

## **Transcription ICANN Buenos Aires SSAC Update Saturday 20 June 2015**

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.

On page: <http://gnso.icann.org/en/calendar/#fjun> The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page

Jonathan Zuck: Welcome to Patrick and Jim from the SSAC to present an activities update and opportunity for Q&A. Over to you Patrick.

Patrick Faltstrom: Thank you very much Jonathan, thank you for inviting me. Apart from me and Jim the chair and vice chair of SSAC we also have a couple of other SSAC members in the room.

I was thinking of asking the SSAC members to stand up but there are also other people standing up so let's try to get - that worked. Thank you Patrick. So can the SSAC members in the room please stand up?

Okay, there are actually two (Julia) and Yoav. So next slide, please. So I will go through a little bit of what we have been doing lately, the current status.

One of the things we have done is we have been working on our communication strategy geeks as we are. So here are new and rewind slides, otherwise we sort of own the sort of repeat boring text slides like meeting after meeting.

So we are 35 members. We are appointed by the ICANN board and it's real important our charter says that we are advising the ICANN community and board on matters related to the secure integrity of the incidents naming and address allocation system and that's really, really important and key and we will come back to that later on in this presentation.

We have 71 publications since 2002 and they are both reports advisories and comments and we are putting numbers in everything that we are publishing. So we advised both ICANN board and staff and also the SO and AC's and communities.

The best way for the communities to get advice is to send us questions and we try to respond to them as good as we can. Next slide, please.

The publication process we use is that we create a work party. They do some research, whatever is needed, do the writing and after that sometimes pretty long period and sometimes shorter we do a review of the result, we approve it and then publish.

SSAC is doing all work internally so even though we have work parties that are sort of working on issues it might not have, it doesn't have to result in a report.

The current work parties have to do with new detail program review, registrant protection, the (D) and FSAC workshops, the document management solution that we work on together with ICANN, how to track board advice also related to the HRT to recommendation on implementation of formal advice from the advisor committees.

And we also have a membership committee that look at the membership status or the members of SSAC. The recent publications are SAC 6 to 9 and advisory on maintaining security and stability of the IANA functions through this transition.

It's the third document out of three where we refer to, where we list our recommendations for the operational communities and I'll come back to that a little bit later.

We on May 29 we released SAC 70, it's an advisory on the use of static TLD public suffix list and I will come back to that and present that a little bit later. And then SAC 71 that we published just a few days ago it's our comments on the cross community working group proposal on ICANN accountability enhancements and I'll come back to that as well. Next slide, please.

Next, do if we look at the current work I mentioned a little bit earlier what we actually are working with. The most important thing here that I think that we will talk a little bit more about has to do with the - it has to do with registries and registrant protection, credential management.

I will talk a little bit more about that group. That group compared to others are actually doing things a little bit more in the open and we do have communication with the registrar's here and in GNSO.

Unfortunately, because of time constraints we were not able to meet with GNSO, the registrars which we think is unfortunate when we have this work party but the registrars canceled that meeting that we had set up with them. I just want to inform you about that.

We do have a separate side meeting where we are trying to do an outreach (unintelligible) but unfortunately there is no formal meeting between us this week. Next please.

So we met two out of three milestones so far in the second quarter 2015. We have a (D) and FSAC workshop on Wednesday and one today for newcomers. So we will have met our goals.

In the third quarter we're looking at the advisory for registrant protection and credential management and the fourth quarter of the calendar year advisor of the new gTLD program review. We hope that will be ready and as well have a (D) and FSAC workshop at ICANN 54. Next slide, please.

So go back one. So the first report I would like to describe is SAC 70 which is the advisory that we have on the use of static TLDs and public suffix lists. Next slide, please.

First of all we don't like the word suffix let me start there. So the reason why we talk about suffix list is just because public suffix list is a name that is chosen for this specific thing.

Everything is domains and what we talk about are top level domains and nothing else. But what this list includes is information about under what domain name registrations that can be made and that is in some cases not under the TLD it's under the second level domain.

This is one kind of use of these kind of lists. The list can include also other kinds of things not only the boundaries of where registrations and so called (unintelligible) are but it could include other category information as well.

Tracking this boundary as just one example is real important for security reasons. When you validate certificates to protect against (unintelligible) and other kind of scripting like issues and other things that can happen. Next slide, please.

So for example Web browsers are using these kind of things. So here are a number of examples of various issues that are related to public suffix lists like (TUD) validation, various navigation issues, highlighting in URL's.

And they're used by all different kind of applications, certificate of authorities and whatever. And what you also see on the right most column is that

different Web browsers use different things in these lists so there's not one common set of things that these lists are used for.

So it is different for example between Google Chrome and Firefox. Next slide, please.

