Post Quantum Cryptography – Guidelines for Telecom Use Cases

Version 2.0

04 October 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

Table of Contents

1 Introduction

1.1 Overview

The GSMA PQTN Task Force has published a set of documents about the impact of Post-Quantum Cryptography (PQC) on telecoms. Each document has a corresponding executive summary.

Figure 1: PQTN Task Force Publication Overview

1.2 Scope

The scope of this document is to provide a set of best practice guidelines that can be used to support the journey to Quantum safe cryptography in the context of the telecom ecosystem. The work builds directly on the outcome of the first impact assessment [GSMA-PQ.01] and takes into consideration the risk assessment framework(s) being adopted by the wider industry and the implementation roadmap for PQC. This document presents a phased approach to migration allowing prioritisation of the actions required. It facilitates forward planning of transformation programmes with key stakeholder groups such as network operators. This new revision of the document focuses on migration, highlighting both common and use case specific aspects. The document highlights the known technical challenges and areas of uncertainty, to raise awareness with stakeholders. Within each use case there is a detailed analysis of aspects such as standards, government guidelines, functional architecture and performance implications.

The Zero Trust framework, briefly covered in this document in 3.7, encompasses Quantum safe cryptography. The Telco use cases in 5.1 List of Use Cases do not consider Zero Trust, as it is out of scope of this document.

This document identifies use cases which provide insight about the trade-offs and feasibility of different PQC solutions, based on the context and technical requirements. Each use case considers the constraints associated with different device types, the need for sensitive data

discovery and protection in relation to store now / decrypt later threats, and builds a view of the cryptographic inventory for that use case. This describes standardisation activity for each cryptographic mechanism, the requirements related to crypto-agility, and identifies where incompatible algorithms with no clear PQC alternatives are currently used. The approach for legacy products and services is considered in a phased way to mitigate risk in the appropriate timeframe. Definition of a detailed automation framework is out of scope, but best practise guidance is included to ensure that processes and mechanisms are developed with automation in mind.

The information included in this document is based on the Post Quantum Telco Network Task Force's best knowledge and insight at the time of writing. This is a rapidly evolving area: views, thoughts and resulting guidelines may change, reflecting the evolution of the field.

This document is intended to serve as input for relevant stakeholders, with the objective to progress quantum readiness agenda within the telco sector.

1.3 Intended Audience

The audience for this document is: stakeholders in the telecom industry (CTO, CIO, CISO), stakeholders in the supply chain (CTO, CIO, CISO), industry analysts, industry regulators responsible for security policy, and security researchers. The recommendations of this document are intended to be relevant for CEOs and Company Boards.

2 Executive Summary

This document builds on the *Post Quantum Telco Network Impact Assessment Whitepaper* [GSMA-PA.01]. It provides guidelines to support the planning, setup and execution of a quantum safe cryptography journey for the telco industry. We highlight dependencies on standards, and encourage constructive engagement with relevant stakeholders (standards bodies, etc.) on telco requirements. This is a second version of a working document that will evolve with solutions, standards and policies. The objective is to provide a current, telco-focused, practical and actionable perspective, based on learnings, experience and best practice.

Feedback from the wider Telco ecosystem is essential for the continuing relevance of the document. The GSMA PQTN Task Force welcomes the opportunity to engage and cooperate. Our report includes:

- The **PQC planning process.** The critical importance of effective governance; the need to build awareness and skills; stakeholder management across the organisation. We highlight the importance of risk- and business impact- analysis to inform the strategy and course of action. It is important to note the iterative nature of implementing controls, risk assessment frameworks and response mechanisms.
- A detailed analysis of an **initial set of Telco use cases** that are impacted by Post Quantum Cryptography. The use case analysis highlights dependency on standards, stakeholder landscape (including the wider supply chain), data discovery, the use of PKI and solutions for cryptographic agility and Quantum safe migration. The list of use cases presented is not exhaustive; additional use cases will be added in upcoming releases..

Network operator use cases	Actions Identified	Customer impacting use cases	Actions Identified
Protection of interface between base stations & security gateway	**Yes**	Virtual Private Network services	**Yes**
Virtualized network functions	**Yes**	SD-WAN services	**Yes**
Cloud Infrastructure	**To be determined**	IoT Smart Meters	**Yes**
SIM (physical)	**To be determined**	IoT Automotive	**Yes**
eSIM Provisioning (remote)	**Yes**	Lawful Intercept	**To be determined**
Devices and firmware upgrade	**Yes**	Privacy of customer data	**Yes**
Concealment of the Subscriber Public Identifier	**Yes**		
Authentication and transport security in 4G and 5G	**Yes**		

Table 1: Summary of actions for Telco Use Cases

- Overview of themes, relevant to the post quantum journey:
    - **Algorithm standardisation processes** and the **migration options** for asymmetric cryptography
    - **Symmetric cryptography** Post Quantum security levels and implication for key sizes
    - Widely used protocols, e.g. **IPSEC and TLS,** and an update on protocol standardisation
    - Challenges of reliance on manual processes. The importance of **automation** to support the adoption of cryptographic agility and quantum safe solutions at scale
    - PQC and the wider security context, including Zero Trust Architecture
- The importance of **proofs of concept and testing**, as new cryptography solutions are developed and implemented, to meet Telco performance, robustness and resiliency requirements for different use cases. Close cooperation between academia, industry and regulation is critical for availability of implementable commercial solutions.
- A multi-country overview of published **government guidance** (updated from the impact assessment whitepaper), highlighting the increased momentum and activities in progress globally.

This document is not intended to prioritise the actions described. It is up to the risk owners, e.g. Telco Network Operators, to prioritise actions based on their business priorities.

2.1 Migration Plan

An inventory of vulnerable assets is a first step. In all likelihood, it will not be required nor possible to protect all these assets. The next step is prioritising the security systems to be migrated first. In this regard, multiple criteria will help the prioritisation:

- How critical is the system to be updated (i.e., consequences of a successful attack).
- The security properties the system provides. Confidentiality may appear as essential, compared to authenticity, because of the “store now, decrypt later” attack that aims at retroactively decrypting data. To assess the impact of such kind of attacks, one should define the sensitivity of the encrypted data. This allows choosing the assets to migrate but also opting for an adequate migration strategy (e.g., phased transition, full update).
- The time needed to update a system. Protecting update mechanisms (e.g., firmware update) may be more urgent than migrating encryption mechanisms since the former may require a longer time that the latter. Breaking authentication often leads to breaking confidentiality.
- Moreover, authenticity may also be more important than confidentiality in other cases. For instance, regarding digitally signed documents (e.g., contracts involving multiple parties). If such documents are expected to remain valid over a long period of time, then the advent of a quantum computer will suddenly invalidate the proof of authenticity and non-revocation that come with these legal agreements. Once the digital signature is rendered null and void, the stakeholders are de facto released from their initial commitment.
- The level of exposure of a system to attacks (e.g., internal server vs. servers connected to the internet) is also a factor to take into account.
- In order for the quantum attacks to be successful, the adversary needs first to collect material (e.g., encrypted data, public keys). The ability to hide (possibly temporarily) such data may prevent the attacks and, in turn, delay the need to update the corresponding cryptographic mechanisms.
- The recommendations (or requirements) from various regulation authorities (e.g., cybersecurity agencies) may affect the transition priorities.

2.2 Migration Prioritisation

Priority may be given on mitigating a subsystem instead of updating the latter. That is, in a phased transition, it may be necessary to (temporarily) accept a trade-off in terms of security in order to thwart attacks from external adversaries (therefore, assuming that there no internal adversaries). Then, this allows spending some time to update other critical subsystems. For instance, one may decide to temporarily use symmetric-key algorithms in an internal subsystem in order to save time to deploy post-quantum cryptographic mechanisms in an external subsystem. Then, in a second phase, the first internal subsystem can be finally migrated to post-quantum cryptography.

3 Planning: Timelines and Dependencies

3.1 Phases (High Level)

The journey to crypto-agility and Post Quantum Cryptography is an integral part of each organisation's overall security strategy in the context of the evolution of the cybersecurity landscape. Continuing to provide cryptographically secure products and services to Telco users remains a business imperative in keeping data and communications secure. The guidance from the *Post Quantum Telco Network Impact Assessment Whitepaper* [GSMA-PQ.01] is to prepare and plan. This increases operators' ability to effectively mitigate security impacts, leverage synergies with other programs, leverage new business opportunities and manage internal and external dependencies.

