Notes for Technical Experts Group Meeting @ ICANN 50
Time: Wed 25 June 2014, 1530 – 1700 London Local Time.
Location: Park Suite, London
Participants: See Appendix

Steve: The basic idea is to hear from you on whatever technically oriented topics you want to talk about. There is a starter list to provoke the discussion, but we are not limited nor required to cover these.

Technical Experts' views on the IANA stewardship transition

Steve: We have the announcement from DoC in early March. What are the issues that need to be dealt with, what's your sense how the dialogue in going, what would you like to say about it?

Warren: Much of these are policy than technical, so I don't know how much useful I as a technical people can say. There are three main parts to the IANA: names, numbers, and protocols. We have a very effective process for dealing with protocol parameters. What people suggest is for each community work on their part of transition, and coordinate in the end. Jari, the IETF chair will speak about this tomorrow.

Jay: One issue, the development of SLA monitoring for IANA. One thing people to try to insert is the automation of the IANA. That should be a separate process.

Patrik: Jari and I are the conveners of the session tomorrow on the IANA stewardship transition.

Liman: I would like to add that for the root zone generation process. NTIA have a small step, but it is also an efficient step. I want to caution against replacement process that is substantial and much bigger. That would create delays much longer.

Warren: So, one small follow on from Jay, there is some technical part in the root zone generation. A number of folks would like to have accountability to transition to. Someone else to be the final holder for the KSK. If that were to happen, we would need to have some technical steps to transition.

Steve: Is that a specific proposal? From what you said to operationalize?

David: I think the core of idea is the owner of the KSK is the only entity that has the

ultimate say about who administers the zone. KSK signs ZSK. ZSK have a three-month window for it to be valid. If people think the IANA is not doing a good job, the holder can transition it to someone else. So that's a function that needs to be thought about.

Jim: The SSAC will be reporting on this tomorrow in the session, we are actively engaged to produce three documents, one document on the IANA now, the roles and players, a second piece a review of the all the contractual relationship that are part of the system, those are intended to be reference materials, the most interesting document is the third one, the SSAC is developing a set of postulate and principles as input to the discussion. The kind of things that the community have to pay attention. There will be details tomorrow, but I just want to call that out.

David: Another aspect we may consider during the transition is the current mechanism by which the root zone is generated. Verisign have the unilateral ability to make changes to the zone. The current process, Verisign signs the zone and put it to the distribution master. This is unusual in a sense where there is no check, after the editing signing, and before it goes out the RSO. One potential change is to add a check, after the zone is edited, a third party check before it is put out for the distribution master for the RSO.

Warren: It sorts of depends what sort of threat you are trying to protect against. If you want to check for errors, an audit would be fine. If you are trying to protect a malicious act, e.g. Verisign become rogue, it would be good to separate the signing and the publication.

[unable to capture the speaker]: The check should not not be a voluntary one, but a mandatory by a third party external to Verisign. There have been times in the past what got published is not what we requested. These sort of things would not occur if the person / entity looks at what Verisign did is separate from Verisign.

Warren: We are looking at this from the security engineers point of view. There are a lot of political issues here.

Steve: It is important to look at that. Some of us involve conversations, where government officials ask what would happen if we are taken out of root? They imagine an overwhelming force from governments with no possibility for resistance. In that case, even if you have two-party checking, you can still apply the pressure to multiple parties.

Warren: It could also apply to ICANN as well.

David: Someone has filed suit against ICANN to remove .ir as part of the effort against terrorism.

Suzanne: That whole thing will be resolved by 4 August.

Root Key Roll-Over

Steve: We had the same KSK. Change it require a bit of mechanics between ICANN and Verisign, what concerns me is the end system required to update the key. We have not tested on this. This doesn't seem to like a right thing to me.

Warren: SSAC has a document on root key rollover where a lot of people in the IETF agree with. ICANN should publish the fact that there will be KSK rollover happening sometime, and if you are an operator, you need to do something. Currently it is baked into software and applications. When it is time to roll, it is unclear how many will be affected. Therefore it is important to communicate. If it is rolled on a non-planned schedule, we have even more issues.

Steve: The roll has two elements, planned time, or scheduled. So an event could be scheduled or unscheduled, and planned or unplanned.

Warren: As more people deploy DNSSEC, we will have more people rely on KSK. So the longer you delay, the larger impact it will have. It is clear we have to roll it one day, the sooner we do it the better.

Jim: One of the things in dealing with end users is we know we are going to roll the key at some point, it is not our process, it is about the end user process. That community will continue to grow. We have to build up best practice on what it is. If we are going down the path of rolling, let's gradually increase the time frame of rolling. The point here is to exercise the growing end user community.

Dan: I want to second both comments from Jim and Warren. We had a great number of discussions of DNSSEC in a number of fronts. There is a growth of DNSSEC adoption; a lot of organization is focusing on growing the base of DNSSEC devices. Last year we had a comment on precisely these points, saying that we need have these operational experience, and we need to understand what the impact it. We are taking DNSSEC to CPE vendors. We need to do this [KSK roll] early. Otherwise, when it substantially breaks something, it would be a big hit for DNSSEC adoption. Imagine if we are helpful in getting large sites adopts DNSSEC, and if we do the roll, and if we break Google or facebook, that could be a real problem. My question is what is the next step?