So one example for example is if you type in (unintelligible) or finance we see if we use Google Chrome version 37.0 we are using the first number up there. You actually end up on the Web page but if you do the same thing in Safari you end up on the Google search page.

So the two browsers interpret the domain name differently where Safari version 706 it doesn't understand that there is a domain name and thinks it's a search train. But this is one example of what these lists are used for. Next please.

So we have quite a large number of findings and I'm not going to read these to you, you can look at them. But we have found that there are tons of things which have to do with correctness people don't understand the list exists, people don't know how they're going to be updated.

There is a knowledge gap exists between the registries and the maintainers of the list there is not a well-defined path for flowing information between the registries and these lists et cetera.

There is no universal library for these things so programmers and developers have to basically or literally invent their own way of dealing with this list. Next please.

It's often the case that there is a great variation of latency in these lists so even if the registry knows that they have to when they change the policy that they need to update the list they know where to send the data.

It still might take quite a long time before certain changes are made. It's also the case that there is a difference between gTLD and ccTLD as to how these lists are used.

So there are quite a lot of things that are basically not really well synchronized or managed. So next slide, please.

So we'll go to the recommendations instead. We have recommendations to as you can see for example to the IETF which is working on a - have a working group on lists like this or alternatives the (unintelligible) working group. So we think that's a good thing please continue.

We would like to see the IETF also develop a consensus definition of public suffix list what that is because it's very good if you use the same terminology. We would like to see ICANN and the Musella Foundation to collaborate a little bit on information materials that explain this that can be given to TLD registry operators.

We also think that ICANN should encourage software develop community to develop and distribute program and operating system libraries. Next slide, please.

We also think application developers should use economical file format and basically agree on how to handle these kind of, these lists so it ends up being more unified.

We want the IANA, we think the IANA should have a PSL containing information about the domain so that registries that today communicate with IANA so these registries which are authoritative actually can to IANA give information that is normally suited for a public (unintelligible).

So we have one authority source for information regarding TLDs. And then a few other recommendations for ICANN. Next slide, please. Any questions on that? Avri.

Avri Doria: Just a quick question. Would the IANA registry that you're asking for come naturally out of the work that you've asked the IETF to do or would it be precipitated in some other way?

Patrick Faltstrom: We do believe that it's sort of both things needs to happen because the ITF work is going to look at what are the economical things in this public suffix list because we do believe that IANA will include just a very, very small amount of the information that you see on some of the other suffix lists.

For example the Musella one and others but the IANA list should contain the minimum material for example at what level in for the TLD at what level do you do registrations for example.

If IANA includes that information the IANA list can be used by the others to bootstrap their lists. So we envision that for example Musella and others will take the IANA list and then add more things that they feel that they need because there is to some degree there is competition between these lists and the developers then use the list that is best for them.

But it would be good to have sort a bootstrap with IANA. Now the reason why IETF is needed is that we do believe that there is some synchronization that is needed where people need to agree on what is actually stored in the list.

So that's why the IETF work is probably also needed. Maybe not a show stopper but that is something that needs to be investigated. There was another question there as well.

Bret Fausett: Thank you, Bret Fausett from the registry constituency. I really like the idea of having an IANA public list. What are the impediments to getting that done? I

mean from the recommendation to getting IANA to do that I would think you could draw a very short straight line?

Patrick Faltstrom: Well I think given that I personally am coming from the IETF I to some degree actually think the easiest thing is now when if ICANN and if ICANN adopt this report and think this report is a good thing the easiest way might be for the IETF to produce and (RFC) which includes IANA consideration section which gives the actual direct instructions to IANA on how to operate the list.

And when that (RFC) is then coming over to IANA ICANN is already aware of the work and they will accept IANA to take on that work and take the additional costs to develop this software et cetera, et cetera.

So I think that could be one path forward which means that I can accept to implement that with IANA and IETF produce the instructions for how that list is maintained. (Stephanie).

Stephanie Perrin: Stephanie Perrin for the record. I think you've just answered my question but for those of us who are not geeks does ICANN have a mechanism to stop the use of proprietary lists? It would be through the (RFC) process; right?

Patrick Faltstrom: No you can never stop anyone to do anything. We don't have any Internet police. Many of us might want one but there is none.

Stephanie Perrin: Okay. So that one is just a hardy perennial that's going to be there forever?

Patrick Faltstrom: Yes. No Avri it's not me.

(David): We can hopefully provide an alternative that is sufficiently attractive that people do it voluntarily I think.

Patrick Faltstrom: No I think we are joking about this but (David) I think you are absolutely right. The way for people to stop using bad solutions is to come up with better solutions by providing good high quality solutions and make it easy for people to go there.