Early preparation is beneficial in supply chain management. The definition of clear requirements and timelines by operators ensures that critical capabilities are available from suppliers and aligned with implementation plans.

As regulation and compliance for Quantum safe matures, this may influence prioritisation and adoption strategy.

Cryptographic agility gives organisations the ability to be more responsive to a rapidly evolving threat landscape by designing solutions to changing cryptographic algorithms in a cost effective and flexible manner. Crypto-agility is not the scope of this document, but we believe that its adoption is an important consideration for future security solutions.

A definition of high-level phases to support the journey to Post Quantum Cryptography and subsequent management is outlined in Figure 4, illustrating the iterative nature of the phases.

Governance is a critical element that underpins all of the phases. Effective governance will ensure support of the organisation's strategic goals, bringing together decision making, funding, execution, compliance and reporting across the organisation.

- Phase 1: Capability and skills development
- Phase 2: Cryptography discovery and analysis
- Phase 3: Business risk analysis
- Phase 4: Prioritisation and planning
- Phase 5: Remediation execution
- Phase 6: Operation and ongoing cryptographic governance

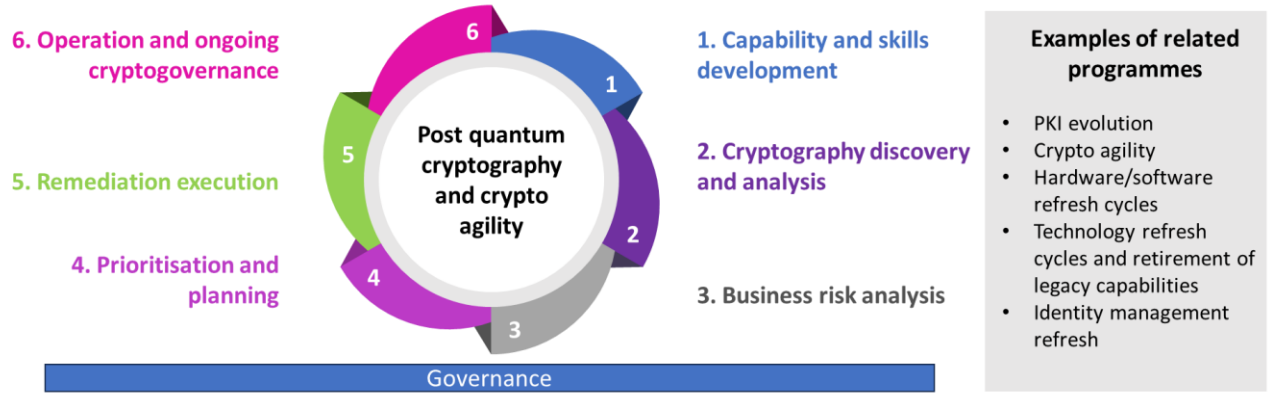


Figure 2: High Level Phases

3.1.1 Capability and Skills Development

Awareness of the quantum threat and development of the skills to support the journey to quantum readiness and Post Quantum Cryptography is critical for organisations across all levels of workforce and leadership. Understanding the threat and the current cryptography landscape enables affected organisations to chart an informed path forward. As Post Quantum Cryptography solutions are defined, the enterprise strategy can include the quantum readiness.

3.1.2 Cryptography Discovery and Analysis

An understanding of where and how cryptography is being used within the organisation is the foundation of a quantum readiness roadmap, that is required for a successful Post Quantum migration. Cryptographic discovery - whose output is a comprehensive cryptographic inventory - is the starting point for the analysis. This exercise is likely to be a cross-organisation activity.

Analysis provides insight on potentially vulnerable cryptographic capabilities in use, including encryption, digital signatures, hashing, ... It also highlights any dependencies on specific products, vendors and on future standardisation activities.

3.1.3 Business Risk Analysis

Business risk analysis provides the ability to make informed decisions on the funding, prioritisation and execution strategy, based on the organisation's strategic priorities and risk appetite. Key outcomes, such as the ability to identify and quantify threats, an understanding of the vulnerabilities and the business impacts are all critical in informing a course of action.

For additional information on quantum risk assessment see [GSMA-PQ.02]. This includes an analysis of commonly used risk assessment frameworks, methodologies and best practices to support this phase, as well as providing an ongoing monitoring capability.

3.1.4 Prioritisation, Planning and Governance

The risk assessment and business risk analysis provide informed input to enable organisations to prioritise and plan activities, as well as a business rationale to justify investment. As part of this phase mapping and management of dependencies, is required. Some of the key dependencies may include (this is not an exhaustive list):

- Standardisation timelines (NIST PQC and relevant downstream standardisation activities)
- Procurement requirements and vendor roadmaps
- Refresh cycles (hardware and software)
- Regulation, policy and government requirements

3.1.5 Remediation Execution

A prerequisite for execution is the preparation phase, including testing of solutions and migration processes. This will involve multiple stakeholders and many dependencies that must be tracked and managed through careful governance.

The process of implementing quantum safe solutions varies. In some cases, PQC will be delivered as part of a business-as-usual software upgrade or as part of a technology refresh cycle. In other cases, PQC may require a specific system implementation with end-to-end solution coordination and testing. Both cases need consideration of interoperability and transition management.

3.1.6 Operation and Ongoing Crypto-Governance

The advance of technology, including Quantum Computers, requires an approach to cybersecurity that can respond to new threats and adapt to changes in regulation, compliance, risk appetite and alignment to strategic goals. The telecommunication industry is a prime target from a cybersecurity perspective, given the critical nature of its services. It is important to view the migration to post quantum cryptography as an ongoing activity that implements controls, risk assessment frameworks and response mechanisms as the cybersecurity landscape develops.

Our recommendation is to create and maintain a Quantum Risk Management (QRM) capability [GSMA-PQ.02].

3.2 Standards, certification, regulation guidance and legislation

The transition to PQC will include standards, certification, guidance and regulation and maybe even legislation.

3.2.1 Standards

Standards will define new cryptographic algorithms (e.g. ML-KEM), the protocols that use those new algorithms (e.g. TLS) and how they are combined to build systems (e.g. 5G). Standards come from recognised national (e.g. NIST), regional (e.g. ETSI), global (e.g. ISO) and sector-specific (e.g. 3GPP, IETF) bodies. (The formal distinction between *de-jure* and *de-facto* standards is less significant that acceptance of organisations' competence in the domain of cryptography or its application).

3.2.2 Certification

Certification gives an assurance about the implementation of a cryptographic standard in a product. The implementation of cryptographic algorithms must avoid known flaws such as side channel attacks that expose key material to timing analysis or power analysis. National governments and industry groups run certification programs where independent test laboratories verify products against certification requirements. One example is the NIST Cryprographic Module Validation Program (CMVP) that tests compliance with the requirements of FIPS 140-3.

3.2.3 Regulation

Regulation includes technical requirements from sector-specific regulatory authorities that have legal backing from national governments. The Monetary Authority of Singapore Circular No. MAC/TCRS/2024/01 is a recent example.

3.2.4 Guidance

Guidance on PQC is published by national cybersecurity authorities. The first round of guidance in many countries covered a high level summary of the risk from Quantum Computing, an overview of NIST process and a recommendation to wait for published standards. The level of detail of guidance has evolved. Some authorities now specify which algorithms should be used and key-lengths. Examples include ANSSI, BSI and NCSC PQC guidance.

After the publication of the NIST PQC standards, we expect national cybersecurity authorities to publish updated PQC guidance.

3.2.5 Legislation

Legislation on PQC may in future be enacted by national governments. So-far legislation has been used as a mechanism to fund governments' own transition to PQC, e.g. Public Law No: 117-260 in the US.

3.3 Post Quantum Cryptography Government Initiatives by Country and Region

Government recommendations on migration to Post Quantum Cryptography are being updated after publication of the NIST standards. Details on the Post Quantum Cryptography Government initiatives previously in an Annex are moved to a separate document for ease of maintenance.

3.4 Crypto-Governance

As Telcos prepare for the implementation of quantum resistant solutions the issue of crypto-governance becomes increasingly relevant. Effective cryptography governance within an enterprise is a critical element of the overall security governance and the rapidly evolving quantum capabilities should be viewed in the wider context of an evolving threat landscape, requiring the evolution of cryptographic solutions and increased agility.

While the concept of cryptography governance is not new, managing a cryptography migration, in conjunction with an evolving standardisation, regulation and compliance landscape, provides a catalyst for establishing or re-enforcing a strong crypto-governance practice that will effectively serve the preparation and migration to post quantum cryptography and beyond.

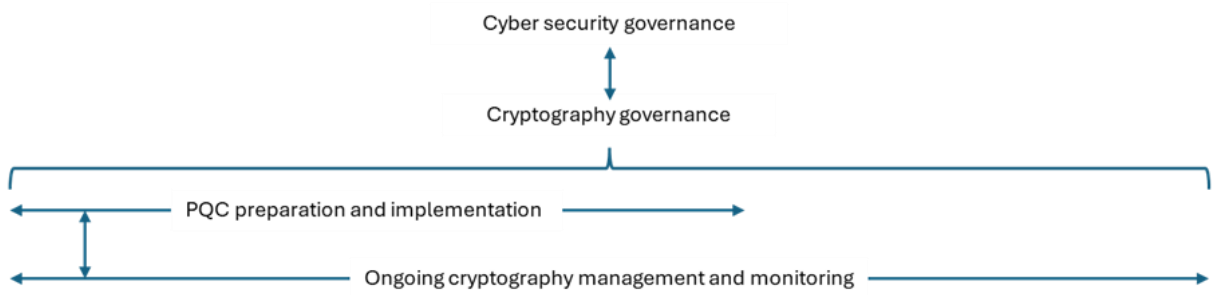


Figure 3: Crypto-Governance

The scope of this document is not specific to any regulation or legislation framework and we will not recommend or endorse any specific governance model: the objective is to highlight aspects that are relevant to Telco organisations that are in the process of preparing and implementing a future proof approach to post quantum cryptography migration. The quantum threat is driving a change in the existing cryptography strategy and the implementation will impact multiple stakeholders within the organisation. An ongoing management and monitoring of cryptography will impact operational processes, including inventory and observability requirements.

Key objectives of the crypto governance agenda include:

- Transparency and accountability from strategy/funding to execution
- Coordination of internal and external stakeholders
- Awareness and skills building across relevant teams
- Engagement with the supply chain
- Coherence with overall cybersecurity governance, risk and compliance, managing evolution of standards, regulation and legislation
- Definition of processes and operationalisation of the implementation

These underpin the phases, as described in this document of the journey towards crypto-agility and post quantum resilience.

3.5 Governance and Decision making issues

Management must take a view on these governance topics for PQC migration.

- Compatibility of regional and national standards. During the transition to PQC there may be inconsistencies as standards evolve. Technical managers must manage these requirements with the supply chain.

- Budget and resource challenges - managing the phase-in of Post Quantum Security alongside other essential cybersecurity priorities. (Can operators identify solutions which meet other business requirements, while at the same time being PQC-ready?)

- Phasing in Post Quantum Security – identifying your critical path and most vulnerable assets

- Formulating a business case for addressing the issue sooner rather than later

3.6 Preliminary Recommendations for Automation

Use of automation is key for the future of cybersecurity. Streamlining end-to-end operations; increasing accuracy of responses; shorter incident response times; reduced costs; enhanced resilience for the organisation.

Automation is a critical enabler for organisations that are implementing crypto-agility and adopting quantum safe cryptography at scale. Reliance on manual processes to manage cryptography is error prone and resource intensive.

Automation provides benefits at all stages of the crypto-agility and quantum safe journey. Automated cryptography discovery tools create a cryptographic inventory, as well as supporting continuous monitoring processes to detect changes in cryptography vulnerabilities. Automation can also support the prioritisation of remediation actions, through vulnerability and compliance analysis, with the aim of monitoring threats and reducing risks. Finally, use of automation in the remediation phase supports the application of remediation patterns to rollout and manage vulnerabilities effectively and consistently.

Automation complements and augments the tasks that require manual intervention (due to dependency on specific business decisions, institutional knowledge and oversight). This is particularly relevant when managing emerging threats and implementing new solutions in a complex and critical telco landscape.

3.7 Zero Trust Architecture Framework Consideration

Security and risk are relative terms. The quantum risk security guidelines, discussed in this document, relate to the upgrade of cryptographic algorithms, engineered to maintain a comparable level of security to today when faced with attacks using classic and/or cryptographically relevant quantum computers. However, the migration to PQC is unlikely to fix any underlying security issues already present in those systems and may be considered as part of a holistic security strategy, for example Zero Trust (ZT) or another approach.

The Post Quantum world will bring challenges not only to cryptography, as is known today, but also to other aspects of security. NIST SP 800-207 document addresses Zero Trust Architecture (ZTA) for enterprises, including and not limited to all enterprise assets and subjects. ETSI GR ETI 002 document extends the ZTA concept to a public telecommunications infrastructure. As mentioned in the document, “... there should be no assumptions as to what happens before or after each hop in and across the infrastructure, starting with the source and ending with the destination of particular data flow at all layers of OSI.” (ETSI GR ETI 002).

3.7.1 Zero Trust Architecture in the Context of Post Quantum Cryptography

Figure 1 points that ZTA is orthogonal to all cryptography algorithms and their corresponding use cases. ZTA encompasses cryptography as well as other aspects of security. ZTA is a methodology of recursive application of steps an organization takes to conform with. Part of those steps is the creation of Zero Trust security policies which could include application of cryptographic algorithms to data.

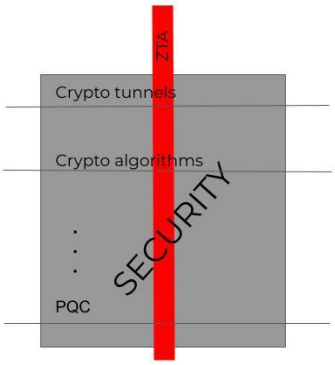


Figure 4: ZTA Framework within Security Realm

The Zero Trust security policies are defined using the Kipling method, shown in Figure 4.

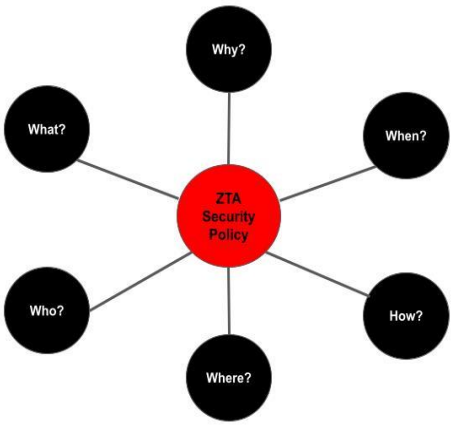


Figure 5: Kipling Method. Elements of ZT Security Policy

ZTA relies upon multiple security mechanisms, including cryptographic algorithms, in order to provide authentication, confidentiality and integrity protection. As Figure 1 illustrates,

ZTA includes mechanisms that are vulnerable to quantum computing (i.e., classical cryptographic algorithms); the quantum threat applies to ZTA as well. Hence, ZTA in the Post Quantum realm must encompass the deployment of Post Quantum Cryptographic algorithms.

4 Cryptographic Algorithms and Protocols

This chapter describes the cryptographic algorithms, schemes and protocols that are the building blocks of security. Each section describes an aspect of the PQC transition. Sub-sections provide greater detail, which may not be required by all readers.

4.1 Algorithm Standardisation: Asymmetric Cryptography

Asymmetric cryptography (or public key cryptography) provides both key-exchange and digital signatures for mobile telecommunications. Asymmetric algorithms such as RSA, elliptic curve and the DSA are vulnerable to a cryptographically relevant quantum computer (CRQC), so replacing these algorithms is the main focus of the PQC transition.

4.1.1 Introduction

The NIST PQC program aims to select and standardize algorithms for key establishment and digital signatures that are intended to resist attackers with access to a CRQC. There are similar efforts in other countries. This subsection describes these standardization processes and the key features of the selected algorithms from the perspective of migration from traditional algorithms.

Applications must take PQC performance into account when planning migration. In general, all of the schemes are (at least) an order of magnitude slower and/or bigger than their traditional counterparts in most metrics and introduce trade-offs that did not previously arise; The increased size of keys (and ciphertexts/signatures) becomes a particular concern if these must be held in a secure element or trusted module with limited resources. The performance figures provided in this section for sizes are a ballpark guide only: the candidates algorithms are defined for multiple security levels, and it may be the case that the final standards documents do not include all parameter sets. In general, when using Post Quantum secure schemes in a hybrid mode in combination with traditional algorithms the performance/size costs will be dominated by the quantum safe scheme.

4.1.2 Key Establishment

4.1.2.1 NIST Key Encapsulation Mechanism Standard

NIST defines FIPS 203 ML-KEM as the algorithm for key encapsulation. (A key encapsulation mechanism is one part of key establishment). It was selected by NIST as the only key encapsulation mechanism (KEM) in the third round of their PQC competition.

Defining a small number of common profiles for key establishment in standards and national guidance (which algorithms, which key lengths) simplifies developing Quantum-safe products and services.

Allowing flexibility is important for interoperability. Avoiding too many options is important for implementation and verification.

Traditional key-establishment algorithms include Diffie-Hellman (DH) key exchange (based on elliptic curves or finite fields), its variants [NIST 800-56A] and key transport based on RSA [NIST 800-56B]. ECDH keys are in the order of 32-130 bytes with ciphertexts in the same size range.

ML-KEM is in general well balanced, with keys and ciphertexts in the order of 1KB and operations that are approximately as fast as ECDH. ML-KEM is as the name suggests a key encapsulation mechanism and is not a direct drop-in replacement for DH key exchange: it is expected that international standards bodies will release further standards that define how to use ML-KEM in place of DH. This is more straightforward in multiple-message protocols

such as TLS [IETF TLS draft] than for DH variants where both parties have static keys and no messages are transmitted (for KEMs, at least one message must be transmitted).

4.1.2.2 Future Key Encapsulation Standards (NIST)

NIST's fourth round is intended to define a KEM based on an alternative to lattice cryptography, for resilience. The intent is to standardise the selected KEM in future.

NIST selected four KEMs for their fourth round. The algorithms remaining are Classic McEliece [McEliece], BIKE [BIKE] and HQC [HQC], all of which based their security on computational problems in code-based cryptography. (A fourth algorithm SIKE [SIKE] was shown to be insecure and has now been withdrawn). All three schemes are slower than ML-KEM but code-based cryptography is regarded as being more mature than the lattice assumptions that underpin ML-KEM. Classic McEliece has smaller ciphertexts (128-240 bytes) than ML-KEM but at the cost of larger keys (261-1357 kB), while HQC and BIKE are more balanced (but still larger than ML-KEM).

4.1.2.1 Alternate Key Encapsulation Guidance

The BSI in Germany [BSI-TR-02102-1] and ANSSI in France [ANSSI22] recommend the use of FrodoKEM [Frodo] (along with Classic McEliece) in their migration documents. FrodoKEM is another lattice-based scheme but with a more conservative design than ML-KEM (FrodoKEM's design is based on *unstructured* lattices, which have received more cryptanalysis).

4.1.2.2 Future Key Encapsulation Standards (ISO)

FrodoKEM, Classic McEliece and ML-KEM are being considered for standardisation by ISO/IEC as an amendment to ISO/IEC 18033-2, Encryption algorithms — Part 2: Asymmetric ciphers [ISO 18033-2].

4.1.3 Stateless Digital Signatures

4.1.3.1 Module-Lattice-Based Digital Signature Standard

NIST published FIPS 204 ML-DSA (Module-Lattice-Based Digital Signature Standard) in 2024 as the primary digital signature standard. It was based on the CRYSTALS-Dilithium [Dilithium] submission. ML-DSA's security is based on lattice-based cryptography, and, like ML-KEM, it was selected for its balanced properties: relatively fast key operations, medium-sized keys (1312-2592 bytes verification key, 2528-4864 bytes signing key) and medium-sized signatures (2420-4595 bytes).

Traditional digital signature algorithms in widespread use today include (EC)DSA (32-64 byte keys and 48-112 byte signatures) and RSA (256 byte keys and signatures).

All these signature algorithms are stateless, meaning that one does not need to keep track of the elements used to generate previous signatures.

4.1.3.2 NIST Stateless Hash-Based Stateless Hash-Based Digital Signature Standard

NIST published FIPS 205 SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) in August 2024. SLH-DSA is more conservative than the lattice schemes and is based on the security properties of hash functions with small key sizes (32-128 bytes), but is much slower and has larger signatures (8-50 kB). SLH-DSA is based on the SPHINCS+ submission [SPHINCS+].

4.1.3.3 Future Digital Signature Standards

NIST plan to publish the standard FN-DSA in 2025 after the process for ML-DSA and SLH-DSA has concluded. FN-DSA is also based on lattice assumptions and is generally slightly more performant than ML-DSA, however the signing algorithm requires double precision floating-point arithmetic which comes with challenges on embedded platforms and fragility in terms of vulnerability to side-channel attacks. FN-DSA is based on the Falcon [Falcon] submission.

ML-DSA and FN-DSA are based on structured lattices; to diversify the post-quantum signature portfolio NIST are conducting another competition with 40 complete submission packages to the initial deadline of June 2023 [NIST On-Ramp]. There will be no new competition for KEMs.

4.1.4 Stateful Digital Signatures

XMSS [RFC 8391] and LMS [RFC 8554] are hash-based signature schemes published by the Internet Engineering Task Force. They are described in a NIST Special Publication in 2020 [SP 800-208], making them ready for usage now.

The schemes are conservative because their security only relies on the properties of hash functions. The understanding of hash functions is much more mature than that for lattice- and code-based cryptography. The schemes are however different in terms of interface from traditional signature schemes such as RSA and DSA: they are built from one-time signatures, and the secret key contains a state that requires (for security) that these one-time signature key pairs are only used once.

4.1.4.1 State Management for Stateful Digital Signatures

The challenge of state management limits the applicability of XMSS and LMS to scenarios where signing happens relatively rarely and only on a single device in a secure environment. Firmware signing is the usual application.

Conformance with NIST SP 800-208 [SP 800-208] forbids export of private keying material from the (single) module that performs signatures, ruling out the use of distributed signing or any key backup. These schemes have a number of parameters that affect performance, so it is difficult to give concrete numbers that make for useful comparisons, however in general XMSS has slightly smaller signature sizes while LMS is more performant.

4.2 Migration Options

The migration from traditional cryptography to quantum resistant cryptography is not as straightforward as just replacing component algorithms with their Post Quantum counterparts. Public key cryptography is used across hardware, firmware, applications, operating systems and cryptographic libraries. In some cases, it is negotiated between the communicating parties.

The migration to quantum resistant solutions is underpinned by the cryptographic algorithms and protocols that are standardised, then implemented in products, subsequently integrated and configured into solutions.

Telecommunications operators must take an end-to-end view across the different systems to coordinate testing and deployment of quantum resistant solutions that consider crypto-agility, backward compatibility and interoperability. We strongly advocate the use of standardised algorithms, protocols and solutions as a way of facilitating migration and minimising cost.

As new products, protocols and solutions emerge consider performance and reliability requirements of the specific use cases.

It is critical to begin working with the wider ecosystem of partners to plan the testing and validation of solutions, consider the migration options, and address supply chain and procurement implications ahead of implementation.

The NCCOE has also defined a list of operational considerations that may be useful in building an execution plan (pqc-migration-project-description-final.pdf (nist.gov)) which includes aspects related to interim/temporary implementations, specifying the relevant procurement requirements, testing and validation of new processes and procedures.

4.2.1 Hybrid Schemes

Hybrid schemes combine different types of cryptography. Originally it meant the combination of symmetric cryptography and public key. For PQC hybrid means combining PQC algorithms with traditional asymmetric cryptography, with symmetric cryptography or even with QKD. While hybrid schemes may be useful in providing a transitional migration and fall-back mechanism, they also introduce a computation and complexity overhead that may be inappropriate in some contexts. It is important to be precise in terminology when describing hybrid and IETF [IETF-draft-flo].

Governments and international bodies are in the process of defining and updating guidelines, with some advocating the use of hybrid migration (use of a traditional algorithm alongside a Post Quantum algorithm). This aspect is for further study.

4.2.2 Digital Signatures for Code Signing

In some contexts where only signatures (and no key exchange) are used such as code signing (secure software/firmware updates), NSA [CNSA], ANSSI [ANSSI22], and BSI [BSI-TR-02102-1] recommend transitioning to the hash-based signature schemes instead of introducing the complexity involved in hybrid protocols. As described above the stateful hash-based schemes have their own implementation challenges.

4.3 Impact on Symmetric Cryptography

In contrast to the asymmetric case, the post-quantum security level ensured by the current set of parameters for symmetric algorithms is more difficult to assess, in particular when it comes to the key sizes.

4.3.1 Symmetric Key Sizes

Grover's algorithm provides a potential quantum advantage (compared to classical computers) for exhaustive key search on symmetric cryptography. The implications are still the subject of ongoing research and debate; no consensus has emerged so far, as illustrated by the positions of the different national cybersecurity agencies. See: 4.10.2 Symmetric Key sizes

4.3.1.1 Technical Discussion

Depending on practical limits for extremely long-running serial quantum computations, the advantage of Grover's algorithm ranges from a quadratic speedup to none at all when also taking quantum-to-classical cost ratios into account [NIST-CALL, NIST-FAQ]. A quadratic speedup would call for a doubling of the current key size (namely moving from 128-bit to 256-bit keys) whereas the alternative scenario would not require any change.

4.3.1.2 NIST Recommendation

NIST [NIST-FAQ] claims that *"AES 128 will remain secure for decades to come"* although this claim is slightly qualified by the sentence which follows:

> *"Furthermore, even if quantum computers turn out to be much less expensive than anticipated, the known difficulty of parallelizing Grover's algorithm suggests that both AES 192 and AES 256 will still be safe for a very long time."*

This seems to suggest that, in some scenarios, Post Quantum security would only be ensured for AES 192 and 256.

Nevertheless, some security levels defined by NIST for its standardisation process correspond to the security of AES-128 and SHA-256 against classical and quantum attacks, which at least shows that NIST considers these to be relevant security levels in a quantum setting.

4.3.1.3 ANSSI Recommendation

ANSSI [ANSSI] recommends using 256-bits key size.

4.3.1.4 BSI Recommendation

IFrom January 2023, the recommendations [BSI-2023] read:

> *"Therefore, Grover attacks on symmetric cryptographic primitives with the classical security level aimed at in this Technical Guideline do not seem relevant for the foreseeable future. Practically, they can nevertheless be defended against with little effort by using a higher classical security level; for example, instead of AES-128, AES-256 can be used as a symmetric block cipher"*

This suggests that moving to 256-bit keys might not be necessary to withstand Grover attacks but that it could nevertheless be a reasonable option given the little effort it requires in most cases, at least compared to the migration of asymmetric cryptographic mechanisms.

4.3.1.5 NCSC Recommendation

NCSC's 2023 white paper [NCSC 2023] states that symmetric cryptography is not significantly affected by quantum computers and that existing 128-bit algorithms such as AES-128 can continue to be used securely.

4.4 Impact on Hash Functions

The impact of quantum computers on hash functions differs according to the considered properties of such functions. Regarding collision resistance, we are only aware of one quantum attack [EQCSAISC] that claims to perform better than classical ones, but this is the subject of debates [cr.yp.to: 2017.10.17]. In all cases, the improvement implied by this attack is rather moderate and would only require a slight increase of the digest size. For example, using SHA-384 instead of SHA-256 would be largely sufficient.

4.4.1 NCSC Recommendation

NCSC [NCSC 2023] 2023 white paper states that secure hash functions such as SHA-256 are not significantly affected by quantum computers and can continue to be used.

4.5 Impact on Widely-used Protocols (TLS, IPSec)

These protocols are developed and standardised by the IETF. They are the building blocks for internet security. The 3GPP standards used in mobile networks depend on them.

Telco Use Cases: System Impacts and Guidelines presents a number of use cases that are prevalent in the telco domain, and this section describes some of the cryptographic protocols that are prevalent in multiple use cases in the context of migration to Post Quantum Cryptography.

4.5.1 On-going standardisation in IETF

Relevant work in the IETF TLS working group:

- Hybrid key exchange in TLS 1.3: the shared secret is used to get confidentiality and data integrity of application data, but entity authentication comes from the signatures that the server provides during the handshake. The hybrid draft only adds ML-KEM to get post-quantum security of the transmitted data, it does not update to hybrid signatures. The consequence is that a QC attacker could impersonate any server, but not read data encrypted in the past from sessions established using this draft.
  Status: mature draft

Relevant work in the IETF IPSECME working group:

- Multiple Key Exchanges in IKEv2: The goal there is to combine the output of one or more Post Quantum key exchange mechanism with the one from a classical mechanism to generate a single shared secret.
  Status: RFC

Relevant work in IETF LAMPS group:

- Use and handling of PQC algorithms in certificates and Certificate Management Protocol (CMP)
- Definition of identifiers for different PQC algorithms
- Specification of PQ/T hybrid certificates
- Status: work in progress as of September 2024

4.5.2 Transport Layer Security Protocol (TLS)

Transport Layer Security (TLS) [TLS-1.3-RFC] is a protocol for a client and server to establish a channel for secure communications at the application layer. TLS also underpins HTTPS and so is the base of Web security.

4.5.2.1 TLS Versions

The TLS protocol provides one-sided or mutual authentication using certificates. The most recent version, TLS 1.3, is standardized as an IETF RFC [TLS-1.3-RFC] however prior versions such as TLS 1.2 [TLS-1.2-RFC] and TLS 1.1 [TLS-1.1-RFC] are still widely used. Many web domains and browsers no longer support TLS 1.1 however many legacy devices and components are still deployed meaning that other entities such as servers may be required to accept incoming connections that only use version 1.1.

4.5.2.2 TLS Cipher Suites

A TLS session is defined by the cipher suite agreed by the participating parties, and will be described by the names of its components. As an example, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 defines the usage of (ephemeral) elliptic-curve Diffie-Hellman for key exchange, RSA for digital signatures, AES-GCM with 128-bit keys for record layer encryption and SHA2 with 256-bit digest for hashing. AES and SHA2 are symmetric algorithms and thus are less vulnerable to quantum computing attacks than ECDHE and RSA signatures which are public-key cryptography algorithms.

4.5.2.3 Hybrid TLS

An IETF draft [IETF-TLS-hybrid] has been proposed for usage of the key exchange component of TLS 1.3 in hybrid mode. In essence, the key exchange phase is conducted two or more times using the regular TLS 1.3 key exchange message exchange process with different underlying algorithms in a side-by-side manner, for example using a traditional algorithm such as ECDHE and a Post Quantum secure algorithm such as ML-KEM, and the resulting keys are combined by concatenating the resulting keys into the key-derivation function that provides session keys to the record layer. As with all hybrid key exchange designs, the goal is that the scheme is secure as long as at least one of the component algorithms is secure. Note that this migration is only on the key exchange component and not on the digital signature component of TLS, so that store-now-decrypt-later attacks (decryption of session traffic) are prevented, while authentication attacks (an adversary acquiring the signing key for a certificate and impersonating the server) are not covered.

Note that TLS 1.3 allows a pre-shared key resumption mode, in which previously generated secret key material is employed to encrypt an initial communication in a resumed session. These resumed pre-shared keys may be reliant on the previous use of asymmetric cryptography or key exchange algorithms that are quantum vulnerable, and are therefore vulnerable to quantum attacks if the algorithms used in a previous session to generate the key material were not Post Quantum secure. In the present document, usage of the term

"pre-shared key" refers only to key material previously shared via means not reliant on quantum vulnerable algorithms. Hence, the pre-installation of secret keys on devices such as SIM cards or the physical sharing of secrets using pen and paper can be classified as pre-shared secrets, with regard to quantum safe discussions, but pre-established secrets used in TLS 1.3 resumption modes, deriving from quantum vulnerable algorithms, are not.

4.5.3 Internet Key Exchange Protocol (IKE)

The Internet Key Exchange protocol is a protocol for two parties to establish a channel for secure communication at the internet layer and is part of the IPsec suite. Like TLS, certificates are used for entity authentication and the key exchange protocol at the heart is based on Diffie-Hellman.

4.5.3.1 IKE Versions

IKE v1 [IKE-v1-RFC] has been replaced by IKE v2 [IKE-v2-RFC]. IKE v2 is very widely used in VPN applications.

4.5.3.2 Hybrid IKE proposals

There are multiple proposals to update IKE for PQC. The IETF-RFC [IETF-IKEv2-mixing] describes an extension of IKEv2 to allow it to be resistant to a quantum computer by using pre-shared keys. Another IETF RFC [IETF-IKEv2-hybrid] published in May 2023 for usage of the key exchange component of IKE v2 in hybrid mode. It follows a slightly different approach than the TLS hybrid draft: an initial secure channel is creating using Diffie-Hellman key exchange, and then a second (and perhaps a third) key exchange is done 'inside' this channel with a Post Quantum secure key exchange mechanism such as ML-KEM as an IKE_INTERMEDIATE extension [IKE-INT].

4.5.4 Cryptographic Inventory Implications

Details of cryptographic inventory related to IPSec, IKE and TLS might include:

- Symmetric encryption algorithms for data at rest: e.g., AES
- IPSec mode: tunnel mode or transport mode
- IPSec header: AH or ESP (authentication header or Encapsulating Security Payload)
- IPSec perfect forward security (PFS): enabled or disabled
- IPSec session lifetime
- IKE protocol version: e.g. v2 versus v1
- IKE cipher suite:
    - symmetric encryption method: e.g., AES_128 CBC, 3DES_192 CBC
    - message authentication code: e.g., HMAC-SHA1, HMAC-SHA256
- IKE hash algorithm: e.g., SHA256, MD5
- IKE authentication method: e.g., pre-shared keys (PSK) or certificates: RSA or ECC digital certificate
- IKE Diffie Hellman Group: identifier of the key used in the DH key exchange. E.g., group 2: 1024 bit, group 19: 256 bit elliptic curve group.
- TLS cypher suites as described in section 4.5.2.2.

- Digest/Used for PRN: SHA384

4.5.5 Public Key Infrastructure

Both the protocols used to communicate with the PKI and the PKI implementation must be updated for PQC.

Protocols such as Certificate Management Protocol (CMP version 2) do not currently provide the necessary crypto-agility, nor the ability to add extended key usages for CMP server authorizations. Additionally, the X.509 certificates that are used by key establishment protocols would have to be updated to support ML-KEM public key as well as the ML-DSA signature of the CA. Additionally, if hybrid schemes are used then those attributes would have to be included in the certificates as well.

4.6 Algorithm Testing and Implementation

It is crucial for providers of cryptographic assets to assess as quickly as possible the potential impacts of PQC migration to their systems.

This document describes many use cases in the telecommunications domain, and it is inevitable that some will be more deeply affected than others, so early testing---as an immediate follow-up to performing a cryptographic inventory---will lead to a smoother migration process. This section describes the challenges that are present in the use cases and provide guidance for mitigating the most severe constraints. It should be noted that in any migration plan it needs to be agreed by all stakeholders whether the upgraded scheme will support a hybrid mode (see Section 4.4.4) or shift directly to PQC, and in many cases this decision will be informed by national and international guidance and recommendations (see Annex A) in addition to the work by the relevant standards bodies.

From a migration perspective the simplest communication protocol to upgrade is a standardized protocol that is performed between two server-grade devices, for example the usage of TLS in the SIM provisioning use case (see Section 5.5). The NIST standard PQC algorithms are generally very performant in terms of execution time on server-grade devices, meaning that speed is unlikely to cause issues when migrating.

4.6.1 Infrastructure Capacity

Even in the case of server-to-server, it is important for MNOs and vendors to assess whether their current infrastructure (servers/HSMs and communication channels) can support the necessary communication overhead incurred by the larger ciphertexts and signatures, and whether it is necessary to upgrade to servers/HSMs that are better suited to the operations present in the NIST standard PQC algorithms. Another necessary step in this use case is to manage the certificates or public keys of the two entities to ensure that the upgraded protocol, whether it be hybrid or PQC only, is performed securely between the intended entities.

4.6.2 Middleware Compatibility

The network should be checked for issues created by non-compliant middleware (software and hardware designed to handle a variety of secondary services and capabilities for operating systems).

Early experiments by Google [G-CECPQ2] showed it is possible that buggy middleware is causing issues with larger than expected keys, whereby “expected” relates to non-PQC implementations. [G-Hybrid] Google identified two ways in which bad middleware can cause problems:

1. Buggy middleware close to a specific site will cause that site to fail to work globally when PQC is enabled for it.
2. Buggy middleware in a local network can cause all sites to fail when PQC is enabled for them, but only when the client is on that network.

It's important to categorize the type of failure because it determines who can fix it: the first case is the sites' failure, the second must be fixed by local network administrators. To mitigate such issues, it is required to identify such issues early such that products that do not cause such complex failures or performance issues can be built and validated.

4.6.3 Firmware Validation

The use case of software/firmware updates Firmware Upgrade / Device Management require that the recipient device can support verification of PQC digital signatures. This requires that the device receives the verification key (in a manner that is secure, meaning that it cannot be maliciously injected by an adversary), and is capable of using it in a way that does not incur performance penalties that are unacceptable to end users of the devices. In this use case the increased size of PQC signatures will in most cases not be a problem since the code bundle that they are associated with is often relatively large, however for a very constrained (e.g. IoT) device it may be important to calculate or estimate verification time.

4.6.4 Constrained Devices

One step further on is any use case that requires a constrained (end-user) device to perform digital signature signing and/or key establishment. This includes Remote SIM Provisioning, Concealment of the Subscriber Public Identifier , Use Case: Virtual Private Networks and IoT Services. This list is not exhaustive for an MNO’s service portfolio. In this case it is a high priority to assess the impact of each use case on the hardware present in the constrained devices. Implementing the NIST standard PQC algorithms on this hardware will often be possible even in devices with constrained memory, however this may come at a cost of reduced speed. An impact assessment also needs to consider the storage and processing of public keys and certificates that are present in PQC.

4.7 PQC Migration

The following table is a collection of observations and suggestions about some common technical features that can found across different systems. This table is not complete in the number of technical features that could be identified, nor in the possible solutions. Constructing a similar table is an exercise that organisations might consider, in order to consolidate and harmonise their PQC migration strategy, by identifying systems across the organisation that are similar, and the solution categories that may be appropriate.

Common Technical Features	Possible Solution	Areas of Applicability
Underpinned by HTTPS / TLS / DTLS	- TLS 1.3 with PQC - DTLS 1.3 with PQC	- HTTPS Web / REST interfaces (e.g. SBI) - DTLS (non-SBI interfaces)
NDS / IP using IPSec	IKEv2 / IPSec with PQC	Inter-domain (e.g. 4G-5G interfaces, N6 to Enterprise), Non-SBI (e.g. N2, N3, N4 interfaces)
Proprietary Implementations (Closed Systems)	- Initially configuration with Symmetric Keys is possible - Relatively more straightforward to design for cryptoagility in closed controlled system	Enterprise IT (e.g. Single-Sign On), Management Plane including Machine to Machine communications e.g. IoT device management platform
Open Interoperable System	- CNSA - Cryptoagility (Necessary in dynamic, open, evolving interoperable system)	World wide web. Web 3.0 and blockchain
Hybridisation	PQC + traditional PKC	Regulated systems where regulations are not updated. Systems which must continue to support pre-quantum algorithms for legacy reasons.
Hybridisation	PQC + QKD/Symmetric key	- Transmitting data with long sensitivity 'shelf life' - Rigid and critical systems which cannot be cryptoagile, as frequent updates may risk in-life operation
Dedicated fibre links not relying on public key cryptography	In line encryption Symmetric key solutions such as: MacSec QKD	Fiber optic connections for data-center connectivity, direct Internet access, Wide Area Access (WAN)

Common Issues	Possible Solution Category	Highly applicable to...
Energy consumption of cryptography a critical issue	i. Fixed or rotating symmetric keys. ii. Lightweight ML-KEM implementation.	IoT Biomedical devices including implants
Regulatory guardrails	Watch and wait for regulatory updates. Be active in sector regulatory groups to drive progress and solutions for the sector. Add in-line bulk encryption until regulatory standards are updated.	Payment Card Processing. Heavily regulated industries: Telecoms (TSA), Financial Medical Devices, Armaments, Systems for Critical National Infrastructure/Government. Pharmaceutical Industry. Computers System Validation standards.
'Crypto-chaos' - *proliferation of standards and primitives creates risk of complexity, interop issues and vulnerabilities*	Open interoperable systems, Cryptoagile systems, Experimental updates, Complex environments in which testing all scenario's is unrealistic	World wide web. Web 3.0 and blockchain
In-life update	Test and deploy, Resilient by design, Virtualisation (rapid switchover and fallback).	Critical infrastructure, Telco control plane/ management networks Medical monitoring devices Safety alarms
Deployment/roll-out	Test and deploy, Phased roll-out, Staff training, Zero touch, VNFs, selecting vendors, Telecoms Security Act compliance.	Affects all stakeholders but particularly likely to require extra foresight and planning for organisations with many complex internal systems and/or additional security requirements.
Regional / National standards are incompatible	Additional primitives standardised outside of NIST program in Europe, e.g. by ANSSI and BSI	International multi-user systems including WWW, interfaces to cloud services, potentially also international cross-border settlement & payment networks
Performance impacts (large signatures, key sizes); MTU size	Select algorithms that are appropriate for each use-case	Radio links, IoT, Control / signalling plane impacts, design requirements on key

		storage and processing resource

4.8 Public Key Infrastructure

Many of the use cases in this document require certified public keys, meaning long-term public keys of a device/entity and an associated identifier are bound together using a digital signature from a certificate authority.

In some of the use cases, data confidentiality will be a priority for migration with entity authentication coming in a later phase. If entity authentication in a protocol in the use case involves long-term Diffie-Hellman keys (as opposed to digital signature keys), then these would need to be migrated to long-term KEM keys, which in turn would need to be certified using a traditional signature scheme. It is therefore important to consider the impact on an ecosystem's public key infrastructure when planning a phased migration process.

X.509 certificates are defined by the ITU and work towards post-quantum X.509 certificates is also done in the IETF [IETF-x.509], via developing guidance and interoperability testing.

4.8.1 Hybrid X.509 overview

A possible way to support the migration is to leverage hybrid certificates.

Despite promising proposals such as the one standardized by ITU, there is currently no universally accepted solution for hybrid certificates. Consequently, it is premature to recommend hybrid implementations as the community continues to evaluate the feasibility and necessity of hybrid solutions.

4.8.1.1 Hybrid X.509 options

In 2019, the ITU-T study group standardized an alternative public key and alternative signature in the X.509 certificates.

By leveraging certificates with multiple public-key algorithms, legacy applications could continue using traditional cryptographic algorithms, and once upgraded, they could start using the new ones. This approach would allow updated and legacy systems to coexist seamlessly.

However, there are also drawbacks to this solution. Hybrid certificates increase complexity and lead to larger certificate sizes, potentially causing issues in protocols or implementations expecting smaller sizes.

4.9 Common Dependencies

4.9.1 Cryptographic Standards

Standardisation of cryptographic algorithms using understood processes and open review is important to give confidence in the security of selected algorithms. Dependencies include:

- **Dependency-PQC-std-kem**. NIST standard PQC algorithm for key encapsulation (FIPS-203 ML-KEM) is a common dependency for PQC migration.
- **Dependency-PQC-std-sig.** NIST standard PQC algorithms for digital signature (FIPS-204 ML-DSA and FIPS-205 SLH-DSA) is a common dependency for PQC migration.
- **Dependency-PQC-std-national.** The publication of national standards for country-specific PQC algorithms, if required by individual countries.
- **Dependency-PQC-guidance.** The publication of guidance from national cybersecurity agencies on the use of PQC algorithms. Guidance typically specifies profiles (key-lengths and modes of operation) from published standards.
- **Dependency-PQC-regulation**. The publication of guidance from national cybersecurity agencies or industry regulators on the migration to PQC.

4.9.2 Other Standards

The IETF defines key protocols that are used in telecom networks and cloud infrastructure. Dependencies include:

- Dependency-TLS. The publication of an updated version of RFC 8446 (The Transport Layer Security (TLS) Protocol Version 1.3) to support the NIST standards (see below for more details).

- Dependency-IPSec. Standards for the integration of post-quantum key encapsulation methods into IKE version 2: RFC9370 (Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2) and RFC9242 (Intermediate Exchange in the Internet Key Exchange Protocol Version 2)

4.9.3 Open Source

Open source is a key component of many systems. Updating open-source projects to support the NIST PQC standards is a pre-requisite. Dependencies include:

- Dependency-Linux. Updates to the Linux Kernel and the Linux KVM hypervisor to implement PQC
- Updates to open source virtulalisation (OpenStack) and containerisation (Docker, Kubernetes, OpenShift) software to implement PQC
- Availability of open source implementations of PQC algorithms
- Updates to open source TLS implementations to implement PQC
- Updates to open source secret stores (Vault, Barbican) to support PQC
- Dependency-OAUTH. The updated implementations of RFC 6749 (The OAuth 2.0 Authorization Framework) and RFC 6750 (The OAuth 2.0 Authorization Framework: Bearer Token Usage) to support the NIST PQC standards.

4.9.4 Vendor Products

Many vendor products which are part of the telecom supply chain (e.g. servers, IP routers).

4.10 Technical Challenges for PQC Migration

The scope of this chapter is to highlight challenges that are not specific to single use cases and that may have wider implications: these are flagged with the scope of raising awareness for relevant stakeholders.

4.10.1 Misalignments between national cybersecurity agencies

The impact of quantum computers on cryptographic algorithms is well known and has led to the following families of recommendations:

- Public key Cryptography: use the current cryptographic mechanisms in conjunction with their post-quantum counterparts in a hybrid approach or replace them altogether by the latter;
- Symmetric Key Cryptography: adapt the current parameters (key size, digest size, etc) to withstand quantum computing.

Unfortunately, there is no consensus on the exact measures to be implemented as illustrated by the examples below. This misalignment between the governmental recommendations is obviously a significant issue for worldwide standards such as those relevant for the telecommunication industry. This suggests that the first step of any migration strategy should be to identify a set of requirements related to key sizes and parameters that would be acceptable in all countries where the systems relying on those standards are deployed.

4.10.2 Symmetric Key sizes

Grover's algorithm provides a potential quantum advantage (compared to classical computers) for exhaustive key search on symmetric cryptography. The plausibility of each scenario is still the subject of ongoing research and debate; no consensus has emerged so far, as illustrated by the positions of the different government agencies.

Depending on practical limits for extremely long-running serial quantum computations, the advantage ranges from a quadratic speedup to none at all when also taking quantum-to-classical cost ratios into account [NIST-CALL, NIST-FAQ]. Concretely, a quadratic speedup would call for a doubling of the current key size (namely moving from 128-bit to 256-bit keys) whereas the alternative scenario would not require any change. Hopefully, further research, in particular on the actual quantum resistance of symmetric algorithms relevant for the telco industry (ZUC, Snow3G, etc), will help to bridge the gap between those positions.

4.10.3 Public Key security Levels

The conservative security posture of ANSSI and BSI is reflected in their recommendations on public key cryptography. Both agencies recommend the use of parameters corresponding to NIST level III or more whereas NIST accepts lower security levels. XMSS and LMS do not have assigned security levels, but are considered as very conservative choices.

4.10.4 Variation in Algorithm Recommendation

SLH-DSA is not part of CNSA 2.0 for signing. SHA-3 and SHAKE are not part of CNSA 2.0 for hashing. BSI approve of FrodoKEM and Classic McEliece---for which the pathway to stable standards via ISO is considerably longer than ML-KEM---however very few other governmental agencies support the use of these algorithms. In the future more national standards will be produced, for example in Korea [Korea-PQC] a standardisation process is underway, leading to further difficulties in assessing whether a product or service is compliant with the guidance in all of the locations in which it is planned to be used.

It should be noted however that these challenges exist already, with different national agencies preferring certain elliptic curve groups over others, and therefore existing policy assessment efforts need to be adapted to the new algorithms.

4.10.5 Variation in Guidance on Hybrid Cryptography

Given the lower maturity of post-quantum cryptography, some security agencies (e.g. ANSSI and BSI) advocate the use of hybrid cryptography, that is, a combination of classical and post-quantum cryptographic mechanisms. When properly implemented, this approach is optimal from the security standpoint as it ensures that the resulting security level is at least as strong as the one of classical cryptography. It however comes with increased complexity and costs which may be undesirable in some contexts, leading the NIST and NCSC to take a neutral stance on this topic. The technical details of deploying hybrid cryptography are described in more detail in Section 4.2.

We note that the hybridisation requirement by ANSSI and BSI does not apply to the hash-based signatures standards XMSS, LMS and SLH-DSA which are considered sufficiently mature to be used alone.

4.10.6 Hybrid Cryptography: Security, Interoperability and Efficiency

Schemes and protocols that employ a hybrid approach to hedge against security failures in either traditional cryptography (likely via a cryptographically relevant quantum computer) or post-quantum cryptography (via advances in cryptanalysis techniques or implementation failures) must be designed and deployed carefully if they are to be effective.

Hybrid interoperability---the goal of providing schemes and protocols that can be interpreted and used by traditional/hybrid/purely post-quantum clients---may not be achieved by schemes/protocols where hybrid security is the primary design goal. Using TLS as an example, if the client sends a hybrid public key then only a hybrid server can interpret this value so a traditional or purely post-quantum server would request a public key that it can interpret or abort the session. A backwards-compatible version would ask the client to send a traditional public key and a hybrid public key in the negotiation phase.

In a phased migration approach, hybrid interoperability may be the primary goal but in many scenarios such as the TLS example, additional data or round trips will be required compared to a protocol that is designed only to be used by hybrid clients. This interoperability overhead comes on top of the overheads that are required to support hybrid cryptography and the large keys/ciphertexts that are present in many post-quantum algorithms.

Cryptographic agility may also be at odds with reducing the attack surface that arises when using hybrid protocols. As the number of standardized post-quantum algorithms grows in the near future, the number of possible combinations of hybrid components increases drastically, making it tempting to limit the combinations to those with algorithm identifiers or formal security analysis. Some post-quantum component algorithms are functionally different to the traditional algorithms that they will be used alongside, leading to many subtleties for security when combining together. For this reason extra care should be taken to follow standardized or approved combinations in hybrid schemes/protocols and to follow up-to-date guidance from national and international authorities.

The migration plan for a use case/organisation may differ between confidentiality protection (to thwart harvest-now-decrypt-later attacks) and entity authentication (to thwart real-time attackers impersonating others), and this should also be reflected in long-term planning for moving from hybrid cryptography to pure post-quantum cryptography. TLS/IKEv2 sessions will likely focus on confidentiality first and then plan to migrate the signatures used for authentication much later, while for firmware signing the migration of the verification keys for authentication will be the main focus. In some special cases such as email encryption, it may be necessary to prioritise non-repudiation for the long-lived data.

4.11 Additional Migration Challenges

4.11.1 Large Data Objects in PQC Algorithms.

Keys, ciphertexts and signatures in post-quantum algorithms can be much larger than their traditional counterparts. There are many candidate schemes because each comes with a profile providing different trade-offs between execution time, object size and ease-of-use.

Large ciphertext size can cause significant challenges in some schemes/protocols where data packets are limited in size. Longer execution times means the energy required on a constrained device is considerably higher for some PQC algorithms. Longer execution time may also affect latency, where the production of session keys/signatures is time critical. It is imperative that deployments enter a testing phase to assess the viability of certain post-quantum cryptography algorithms to minimise the performance impact.

4.11.2 Implementation Restrictions for PQC Algorithms

Some implementation challenges arise in post-quantum signatures that were not present in traditional algorithms.

- NIST SP 800-208 stipulates that LMS and XMSS signing must be done in a controlled environments to preserve the secrecy of the signing state.
- FN-DSA requires double-precision floating-point operations for its signing procedure. Side-channel resistant implementations on embedded/end-user devices will be extremely challenging.

4.11.3 Certificate Issuance for KEM Public Keys

In many contexts, entity authentication via signatures is not preferable and long-term KEM keys should be used in key establishment protocols instead.

This may be because ML-DSA signatures are larger than KEM ciphertexts, or because the protocol requires deniability for one party, or in some cases the protocol currently uses long-term DH keys for other reasons so migration doesn't consider signatures. For long-term keypairs, it is usually necessary for a certificate authority to sign the public key when provided with a proof that the request comes from the owner of the secret key (this CA might have the public key corresponding to its own signing key signed by a root CA). Certificate Signing Requests can be made in a non-interactive, offline manner as defined in PKCS #10 [RFC 2986], so that the CA can receive many requests and just process them whenever it has capacity. This is possible for digital signature schemes and Diffie-Hellman keypairs, but more challenging for KEMs: requests need to carry a much larger proof of knowledge of the

decapsulation key in order to keep the 'offline' mode (suggestions have been made [CCS 2022] but there are no active efforts for standardisation in this direction).

Therefore any use case involving a protocol that is considering a component with long-term KEM keys needs to ensure that the CSR process can either handle online requests or large request packages.

4.12 Migration Strategy and Timeline

4.12.1 Vendor Migration Strategy

- Interaction with operators including through standards groups

4.12.2 Operator Migration Strategy

The migration strategy comprises many parts:

- Architecture
    - Interaction with standards groups
    - Creation of Cryptographic inventory
    - Update interaction with standards groups to match priorities
    - Vendor solution discovery and assessment
    - Testing phase
- Business case to board
    - Budget and timeline approved
    - Recruiting additional staff if required
- Technical Plan
    - Contingency plan for roll back of updates
    - Phased roll out.
    - Repeat as required for the phases of PQC
- Shifting approach
    - Add PQC as option to existing protocols (e.g. TLS)
        - Gradual prioritization of PQC over PKI
        - Removing PKI option
- Merging approach
    - Hybridization PKI+PQC
    - Gradual prioritization of PQC only
- Removing PKI option
- Stepwise approach

- Hybridization of existing mechanisms with symmetric keys as backup
- Adding PQC
- Gradual prioritization of PQC over PKI
- Removing PKI
- Removing hybridization

4.13 Legacy Systems

One of the main technical challenges to achieve quantum resistance is arguably the one constituted by legacy systems which include components that do not support PQC and cannot be updated to that end.

In this situation, it is worth considering alternative migration strategies where the quantum risks would only be mitigated, for example by relying on other components of the systems that can be updated or by tunnelling the transmitted data through a quantum-safe channel. While this significantly changes the trust model, this approach can still allow to retain a relevant security level, as illustrated in the Remote Sim Provisioning use-case.

4.14 Device Management Interfaces

Network nodes in the core network (e.g. switches, routers, security gateways) generally have management interfaces which are protected using classical cryptography.

Protocols used for management and monitoring include, but are not limited to:

- HTTPS (for web GUI and API interfaces)
- SSH (including SCP and SFTP)
- SNMPv3

SNMPv3 is not affected as it does not use any vulnerable key exchange or authentication methods.

All of these interfaces are potentially at risk if accessible over untrusted networks and need to be included in a post-quantum migration strategy.

Management interfaces generally fall into two broad categories:

- Interfaces which use generic clients, such as Web-based graphical user interfaces which are accessed using generic web browsers, or SSH interfaces which use generic SSH clients. In some cases, the remote side may be a server (e.g. a licence server, or security package server) in which case this category includes connections to generic web servers.
- Interfaces which use standard protocols, but which communicate with specialised clients or servers. This can include connections to third-party monitoring systems.

In both cases there are dependencies from both sides. On the network equipment, vendor support will be necessary to provide post-quantum protocol support, for each management interface, and in many cases post-quantum protection for these interfaces will not be provided in one shot but rather will be part of a staged vendor roadmap. E.g. HTTPS management interfaces may have support before SSH interfaces. For the client side,

support must be available in the relevant tools, browsers, SSH clients etc. For the most part, major vendors are already working on this, with pre-standard post-quantum versions of OpenSSL and OpenSSH already available, as well as initial support in some browsers. However, TLS standards are lagging IPSec in the IETF, and interoperability will be an issue until stable standards are published.

For specialist third-party tools, vendor support may be more of an issue. For example, post-quantum support may not be a priority for a monitoring tool vendor whose products may be primarily used in closed networks.

When planning migration for these interfaces then, several dependencies need to be considered:

- Dependency-PQC-std-kem
- Dependency-PQC-std-sig
- Dependency-TLS
- Availability of supporting protocol standards (for integration of PQC info IPSec, SSH, etc)
- Vendor support

In some cases, where the above dependencies can't be met, it may be possible to tunnel management data through insecure networks using quantum-safe VPNs.

5 Telco Use Cases: System Impacts and Guidelines

This chapter considers a set of telecom use cases for migration to PQC. In each case the document describes the scope of the use case, the system context and considerations. Some of the use cases also include migration strategy, dependencies and an outline of the migration process.

5.1 List of Use Cases

Use cases are divided into those that directly affect customers or partners, and use cases internal to the operator.

5.1.1 Internal to MNO Use Cases

- Protection and configuration / management of link between base stations and security gateway.
- Virtualized network functions (on cloud, on NFV infrastructure), including integrity of the uploaded firmware and VNFs. Authentication of privilege access.
- Cloud Infrastructure (to support virtualized network functions).
- RSP (Remote Sim Provisioning / eSIM), for M2M (SGP.02), Consumer Electronics (SGP.22) and IoT (SGP.32).
- Devices and firmware upgrade. This is linked to code signing and ability to have Root of Trust in the device to enable further secure and trustable updates.
- Concealment of the Subscriber Public Identifier
- Authentication and transport security 4G (MME-S-GW-P-GW)

5.1.2 Customer Facing Use Cases

- Quantum-Safe VPN
- Quantum-Safe SD-WAN (for enterprise and government clients)
- