ERICSSON

Date: January 10, 2025

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on NIST IR 8547
Transition to Post-Quantum Cryptography Standards

Dear NIST,

Thanks for your continuous efforts to produce open-access security documents. Please find below our comments on the initial public draft of IR 8547:

The US government has been the clear thought leader in PQC migration with excellent advice [1–3] such as:

> *"Create migration plans that prioritize the most sensitive and critical assets."*
>
> *"prioritize the assets that would be most impacted by a CRQC, and that would expose the organization to greater risk"*
>
> *"Prioritization should be given to high impact systems, industrial control systems (ICSs), and systems with long-term confidentiality/secrecy needs."*
>
> *"This prioritization schema ensures that agency will focus their resources on defending the cryptography, functions, and data most vulnerable to a CRQC. Once migration begins, agencies will continuously re-assess their prioritization and timelines."*

The new requirement in NIST IR 8547 to deprecate ECC and RSA by 2030 is in stark conflict with the above recommendations. FIPS 203–205 are just hot off the press, and it will take several years until hardened and certified hardware and software implementations are available, and even more years before they can be deployed in practice. As NIST correctly states, cryptographic migration has in the past often taken 20 years after standardization, the transition to PQC is unprecedented in scale, and for many applications the new PQC algorithms are not a drop-in replacement. Almost 100% of all

existing hardware as well as hardware that are deployed in the next few years needs to be replaced in industries, health care, education, transport, telecom, and homes. For many use cases, turning off ECC and RSA by 2030 means that no prioritizations whatsoever are possible and that later standards such as FN-DSA, Classic McEliece, BIKE, HQC, MAYO, UOV, HAWK, FEAST, etc., are not even an option.

One implication of this new 2030 deprecation in NIST IR 8547 is that most industries will go for 100% hybrids aligning with ANSSI's and BSI's requirements that "*Post-quantum algorithms must be hybridized*" [4] and "PQC only in hybrid solutions" [5]. When SIKE was presented at the first PQC workshop, Shamir said: *"I don't think this should be deployed in the next 20 years".* Similar things can be said about early implementations, many of them have severe implementation bugs and side-channels. The 2030 deprecation date for RSA and ECC means that industry need to pick the very first available implementations of ML-KEM and ML-DSA and use them in production systems, which without hybrid schemes creates unacceptable risks.

NSA expects the transition to quantum-resistant algorithms for NSS to be complete by 2035 [6]. It is hard to understand why the US government thinks that Mr. Arkko's connected toaster [7] should follow the same timeline as US national security systems protecting highly classified data that need to be confidential for many decades. Formulated differently, it is hard to understand why the US national security systems do not have harder requirements than Mr. Arkko's connected toaster.

We suggest that NIST IR 8547 is rewritten with a strong focus on prioritization. Firm dates for deprecation and disallowment of quantum vulnerable algorithms are better handled in future revisions of SP 800-131A [8]. Both prioritization and timelines should be continuously re-assessed.

A rewritten NIST IR 8547 focusing on prioritization should include:

- Different recommendations for federal agencies, industries, and the general public, which are the groups NIST states its recommendations are for.

- Different recommendations depending on use case (long-term roots-of-trust for firmware update, binding signatures for non-repudiation, short-term signatures for authentication, encryption of classified data, encryption of metadata, etc.).

- Different recommendations based on the required protection lifetime of the node or data.

- Different recommendations based on how long-time migration takes (already deployed hardware vs. easily updatable software)

- Value of the protected node or data. Early CRQCs will most likely be very expensive, meaning that early attackers will focus on very high-value targets [9].

The rewritten NIST IR 8547 can, for example, define four categories (ranging from most time-sensitive, Category I, to least critical, Category IV) with differing migration timelines and provide guidance on how to identify the appropriate category. The actual assessments should be deferred to industry-led standardization bodies, which have the in-depth knowledge of how NIST algorithms are utilized, the required protection lifetimes, the value of the protected node or data, and the timelines for

system upgrades driven by other factors. Such an industry-led, standards-based approach is vastly preferable to top-down regulation and fosters technical innovation and economic growth.

The broad-brush approach required by NIST IR 8547 can have severely negative consequences.

- A broad-brush approach without prioritization may lead to that highly prioritized systems are updated later than they should be. In case of delays due to complication in the migration, which does not seem unlikely, some of the most prioritized systems might miss the 2030 deadline.

- If and when a CRQC will be developed is still uncertain. Already now deciding that almost all deployed hardware in all industries need to be replaced comes with astronomical economical costs. It is not unlikely that we in 2035 are still very far from building a CRQC. Nvidia CEO Jensen Huang recently said that the quantum computers won't be "very useful" for 15–30 years [10]. And even a very useful quantum computer is far from being a CRQC.

- NIST is the de facto global crypto SDO driving long-term cryptographic standards. NIST requirements have always been seen as very reasonable taking practical security and existing deployments into account. Requirements that are seen as unreasonable, like replacing all existing hardware and downgrading constrained IoT to symmetric group keys without PFS, might lower trust in NIST as a global SDO.

