**DNS Cryptography**

There are two topics that were investigated by the SSR2 Review Team. First, the team investigated the transition from the RSA algorithm to an elliptic curve algorithm for DNSSEC signatures. Second, the team investigated the need to transition to a post-quantum digital signature algorithm.

**Elliptic Curve Cryptography**

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.

ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

The technology can be used in conjunction with most public key encryption methods, such as digital signature, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage

**Post Quantum Cryptography**

Most people had not heard of quantum computing a decade ago, but in recent years, it has captured the public’s imagination. Part of this interest comes from the unique computational power of a quantum computer. The US National Academy of Sciences recently issued a report on “Quantum Computing: Progress and Prospects,”[[1]](#footnote-1) with the high-level conclusion that now is the time to start preparing for a quantum-safe future.

DigiCert has estimated that it takes several quadrillion years to factor a 2048-bit RSA key[[2]](#footnote-2) using classical computing technology. In the future, if a large-scale quantum computer is invented, it can break the same key much faster, perhaps only a few months. There are still many technical challenges that must be overcome before it is possible to build a quantum computer that threatens RSA and ECC, the two main asymmetric cryptographic algorithms are used to secure the Internet.

Progress towards a large-scale quantum computer must track not only the scaling rate of the number of physical quantum bits or “qubits” the computers have, but also error rates. Error rates are important because they have a big impact on the number of physical qubits required to make a logical qubit. Physical qubits are the individual quantum systems that represent either a zero or a one; however, physical qubits are prone to errors, through unavoidable interactions with their environment, even at temperatures approaching absolute zero. Many physical qubits can be combined into a single logical qubit, and the additional qubits are used to detect and correct these errors. Researchers have yet to produce even a single logical qubit, however progress is rapidly being made towards that goal. Once logical qubits are available, tracking the number of logical qubits will be the metric to track.

Industry standards groups are also preparing for a post-quantum future. The most well-known activity is the NIST post-quantum cryptography project[[3]](#footnote-3), which is working with researchers around the world to develop new cryptographic primitives that are not susceptible to attack by quantum computers. One can expect that project to take several more years before the resulting algorithms are ready for standardization.

In the meantime, researchers agree that hash-based signatures are post-quantum safe. These signature algorithms have been specified by the IRTF in the Crypto Forum Research Group (CFRG), and they use small private and public keys, and they have low computational cost. However, the signatures are quite large, and a private key can only be used to produce a finite number of signatures. While these algorithms are available today, these last two properties make hash-based signatures undesirable in the DNSSEC environment.

Root KSK DPS[[4]](#footnote-4) states

**6.1 Key lengths and algorithms

“ Key pairs are required to be of sufficient length to prevent others from determining the key pair's private key using crypto-analysis during the period of expected utilization of such key pairs.

 The current RZ KSK key pair(s) is an RSA key pair, with a modulus size of 2048 bits.”**

**6.5 Key signing key roll-over

“ Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

 RZ KSK roll-over is scheduled to facilitate automatic updates of resolvers' Trust Anchors as described in RFC 5011 [RFC5011].

 After a RZ KSK has been removed from the key set, it will be retained after its operational period until the next scheduled key ceremony,

 when the private component will be destroyed in accordance with section 5.2.10.”**

The DPS says nothing about how changes to key length, key type, and algorithm may be performed.

Some clarifications may be along those below:

* Why is there no information about changes to root KSK type, length and algorithm?
* Are there any studies about transitioning root KSK to new algorithm or key size?

Recent guidance from NSA is suggesting 3072 bits for RSA and Diffie Hellman[[5]](#footnote-5) and preparation for post quantum algorithm.

Answers to these questions could be derived from the questions below already sent to Staff.

* Does the TEG or some other group provide information about new crypto algorithms?  Where?
* What resources and processes are in place to track and make the Board aware and factor into strategic planning for this?
* What analyses or study/studies have been done?

**Recommendations**

1. The National Academies Press, “Quantum Computing: Progress and Prospects,” <doi:10.17226/25196>, 2018. [↑](#footnote-ref-1)
2. https://www.digicert.com/TimeTravel/math.htm [↑](#footnote-ref-2)
3. https://csrc.nist.gov/projects/post-quantum-cryptography [↑](#footnote-ref-3)
4. <https://www.iana.org/dnssec/icann-dps.txt> [↑](#footnote-ref-4)
5. https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf) [↑](#footnote-ref-5)