Then that will be used and use of the bad solutions will stop. So I think you're absolutely right there spot on thank you (David).

So next we just released these comments on the comments on the cross community working group proposal and it might be the case that's interesting for people for me to explain this for people that have not read it. So next slide, please.

If we look at the charter this is real important. The FSAC charter says that FSAC advice is the ICANN community and board on matters related to the security and integrity of the Internet naming an address allocation system.

And FSAC has neither been given nor sought understanding for this advice either, other than that it be evaluated on its merit and adopted or not according to eh valuation by the effective parties.

So just because we give recommendations for example to sort of the registries or the contracted parties of course they can ignore the report if it's not good enough.

So our reports stand based on its quality and that is and so far I think we have been pretty successful. Next slide, please.

So because of this we have no way to participate or evaluate the legal structure required that is discussed in the accountability document. Because that is simply not in our charter.

So we are really concerned in the way in which the proposed new SO AC membership model might affect the way in which SSAC operates. So

basically we're saying that we don't think having us have two seats in this membership committee is a good idea. Next slide, please.

So the only thing we say apart from questioning our role in that membership in the suggested membership we are saying that we are expecting that the community will adopt an organization structure that recognized that the role and importance of high quality expert advice on security and stability.

And of course we do note that in the proposed updated bylaws there is one commitment, commitment number one actually do way that ICANN is committed to ensure the security and stability yada, yada some wording.

And of course we think that's a good thing but it's also important that the actual structure, the auditing the oversight also matches that commitment. So that's it.

So you can go and read the report to yourself. We should send it over to the CCWG accountability. Any questions?

Jonathan Zuck: Yes one from Thomas here.

Patrick Faltstrom: Thomas yes.

Thomas Rickert: Actually it's not a question but maybe a clarification since you were speaking to the potential new role of ASAC under the new structure. When the CCWG made its proposal and offered to all advisory committees the possibility to participate in a structure where a community path can be exercised this was an offer.

And there were no plans that I've heard anybody voicing in the CCWG that should you not wish to exercise those powers as a voting member that you should be deprived of your advisory role or its impact.

So there is nothing on our plate to change the role.

Patrick Faltstrom: Thanks for that clarification. I also should note that so people know that that we were offered to be a chartering organization for the CCWG accountability. We decided to support the creation but not be a chartering organization.

So we are not the chartering organization for this. We are for the CWG names though.

Jonathan Zuck: Thanks Patrick. Any other questions or comments? Was there something you (unintelligible)?

Patrick Faltstrom: Yes next slide, please. Yes there is nothing more on that, there is one more topic. So the last topic that I wanted to present here has to do with the registrant protection and credential management.

It is something that we are going to have a discussion with the registrars here at this meeting. It's ongoing work that we have but we don't have a meeting with the - we don't have an informal meeting between SSAC and the registrars. Next slide, please.

So we have previous work in SAC 40 and 44 where we are defining best practice guidelines for credential lifecycle management or domain names. And the target audience of course is just everyone. Next.

So what we are looking at has to do with credential lifecycle and we are concentrating on best practices and that's why we are communicating with the registrars to basically interview them on what the best practices are.

Try to understand what is currently in use and then do evaluation of that. Next slide, please.

So what we have been looking at are for example what at what the problem is, the recent attack issues that we're seeing, what kind of credential types are used, what types there are, what views there are of them.

The lifecycle of today and the practical checklist is part of the deliverables that we hope that we can produce. Next slide, please.

So we do have a first draft and we have consulted with the community at ICANN 52, we're doing it now at ICANN 53 and the whole idea is to produce a final draft in the next quarter and do, possibly do further consultations. Next slide, please.

So the things that we are looking at is that we have tossed around the list that we have of use of credential and how the current lifecycle is managed. So we're looking at things for example success and challenges with possible requirements to factor authentication, registrant engagement, storage and (unintelligible) credentials, distributional credentials.

How to release or renew and revoke them. And this is something that is of course is a problem in many systems including for example in Sweden I just saw in the news yesterday there was another sort of attack made against the banking system because people managed to steal electronic IDs from people.

Simply by asking for a new electronic, a new password and then they just go to the mailbox and just steal the physical mail that is sent to the person's home address because people think that is secure.

And then we are specifically looking at things like challenges for small registrars. So we're also looking at the implementation issues for small registrars. Next slide, please.

Yes that was actually it. So discussions are ongoing and if anyone is interested in talking more with us about that please reach out to us and we will put you in contact with Marika Koning and Ben Butler the SSAC members that work with these issues.

Jonathan Zuck: Thanks Patrick there is a couple of people interested in following up so James Bladel.

James Bladel: Thanks Jonathan, thanks Patrick, James speaking for the transcript. And just a quick question as far as scoping of what falls under the heading of credentials management.

Are you referring specifically to registrant account credentials or are you also looking at for example registrar communications with registry credentials or auth info codes or how broad is that universe?

Patrick Faltstrom: We are as far as I remember now actually Ben is on his way here and they are the ones that actually should talk about this but I think we are only talking about the registrant, registrar communication, those credentials not registrar registry.

James Bladel: Okay, I hope we have a chance to interact even though we work for the same company Ben and I run kind of in different circles. But, you know, I think some registrar I don't know some registrars I believe allow registrants to create or reset auth info codes that could be considered...

Patrick Faltstrom: Yes there are a couple, yes I know there are a couple of (unintelligible) cases for example some of the incidents have also been when in those cases registrants interact directly with the registry director indirectly.

And that of course happens when first of all (unintelligible) registrars but there are also some other kind of sort of registry lock similar kind of events as well.

So this is one of the reasons why we want to have this communication because compared to the other reports we want this to be focused and so that it must be scoped.

So I think giving you feedback on how to scope it is also good feedback to Marika and Ben.

Jonathan Zuck: Thanks, Bret.

Bret Fausett: Thank you Patrick. I was just looking for a pointer to the draft you talked about of the last document.

Patrick Faltstrom: It is not publicly available but we are using that as a basis for the discussion with the ones that want to interact with us. So that you don't find it means that our security is completely under control.

Bret Fausett: So if - how do we know where you are to provide comments on where you should go?

Patrick Faltstrom: Send me your email address and I will put you in contact with Marika and Ben.

Jonathan Zuck: Thanks (Makaley).

(Makaley Neiman): Thanks (Makaley Neiman) for the record. Now just speaking because you did mention the interaction with registrars I mean for the registrars here a couple of the (XCOM) are meeting with Ben and I believe Marika as well on Sunday to discuss this.

The main reason that we're not doing it as part of our Tuesday meeting is just down to the fact that there is so much already on that schedule. I've been trying to squash something actually and just wasn't a good idea for a multitude of reasons, thanks.

Patrick Faltstrom: So for example one of the outcomes of the meeting that we'll have tomorrow might be for example that we come up with a strategy on how you are going to distribute the information further to help us get in contact with the correct persons.

Jonathan Zuck: Okay Bret you've come in again or is that previously? Okay, Volker.

Volker Greimann: Thank you, one thing first of all I thank you for taking this work and I think many registrars will be very pleased to engage with you on that. One thing that I would like to just throw into the rounds this year, that many registrants do not have direct accounts with their registrar.

Simply because they interact with a reseller of that registrar and they have their accounts with that reseller. So certain information is transferred from a registrar to a third entity, maybe into a fourth entity and then to the registrant where they have their accounts.

And in that case for example it's also very hard for the registrar to verify when the registrant contacts them because of a problem with a reseller or reseller of a reseller if that person is really the registrant because they don't have an account and the registrar has no real way of verifying that.

And the other thing is having a lack of an account directly would also necessitate having these best recommendations to circle down the chain of account providers and resellers and what have you.

Patrick Faltstrom: Yes that is absolutely correct and there are a couple of other kind of interesting situations when you for example have someone that has a whole set of sector domain names that they have asked someone else to sort of take care of.

In those cases it might even be the case that this caretaker is acting legally as well on behalf of the registrants and there are some registry's out there that for example validate the registrant by sending email or whatever to the registrant itself even though its registrar as the middle man.

But if then the registrar caretaker is then the technical contact or admin contact or something it might be the case that even though the overall scheme is set up so that two different parties where one is the registrant is supposed to be involved in the exchange of information in reality it's the same entity.

So there are all different kind of sort of weaknesses that are added just because the domain name management of course to be able to - it must also be sort of convenient and working functionally well for the domain name holder right.

So you talk about similar kind of things that you have in a reseller or something that is taking care of all the domain names for a registrant and that can absolutely create weakness.

Yes there are all different kinds of things like that so but thank you very much for giving like reminding us about yet another situation that might complicate things. Thank you.

Jonathan Zuck: Good, thanks Patrick.

Patrick Faltstrom: And we are done we just have, let me just go to the next slide. Just to show you that we are actually interested in knowing how we are looking at these kind of things, how we advertise things.

So we are doing these kind of administrative stuff as well. So we don't mind ASAC members and also our support staff to talk with you about how we

operate and how you feel that we might change the way we operate to be more useful for you. Thank you very much.

Jonathan Zuck: Okay, than you both Jim, Patrick for coming to work with us and highlighting the key areas that we should be concentrating on. All right that completes that session.

We'll just pause for a moment and then pick up on the next one.

END