ERICSSON

Date: May 24, 2023

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on SP 1800-38A, Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography

Dear NIST,

Thanks for your continuous efforts to produce well-written open-access security documents.

Please find below our comments on SP 1800-38A:

- We think the term "post-quantum" is likely to be confusing to many readers as post-quantum cryptography needs to be deployed **before** Cryptanalytically Relevant Quantum Computers (CRQC) are built. We suggest that NIST only use the term "quantum-resistant". This would also align NIST with CNSA 2.0 [1].

- We think SP 1800-38A should mention Cryptanalytically Relevant Quantum Computers (CRQCs). It is important that readers understand that there is a huge difference between current quantum computers and CRQCs.

- We are surprised that NIST SP 800-57 Part 1 [2], the globally used standard for migration between cryptographic algorithms with different security levels is not even mentioned in SP 1800-38A. NIST SP 800-57 Part 1 has been an excellent tool for governments, industry, and other standardization organizations. It is as relevant for the migration to quantum-resistant algorithms as it was in the migration from 3DES to AES and from SHA-1 to SHA-2. The migration to quantum-resistant algorithms is not different. NIST should, as it has always done in the past, well in advance announce an expiration date for algorithms like RSA-3072 and P-256 so that industries can migrate based on the security life of the data the algorithm is protecting. NIST should consider updating SP 800-57 to include the time required for algorithm update (the y in Mosca's xyz theorem). Many systems are unfortunately not following NIST SP 800-57 recommendations to be flexible in order to accommodate cryptographic updates.

- Migration should not come at once; the first step is to categorize and do a risk assessment. The migration should then start with systems identified as high risk and high value. The NIST Risk

Management Framework (RMF) [3] is a widely deployed and solid framework, but it needs to be modified to cover PQC. We think NIST should extend or modify the RMF so that it covers PQC risks and walk readers through the migration risk analysis process. If CRQCs are ever built, early CRCRs will likely be very expensive and only used in targeted attacks to recover keys and ciphertexts that are of particular interest. Items that might be vulnerable for a long time include information that needs confidentiality over long periods of time, verification of software and firmware updates, and digital signatures for non-repudiation. NIST SP 800-57 Part 1 Rev. 5 gives an example where the security life of the data is 4 years, see the figure below. Given that NSA expects the transition to QR algorithms for NSS to be complete by 2035 [1], many other use cases that do not need to protect classified TOP SECRET information for 50-75 years can migrate at a later point. DNSSEC has for example taken the decision to not migrate at this point in time [4].

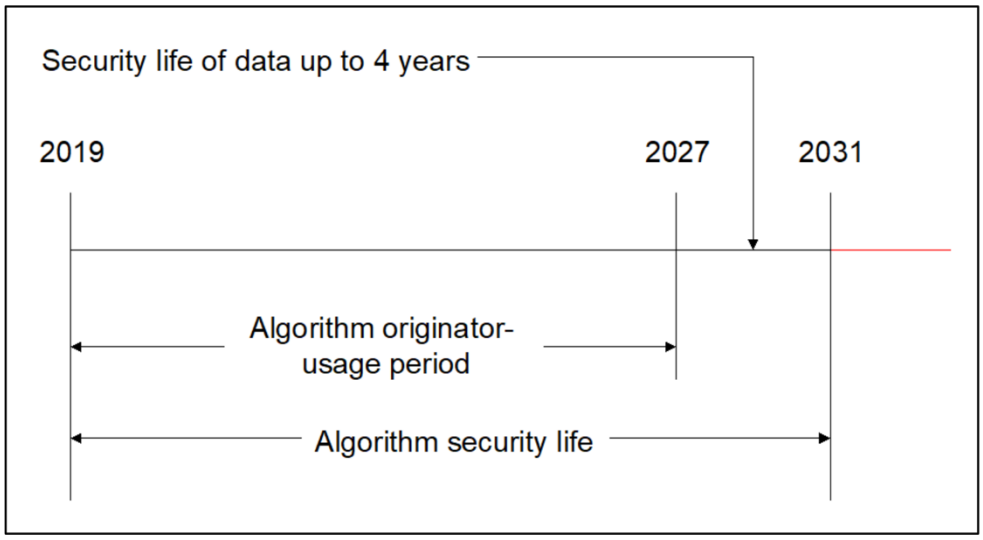

Figure 2: Algorithm originator-usage period example

– We think SP 1800-38A should give a bit more information on the current status of quantum-resistant algorithms. Most uses of public-key cryptography are in security protocols. After NIST has standardized quantum-resistant algorithms, updates to security protocols such as TLS, IKEv2, X.509, COSE, JOSE, and HPKE need to be standardized by the IETF and other standardization organizations like 3GPP needs to update their standards with profiles of the IETF protocol standards. Implementations need to be hardened and, in some cases, certified before they are used. Using non-standardized algorithms and protocols, or non-hardened implementations would lower security rather than strengthen it.

