I may ultimately be providing the DNS on or I may be allowing third parties to...

((Crosstalk))

Steve Crocker: And so a third party or - could get their name servers qualified for that service.

Matt Serlin: Yeah.

Steve Crocker: That is actually one of the models that we pushed back and forth on and I said oh that's a hell of a lot of extra machinery to impose on the registrars so I made them take it off.

Matt Serlin: Yeah but I can tell you that none of us want to make these kinds of - these depths of changes to our whole platform.

Man: Yeah.

Matt Serlin: Yeah so I guess, Steve, a question then I think I'm going to yield to Michele. You know, it's the first time a lot of us are seeing this. What's the - what's the best way to get a dialogue going obviously outside of the 30 minutes that we have here that's clearly insufficient. You know, what's the feedback mechanism for the registrar community to digest and kind of feed back to?

Steve Crocker: Well the - I think the, you know, from a process point of view we fully understand that this is, you know, not the right setting to do problem solving in depth. But it felt like a good opportunity, in which we greatly appreciate, to bring the topic up and, you know, sort of define it and give it a name (when) we have some attention.

And you say what would make sense. What would be - what would be helpful from your perspective to answer the question of how to proceed down this path? From our point of view this is stuff that we do for real, I mean, this is our day-job stuff. Any time, any place you say.

Matt Serlin: Yeah, I mean, I think, you know, I think a brainstorming white-boarding session, you know, where we can sit down and, you know, at least have some time to think - you know, take some time to think about it and come to the table with some ideas and to brainstorm on it and whether or not, you know, we shoot do that in Beijing in person or try to do some sort of a, you know, a teleconference between now and then just to get the ball rolling. You know, we can take that on board and think about that.

Steve Crocker: Is there a small, you know, informal work party that would be helpful to get together not so much as an official negotiation but as a thought process to sketch out some ideas that could then be shared?

You know, it's not an ownership issue, it's just the question of - our perceptions are colored by where we sit and your perceptions about what works for you guys is, of course, going to be far more authoritative and so we'd benefit from that kind of interaction. I mean, you've got your business models, you know what your operational requirements are and, etcetera, etcetera, etcetera.

Matt Serlin: Yeah, no I think it makes sense to put together a small team. And Michele leaned over to me and volunteered himself to lead that. And so I'll allow him the pleasure to do so. And I think he had some comments to, Michele.

Steve Crocker: Let me just put one more thing on the table. There is comparable discussion taking place with some of the ccTLDs and their approach seems to be to have the - registry in the middle of some of these kinds of operations as having direct interactions.

And we're deeply aware that that's not a line that eager to cross in this community. So that leaves the registrar in the middle and so it's with that respect that we come and try to engage in this conversation.

Matt Serlin: Yeah, Michele.

Michele Neylon: Yeah, thanks. Oddly enough, Steve, I remember having this conversation with you - I can't remember which ICANN it was; it was several back. I mean, we recognize that there was an issue here that needs to be addressed. So I know that some of this has been discussed quite (easily) on several of the GNS operations lists. But the reality is for a lot of the people here they're not involved in that part of it.

So just to clarify a couple of things - partially for my own sanity. When we speak about our and all this kind of thing - you made that reference a couple of times - who are you speaking about exactly? I mean, where is this coming from? Is this, you know, that might help us to - give me something to...

Steve Crocker: Well Olafur and I are - so thank you for asking; let me be just completely clear. Until I walked into this room I was Chair of the Board of Directors of ICANN. I took that hat off so I'm here in capacity of the CEO of Shinkuro. We have a contract with (Humabra) and Homeland Security in concert with other players from (Spart) and NIST to help push the adoption of DNSSEC across the community.

So we're here in our capacity as technicians working in this area thinking through the system issues of DNSSEC of the options broadly. So - and then within that as we focus on some of the second order issues like okay you've got the basic relationship set up and now there's going to be a key rollover and there's going to be a large number of these key rollovers not so frequently but enough so that it's not just a one-person at a time.

How do you make all that work smoothly enough so that this becomes an operational - becomes operational without much hassle as opposed to having to have a man in the middle of each of these operations and errors that would crop up from that.

And so it's in that capacity that we're here on behalf of the DNSSEC Deployment Initiative, if you will and seeking engagement where we understand engagement is semi-technical and semi-business and that it's a complicated set of tradeoffs in the - in all of that.

If we were designing all of this from scratch and we had control of all the parts we'd whip up a small (program) to automate this and, you know, be tight

and efficient and all that. But there's obviously an awful lot of established ground about how all this works and so it's harder to fit all this in.

Michele Neylon: Okay I think maybe the best thing would be - because if we try to get into this now I can see it quickly developing into a screaming match so we won't do that. It might be best if I liaise with you and then we can get - see if some registrars both - more the operational side of the registrars to see if we can engage in some kind of dialogue via email or whatever and, you know, thrash out exactly what the issues are that you perceive and what the potential solutions, if any, are.

I mean, some of the stuff you put up here I can see other issues with it. I mean, you might solve your technical problem around DNSSEC but in the process you'd open up other problems, I mean, splitting out contacts, I see as having an advantage for certain uses and I can see it as having a lot of disadvantages for others.

I mean, if I'd - asking a registrar to give a third party access to their DNS is - well - it happened with a high profile domain there recently didn't it, Matt?

((Crosstalk))

Matt Serlin: Yeah, I mean, I think, you know, like Michele said trying to have that dialogue, you know, obviously like I said before it's the first time a lot of us are seeing this so, you know, I understand that you put this together just as a first attempt to try to solve some problems so I think let's...

((Crosstalk))

Olafur Gudmundsson:I would not use the world "solve" we are more like educate

Matt Serlin: Yeah.

Michele Neylon: It has to be both ways of course.

Olafur Gudmundsson: Oh of course. We either need to be educated or for what it makes sense and another thing we may also discover is that what makes sense for one registrar may not make sense for another one.

Matt Serlin: That's right. Okay well with that we are just at the top of the hour and I see our registry friends have made their way in so, Steve, Olafur, thank you for taking the time and we'll have, you know, further follow up as discussed.

Steve Crocker: And let me thank you as well. Thank you as well for allocating the time. I know a lot about packed schedules and yours is as packed as anybody's so. So anyway thank you. Next step is we'll hear from Michele?

Matt Serlin: Yeah. You will always hear from Michele.

Michele Neylon: Don't worry. I'll email you for the next five minutes.

Steve Crocker: Yeah, thank you.

((Crosstalk))

Matt Serlin: With that let's welcome our registry folks. Maybe, David, Jeff and folks that are going to sit up around the table we've got space to my left. Ben, you might want to free up that seat next to you as well...

Man: We're down here, we've got a place down here.

Matt Serlin: Excellent. Yeah, otherwise just squeeze in. Hi, Jeff. Hi, Jonathan. How are you?

I should point out that we had a little bit of a back and forth on the room location for this meeting so historically, in the last several meetings, at least,

we've - the registry folks have come to the registrar room because we generally have a bigger room.

And I think in the sign of shifting time the Registries Stakeholder Group actually had the larger room this time with their growing number of members and the NTAG folks. But for logistical reasons we actually weren't able to move into their room so we will probably end up in a larger room with the registry folks next time so...

END