Warren: When we talk about CPEs, if something were to break, it should be in this period during which people experimenting the CPE. If it is later, it is much harder to change.

Liman: I am also in support of doing this sooner than later. The longer we wait, the

closer we get to unscheduled roll.

Jay: Is it possible for IANA to build a test root for IANA to roll it every couple of hours.

Steve: Couple of hours is short, but the idea make sense.

David: During the period of when we are designing the validatable root zone, someone made the point to have a separate infrastructure to test. The counter argument is that if we have a separate infrastructure for the alternative root operators to validate their existence. There are other political issues with it.

David: There is another side to this as well. If I am a resolver operator, every time you roll the key, you force me to change the configuration; I will hate you every time. Then at some point, we will just turn it off.

Martin: In 2008, we had a document about testing DNSSEC implementation. My point is, we have actually gone through this before, and it is not done on a live root.

Liman: If you are going down the path of setting up a test root, I suggest you reach out to root server operators. There is a lot of infrastructure out there.

David: [Not captured]

Dan York: I like the idea of having something for testing. I heard they were using DoD to test. Providing some mechanism, if ICANN can do that, it would be very helpful. DNSSEC API, make this appealing to developers. We have seen a strong interest in the SMTP of using DANE, as well as jabber community of using it. The drumbeat is that the time is soon to make this happen. ICANN need that operational experience, and we as a community need that experience.

IDN Issues

Ram: A few things going on there worth discussing. The development of materials to look at variants can be delegated for the root. There is the generation and integration panel. There are language communities that are asked to put forward generation panel to recommend allowable labels for their community. There are some push backs on this: 1) why wait for the policy development pieces, why not do that in parallel with the technical development. 2) the second is the way variance are being considered, the board has a resolution that no variants should be allowed in the root as TLDs. There is expectation that once the repertoires is defined, that the restriction is removed. It would be good to get some input on this.

The second linked aspect is the universal acceptance of TLDs. Where various software, application does not recognize TLDs more than 3 letters. Clearly this affects IDNs. The idea is that this problem is too big for ICANN to solve. ICANN has a document that is up for public comment. It would be good for the technical community to look at.

Steve: Could you find a pointer and send it out?
[The URL of the document is at: https://www.icann.org/public-comments/tld-acceptance-initiative-2014-06-18-en

David: One of the big questions I have in this space is what is exactly a variant. I ask N people and I get N+1 variation on this. When people say variant, what does it really mean?

Patrik: I fully support David.

Suzanne: There is element that we need to keep clearing the community on this. In the DNS community, there is not enough consensus what is a variant, and it is not a technical issue at that level.

Ram: While there is no universally definition of variant. If you talk to people inside communities, there is quite a deal of conversation. What you don't have is a level up. On that ground, ICANN is engaging about variants.

Ram: There is a whole amount of volume of queries waiting without good answers and without getting to those answers.

Kuo-wei: I found the Chinese community's position is changing, I don't know what it is. It seems what they are asking is a policy reason, they try to pay one to get two. In this week, they are willing to pay two and buy two. It is interesting to see what will happen after this week. There are also difficulties in reaching out Japanese and Korean community.

Ram: ICANN has been publishing a repository of language tables. If would be useful to get your input on whether that's a useful function.

Martin: This is interesting stuff. Is there a way for the technical community to separate the technical problem from the policy problem? As a test case, when you talk about IDNs, at what point you look at plain ASCII, is color and colour a variant?

Jim: I want to pick up Ram's point about whether there is a point for script and language tables. I want to make a recommendation. You cannot do validation if you cannot create contact information based on known scripts and languages. That will create motivation for those tables.

Kuo-wei: I agree with Martin we should separate out technical with policy issues. All of us need learning.

Warren: There was a fascinating presentation on script tables and label generation tables, there would make a lot of automation of these much easier, so they can be parsed.

Ram: To one of Martin's question, if you look ASCII case folding, those are built in by default. If you look at IDN, that does not have automatic case folding, those are considered variants.

Martin: It is useful to have those case folding documents.

Suzanne: Folks who are interested in the deep dive, there are a lot of deep dive into these issues that talks a lot bout these things. ICANN has a document on this:

https://www.icann.org/en/topics/idn/idn-vip-integrated-issues-final-clean-20feb12-en.pdf

Patrik: We are seeing multiple groups are converging, and we cannot impose on others. But we have only one root zone. So this is what the SSAC is pointing out.

David: It is not about domain names, it is also application support as well. At what point does ICANN's role start and stop. Patrik is saying that it is stopped at the root zone. But what about second level, are they exempt?

Kuo-wei: We should allow them to speak up. Currently procedure wise we ask them to have a variant set, and then it goes to the variant. But there is non-technical point here.

