SAC062
SSAC Advisory Concerning the Mitigation of Name Collision Risk

An Advisory from the ICANN
Security and Stability Advisory Committee (SSAC)
07 November 2013

Preface

This is a Advisory to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning ICANN's proposal to mitigate name collision risks. The SSAC advises the ICANN community and Board on matters relating to the security, stability, and integrity of the Internet's naming and address allocation systems. This includes operational matters (*e.g.*, matters pertaining to the correct and reliable operation of the root name system), administrative matters (*e.g.*, matters pertaining to address allocation and Internet number assignment), and registration matters (*e.g.*, matters pertaining to registry and registrar services). SSAC engages in ongoing 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. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Advisory, references to SSAC members' biographies and statements of interest, and SSAC members' objections to the findings or recommendations in this Comment are at the end of this Comment.

Table of Contents

Executive Summary

In the context of top level domains, the term "name collision" refers to the situation in which a name that is properly defined in the global Domain Name System (DNS) namespace (defined in the root zone as published by the root management partners - ICANN, U.S. Dept. of Commerce National Telecommunication Information Administration (NTIA), and VeriSign) may appear in a privately defined namespace (in which it is also syntactically valid), where users, software, or other functions in that domain may misinterpret it.

The Security and Stability Advisory Committee (SSAC) provides the following advice to ICANN based on its assessment of the issues identified in the Interisle study and ICANN's proposal to mitigate potential collision risks.

With respect to the action on high-risk strings, the SSAC asserts the principle that strings with documented evidence of broad and significant private usage should be considered for permanent reservation for internal use to reduce security and stability issues, as well as to provide a stable namespace for parties using other strings to migrate to if they do not use fully-qualified domain names (FQDNs). The SSAC recommends ICANN work with the wider Internet community, including at least the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF), to identify (1) what strings are appropriate to reserve for private namespace use and (2) what type of private namespace use is appropriate (*i.e.*, at the TLD level or at any level).

With respect to trial delegation that was suggested by the ICANN New generic Top Level Domain (gTLD) Program Committee (NGPC) of the ICANN Board of Directors as a risk mitigation strategy option, the SSAC explores different types of trial delegation, their potential benefits, and risks of each option. The SSAC recommends that ICANN answer a set of key questions before delegating any TLD on a trial basis:

- *Purpose of the trial:* What type of trial is to be conducted? What data are to be collected?
- *Operation of the trial:* Should ICANN (or a designated agent) operate the trial or should the applicant operate it?
- *Emergency Rollback:* What are the emergency rollback decision and execution procedures for any delegation in the root, and have the root zone partners exercised these capabilities?
- *Termination of the trial:* What are the criteria for terminating the trial (both normal and emergency criteria)? What is to be done with the data collected? Who makes the decision on what the next step in the delegation process is?

With respect to the NGPC's decision to ask ICANN to develop a long-term plan to manage name collision risks related to the delegation of new TLDs, and to work with the community to develop a long-term plan to retain and measure root-server data, the SSAC supports this recommendation and views it as consistent with previous SSAC recommendations to establish measurement, monitoring and data sharing capability for the root server system. The SSAC believes that such a capability must be defined and deployed promptly. The capability must be sufficiently flexible to accommodate additional data that might need to be collected and analyzed for name collisions as well as other future requirements.

Finally, there is a possibility that significant security or stability problems may occur as a result of name collision after delegation, which could warrant taking emergency action, including the rapid reversal of the delegation of a TLD. The SSAC recommends ICANN update its procedures to prepare for such an emergency. Specifically, the SSAC recommends ICANN address two issues: first, the existing root zone management process needs to be updated to accommodate the potential need to rapidly reverse the delegation of a TLD; second, the un-delegation of any TLD is a significant event, and must be done with due process, openness, and a clear consideration of the impact on the name space that would be removed from the DNS. Therefore, ICANN must establish a set of conditions that make it evident that the only mitigation option available is the complete removal of the delegation of a TLD.

1. Introduction

The term "name collision" refers to the situation in which a name that is properly defined in one operational domain or naming scope may appear in another domain (in which it is also syntactically valid), where users, software, or other functions in that domain may misinterpret it as if it correctly belonged there. The circumstances that may cause this can be accidental or malicious. In the context of Top Level Domains (TLDs), the conflicting namespaces are the DNS namespace defined in the root zone as published by the root management partners (ICANN, U.S. Dept. of Commerce National Telecommunications Information Administration (NTIA), and VeriSign) and any privately defined namespace, whether that namespace is defined only for the Domain Name System (DNS) or is also intended to "work" for other namespaces such as Active Directory.

On 5 August 2013, ICANN published Interisle's study entitled "Name Collision in the DNS"[1] (hereafter called "Interisle study") as well as a staff proposal[2] to mitigate the potential risks associated with name collisions involving new generic TLDs (gTLDs). The staff proposal was posted for public comment and subsequently updated[3] by staff based on the public comments.[4] The ICANN Board of Director's New gTLD Program Committee (NGPC)[5] approved the staff-revised proposal on 7 October 2013.[6]

[1] See "Name Collision in the DNS," Interisle Consulting Group, version 1.5, at: <http://www.icann.org/en/about/staff/security/ssr/name-collision-02aug13-en.pdf>.

[2] See "New gTLD Collision Risk Mitigation Proposal," ICANN at: <http://www.icann.org/en/about/staff/security/ssr/new-gtld-collision-mitigation-05aug13-en.pdf>

[3] See "New gTLD Collision Occurrence Risk Mitigation Proposal," ICANN,4 October 2013 at: <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-1-07oct13-en.pdf>.

[4] See http://forum.icann.org/lists/comments-name-collision-05aug13/.

[5] See http://www.icann.org/en/groups/board/new-gtld for NGPC Charter and Membership.

[6] "Approved Resolution of the New GTLD Program Committee," ICANN. 7 October 2013. Retrieved October 11 2013 from http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-07oct13-en.htm.

The SSAC provides this document as advice based on its assessment of the issues identified in the Interisle study and ICANN's updated proposal to mitigate potential name collision risks.

The SSAC in general supports the NGPC proposal. This advice focuses on three specific areas of the NGPC proposal where SSAC has advice: the action on high-risk strings, trial delegation, and the development of a monitoring framework for the root zone.

2. High Risk Strings

ICANN's updated proposal states:

> "Based on the analysis of frequency of occurrence and the perceived severity of impact, ICANN will defer delegating ***home*** and ***corp*** indefinitely.
> ICANN will collaborate with the technical and security community to continue to study the issues presented by these strings."

The SSAC asserts the principle that strings with documented evidence of broad and significant private usage should be considered for permanent reservation for internal use to reduce security and stability issues, as well as to provide a stable namespace for parties using other strings to migrate to if they do not use fully-qualified domain names (FQDNs).

The fact that proposed TLD strings have been used by various parties in the global DNS namespace (as shown in the Interisle study) demonstrates that parties have a need for private use strings, similar to the use of private Internet Protocol (IP) address space as described in Request for Comments (RFC) 1918.[7] This has been a long-standing practice, as evidenced by the widespread use of ***home*** and ***corp*** today, and potentially other strings identified in the Interisle report.

Thus, the SSAC recommends that ICANN initiate a discussion on whether some strings should be permanently reserved for private use. Two important considerations for this discussion are: 1) what strings should be considered, and 2) whether the strings should also be reserved as second and lower level domains or only at the TLD level. For the first question, the SSAC notes that the Internet Engineering Task Force (IETF)/Internet Architecture Board (IAB) have discussed issues of local scope namespaces before, in for example RFC 6761 establishing a registry for future reservation of such namespaces and the appendix G of RFC 6762 describing existing usage of several such names. However, RFC 6762 does not reserve those strings.

[7] See RFC 1918: Rekhter, Y., Moskowitz, B., Karrenberg, D., and G. de Groot, "Address Allocation for Private Internets", February 1996 at: https://tools.ietf.org/html/rfc1918.

Recommendation 1: ICANN should work with the wider Internet community, including at least the IAB and the IETF, to identify (1) what strings are appropriate to reserve for private namespace use and (2) what type of private namespace use is appropriate (*i.e.*, at the TLD level only or at any additional lower level).

3. Trial Delegation

Section 3.2 of the NGPC mitigation proposal suggests that a trial delegation of some form be available to applicants as an appropriate risk mitigation strategy. The SSAC notes that there could be several types of trial delegation. In this section, we explore the types of trial delegation, perceived benefits, and potential risks.

The following questions are important while considering trial delegations:

- *Purpose of the trial:* What type of trial is to be conducted? What data are to be collected? The SSAC notes that trial delegations have been performed by ICANN in the case of IDN.IDN.[8] It was done with an explicit intent to determine impact on the DNS, and was implemented at both the TLD and the second level domain (SLD) levels. Test conditions were also established.[9]
- *Operation of the trial:* Should ICANN (or a designated agent) operate the trial or should the applicant operate it? What are the emergency rollback decision and execution procedures?
- *Termination of the trial:* What are the criteria for terminating the trial (both normal and emergency criteria)? What is to be done with the data collected? Who makes the decision on what the next step in the delegation process should be? The un-delegation of any TLD, even those set up for trial purposes, is a significant event, and must be done with due process, openness, and a clear understanding of the impact on the name space that will be removed from the global DNS.[10]

3.1 Types of trial delegation

There are two broad types of trial delegation:

- DNS Infrastructure Testing (Type I)
- Application and Service Testing and Notification (Type II)

In all cases, the Times to Live (TTLs) on DNS records that are part of the delegation should be in the order of minutes to at most a few hours. If any significant consequences develop, it will be necessary to initiate an emergency rollback process and the propagation of this change throughout the global DNS infrastructure should be minimized.

[8] See http://www.icann.org/en/news/announcements/announcement-15oct07-en.htm.

[9] See http://idn.icann.org/#Limited_evaluation_period.

[10] Recently, ICANN announced its decision to un-delegate IDN.IDN trial delegations. The rationale and process for making such a decision is unknown. The SSAC notes the lack of a report on findings from the IDN.IDN trial delegations, which would explain how the goals of the trial delegations were achieved and provide proper exit conditions for the un-delegation of a TLD.

3.1.1 DNS Infrastructure Testing (Type I)

A TLD could be temporarily delegated in the public DNS root zone for the sole purpose of collecting data regarding DNS queries that reach the authoritative server(s) for the TLD. Registration of domain names would not be permitted, and the only names permitted to exist in the zone would be those required as part of the data collection or testing. There are two variations to this type.

- **Type I-a**: The authoritative name server(s) for the TLD zone log every name in any request received, the time at which the request arrived, the Resource Record TYPE (RRTYPE) and CLASS in the request, and the source network of the request. The name server responds with RCODE 3 (Name Error or Non-Existent Domain (NXDOMAIN)) to every request.

- **Type I-b**: The trial delegation would establish the prevalence of how the trial-delegated TLD is used in internal configurations and how frequently it is used as part of the search path.[11] The basis for an experiment that activates certain SLDs under a trial-delegated TLD to capture and compare queries generated by a large number of sources was first proposed by Kolkman, et. al. in "Using Test Delegations from the Root Prior to Full Allocation and Delegation." [12]

3.1.2 Application and Service Testing and Notification (Type II)

The trial delegation could collect data on how names in the TLD are used and support a notification mechanism to users of the queried names. This type of delegation could trigger a name collision and thus provide a more complete test of potential consequences.

The authoritative name servers(s) would respond with wildcard and synthesized responses, as appropriate, for all queried strings that direct clients to one or more application servers deployed as part of the trial delegation. The name servers would log all queries as described in the DNS Infrastructure Testing trial delegation but would *not* respond with RCODE 3 ("Name Error" or "NXDOMAIN").

The application servers would listen for and accept application and service queries and connection requests, responding with an appropriate failure response indicating that the domain name the client is using is being sent to the public Internet and that this may not be what the client intends. Details about the queries and requests would be logged, including content, the time of receipt, and the network layer source addresses of the

[11] Search path behaviors are defined in RFC 1535. There could be side effects of name collision with respect to search paths as certain name resolver libraries first query the original name, and if the query returns an NXDOMAIN, they apply the local search list to the original name. When this process occurs in the context of a visible gTLD name colliding with the local name there is the possibility of the name resolving in the context of the gTLD, which then bypasses the application of the local search list.

[12] See "Using Test Delegations from the Root Prior to Full Allocation and Delegation" at: http://tools.ietf.org/html/draft-kolkman-root-test-delegation.

messages. Immediately after responding and logging, any connection request would be terminated (to minimize ongoing network issues). The list of applications and services to be studied should include, but is not limited to, Hypertext Transfer Protocol/Secure (HTTP/S), Simple Mail Transfer Protocol (SMTP), Extensible Messaging and Presence Protocol (XMPP), DNS, Network Time Protocol (NTP), Secure Shell Protocol (SSH), File Transfer Protocol (FTP), and Telnet.

An extension of this type of trial delegation would be to consider staffing a call center. The purpose of the call center would be to explain what is going on and to guide callers to additional resources, such as a knowledgebase or resource center that explains known issues and recommended mitigations.

3.2 Potential Benefits of Trial Delegation

The SSAC notes three benefits to trial delegation:

- It will produce more information (or at least data) about the consequences of delegating a proposed TLD, and that will help the ICANN Board make its decision about "real" delegation. ***(Type I and II trial delegation)***

- It will alert users by causing name collisions to occur and offering assistance with mitigation (e.g., helpful web page notices and informational chat/voice services at no cost to the user). ***(Type II trial delegation with proposed extension)***

- If the trial delegation is operated by ICANN, it would presumably be easier to quickly reverse the delegation if a significant consequence is discovered that required immediate mitigation. ***(Type I and II trial delegation).*** Otherwise, communications channels should exist with ICANN and the call center operator(s) to collect feedback and assess potential impacts.

3.3 Potential Risks of Trial Delegation

3.3.1 Risks related to DNS

From a DNS client perspective, the receipt of an RCODE 3 response from a trial delegation authoritative name server is indistinguishable from what is returned when the trial delegation is not active. Thus, trial delegation type I-a and type I-b introduce the least technical risk of a name collision.

Using wildcard records and synthesized responses in the DNS as described in the type II trial delegation presents a set of technical risks documented in several advisories from the

SSAC[13] and the IAB.[14] ICANN also prohibited the usage of wildcard records in the new gTLD program.[15]

As stated by the Interisle study, it is not possible to know in advance if the collection of data over a two-day period from the root servers is sufficient, or whether a longer sampling period is necessary. One view is that the two-day Day in The Life (DITL)[16] data, plus additional data provided by resolvers (*e.g.*, the Google resolver data[17] provided during the public comment period), is enough to calculate the risks associated with name collision. If better decisions are to be made, additional data from other sources would be needed, not simply a longer interval than two days of root server or authoritative TLD server data. Another view is that increasing the two-day sample to a week or more will catch events that only occur on a less frequent basis, or that were not within the observation space of the previous DITL collection window (e.g., non-participating root servers or lack of full coverage across root server "instances" for a given operator). While precision may be obtained within the DITL dataset, the DITL snapshot is far too short a window to ensure any level of accuracy. It should also be acknowledged that collecting more data will increase the risk that the system can be "gamed" and this will need to be considered as part of any additional analysis.

3.3.2 Other Considerations

Using wildcard resource records and synthesizing responses during a trial delegation period may be declared as acceptable for the purpose of satisfying the needs of the trial delegation. The SSAC remains committed to its prior recommendations related to wildcards and synthesized responses.

Some protocols pass authentication information to servers as part of the connection request. The trial delegation provider in the Application and Service Testing and Notification type of trial delegation would have access to this information. A policy and applicable procedures would need to be developed to handle and destroy this information.

If a consequence that causes significant harm is discovered during the trial delegation period, an emergency rollback process might be necessary that may include removing the delegation from the root zone. In other cases, returning NXDOMAIN (turning off wildcard) will be sufficient to mitigate the harm. This action will necessarily have to be decided and executed in as short a period of time as possible. However, the existing root

[13] See SAC 006: Redirection in the COM and NET Domains, SAC 015: Why Top-Level Domains Should Not Use Wildcard Resource Records, SAC 032: Preliminary Report on DNS Response Modification, SAC 041: Recommendation to prohibit use of redirection and synthesized responses by new TLDs.

[14] See http://www.iab.org/documents/correspondence-reports-documents/docs2003/2003-09-20-dns-wildcards/.

[15] See page 75 of New GTLD Agreement. http://newgtlds.icann.org/en/applicants/agb/agreement-approved-02jul13-en.pdf.

[16] DITL (day in the life of the Internet) is an annual large-scale simultaneous collection of Internet traffic for research purposes from a core component of the global Internet Infrastructure. The most recent collection event can be found at https://www.dns-oarc.net/node/325.

[17] See http://forum.icann.org/lists/comments-name-collision-05aug13/msg00072.html.

zone management process is not designed for changes that may occur in the order of minutes.

It may be difficult to determine when a consequence is itself harmful or to set the threshold for when a consequence is being experienced broadly and thus considered significant. It may be that the decision could be different depending on whether the delegation is operated by ICANN or by the applicant.

Finally, using trial delegation to notify users can create secondary effects that are negative. Because of the different protocols from which data will be collected, users may not be alerted in a consistent way. In some protocols and clients, the error message is often displayed to the user. In other protocols and clients that is not the case. On the positive side even though some users might not see the message, and some users that do see the message cannot do anything about it, there are still users that will see the message and can do something about it.

Recommendation 2: ICANN should explicitly consider the following questions regarding trial delegation and clearly articulate what choices have been made and why as part of its decision as to whether or not to delegate any TLD on a trial basis:

- *Purpose of the trial:* What type of trial is to be conducted? What data are to be collected?
- *Operation of the trial:* Should ICANN (or a designated agent) operate the trial or should the applicant operate it?
- *Emergency Rollback:* What are the emergency rollback decision and execution procedures for any delegation in the root, and have the root zone partners exercised these capabilities?
- *Termination of the trial:* What are the criteria for terminating the trial (both normal and emergency criteria)? What is to be done with the data collected? Who makes the decision on what the next step in the delegation process is?

Finally, there is a possibility that significant security or stability problems may occur as a result of name collision following the formal delegation of a TLD, which may not have arisen during the trial delegation. This could warrant taking emergency action, including the rapid reversal of the delegation of a TLD.

Should the rapid reversal of a delegated TLD be required, ICANN needs to address two issues: first, the existing root zone management process needs to be updated to accommodate the potential need to rapidly reverse the delegation of a TLD. Second, the un-delegation of any TLD is a significant event, and must be done with due process, openness, and a clear consideration of the impact on the established name space that would be removed from the DNS. Therefore, ICANN must document a set of conditions that make it evident that the only mitigation option available is the complete removal of the delegation of a TLD.

Recommendation 3: ICANN should explicitly consider under what circumstances un-delegation of a TLD is the appropriate mitigation for a security or stability issue. In the case where a TLD has an established namespace, ICANN should clearly identify why the risk and harm of the TLD remaining in the root zone is greater than the risk and harm of removing a viable and in-use namespace from the DNS. Finally, ICANN should work in consultation with the community, in particular the root zone management partners, to create additional processes or update existing processes to accommodate the potential need for rapid reversal of the delegation of a TLD.

4. Root Server System Monitoring

The SSAC notes the NGPC decision recommends to the ICANN Board that:

> "…it direct the ICANN President and CEO to develop a long term plan to manage name collision risks related to the delegation of new TLDs, and to work with the community to develop a long-term plan to retain and measure root-server data."[18]

The SSAC supports this recommendation and views it as consistent with previous SSAC recommendations to establish measurement, monitoring and data sharing capability for the root server system.[19] Additionally, the SSAC believes that such a capability must be defined and deployed promptly. The capability must be sufficiently flexible to accommodate additional data that might need to be collected and analyzed for name conflict/avoidance as well as other future requirements.

Furthermore, the establishment of instrumentation capabilities across the root server system in order to collect longer-term data regarding applied-for strings and other content-level behaviors going forward would be of clear benefit.

5. Acknowledgements, Statements of Interests, and Objections, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of our process. The Acknowledgments section lists the members who contributed to this particular document. The Statements of Interest section points to the biographies of all Committee members and any conflicts of interest—real, apparent, or potential—that may bear on the material in this document. The Objections section provides a place for individual members to disagree with the content of this document or the process for preparing it. The Withdrawals section is a listing of individual members who have recused themselves from discussion of the topic. Except for members listed in the Objections and Withdrawals sections, this document has the consensus approval of all members of the Committee.

[18] See NGPC Resolution http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-07oct13-en.htm#1.a

[19] See Recommendation 4 in SAC 046.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Report.

SSAC Members:
Don Blumenthal
Lyman Chapin
James M. Galvin
Mark Kosters
Patrik Fältström (Work Party Chair)
Robert Guerra
Sarmad Hussain
Danny McPherson
Ram Mohan
Russ Mundy

ICANN staff:
Francisco Arias
Julie Hedlund
Barbara Roseman
Steve Sheng (editor)

5.2 Statements of Interest

SSAC member biographical information and Disclosures of Interest are available at: http://www.icann.org/en/groups/ssac/biographies-08oct13-en.htm.

5.3 Objections and Withdrawals

Objection from KC Claffy and Paul Vixie

Our objection to SAC 046 (SSAC Report on Root Scaling[20]) applies here, although can now be strengthened with evidence from the Interisle study. That is, some proposed new TLDs will cause name collisions that will likely put some users at positive but unknown and unmeasurable risk of some unknown and unmeasurable harm. As has been true for years, and despite many recommendations to address data sharing issues, the current models of data collection and sharing among stakeholders are insufficient to show that adding a given TLD will not harm the interests of global Internet users. The proposed approach to experiment with trial delegation is an interesting research direction, but is vaguely described and itself carries security and stability risks. It may not work.

A larger issue is related to the current composition of this committee, which includes ICANN board members with legal fiduciary responsibility to ICANN and/or companies

[20] See https://www.icann.org/en/groups/ssac/documents/sac-046-en.pdf.

who will substantially profit from new gTLDS. Since SSAC reports reflect committee consensus, notwithstanding withdrawals and objections, this structure implies that no report will contain anything that could bring harm to ICANN or a company represented by any members of the committee with such fiduciary responsibilities.

In 2003 when ICANN asked this committee to provide advice with respect to the impacts of a disruptive change Verisign launched into the root zone,[21] Verisign employees on the committee recused themselves from any discussions related to drafting the report or its recommendations. There has been no such independence, and thus objectivity, on any SSAC report relating to new gTLDs.

Withdrawal from David Conrad

Due to an indirect contractual relationship I have with ICANN, I feel that I may be seen to be in a conflicted position with respect to the efforts of the name collision work party. As such, I have withdrawn from participating in the work party and will not comment on the document prior to publication.

[21] See http://www.icann.org/committees/security/ssac-report-09jul04.pdf.