Comments on Identifier Technology Innovation Panel Draft Report

VeriSign, Inc.
April 30, 2014

Verisign appreciates the work done by the Identifier Technology Innovation (ITI) panel over the past year to review longer-term developments in this area and recommend actions to ICANN and the ICANN community, as summarized in its February 2014 report [1].

The history of successful research and development enabled by the Internet's "permissionless innovation" model [2] demonstrates the benefits of community-led advances based on "rough consensus and running code" [3]. Reflecting a variety of Internet community initiatives around DNS and identifier technology, the panel has selected a reasonable set of longer-term topics for its advice. The actual impact of those topics may well vary over time, as the community continues to explore and apply new insights, and as specific use cases – not one of the deliverables of the report – become better defined.

Verisign encourages ICANN to continue to draw from the ongoing innovation by its stakeholders as it develops and implements its strategic plans. In particular, the report's fourfold objectives of providing a technology roadmap, best practice recommendations, technology guidance and community engagement around identifier technologies should not be taken as implying a new operational role for ICANN in any or all of the above, but rather as a framework for ongoing innovation by the Internet community that ICANN supports.

Some additional comments are in order for a few of the topics.

- **Open root publication.** The panel's report introduces a new approach for making root zone records available more broadly by distributing DNSSEC-signed root zone files via a new, open network of alternate root servers. The report claims that to the extent that the current deployment of root servers is criticized for geopolitical limitations, this approach would "just make the issue go away" (Section 4.2).

  In principle, the approach makes a lot of sense: as the DNSSEC-signed root zone file becomes more widely available, the DNS becomes more resilient.[1] But in practice, such an approach is not a panacea, because, until DNSSEC is broadly validated, the more servers that are considered "authoritative," the more opportunities there are for data integrity to be compromised (the natural tradeoff between integrity and availability). This is particularly pertinent because the

[1] It's important, however, not to conflate the *number* of root server instances in a given region with the aggregate *capacity* of those instances. If the objective of a use case is to improve DNS performance in a region, a single large instance may well outperform a network of small instances.

approach “will allow any name server operator to capture traffic headed toward the root server system and respond to it locally” (Sec. 9.4).

Any eventual deployment of the approach should also include careful operational oversight of the proposed “universal anycast” catchments to audit attempts to misuse the traffic capture. Such auditing is already needed to detect misdirection of traffic routed to the root server system today, but the proposed scale is much greater for the alternate root servers, given the proposal of making a root server an “unmanaged utility” that can be served up by anyone. The complexities of DNSSEC key rollover and trust anchor updates in the root zone [4] further reinforce the importance of such oversight.

For the current root server system, it remains vital that root-server instrumentation be implemented per RSSAC001 and 002 (a point amplified, in the context of name collision risk management, in the JAS Global Advisors Phase One Report [5] at Recommendations 10 and 11). It should be obvious that a root system distributed as broadly as is proposed would pose unprecedented challenges to root server system visibility, the implications of which must be considered very carefully in navigating policy objectives.

- **Root zone signing.** Shortly after the panel’s report was published, NTIA announced its intention to transition the oversight of the IANA function to a multistakeholder process [6]. The transition has brought increased attention to the importance of root zone management.

  The panel’s longer-term goal of a “system for initiating a shared zone consisting of the zone itself, rules, and individual journals” (Section 4.3) already has its parallel in the objectives for more transparency and accountability of the root server system under its current shared control. In general, there is still room for improvement in current practice. Fantastic algorithmic approaches for distributed DNSSEC signing might help in the longer term, but with or without them, the key to effective delivery is a well-managed set of checks and balances for implementing the rules the community has agreed on, such as RSSAC001 and 002 referenced above.

  In remarks at ICANN 49 in Singapore, Pat Kane, senior vice president and general manager, Verisign Naming and Directory Services, reiterated the importance of the expertise of the Root Zone Maintainer role that Verisign currently provides, stating “We strongly believe that if there is a transition to another party, this technical role -- for this technical role, that our record and the operational practices that made that record possible should be the standard to which successors are held” ([7], page 33). Along these lines, the simple four-step outline of the root-zone update process in the panel’s report glosses over one of the checks and balances already available: The Root Zone Maintainer, in addition to signing and distributing the root zone file, also vets the correctness of any changes, a community benefit well illustrated by recent examples [8].[2]

- **Name collisions.** Verisign supports the panel's recommendation (Section 4.6) to test ICANN's guidance on name collision mitigation [9], and has provided a longer set of comments on the name collisions issue separately [10][11].

- **DNS API.** The new programming interface mentioned in the panel's report (Sections 5.4 and 10.2) is now available as the getdns API [12]. The API was just tested at a hackathon at The Next Web conference [13]. Among the features of the API, as previewed in the presentation by Paul Hoffman in Section 10.2, is support for DNSSEC validation at the client, one of the panel's unanimous recommendations.

References

[1] *Identifier Technology Innovation Panel – Draft Report.* ICANN, February 21, 2014. http://www.icann.org/en/about/planning/strategic-engagement/identifier-technology/report-21feb14-en.pdf

[2] Leslie Daigle. *Celebrating 25 Years of the World Wide Web – What's Next for the Internet?* Tech Matters, Internet Society, March 12, 2014. http://www.internetsociety.org/blog/tech-matters/2014/03/celebrating-25-years-world-wide-web-%E2%80%93-what%E2%80%99s-next-internet

[3] David D. Clark. "A Cloudy Crystal Ball – Visions of the Future." In *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, pages 540-543. CNRI, July 13-17, 1992. http://www.ietf.org/proceedings/24.pdf

[4] *SAC063: SSAC Advisory on DNSSEC Key Rollover in the Root Zone.* ICANN Security and Stability Advisory Committee, November 7, 2013. http://www.icann.org/en/groups/ssac/documents/sac-063-en.pdf

[5] *Mitigating the Risk of DNS Namespace Collisions: Phase One Report.* JAS Global Advisors, February 24, 2014. http://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-26feb14-en.pdf

[6] *NTIA Announces Intent to Transition Key Internet Domain Name Functions.* National Telecommunications and Information Administration, United States Department of Commerce, March 14, 2014. http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

[7] *IANA Accountability Transition | Transcript.* ICANN, March 24, 2014. http://singapore49.icann.org/en/schedule/mon-iana-accountability/transcript-iana-accountability-24mar14-en.pdf

[2] The discussion of replication at the start of Section 4.2 also requires clarification: In the standing process implemented by the Root Zone Management Partners, the root zone is generated not by any one entity, but through the defined roles of ICANN, the Department of Commerce, and Verisign as Root Zone Maintainer.

[8] Burt Kaliski and Patrick S. Kane. *Update on Root Zone System Changes.* Email to Vernita D. Harris, February 21, 2014. http://www.scribd.com/doc/209471521/Update-on-Root-Zone-System-Changes

[9] *Guide to Name Collision Identification and Mitigation for IT Professionals.* ICANN, December 5, 2013. https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[10] Burt Kaliski. *Verisign preliminary comments on "Mitigating the Risk of DNS Namespace Collisions" Phase One Report.* comments-name-collision-26feb14 discussion thread, March 31, 2014. http://forum.icann.org/lists/comments-name-collision-26feb14/msg00010.html

[11] Burt Kaliski. *Verisign additional comments on "Mitigating the Risk of DNS Namespace Collisions" Phase One Report.* comments-name-collision-26feb14 discussion thread, April 21, 2014. http://forum.icann.org/lists/comments-name-collision-26feb14/msg00023.html

[12] Paul Hoffman (editor). *Description of the getdns API (document version February 2014).* Accessed April 28, 2014. http://vpnc.org/getdns-api/

[13] Allison Mankin. *Introducing getdns: a Modern, Extensible, Open Source API for the DNS.* Between the Dots, Verisign, April 23, 2014. http://blogs.verisigninc.com/blog/entry/introducing_getdns_a_modern_extensible