Ram: Moving away from variants, there is a set of issues, that just set of issues just out. What out displaying local characters in WHOIS. If customer information is presented solely in a local language, there is issue for access, and for law enforcement. Those are not technical, but its decision has knock on impacts.

Wendy: Picking up first on Martin's early comment. Would it be nice to separate the technical and policy issues, but it doesn't seem to work that way very frequently. At W3C, we are looking at the web application layer. Colleagues in the internationalization area could be useful resources and share comments.

Privacy Issues

Steve: There are two different elements. One is what our privacy policies are. Do we have comprehensive information of what we keep and what the policies are? And there is the IETF, what information get exposed and what information we are in use. I would raise it for people to see what concerns we have.

Warren: There has been a lot of revelation recently about surveillance. The IETF is taking those very seriously. There is an Internet draft where we come to consensus where pervasive surveillance is an attack against the DNS. We should deal it as we did it as any other attack. The IAB has restarted its privacy program. There is also work in existing protocol on how privacy can be protected. The IETF security director presented on the tech day.

Warren: Issues related to ICANN is specific to the DNS. By watching the DNS, you could glean a lot. There is work to encrypt the DNS, at the end user level and at the recursive resolver level. This is very early days; there is no consensus on what should be done.

Wendy: Plenty of the privacy discussions happening are under the preview of supporting organization discussions. For example in GNSO around WHOIS privacy. It may be one view of the board is reviewing the proposal made and make sure the privacy considerations are adequately dealt with in recommendations.

David: Are community making formal statements about privacy? Or it is just informal.

Wendy: For example some groups made to ICANN, one about article 29 work party. Those are particular matters. It would be interesting to think about a general question to SO/ACs what they should be thinking about privacy.

Steve: Are IETF thinking of having privacy considerations just as they do security considerations?

Warren: Yes.

Mike: I think it would be useful to have a look at what is the privacy working group. The expert working is not a GNSO issue. It also has implications for CCNSO. It is going to have impact for CCs and RIR and others as well. There is a lot more for GNSO policy.
Ray: There is a great tendency to immediately react to something and ignore the general solution. It does make a good point of the application of the EWG's report to regional registries. People are looking at technical solutions for privacy. Surveillance is one thing, investigation is another. It is a complex issue; we cannot allow ourselves the trap to make a simple recommendation.

Mark: Part of the weirds protocol has the ability protect privacy through access control.

Margie: With respect to the EWG, it is considered in its final report.

Howard Benn: How we deal this in the world of mobile. We encrypt everything from the phone, and also described legal intercept (33106). We will happily share any information that ICANN find useful.

Bruce: One side is securing the link; the other part is the access control. The other aspect is the storage. One thing people are over emphasizing the transmission.

Jay: For the EWG, one CC is sitting on the EWG is .CN, and their view is different from many ccTLDs.

Margie: we also reached to ccTLD. WE have .uk, .au and Nigerian ccTLD, so there is fair amount of involvement of ccTLDs.

Mike: It is been a second time illuminating conversation, this seems to be steve crocker show, I want to know how to make it more inclusive.

Steve: That's an important question. First of all, a note was sent out was mailing list, that would serve we have you properly on the list. I look to transition that, the other part is what experts are to be invited. If you know of people that you think ought to be here.

Appendix I: Participants (ordered by first name)

First Name	Last Name	Organization
Ashwin	Rangan	ICANN Staff
Bill	Graham	ICANN Board
Bill	Manning	RSSAC / ISI
Bruce	Tonkin	ICANN Board
Chris	Grundemann	Internet Society
Dan	York	Internet Society
Daniel	Dardailler	W3C
Daniel	Migault	IETF
David	Conrad	Virtualized, LLC.
Elise	Gerich	ICANN Staff
Fabio	Leite	ITU
Feliz	Yilmaz	ASO / RIPE NCC
Francisco	Arias	ICANN Staff
Francisco	da Silva	ETSI
Gonzalo	Navarro	ICANN Board
Howard	Benn	ETSI / Motorola
Izumi	Okutani	JPNIC
Jacques	Latour	CIRA
Jay	Daley	InternetNZ
James	Galvin	SSAC / Affilias
Jonne	Soininen	ICANN Board / IETF
Jorg	Schweiger	DENIC
Karine	Perset	ICANN Staff
Kaveh	Ranjbar	RIPE NCC
Kuowei	Wu	ICANN Board
Lars	Liman	RSSAC / NetNod
Margie	Milam	ICANN Staff
Mark	Kosters	ARIN
Martin	Levy	ASO
Mike	Silber	ICANN Board
Patrik	Fältström	SSAC / Netnod
Paul	Mockapetris	ICANN
Paul	Wilson	APNIC
Ram	Mohan	ICANN Board
Ray	Plzak	ICANN Board
Rienhart	Scholl	ITU
Sebastien	Bachollet	ICANN Board
Steve	Crocker	ICANN Board

Steve	Sheng	ICANN Staff
Suzanne	Wolfe	ICANN Board
Tripti	Sinha	RSSAC / University of Maryland
Warren	Kumari	IETF / Google
Wendy	Seltzer	W3C
Wilfried	Woeber	ASO