Ericsson Technology Review

#5, May 2026

Migrating telecom to quantum-resistant cryptography on a global scale

Charting the future of innovation

Ericsson Technology Review — Charting the future of innovation | #5, May 2026

Migrating telecom to quantum-resistant cryptography on a global scale

Authors:
John Preuß Mattsson, Erik Thormarker, Masoud Asadi, Sini Ruohomaa

Cryptography underpins the security of our modern digital society, protecting the confidentiality and integrity of the ICT systems that enable connectivity across mobile networks, cloud platforms and critical infrastructure. The emergence of large-scale quantum computing will eventually render today's widely deployed public-key cryptography insecure, prompting the largest cryptographic migration in history.

ISSN 0014-0171 284 23-3439 | Uen

Ericsson, SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000

Migration to post-quantum cryptography (PQC) has become a strategic priority for governments and industries worldwide. With the publication of the Federal Information Processing Standards (FIPS) 203 Module-Lattice Key Encapsulation Mechanism (ML-KEM), FIPS 204 Module-Lattice Digital Signature Algorithm (ML-DSA) and FIPS 205 Stateless Hash-based Digital Signature Algorithm (SLH-DSA) in August 2024, PQC moved into implementation and deployment. Clear timelines are now emerging; high-priority systems should migrate before 2031, and full transition should be completed by 2035. For telecom networks — long-lived, globally interconnected and foundational to critical services — preparation and deployment must begin immediately.

When we examined the quantum threat in an Ericsson Technology Review article published in 2021 [1], the US National Institute of Standards and Technology (NIST) selection process was nearing completion. In 2024, standardized algorithms for key exchange and digital signatures became available [2], providing practical replacements for the Rivest–Shamir–Adleman (RSA) cryptosystem and Elliptic Curve Cryptography (ECC).

The challenge has now shifted from algorithm selection to global-scale integration, implementation and deployment — particularly for key exchange (to protect data confidentiality) and for long-lived trust anchors embedded in telecom infrastructure during manufacturing.

Post-quantum cryptography — what does it mean?

PQC is the standardized transition from quantum-vulnerable public-key algorithms to quantum-resistant ones, enabling telecom and IT systems to protect long-lived data, digital identities and critical infrastructure against both current and future adversaries. PQC algorithms are designed to withstand attacks from classical and quantum computers alike. Like traditional cryptography, they run on today's classical hardware and can be integrated into existing protocols and systems.

It is important to distinguish PQC from other approaches. In our 2021 article [1], we explained why quantum key distribution (QKD) is not a practical or scalable alternative to PQC for real-world networks. Since then, standardization bodies and national cybersecurity agencies have published

Terms and abbreviations

3GPP – 3rd Generation Partnership Project | **AKA** – Authentication and Key Agreement | **AMF** – Access and Mobility Management Function | **AUSF** – Authentication Server Function | **CP** – Control Plane | **DTLS** – Datagram Transport Layer Security | **EAP** – Extensible Authentication Protocol | **ECC** – Elliptic Curve Cryptography | **ECDSA** – Elliptic Curve Digital Signature Algorithm | **gNB** – gNodeB | **GPRS** – General Packet Radio Service | **GTP-U** – GPRS Tunneling Protocol-User Plane | **HSM** – Hardware Security Module | **HTTP2** – Hypertext Transfer Protocol Version 2 | **HQC-KEM** – Hamming Quasi-Cyclic Key Encapsulation Mechanism | **IP** – Internet Protocol | **IPsec** – IP Security | **IPX** – Internet Packet Exchangee | **JOSE** – JSON Object Signing and Encryption | **JSON** – JavaScript Object Notation | **KEM** – Key Encapsulation Mechanism | **L1** – Layer 1 | **L2** – Layer 2 | **MAC** – Medium Access Control | **ML-DSA** – Module-Lattice Digital Signature Algorithm | **ML-KEM** – Module-Lattice Key Encapsulation Mechanism | **NAS** – Non-Access Stratum | **NEF** – Network Exposure Function | **NG** – Next Generation | **NG AP** – NG Application Protocol | **NIST** – National Institute of Standards and Technology | **OAuth** – Open Authorization | **O-RAN** – Open Radio Access Network | **PDCP** – Packet Data Convergence Protocol | **PKI** – Public Key Infrastructure | **PQC** – Post-Quantum Cryptography | **QKD** – Quantum Key Distribution | **QUIC** – Quick UDP Internet Connection | **RAN** – Radio Access Network | **RLC** – Radio Link Control | **RRC** – Radio Resource Control | **RSA** – Rivest–Shamir–Adleman | **SCTP** – Stream Control Transmission Protocol | **SDAP** – Service Data Adaptation Protocol | **SEPP** – Security Edge Protection Proxy | **SLH-DSA** – Stateless Hash-Based Digital Signature Algorithm | **SMF** – Session Management Function | **SUCI** – Subscription Concealed Identifier | **TCP** – Transmission Control Protocol | **TLS** – Transport Layer Security | **UDM** – Unified Data Management | **UDP** – User Datagram Protocol | **UPF** – User Plane Function | **X25519** – Elliptic Curve Diffie–Hellman over Curve25519

