SSAC
ICANN Security and Stability
Advisory Committee

12 December 2016

Subject: SAC088: SSAC Response to ccNSO Comments on SAC084

To: Katrina Sataki (ccNSO Chair)

CC: Bart Boswinkel (ccNSO support staff), Chris Disspain, Ram Mohan (ICANN Board)

Dear Katrina,

The SSAC would like to thank the ccNSO again for its feedback on SAC084. Please see below for the SSAC's detailed response to your comments.

Per its Charter,[1] the Security and Stability Advisory Committee (SSAC) focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). The SSAC engages in threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate.

While the SSAC responses focus on the substantive content issues raised by the ccNSO, the SSAC acknowledges that the some of the criticisms in the ccNSO Comment on SAC084 related to two matters of process: first that SAC084 was sent straight to the Board and this was perceived as "bypassing" the Community; and second that SSAC does not have formal "representatives" on working groups such as this. With regard to the first, the SSAC's practice has always been that any formal SSAC document is made available to the ICANN Board prior to its public release. This is the case irrespective of whether the recommendations are directed to the ICANN Board or not. This practice was not intended to display any disrespect to the ccNSO in this instance. With regard to the second, the small size of the SSAC precludes its formal participation in many of the ICANN Community working groups, although SSAC members may choose to participate in their individual capacity. Any formal views of the SSAC are expressed in formal documents after achieving consensus within the SSAC.

---

[1] See SSAC Charter <https://www.icann.org/groups/ssac/charter>

We welcome further dialog if questions and issues remain.

Patrik Fältström
Chair, ICANN Security and Stability Advisory Committee (SSAC)
on behalf of the SSAC

SAC088: SSAC Response to ccNSO Comments on SAC084

Confusability is a Security Concern

Confusability cannot be considered in isolation from other issues related to security. Phishing and other social engineering attacks based on domain name confusion are a security problem for end users.[2] As such, adding a label to the root zone that is potentially confusable violates the Inclusion Principle's requirement that a TLD label be known to be 'safe'.[3]

Err on the Side of Conservatism for the Root Zone

The Conservatism Principle[4] reflects an "err on the side of caution" ethic that is very different from "give TLD applicants what they want unless it is clearly unsafe to do so." Because the root zone of the DNS is a globally shared resource, the decision to add a label to the root should be governed by a conservative bias in favor of minimizing the risk to users and minimizing the potential for mistakes that later must be changed or overridden in difficult or incompatible ways, if such change or overriding is even feasible.

In applying the Conservatism Principle to labels that use bicameral scripts,[5] which distinguish between "upper case" and "lower case" orthographic forms,[6] the SSAC believes that the default finding should be to reject the label if confusability exists in either form. We know of no way to require that bad actors present domain names to users only in the "safe" form.

Local Linguistic Communities and the Global Internet Community

While certain aspects of ccTLD policy are a matter for local Internet communities to determine, aspects of ccTLD policy that have an impact on the global domain namespace need to take into account the interests of the global Internet community. Delegation of TLDs into the root zone is one such aspect that impacts the global namespace and all of the Internet's users. RFC 1591 states that "[t]hese designated authorities are trustees for the delegated domain, and have a duty to serve the community. The designated manager is the trustee of the top-level domain for both the nation, in the case of a country code, *and the global Internet community*. [emphasis added]"[7]

The universal expectation is that TLDs will operate in an interoperable and stable manner without confusion. When new TLDs are introduced, collision, confusion, and stability concerns must be adequately considered. Script and language specific issues, such as case folding, diacritical marks, etc., have to reflect the reality of an LDH-based (Letter Digit Hyphen) DNS

---

[2] See Reports from the Anti-Phishing Working Group <http://www.antiphishing.org/resources/apwg-reports/>

[3] See SAC084 <https://www.icann.org/en/system/files/files/sac-084-en.pdf>

[4] id.

[5] The bicameral scripts used to write languages that are still in modern use are Latin, Cyrillic, Greek, Coptic, Armenian, Adlam, Varang Kshiti, Cherokee, and Osage.

[6] The subject of "case" is in fact even more complicated than this; for example, Unicode defines three cases for plain text in basic Latin (Upper, Lower, and Title) <see http://unicode.org/faq/casemap_charprop.html>

[7] See RFC 1591, section 3 <https://tools.ietf.org/html/rfc1591#section-3>

system.[8] Because the root zone of the global DNS is a shared resource, it is unrealistic to expect local linguistic conditions to always be accurately represented in TLD labels.

Allowing local policy to override the concerns of the global Internet community for issues that impact the global namespace violates the Conservatism Principle.[9] While a given TLD application may represent "the free choice of a specific linguistic community,"[10] it is ultimately the larger Internet community that must weigh that application against the stability of the global namespace.

Harmonization Efforts Needed for Confusability Evaluations Between ccTLDs and gTLDs
The ccNSO comment states:

> Evaluation of the risks posed by the IDN ccTLD process has to take place in the context of the enormous expansion of the namespace since 2012. In commenting on the Conservatism principle, the SSAC Paper fails to mention the impact of the new gTLD programme. A process which resulted in the co-existence of 'fan/fans', 'pet/pets', 'accountant/accountants' and numerous other singulars and plurals cannot be described as adhering to the principle of 'Conservatism'.

The fact that SSAC has not commented specifically on the acceptance of singular and plural forms in the new gTLD program should not be interpreted as implicit approval of the proposition that those forms are not confusingly similar in the context of the Conservatism Principle.[11] The SSAC believes that a clear and consistent set of rules for 'confusing similarity' should be developed and the resulting rules should be applied to both ccTLDs and gTLDs.

Evaluate ASCII and non-ASCII Labels Equally

The ccNSO comment states:

> "The SSAC Paper states in relation to non-ASCII characters that, 'the number and kinds of possibilities for usability and confusability problems is much greater [than with ASCII characters].' A natural conclusion from this statement is that IDNs should hold to stricter criteria than ASCII strings."

The SSAC believes that this comment misinterprets the Inclusion Principle referred to in SAC084.[12] A TLD label should be added to the root zone only if it is known to be "safe" in terms of usability and confusability. This is similar to code points, where a code point should only be added (included) to a list of accepted code points if it is known to be "safe" in terms of usability and confusability in the context of that zone[13].

---

[8] See RFC 5890 <https://tools.ietf.org/html/rfc5890>
[9] See SAC084 <https://www.icann.org/en/system/files/files/sac-084-en.pdf>
[10] See ccNSO Comment on SAC084, page 4
[11] See SAC084 <https://www.icann.org/en/system/files/files/sac-084-en.pdf>
[12] id.
[13] See RFC6912 <https://tools.ietf.org/html/rfc6912#section-4.2>

Because there are many more non-ASCII characters than ASCII characters, the number of possible confusingly similar labels that can be constructed with non-ASCII characters is much greater than the number that can be constructed using only ASCII characters. Nevertheless, every label must be evaluated against the same confusability criteria, regardless of what types of characters it includes.

Add Principles as Part of String Evaluation

The security and stability of the DNS as a global resource for all Internet users depends on the principles articulated in SAC084.[14] The SSAC recommends that these principles be applied as part of any process that evaluates IDN or ASCII character strings as potential new TLD labels.

---

[14] See SAC084 <https://www.icann.org/en/system/files/files/sac-084-en.pdf>