Crypto4A's Comments on ICANN's SSR2 Final Report

Jim Goodman & Bruno Couillard, Crypto4A

April 7, 2021

Crypto4A has read and reviewed ICANN's SSR2 Final Report (dated January 25, 2021) and has the following comments:

1. Page 55 of the report includes a blanket statement regarding the unsuitability of Hash-Based Signatures (HBS) for use as a post-quantum safe signature mechanism due to their finite capacity and relatively large signature size[1]. The authors note that NIST is working on devising post-quantum safe signature schemes as part of their Post Quantum Cryptography (PQC) standardization effort. Unfortunately, that effort's timeline will mean that recommendations won't be made for several years (2024 is the projected standardization date for digital signatures[2]). HBS has already been standardized by NIST (SP800-208), and new variants are being proposed to address the size concerns without compromising their security[3]. Furthermore, recently the NIST team has raised concerns[2] regarding the security of one of the potential finalists (Rainbow) that call into question the diversity of alternatives given that the remaining two finalists (Dilithium and Falcon) are both lattice-based schemes. This could result in a lack of algorithm diversity for DNSSEC signatures. Hence, Crypto4A feels it is prudent to not dismiss the potential use of HBS for DNSSEC at this point in time, but instead continue to investigate methods to mitigate the aforementioned concerns while we wait for NIST's PQC process to reach its conclusion.

2. Recommendation 23.1 identifies the need to prepare for the transition to some form of post-quantum signature algorithm, but doesn't provide specific details regarding the likely timing of this transition, or potential candidate algorithm. Furthermore, current root and top-level domain DNSSEC practice statements[4] explicitly state the need to use Hardware Security Modules validated by NIST's FIPS 140-2/3 certification process. In the past NIST has discussed potential methods for transitioning from classical (e.g., RSA or ECDSA) to post-quantum algorithms in a FIPS-compliant manner via the use of a dual signature method that signs objects with both a post-quantum and a classical FIPS-compliant signature method[5]. This approach is intended to serve as a stop-gap until NIST's PQC standardization process identifies, and standardizes, an appropriate PQC signature mechanism. If the dual signature method were considered for adoption by DNSSEC then it would lead to combined signature sizes on the same order as HBS (e.g., RSA4096 + Falcon Level

[1] Benefits are mentioned as well, but ICANN's position appears to be that they don't outweigh the aforementioned issues.

[2] As mentioned in their recent presentation at Real World Crypto 2021, which is available online at https://rwc.iacr.org/2021/slides/moody.pptx

[3] Available at https://tools.ietf.org/html/draft-fluhrer-lms-more-parm-sets-02

[4] For example: https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html

[5] Referenced as part of NIST's PQC FAQ at https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

1 ≈ 512 + 666 = 1178 bytes whereas LM-HBS(h/w/n = 20/8/24) = 1144 bytes). This may help motivate further study/consideration of HBS-based techniques.

3. Recommendation 23.2 highlights the complexities and difficulties associated with the DNSKEY algorithm rollover process. ICANN may want to consider looking at some of the key rotation mechanisms and concepts being proposed for decentralized key-management infrastructure (DKMI). One such proposal, Key Event Receipt Infrastructure (KERI)[6], uses the notion of pre-rotation to provide secure verifiable key rotation, and can be done in a quantum-safe manner via an appropriate choice of hashing function used to generate the digest of the next public key in the rotation. In a very simplified view of the process, two keypairs are generated at inception, with the first being used, and a hash of the second public key being provided as a form of commitment to the next keypair. The first keypair becomes the current keyset, while the second keypair remains hidden as the next keyset. When a rotation is to be performed the first keypair is discarded, the second keypair now becomes the current keyset, a third keypair is generated as the next keyset, and a hash of the third public key is provided as a commitment to the next keypair. This update/generate/hash/distribute sequence is repeated with each rotation operation. All key rotation messages are signed with the current keyset being enabled by the message, and the current public key provided as part of that rotation message can be hashed and compared to the commitment provided with the previous rotation message to ensure the rotation sequence hasn't been tampered with. We don't claim that this approach is a perfect fit to the DNSSEC rollover process, but the concepts it promotes may prove useful for researchers and designers thinking about the future of DNSSEC.

Crypto4A would like to thank ICANN for their efforts to promote thinking about post-quantum cryptography in the SSR2 report as we feel it is a critical, and often overlooked, element of any security-related planning for the future. We are committed in supporting these efforts in whatever way we can.

[6] Available at https://arxiv.org/abs/1907.02143