recommendations that align with this assessment, noting that QKD deployments often rely on trusted intermediaries, which conflict with the end-to-end security models used in today's multi-layer communication systems.

Similarly, while quantum random number generators (QRNG) are emerging as an alternative source of randomness, well-established cryptographically secure random-number generators such as those in modern central processing units (CPUs) remain secure. The overall direction from standardization bodies and national cybersecurity agencies is clear: PQC is the only feasible approach for achieving quantum-safe security, and its adoption is a priority [3].

In short, it is widely recognized that PQC will be essential for protecting digital communications at scale. In practice, the transition spans multiple layers – from algorithms and protocols to key management, implementations and operational processes.

The cryptographic building blocks of a digital trust system

Signature algorithms are an important tool for transferring trust across time and space. To achieve this, the algorithm building blocks form a stack that reaches from the underlying mathematics to human processes and digital representations. **Figure 1** illustrates how different components work together to ensure the trustworthiness of a public key infrastructure (PKI).

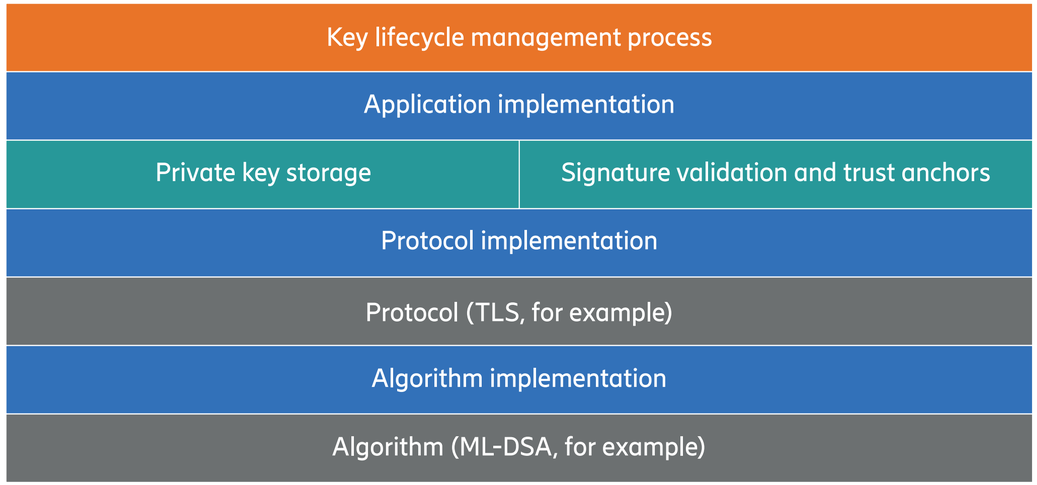

Figure 1: The building blocks of a PKI

Securing all aspects of the stack requires attention to the specific issues related to each layer. For example, when implementing a cryptographic algorithm, we must ensure functionally correct behavior, but also strictly follow best practices of implementation security. Otherwise, side channel information such as the execution time of an algorithm may leak secret information, including keys. In recent years, artificial intelligence has been increasingly used as a tool for attackers to exploit side channel information. New algorithms have required updating mitigation best practices. The upcoming NIST standard FN-DSA (Falcon Digital Signature Algorithm) has proven to be particularly challenging, as it uses floating point representation of numbers to optimize the algorithm performance, while side channel mitigations have so far focused on integers.

The protocol layer interacts with algorithm security as well. In key establishment, algorithm implementation concerns have motivated a hybrid solution where the final key is a combination of traditional and PQC key exchange. The key is secure, as long as at least one of the algorithms remains secure. Hybrid signatures, in contrast, are more complex to deploy as a temporary workaround, and available solutions are not yet mature. The most acute need for PQC for authentication and integrity use cases is the replacement of long-lived trust anchors, which generally are well protected from side channels. At the moment, the best options for migration are standalone ML-DSA and SLH-DSA.