– *"Identifying interoperability and performance challenges that applied cryptographers may face when implementing the first quantum-resistant algorithms NIST will standardize in 2024."*

  Challenges with the already standardized quantum-resistant stateful hash-based algorithms LMS and XMSS [5] should also be in scope. CNSA 2.0 [1] approves these for firmware and

software signing. LMS and XMSS are however impossible to use in many applications as NIST forbids keying material to be exported, even in encrypted form [5].

- NIST should formally define the term crypto agility and discuss it in SP 1800-38A. Crypto agility is quickly turning into a marketing phrase and being used to sell out of the box PQC migration solutions. An industry definition from NIST is needed to define crypto agility as the ability to swap out algorithms without deep code revision or immense downtime, instead of a one-time migration.

- SP 1800-38A seems to indicate that NIST is likely to recommend tools for the discovery of quantum-vulnerable algorithms. We are skeptical to such tools for a number of reasons. Tools of this kind typically:
  - require substantial and costly work to integrate into existing systems, especially in multi-vendor systems.
  - give a large number of false positives that require qualified and expensive work to discard.
  - give a large number of false negatives. This gives a false sense of security and means that other types of risk assessment and classification are needed anyway.

  Vendors can typically quickly give information on how and where public-key cryptography is used in their products.

- We suggest that SP 1800-38A should very clearly state that Quantum Key Distribution (QKD) is not a viable option for migration to quantum-resistant cryptography. Modern infrastructure is implemented with zero trust principles where cryptography is used for confidentiality, integrity protection, and authentication on many of the layers of the network stack, often all the way to software in the cloud. QKD is an unauthenticated physical point-to-point key exchange protocol that requires new hardware and trusted relays. It might make sense to connect quantum computers and quantum sensors into a quantum internet, but a quantum internet has nothing to do with security. As explained in [6], [7], and [8], QKD does not offer acceptable practical security and is basically useless in practice:

  "QKD protocols do not provide authentication they are vulnerable to physical man-in-the-middle attacks."

  "increases infrastructure costs and insider threat risks"

  "increases the risk of denial of service"

  "does not support the usage of QKD"

  "does not endorse the use of QKD"

  "It's a clever idea, but basically useless in practice"

- Since it has been suggested in the past that CRQCs "reduces symmetric security levels by half" (see e.g., p. 9 of [9]), we think SP 1800-38A should make an explicit statement that 128-bit

symmetric cryptography is quantum-resistant and will likely remain secure for decades to come as explained in [10] and [11]:

> *"Presently envisioned quantum computing architectures typically indicate that the cost per quantum gate could be billions or trillions of times the cost per classical gate."*
>
> *"Plausible values for MAXDEPTH range from 2^{40} logical gates (the approximate number of gates that presently envisioned quantum computing architectures are expected to serially perform in a year) through 2^{64} logical gates (the approximate number of gates that current classical computing architectures can perform serially in a decade)"*
>
> *"Grover's algorithm requires a long-running serial computation, which is difficult to implement in practice. In a realistic attack, one has to run many smaller instances of the algorithm in parallel"*
>
> *"Taking these mitigating factors into account, it is quite likely that Grover's algorithm will provide little or no advantage in attacking AES, and AES 128 will remain secure for decades to come."*

NIST Post-Quantum Cryptography project specified their quantum security levels based on symmetrical algorithms where security level I is defined as AES-128 [11]. Even if a Cryptanalytically Relevant Quantum Computer (CRQC) able to break RSA-2048 in a few hours is ever built, such a CRQC would not pose any practical threat at all to any 128-bit symmetrical algorithms. Using NIST's assumptions about quantum computer performance [11], a huge cluster of one billion CRQCs (according to one estimate costing one billion USD each) would take a million years of uninterrupted calculation to find a single AES-128 key.

If the price—performance ratio of classical computers continue to decline, which seems likely, AES-128 will however eventually need to be phased out because of classical computers. NIST should update SP 800-57 [2] to provide more guidance on how long NIST believes 128-bit security is acceptable.

Best Regards,
John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols

[1] NSA, “Announcing the Commercial National Security Algorithm Suite 2.0”
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[2] NIST SP 800-57 Part 1, “Recommendation for Key Management: Part 1 – General”
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[3] NIST, “NIST Risk Management Framework”
https://csrc.nist.gov/projects/risk-management/about-rmf

[4] ICANN, “Quantum Computing and the DNS”
https://www.icann.org/en/system/files/files/octo-031-11feb22-en.pdf

[5] NIST SP 800-208, “Recommendation for Stateful Hash-Based Signature Schemes”
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf

[6] NSA, “Quantum Key Distribution (QKD) and Quantum Cryptography (QC)”
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[7] NCSC, “Quantum security technologies”
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[8] Schneier, “GCHQ on Quantum Key Distribution”
https://www.schneier.com/blog/archives/2018/08/gchq_on_quantum.html

[9] NISTIR 8319, “Review of the Advanced Encryption Standard”
https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8319.pdf

[10] NIST, “Post-Quantum Cryptography FAQs”
https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

[11] NIST, “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”
https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf