Verisign Minority Statement on RySG Support for NTAG Name Collision Letter

Verisign does not support the New gTLD Applicant Group (NTAG) letter on Name Collisions. We agree with some statements made in the letter, but do not agree with the analysis, conclusions and recommendations made.

Verisign's own analysis and recommendations can be found in the Verisign Labs Security, Security and Resiliency Report #2 at http://techreports.verisignlabs.com/docs/tr-1130008-1.pdf and explained further in this blog post:
http://blogs.verisigninc.com/blog/entry/new_gtld_ssr_2_exploratory

We understand the urgency felt by applicants to move forward as quickly as possible to delegation. Verisign also wants the responsible and timely launch of new gTLDs, including our own and those of our applicant customers. However, we believe that these known SSR risks must be addressed and resolved, or the ICANN Board needs to communicate its rationale for ignoring the SSAC's advice and recommendations on these important issues.

The Interisle study and ICANN-proposed mitigation plan finally acknowledged the very legitimate and long-standing SSR issues previously raised by the SSAC, Verisign and others. As such, the report and mitigation recommendations are a small step in the right direction, but the study was based on a very limited data set and was superficial at best. Even Interisle acknowledged the limitations they faced both in time constraints and limited access to data and that more study can be done. The primary metric used by Interisle was query volume. While that's one indicator of risk, it's not the only one, and ICANN's proposed mitigation plan does not account for the rest. More in-depth study is needed to make informed decisions.

ICANN should have addressed these issues years ago. With appropriate in-depth studies, the strings carrying the greatest risk (by whatever measure) could have been placed on the reserved list and blocked from application. Instead, ICANN is now scrambling to assess which strings are problematic while minimizing its own risks. In its proposed mitigation plan, at the 11th hour, ICANN is now attempting to abdicate their own responsibility by shifting the burden for alerting potentially impacted parties (users, enterprises, governments) to new gTLD registries alone. This is not consistent with the recommendations made in SAC045 from November 2010.

ICANN must accept responsibility for communicating the potential risks associated with name collisions. We believe this should include a significant outreach campaign to Internet infrastructure and service providers (those who will receive customer/consumer complaint calls) and to enterprises who serve significant numbers of Internet consumers. Furthermore, in addition to forewarning potentially impacted parties time and resources must be allotted to enable them to mitigate issues that may arise, the current proposals seem to wholly ignore this necessity. At a bare minimum, they should provide an official ICANN statement to registries to help explain the issue….something that should have been resolved well before applicants chose which strings to submit and before they paid their $185k application fees. ICANN is preparing to transfer risk to unknowing end-users, enterprises and (now) new gTLD applicants while sitting on the over $100 million legal risk fund collected from applicants.

The following explains Verisign's position and reasons for not supporting the NTAG letter:

<u>Verisign agrees with the following points</u>:

- *"We, the members of the new gTLD Applicant Group, are greatly concerned about the substance and tone of recent staff recommendations concerning security and stability issues with the new gTLD program."*
    - Verisign is also concerned about the substance of the August 5 ICANN staff recommendations. We believe they are inadequate. The recommendations are based on an insufficient data set and focus only on a subset of the SSAC recommendations made in SAC045, SAC046, SAC057 and reiterated in SAC059.

- *"With such a long history of productive discussions, it is dismaying to see a great deal of uncertainty about the New gTLD program being introduced at such a late point in the process."*
    - Verisign strongly agrees with this statement. The naming collision issue, among the other remaining issues, has been known since 2009. The ICANN Board and Staff should have addressed and resolved these issues long before applicants selected their new gTLD strings and paid their $185,000 application fees.

- *"We applicants believe that some valid issues have been raised and we are fully willing to engage with such parties individually or as a group. We are particularly aware that the delegation of gTLDs that correspond to widely used internal namespaces can lead to the leakage of sensitive data and other unpredictable effects."*
    - Verisign agrees with most of this statement. The Interisle Consulting Group study, ICANN's August 5 mitigation recommendations and the NTAG have recognized and validated the risks raised by SSAC and by Verisign Labs' March 28, 2013 Security and Stability Report. However, the "widely used" language is subjective and is based on numerical query rates, not the potential impact of the name collision.

- *"We believe that merely counting the number of requests for each string is completely insufficient when judging risk, and that any reasonable conclusions made from the data must take into account the true origin of the "collision."*
    - Verisign agrees that query volume alone is not a sufficient measure of risk – there are many other factors that should be considered as part of the impact analysis for each string. Verisign's SSR-2 report discusses these in significant

detail, and it also clearly denotes that what constitutes risk should be defined by the community.

<u>Verisign does not agree with and/or questions the following statements</u>:

- *“Numerous investigations into gTLD safety have happened and continue to happen in the GNSO, SSAC, RSSAC, and other relevant bodies, and as conscientious citizens of the ICANN community we participate in and applaud these efforts.”*

    - Verisign believes this is an overly broad statement without adequate supporting data. At a minimum, the “investigations” or studies recommended by SSAC have not been completed. The “GNSO, SSAC, RSSAC and other relevant bodies” have not concluded that the potential risks have been resolved.

- *“We believe that none of Interisle's findings give cause to delay the new TLD program and that none of the 20% of strings classified as "unknown risk" pose any danger to the DNS or the Internet community and should therefore proceed unhindered.”*

    - Verisign recognizes that the above statement may represent the beliefs of some of the NTAG, but it is not supported by data. Furthermore, given that the NTAG seems to agree that query volume in isolation is not a sufficient indicator of risk, we believe this statement conflicts with the NTAG’s very own position as conveyed earlier in their letter. Furthermore, based on these elements, we do not believe that drawing an arbitrary line for what constitutes risk at a convenient 20% is responsible. Actual analysis needs to take place based on a risk matrix composed of attributes that are deemed appropriate by the community.

- *“This letter represents our initial feedback on this potential name collision issue, and is intended to provide guidance that can be implemented quickly without placing the DNS or Internet users at risk.”*

    - We believe this statement recklessly recommends ignoring risks without adequate supporting data and analysis.

- *“Even this 3% figure may be overstated due to the difference in TTL treatment and the behavior of caching resolvers.”*

    - The 3% figure isn't overstated, it was measured. Given, negative caching effects are different, but that's orthogonal to the issue at hand.

- *“When we looked at the breakdown of requests provided in Table 12, we found that the vast majority of requests either posed no potential risks or risks that could be handled with simple mitigations.”*

    - Which strings and what simple mitigations and how does this contrast with the earlier statement *that "none of the 20% of the strings classified as "unknown risk" pose any danger to the DNS or the Internet community and should therefore proceed unhindered?"*

- The Sections titled *"Previous Expansions Caused No Known Issues"* and *"Risk Measurement is Easily Tampered With"*

    - These arguments seem in conflict with the letter's previous statement that "merely counting the number of requests for each string is completely insufficient when judging risk."

- *"There is no reason for ICANN to delay the 279 "uncategorized" names any further and reasonable protections can be put in place while the existing new TLD calendar is executed. None of these strings pose any more risk than .xxx, .asia and other currently operating TLDs."*

    - For consistency, the letter previously argued that the classification model was "completely insufficient" If that's indeed the case then you can't turn around and use the same model to apply to previously delegated strings from the past to say there's no risk. This is precisely why Verisign believes that a systematic approach that appropriately weighs all aspects of what constitutes risk and rates the strings on a dataset of sufficient duration is critical.

- *"We believe strongly that the expansion of the namespace will improve the safety, stability and performance of the Internet."*

    - This statement has no technical basis.

- *"Proceed with the "Unknown Risk" Strings using the "Low Risk" Mitigations -- We recognize that a small number of applied for names may possibly pose a risk to current operations, but we believe very strongly that there is no quantitative basis for holding back strings that pose less measurable threat than almost all existing TLDs today. This is why we urge the board to proceed with the applications classified as "Unknown Risk" using the mitigations recommended by staff for "Low Risk" strings. We believe the 80% of strings classified as "Low Risk" should proceed immediately with no additional mitigations."*

    - This recommendation cannot be reconciled with the previous statement that the general classification model is "completely insufficient." Where is the evidence that there is "no quantitative basis" for further evaluation and possible mitigation?

- 3) Accelerate Handling of the Certificate Collision Issue -- NTAG members have discussed the handling of the CA collision issue with prominent members of the Certificate Authority industry and believe that a much more efficient solution exists than the current agreement with the CA/Browser Forum. We believe that the Board can write to the CA/B Forum today and inform them that all but a handful7 of new TLDs are very likely to be delegated in the next two years and, for the benefit of their customers, the 120 day revocation process should begin today.

    - This ignores that revocation alone is insufficient to address the issue. Furthermore, not all CAs are members of the CA/B forum. Furthermore, it only takes ONE certificate from any trusted CA to undermine the security of an entire new gTLD. This also ignores that people using those certificates now MUST have some timelines to make operational changes before their certificates are revoked, a problem only a small number of the CAs themselves have commented on, and have yet to accommodate. SAC057 and the entire set of discussions around this wholly ignore this key consideration.

Verisign believes, and has reiterated multiple times, that a single two day snapshot of data across a subset of the root servers annually is completely insufficient to assess risk and that and an early warning and instrumentation apparatus needs to exist at the root server system to enable all strings to be evaluated and addressed in a sustainable way. SAC045 and other SSAC documents have recommended various aspects of this over the past 4-plus years. Intersecting those measurements with a community developed risk matrix is the appropriate manner to measure risks of delegations of each individual string and proceed safely.