Key management focuses on keeping private keys safe. Challenges in this layer have impacted the deployability of stateful signature schemes such as the XMSS (eXtended Merkle Signature Scheme) and the LMS (Leighton–Micali Signature), which were standardized in 2018 by the IETF (Internet Engineering Task Force) to provide an early alternative for quantum resistance. Securing stateful keys and, in particular, ensuring their state is always correctly represented has proven to be particularly difficult to implement, as existing cryptographic tools have not had similar requirements. Potential users would need to rely heavily on careful application of human-controlled processes to avoid classical key compromise.

Security relies on all layers of the stack working together.

Cryptographic transition impacts the algorithm and protocol level, with minor adjustment needed in key storage and applications. Security relies on all layers of the stack working together: even the perfect algorithm will fall to a critical implementation mistake or insecure management of private keys.

Post-quantum cryptography algorithm standards

ML-KEM (FIPS 203) and ML-DSA (FIPS 204) are the main algorithms that will be used in most telco use cases, with SLH-DSA (FIPS 205) also being used to a more limited extent. Since publishing these algorithms in 2024, the NIST has been working on plans to standardize additional ones that can serve as backup algorithms and complements. Ericsson has been – and continues to be – an active participant in the NIST PQC process [4,5] and has been the driver for hedged signatures.

We expect the NIST PQC algorithms to become globally accepted standards similar to previous important NIST algorithms such as AES (Advanced Encryption Standard), GCM (Galois/Counter Mode), SHA-2/3 (Secure Hash Algorithm 2/3) and ECDSA (Elliptic Curve Digital Signature Algorithm). The new algorithms have been chosen through an open process and from a large set of candidates submitted by leading cryptographers from all over the world. It should be noted that the study of the selected algorithms did not start with the NIST PQC process: all selected algorithms build on decades of research, ensuring strong trust in their security. The use of globally accepted and trusted algorithms is important for global standards like those of the 3GPP (3rd Generation Partnership Project), the O-RAN (Open Radio Access Network) Alliance and the GSMA (GSM Association), but it is also vital to ensure production-grade implementation support in libraries, tools and hardware.

Migration timelines

The migration of large-scale systems to PQC consists of the identified requirement to migrate to new algorithms, algorithm design, identification and standardization of best practices of using the algorithms, implementation of the relevant building blocks, and ultimately implementation and deployment into actual end products. Historically, algorithm migrations in deployed systems have taken more than a decade, depending in part on the maturity of the target algorithms.

There is overall alignment among governments globally about the use of the NIST PQC standards.

One of the first announcements of plans to transition to quantum-resistant cryptography came from the US National Security Agency in 2015. Since the publication of FIPS 203–205, several governments have published timelines for how they think industry and society should migrate to PQC. Many of these recommendations call for migration as soon as possible, starting with high priority use cases and systems by no later than 2030, with the goal of completing the migration by 2035 at the latest.

The gap between today's quantum computers and the ones that could break today's deployed quantum-vulnerable public-key cryptography is very large, but it has shrunk in recent years through newly discovered optimizations. For example, the German security agency BSI (Bundesamt für Sicherheit in der Informationstechnik) estimated in 2024 that it was now likely that such quantum computers could be built within the next 16 years [6]. In terms of prioritization, governments are focusing on use cases where encrypted data needs to be protected for more than 10 years, for example, or very long-lived authentication keys such as those used for code signing and firmware updates [7].

There is overall alignment among governments globally about the use of the NIST PQC standards as the primary public-key algorithms for quantum resistance, but there are some differences in recommendations with respect to how to apply them. For lattice-based cryptography, the European Union recommends using standardized and tested hybrid solutions whenever feasible and suitable [7], while the UK, the US, Canada and Australia either prefer standalone PQC or at least do not recommend hybridization. No governments are mandating hybridization for SLH-DSA. France's ANSSI (l'Agence nationale de la sécurité des systèmes d'information) states that it has the highest confidence in ML-KEM, ML-DSA and SLH-DSA and that it will only mandate hybridization of lattice-based algorithms during the transition period [8]. Ericsson is very active in driving dialogue in this space [9].

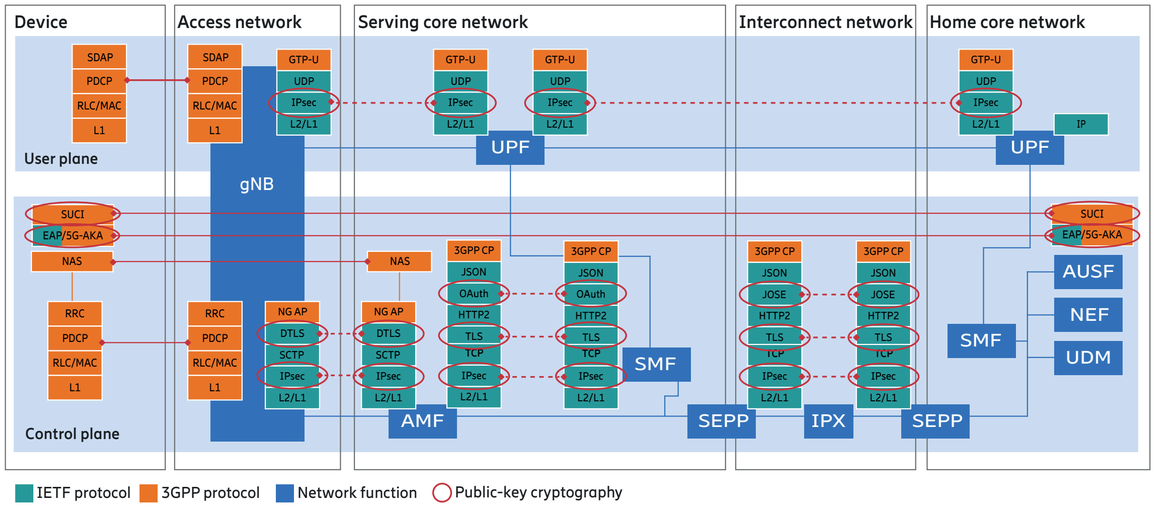

Figure 2: Public-key cryptography in the 3GPP 5G connectivity layer

Post-quantum cryptography in telecom standards

The 3GPP, O-RAN and GSMA standards make use of public-key cryptography primarily through IETF security protocols and standards such as Transport Layer Security (TLS), Internet Protocol Security (IPsec) and ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) Recommendation X.509 certificates. An exception is the subscriber identity encryption on the radio interface (the 5G-AKA or Subscription Concealed Identifier), introduced with 5G SA (5G Standalone), which is specified by the 3GPP directly. The IETF is in the final stages of publishing RFCs (Requests for Comments) for how the NIST PQC algorithms are integrated into important security protocols and standards like TLS, IPsec, and X.509 certificates. For its uses of IETF security protocols, the 3GPP specifies generation agnostic cryptography profiles, which are updated regularly through the 3GPP releases.

5G relies on IETF protocols for almost all uses of public-key cryptography. **Figure 2** illustrates public-key cryptography in the 3GPP 5G connectivity layer.

Ericsson is very active in driving PQC migration in telecom and internet standards. In our view, 5G standards will be updated to support PQC, and 6G – which is expected to come into deployment in 2030 – will have full PQC support from the first release. This means that a PQC alternative should be supported everywhere public-key cryptography is used in the specifications.

Symmetric cryptography is not affected by attacks from quantum computers, as we noted in our previous article [1]. Important standards development organizations such as NIST, the IETF and the 3GPP have clarified this [10,11]. NIST has even defined the security categories for the new PQC algorithms based on the quantum resistance of symmetric cryptography. 5G and earlier 3GPP generations use a lot of symmetric 128-bit cryptography that will thus remain secure even when considering attacks from quantum computers. This is especially important as the symmetric algorithms used on the 3GPP radio interface often depend on hardware implementations in user equipment chipsets and network RAN equipment. 6G will likely use new 256-bit algorithms designed by ETSI SAGE (European Telecommunications Standards Institute - Security Algorithms Group of Experts) on the radio interface for performance reasons.

A PQC alternative should be supported everywhere public-key cryptography is used.

Quantum-resistance security strength categories are defined in terms of symmetric algorithms. There are five categories, each with its own attack types:

1. Key search on a block cipher with a 128-bit key (for example, AES-128 or SNOW 3G)
2. Collision search on a 256-bit hash function (for example, SHA3-256)
3. Key search on a block cipher with a 192-bit key (for example, AES-192)
4. Collision search on a 384-bit hash function (for example, SHA3-384)
5. Key search on a block cipher with a 256-bit key (for example, AES-256 or SNOW 5G)

An algorithm qualifies for a given category if breaking it requires computational resources comparable to, or greater than, those needed for the corresponding attack type.

With the quantum resistance of symmetric cryptography in mind, adding pre-shared symmetric keys to security protocols like IPsec was previously considered as a method for quantum resistance, before PQC algorithms had been standardized. Establishing pre-shared symmetric keys between any two nodes that need to communicate is a major effort in addition to maintaining the traditional PKI that is still needed. With the integration of NIST PQC algorithms into IETF security protocols, this complex alternative no longer needs to be considered. The US Pentagon [12], for example, has made clear that it will not test or use any such commercial solutions.

While PQC signatures, ciphertexts and public keys are significantly larger than those based on quantum-vulnerable RSA and ECC (such as ECDSA), ML-KEM, ML-DSA and SLH-DSA are nonetheless well suited to meet telco needs. If we consider authentication in TLS or IPsec connection establishment, for example, the use of PQC means that the certificate chains exchanged between peers will have significantly larger byte size. This is only at connection establishment, however, and since telco use cases tend to rely on relatively long-lived connections, even if the extra data exchange leads to an additional round trip taking a few tens of milliseconds, it is not expected be a significant problem.

Table A in **Figure 3** provides a comparison of sizes and performance of quantum-vulnerable and quantum-resistant digital signature schemes.

The ML-KEM key and ciphertext byte size indicated in Table A will be even less noticeable at TLS or IPsec connection establishment. FN-DSA and HQC-KEM (Hamming Quasi-Cyclic Key Encapsulation Mechanism), which will be standardized by NIST, can be seen as backup or complement

Table A: Comparison of quantum-vulnerable and quantum-resistant digital signature schemes

		Sizes (in bytes)		Operations per second (higher is better)	
Algorithm	Security category	Public key	Signature	Signing	Verification
ECDSA P-256	N/A	32	64	27,000	10,000
RSA-3072	N/A	384	384	300	33,000
ML-DSA-44	2	1,312	2,420	14,000	31,000
ML-DSA-65	3	1,952	3,309	9,000	18,000
ML-DSA-87	5	2,592	4,627	7,000	11,000
SLH-DSA-128s	1	32	7,856	3	1,400
SLH-DSA-128f	1	32	17,088	50	600
FN-DSA-512	1	897	666	7,000	46,000

Table B: Comparison of the quantum-vulnerable X25519 and the quantum-resistant ML-KEM and HQC-KEM

		Sizes (in bytes)		Operations per second (higher is better)	
Algorithm	Security category	Client	Server	Client	Server
X25519	N/A	32	32	25,000	25,000
ML-KEM-512	1	800	768	60,000	121,000
ML-KEM-768	3	1,184	1,088	37,000	77,000
ML-KEM-1024	5	1,568	1,568	26,000	53,000
HQC-KEM-128	1	2,249	4,497	7,000	15,000

Figure 3: Comparisons of quantum-vulnerable and quantum-resistant algorithms

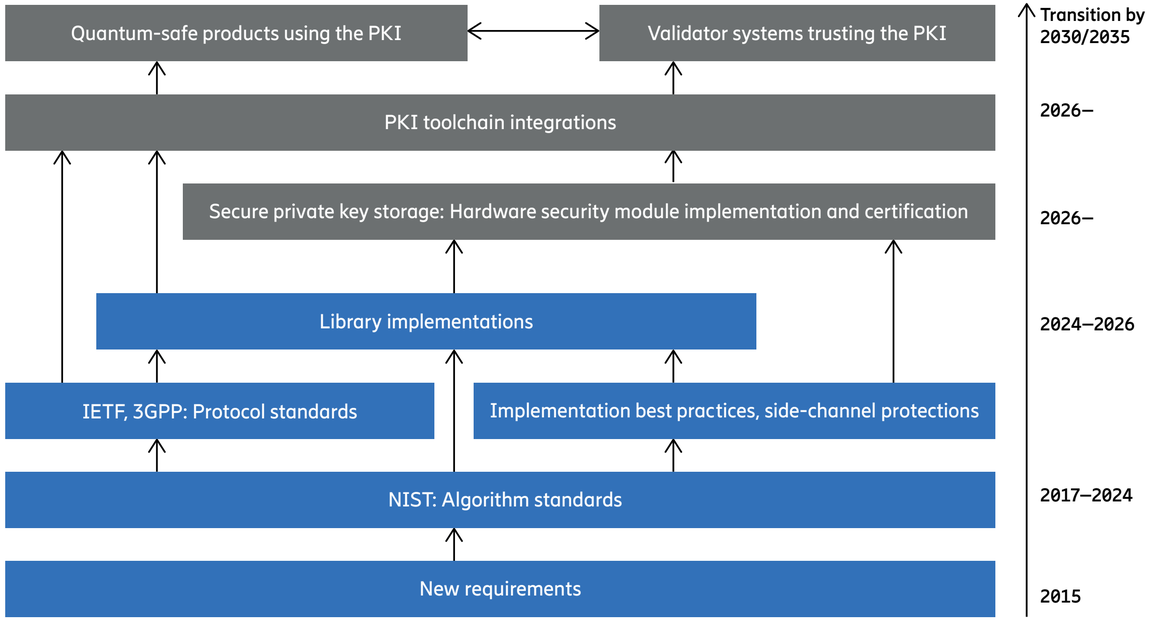

Figure 4: Interdependencies of different phases of the quantum-safe transition

algorithms that can be used and supported based on need. In terms of CPU performance, the new algorithms are sufficient, as can be seen in Figure 3. ML-KEM can, for example, be faster on a server-type machine than today's very fast X25519 algorithm.

Table B in Figure 3 provides a comparison of sizes and performance between the quantum-vulnerable X25519 and the quantum-resistant ML-KEM and HQC-KEM. KEMs can serve as drop-in replacements for ephemeral key exchange in protocols such as TLS and IPsec, as well as for public-key encryption in applications such as SUCI.

Migration path for telecom infrastructure

Migrating key exchange used for encrypting data in transit has been underlined as particularly urgent, due to the risk of an adversary being able to record intercepted traffic now and attempt to decrypt the messages in the future using a quantum computer. Updating key exchange in, for example, TLS to ML-KEM is a protocol-internal process. This is in contrast to upgrading PKI, where there are many stakeholders and dependencies across different layers. Thanks to the secure negotiation that is already built into protocols such as TLS and IPsec, PQC key exchange can be used as soon as both ends of a connection support it.

An important detail for TLS is that only TLS (and DTLS (Datagram Transport Layer Security)) version 1.3 will support PQC. QUIC uses TLS version 1.3 in connection establishment. PQC key exchange is already widely used on the internet.

Migrating the roots of trust of authentication to use PQC should be prioritized equally to updating key exchange [7]. Devices for which hardware-assisted security uses bootstrap trust anchors that cannot be updated in the field are a particularly critical target. Additionally, the algorithm transitions of PKIs tend to take considerable time due to the need to distribute new trust anchors and capabilities everywhere.

PKI uplift does not end at the point of standardizing the cryptographic algorithms, as several additional steps are still needed. **Figure 4** shows a high-level overview of the interdependencies in PKI migration. The blue steps have been established and the grey steps are in progress.

Implementation aspects

Digital signatures are often used through X.509 certificates, which thanks to their built-in cryptographic agility have already been updated to be able to use the new algorithms [13,14]. Software library support has also followed closely behind the final standards. To protect the trust anchors and certificate authority keys of PKIs, it must be possible to store and securely use their private keys through hardware security modules (HSMs), which must implement the published standards. Additionally, the HSM must pass FIPS evaluation to be able to operate in an approved mode necessary for compliance in many application areas. The new algorithms have also required some adaptations to application-level software, and the delay for the full adjusted PKI toolchain availability includes the availability for the final tools for certificate and software signing.

Mechanisms such as secure boot and hardware attestation rely on low-level hardware-assisted security elements that are generally introduced during the manufacturing process. It is therefore essential both that silicon manufacturers introduce the new algorithms into their hardware and that vendors of long-lived equipment that includes that hardware – ships, cars and critical infrastructure including telecommunication equipment – are able to introduce the relevant trust anchors to their products.

These lowest layers of firmware depend on hardware-assisted security elements, and on higher layers they can hand over system integrity protection to software-based validation mechanisms, which can more easily refresh the algorithms used in a software update. For example, the validation of incoming over-the-air software update packages does not require hardware assistance and can use quantum-safe signatures as soon as the needed PKI is available for the device. On the other hand, resistance against low-level attacks is important for physically exposed equipment operating outside the safety of server rooms and requires a hardware root of trust.

Migrating the key exchange used for encrypting data in transit has been underlined as particularly urgent.

Trust-anchor update capability is also an important part of cryptographic agility – that is, the ability to change algorithms should the need arise. As explained earlier, there is strong trust in the security of the new algorithms, but implementation mistakes and weaknesses such as side channels could be discovered. New alternatives that are standardized by NIST may turn out to have improved performance or be more suited for constrained use cases, for example.

Overall, having a fallback algorithm in order to introduce new trust chains or even a new algorithm as a software update is very valuable for long-lived and exposed devices. In the context of device and software interoperability, it should be noted that both ends of a connection will need to support the new algorithms, and the verifier end needs the updated trust anchor to complete a cryptographic transition. For example, in cloud software deployments, it is not sufficient for one vendor to produce quantum-safe signatures; the receiving cloud platform must be able to validate these signatures as well and to only accept secure signature algorithms. Here, standardization, national regulation and industrial collaboration organizations carry an important role in aligning systems to a shared set of secure and performant algorithms over time.

Conclusion

Telecommunication networks are long-lived, globally interconnected systems with stringent security and interoperability requirements. The transition to post-quantum cryptography (PQC) is therefore not simply an algorithm upgrade; it is a coordinated transformation across standards, implementations, hardware roots of trust and operational processes.

The most urgent priorities are clear: migrate key exchange to mitigate “harvest now, decrypt later” risks and replace long-lived trust anchors that form the foundation of digital authentication. At the same time, operators and vendors must ensure cryptographic agility, enabling future algorithm updates as standards evolve and implementation experience grows.

The availability of globally standardized PQC algorithms provides a solid technical foundation. The remaining challenge is disciplined, large-scale execution across the telecom ecosystem. Through continued collaboration among standards bodies, governments, operators and equipment vendors, the industry can ensure that 5G evolution and 6G deployment are built on quantum-resilient security foundations. Acting now will secure trust in telecom networks well beyond the transition to a post-quantum world.

The authors

John Preuß Mattsson is an expert in cryptographic algorithms and security protocols whose work focuses on applied cryptography, privacy, IoT security, post-quantum cryptography and trade compliance. Since joining Ericsson in 2007, he has significantly influenced cryptography, internet and cellular security standards through his work with organizations such as IETF, IRTF, 3GPP, GSMA and NIST. Preuß Mattsson holds an M.Sc. in engineering physics from KTH Royal Institute of Technology in Stockholm, Sweden, and an M.Sc. in business administration and economics from Stockholm University.

Erik Thormarker is a master researcher at Ericsson Research, where his work focuses on cryptography and security protocols, as well as 5G and 6G security. He actively contributes to standardization efforts within organizations such as the Internet Engineering Task Force (IETF), GSMA and 3GPP. Thormarker holds an M.Sc. from the joint master’s program in mathematics at KTH Royal Institute of Technology and Stockholm University. He joined Ericsson in 2018.

Masoud Asadi is a senior expert in RAN security architecture at Ericsson, leading strategic initiatives that define secure architectures for 5G and future 6G radio networks. He collaborates with senior stakeholders across technology and product organizations to embed robust security principles into global RAN solutions. An important part of his work is to align deep technical insight with long-term security strategy and industry impact. Asadi joined Ericsson in 2001 after studying computer science at KTH Royal Institute of Technology.

Sini Ruohomaa joined Ericsson in 2014 after completing a doctoral dissertation on the subject of trust management. In her current role as an expert in cryptographic signing services, she uses cryptography and PKI to secure identities and system integrity in critical communication infrastructure. Ruohomaa holds a Ph.D. in computer science from the University of Helsinki in Finland.

References

1. Ericsson Technology Review, Quantum technology and its impact on security in mobile networks, December 7, 2021, Preuß Mattsson, J.; Smeets, B.; Thormarker, E. ↗
2. NIST, Post-Quantum Cryptography, December 11, 2025 (updated) ↗
3. Försvarsmakten (Swedish Armed Forces) et al., Position Paper on Quantum Key Distribution, January 2024 ↗
4. NIST 2022 PQC Standardization Conference, Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange, Preuß Mattsson, J.; Selander, G.; Smeets, B.; Thormarker, E. ↗
5. NIST 2025 Workshop on Guidance for KEMs, ML-KEM is Great! What's Missing?, Preuß Mattsson, J. et al. ↗
6. German Federal Office for Information Security, The status of quantum computer development ↗
7. European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, June 11, 2025 ↗
8. ANSSI, ANSSI views on technical aspects of the migration to PQC, March 25, 2025 ↗
9. Ericsson, Comments on EU Roadmap on Post-Quantum Cryptography, August 29, 2025, Preuß Mattsson, J. ↗
10. IETF Statement on Quantum Safe Cryptographic Protocol Inventory ↗
11. 3GPP Statement on PQC Migration ↗
12. Pentagon, Preparing for Migration to Post Quantum Cryptography, November 20, 2025 ↗
13. RFC 981, Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), October 2025 ↗
14. RFC 9909, Internet X.509 Public Key Infrastructure – Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), December 2025 ↗

Further reading

- Ericsson, Quantum-safe networks ↗
- Ericsson, Telecom security ↗
- Ericsson, Network security standards ↗