Comments on Post-Quantum Cryptography in ICANN's SSR2 Final Report

Andy Fregly and Burt Kaliski
VeriSign, Inc.
March 9, 2021

(These comments are provided in response to ICANN's call for public comments on the document "Second Security, Stability, and Resiliency (SSR2) Review Team Final Report."[1])

Verisign offers the following brief comments on certain findings in the ICANN SSR2 final report relative to the applicability of hash-based public-key cryptography to DNSSEC. The following excerpt (from page 55 of the report) contains the statements of concern:

> "In the meantime, researchers agree that hash-based signatures are post-quantum safe. The Internet Research Task Force (IRTF) has specified these signature algorithms in their Crypto Forum Research Group (CFRG), using small private and public keys with a low computational cost. **However, the signatures are quite large, and a private key can only produce a finite number of signatures. These two properties make hash-based signatures undesirable in the DNSSEC environment.**" (emphasis added)

We appreciate the early attention to the potential for future changes in DNSSEC's algorithms in response to the anticipated standardization of post-quantum digital signature algorithms in the coming years. DNSSEC's ongoing resilience would benefit from the availability of digital signature algorithms of different types that would not likely be subject to the same attack methods.

While the report (p. 55) has outlined advantages and disadvantages of the hash-based family of signature algorithms under consideration by NIST, the relevant post-quantum cryptography specifications are still evolving. Indeed, the findings quoted have no corresponding recommendation. Although Recommendation 23, which appears immediately following the quoted statements, advises PTI operations to prepare for a rollover to a new signature algorithm, the recommendation leaves the algorithm unspecified. We encourage ICANN to continue to track developments without prematurely concluding for or against any candidate.

In a January 2021 update[2] on NIST's post-quantum cryptography project, Dustin Moody noted the recent cryptanalytic advances against the multivariate family of algorithms. If multivariate signature algorithms are ultimately not adopted, the other main family under review is the lattice-based family. NIST has previously recognized the risk of having only lattice-based algorithms and has advocated for

[1] ICANN, *Second Security, Stability, and Resiliency (SSR2) Review Team Final Report,* January 25, 2021, https://www.icann.org/public-comments/ssr2-final-report-2021-01-28-en

[2] Dustin Moody, *An Update on the NIST PQC "Competition",* presented at Real World Crypto (RWC) 2021, January 12, 2021, https://rwc.iacr.org/2021/slides/moody.pptx. See also video recording, https://youtu.be/X0Y6D5zLI-Y at 16:34, 17:56 and 18:45

the development of signature algorithms of other types.[3] Therefore, ruling out hash-based signatures at this time may lead to a future lack of algorithm diversity in DNSSEC.

To ensure that an appropriate variety of choices are available for DNSSEC, we encourage ICANN to ensure that its concerns about the applicability of candidate algorithms to the DNSSEC use case and their desirable characteristics are appropriately reflected in the evaluation processes for such algorithms, e.g., as currently conducted by NIST or within the IETF.

Verisign has published two recent blog posts about hash-based signatures that provide additional perspective on our research into hash-based signatures and DNSSEC.[4,5] (Our statements in these posts do not necessarily represent Verisign's plans or position on possible new products or services.)

We would like to thank ICANN for its efforts on the SSR2 report including early attention to post-quantum cryptography, and look forward to supporting ICANN in further developments.

[3] NISTIR 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NIST, July 2020, https://doi.org/10.6028/NIST.IR.8309. See Page 26: "In particular, NIST would be interested in a general-purpose digital signature scheme which is not based on structured lattices."

[4] Burt Kaliski, Securing the DNS in a Post-Quantum World: New DNSSEC Algorithms on the Horizon, Verisign Blog, January 19, 2021, https://blog.verisign.com/security/securing-the-dns-in-a-post-quantum-world-new-dnssec-algorithms-on-the-horizon/

[5] Burt Kaliski, *Securing the DNS in a Post-Quantum World: Hash-Based Signatures and Synthesized Zone Signing Keys*, Verisign Blog, January 21, 2021, https://blog.verisign.com/security/securing-the-dns-in-a-post-quantum-world-hash-based-signatures-and-synthesized-zone-signing-keys/