Comments:

- The report should clarify early on that "deprecated" and "disallowed" also apply to already deployed hardware, much of which cannot be updated. Organizations striving to use only "acceptable" cryptography will need to replace almost all existing hardware, as well as hardware deployed over the next few years, before January 1, 2031.

- The report should emphasize that migration of algorithms for firmware signing is urgent. CNSA 2.0 requires that the first use case to migrate to PQC should be the asymmetric algorithm used for digitally signing firmware and software [11]. We agree with the NSA. Hardware is often in use for many decades, and unlike software implementations, the algorithms for firmware signing typically cannot be updated once deployed.

- *"These guidelines had projected that NIST would disallow public-key schemes that provide 112 bits of security on January 1, 2031. However, based on the need to migrate to quantum-resistant algorithms during this timeframe, NIST intends to instead deprecate classical digital signatures at the 112-bit security level."*

  SP 800-57 disallow 112 bits of security from 2031 minus the lifetime of the protected data. For most encryption use cases 112-bits is already disallowed. We are strongly against NIST changing the previously required timeframe. Changing the timeframe distorts market competition and unfairly benefits companies that have neglected their cryptographic hygiene. While it is very uncertain when or if CRQCs will be built, it is very certain that hostile nation states will be able to break 112-bit security in a few decades.

- *"Cryptographic algorithms … future quantum computing may be able to break these algorithms"*

  Quantum computing will never be a practical threat to any symmetric crypto [12–13]. As explained in the keynote at CHES 2024, a quantum computer breaking a single AES-128 key would require qubits covering the surface area of the Moon [14].

- *"FIPS 186 specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) and adopts the RSA algorithm specified in RFC 8017 and PKCS 1 (version 1.5 and higher)"*

  RFC 8017 is the latest version of PKCS #1. FIPS 186 does not refer to any earlier versions of PKCS #1. RSASSA-PKCS1-v1_5 is included in PKCS #1 Version 2.2. Suggestion:

  "FIPS 186 specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) and adopts the RSA algorithm specified in RFC 8017 (PKCS #1 Version 2.2)"

- *"These algorithms are vulnerable to Shor's Algorithm on a cryptographically relevant quantum computer."*

  Might be good to inform the reader about the existence of the new state-of-the-art Ekerå-Håstad and Regev algorithms, which are based on Shor's algorithm and significantly improves it [9].

- *"Due to this need to maintain state, HBS schemes are not intended for general use".*

  We think the document should state the intended use case instead of writing what it is not for.

- *"However, hybrid solutions add complexity to implementations and architectures, which can increase security risks and costs during the transition to PQC."*

  We think NIST should also emphasize the security risks of deploying early implementations of cryptographic algorithms. Early implementations often have implementation bugs and side-channels.

  NIST has done a truly excellent work with the standardization of ML-KEM and ML-DSA. ML-DSA offer strongly unforgeability (SUF-CMA), and both ML-KEM and ML-DSA exclusively utilize SHA-3, which has superior properties to SHA-2, and is much easier to protect against side-channel attacks. NIST should caution readers about the limitations of hybrid solutions that only achieve EUF-CMA or combine ML-KEM and ML-DSA with SHA-2.

- *"Such approaches are not considered hybrid solutions if each session only uses a single cryptographic algorithm"*

  Very good that NIST highlights this issue. We have seen unserious companies promoting such solutions as hybrid implantations. Related to this, NIST should also emphasize the differences in migrating to PQC within protocols that do or do not support algorithm negotiation. For protocols with algorithm negotiation, such as TLS, IKEv2, and EDHOC, adding support for PQC algorithms can significantly enhance security. However, for protocols without algorithm negotiation, such as

S/MIME and firmware updates, security improvements are only realized when RSA and ECC are fully disabled on the receiving side.

John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols
MSc Engineering Physics/Theoretical Computer Science
MSc Business Administration and Economy

[1] Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

[2] Quantum-Readiness: Migration to Post-Quantum Cryptography
https://www.cisa.gov/sites/default/files/2023-08/Quantum Readiness_Final_CLEAR_508c%283%29.pdf

[3] Report on Post-Quantum Cryptography
https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[4] ANSSI plan for post-quantum transition
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf

[5] Post-Quantum Policy & Roadmap of the BSI
https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_stephan-ehlen_bsi_post-quantum-policy-and-roadmap-of-the-bsi.pdf

[6] 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

[7] Now, Even Granny's Fuzzy Slippers Are Texting You
https://www.wsj.com/articles/SB10001424052702303544604576434013394780764

[8] Transitioning the Use of Cryptographic Algorithms and Key Lengths
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[9] On factoring integers, and computing discrete logarithms and orders, quantumly
https://www.wsj.com/articles/SB10001424052702303544604576434013394780764

[10] Quantum Computing Stocks Dive After Nvidia CEO Says Tech 15-30 Years Away
https://www.msn.com/en-us/news/technology/quantum-computing-stocks-dive-after-nvidia-ceo-says-tech-15-30-years-away/ar-AA1x8Tix

[11] 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

[12] IETF Statement on Quantum Safe Cryptographic Protocol Inventory
https://datatracker.ietf.org/liaison/1942/

[13] 3GPP Statement on PQC Migration
https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip

[14] Quantum Attacks on AES
https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s