Comments on ICANN’s Draft Report of the Root Zone DNSSEC Algorithm Rollover Study

Burt Kaliski and Duane Wessels
VeriSign, Inc.
December 4, 2023

(These comments are provided in response to ICANN’s call for public comments on the document “Root Zone Algorithm Rollover Study (Draft).”[1])

Introduction

The Domain Name System Security Extensions (DNSSEC) have enabled resolvers, applications and other relying parties to validate DNS data for more than a decade. During that time, following recommended practices for cryptography, DNSSEC key signing and zone signing keys have been updated at various frequencies throughout the DNS hierarchy, including the root,[2] and DNSSEC signature algorithms have been changed occasionally as well, with the first such change at the root now under review.

ICANN’s leadership has been instrumental throughout these changes, from the 2010 rollout of DNSSEC at the root[3] to the first root zone KSK rollover in 2018 to the planning for this algorithm rollover.

Verisign supports the recommendations in the report and appreciates the opportunity to contribute to its development in our role as the Root Zone Maintainer. As the report text is necessarily limited in scope, we also wanted to offer additional observations in three areas that may be helpful in providing broader context for the use of the report.

On Mitigating Potential Instability

As announced in August,[4] Verisign is in the process of an algorithm rollover for three of the top-level domain (TLD) zones that we operate. The .edu and .net rollovers were completed in September and November respectively. The .com rollover is currently underway and will conclude later this month.

As part of the rollovers, we have been closely monitoring the data contemplated in draft recommendation 8 — “response sizes and the amount of traffic subject to truncation …” — to prepare

[1] ICANN. *Draft Report of the Root Zone DNSSEC Algorithm Rollover Study.* Oct. 19, 2023. https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023

[2] ICANN. *First Root KSK Rollover Successfully Completed.* Oct. 15, 2018. https://www.icann.org/en/announcements/details/first-root-ksk-rollover-successfully-completed-15-10-2018-en

[3] ICANN. *DNSSEC Deployment in Root Zone of DNS Begins at ICANN.* Jan. 27, 2010. https://www.icann.org/en/announcements/details/dnssec-deployment-in-root-zone-of-dns-begins-at-icann-27-1-2010-en

[4] Wessels, D. *Verisign Will Help Strengthen Security with DNSSEC Algorithm Update.* Verisign blog, Aug. 10, 2023. https://blog.verisign.com/security/dnssec-algorithm-update/

for any potential operational impact. Section 4 of the report notes the possibility of "increased query load from misbehaving recursive resolvers." During our monitoring, we encountered evidence of misconfigured resolvers that fail to retry truncated responses over TCP transport and instead retry repeatedly over UDP. SIDN Labs observed similar behavior during its recent algorithm rollover for the .nl TLD, noting that "it seems that some resolvers still don't have reliable DNS-over-TCP support, despite TCP always having been a central feature of the DNS protocol."[5]

We have prepared for the possibility that interacting with these misconfigured resolvers according to currently recommended DNS practices, including RFC 9471, may increase both the volume of traffic from the resolvers during the "double signing" period of the rollover, and the risk that the resolvers are unable to handle the algorithm rollover.

As the draft report notes, the potential instability introduced to resolvers during the algorithm rollover is primarily due to larger response sizes which, per Section 5.6, "can vary depending on the query name, the number of delegated name servers, and their corresponding glue records" in addition to the number and size of the DNSSEC signatures.

One way to reduce the size impact is therefore to reduce the size of the zone signatures in the response. draft recommendation 10 accordingly contemplates a temporary change from 2048-bit RSA to 1536-bit RSA. (This option is not applicable to Verisign's TLD algorithm rollovers as our RSA zone key size is already reduced, at 1280 bits.)

Another way to reduce the size impact is to reduce the number of glue records returned, an arrangement that could be coordinated between ICANN and TLD operators if needed.

We appreciate the design team's careful attention to the increased size impact, reflected in draft recommendations 7–10, and are prepared to share data and insights from our experience with the .edu, .net and .com algorithm rollovers as needed to support the root zone rollover preparations.

Outreach to Applications Using DNSSEC Trust Chains

Building on the successful outreach efforts to during the 2018 KSK rollover, draft recommendations 19–22 contemplate engagement with resolver operators and other validators prior to an algorithm rollover. Such ecosystem-level preparation is both vital to ICANN's mission and essential to "those relying on DNSSEC protections," who, as the report notes in its introduction, must "perform their duties as well."

Among the other validators, in addition to resolvers in the traditional DNS ecosystem, we encourage ICANN to include emerging applications that use a DNSSEC chain of trust as evidence of actions by a domain name registrant, for instance when integrating a DNS domain name for use as an identifier in an application.[6] While many applications rely on recursive resolvers for DNSSEC validation --- indeed, as stated in the report, "[s]tub resolvers, by definition, only communicate with recursive resolvers, and most do not perform DNSSEC validation" — other applications perform DNSSEC validation themselves.

[5] Müller, M. Algorithm Rollover: The Effects on Our Network Traffic and Resolvers. SIDN Labs blog, Aug. 22, 2023. https://www.sidnlabs.nl/en/news-and-blogs/algorithm-rollover-the-effects-on-our-network-traffic-and-resolvers

[6] Sheth, S. *Bridging Perspectives: Understanding the Challenges and Opportunities in Current DNS Integrations.* Presented at ICANN DNS Symposium 2023, Sept. 5, 2023. https://www.icann.org/en/system/files/files/presentation-bridging-perspectives-challenges-opportunities-current-dns-integrations-05sep23-en.pdf

Ensuring those applications also appropriately support new algorithms will be as important to DNSSEC's overall impact as enabling recursive resolvers, and perhaps, due to their relatively new presence at a higher layer in the infrastructure, somewhat easier to accomplish.

Preparing for Post-Quantum Cryptography

Draft recommendation 26 proposes a timeline for the algorithm rollover "following the second KSK rollover, in approximately five years"— or around 2028–2029. Meanwhile, the timeline for the US government's migration to post-quantum algorithms includes dates as early as 2035.[7] Accordingly, with root zone KSK rollovers planned at five-year intervals[8], the second root zone algorithm rollover in the mid-2030s may well involve the incorporation of post-quantum cryptography. That timeline means that while post-quantum DNSSEC is still long-term for deployment, it should be medium-term for standardization and thus short-term — now — for research and development.

Such considerations, as well as the various potential deployment delays outlined in Section 6.3, have motivated Verisign's increased attention to this technology area in the past few years, exemplified in our co-authorship of an Internet-Draft titled "Research Agenda for a Post-Quantum DNSSEC."[9] In addition, we have announced[10] a public, royalty-free license to Merkle Tree Ladder mode,[11] a technique we developed for reducing the size impact of signature algorithms in applications such as DNSSEC.

If the DNSSEC use case is not adequately considered as post-quantum cryptography is standardized and deployed over the next decade, the software and hardware supply chain for post-quantum signature algorithms may well be optimized for other use cases that do not reflect DNSSEC's unique operational requirements. Put another way, the "primary reason for not going to PQ algorithms in the near future" (Section 5.1.2) — that current algorithms with their large signature sizes (or key sizes) aren't a good match for DNSSEC — should also be a primary reason for engaging with the community to identify techniques that are a better fit. This concern makes ICANN's early attention to post-quantum DNSSEC, including its publication of OCTO-031[12] and its leadership in establishing and co-chairing the IETF's Post-Quantum Use In Protocols (PQUIP) working group,[13] particularly important. We appreciate ICANN's efforts and are grateful for the opportunity to collaborate.

[7] The White House. *NSM-10: National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.* May 4, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[8] RZ KSK PMA. *DNSSEC Practice Statement for the Root Zone KSK Operator.* 6th edition, Nov. 4, 2020. https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html

[9] Fregly, A., van Rijswijk-Deij, R., Müller, M., et al. *Research Agenda for a Post-Quantum DNSSEC.* Internet-Draft, September 26, 2023. https://datatracker.ietf.org/doc/draft-fregly-research-agenda-for-pqc-dnssec/

[10] Kaliski, B. *Next Steps in Preparing for Post-Quantum DNSSEC.* Verisign blog, July 20, 2023. https://blog.verisign.com/security/post-quantum-dnssec-preparation/

[11] Harvey, J., Kaliski, B., Fregly, A., and Sheth, S. *Merkle Tree Ladder Mode (MTL) Signatures.* Internet-Draft, July 10, 2023 (last updated October 23, 2023). https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/

[12] Hoffman, P. OCTO-031: *Quantum Computing and the DNS.* ICANN OCTO, Feb. 11, 2022. https://www.icann.org/en/system/files/files/octo-031-11feb22-en.pdf

[13] Post-Quantum Use In Protocols (pquip). IETF, accessed Dec. 1, 2023. https://datatracker.ietf.org/wg/pquip/

Conclusion

DNSSEC offers a fundamental service for authenticating internet infrastructure data. As ICANN's draft report has shown, maintaining the security, stability and resiliency of that service requires ongoing attention to the management of DNSSEC keys and algorithms, and in particular to how the most critical component —the root zone KSK — is changed over time.

Verisign supports the recommendations in the report, to which we have contributed in our role as Root Zone Maintainer. We have offered here some additional observations as a community member which we hope are helpful to the overall effort. We encourage continued, data-driven community engagement to prepare for the root zone algorithm rollover and look forward to delivering on the eventual algorithm rollover, further strengthening DNSSEC for the long term.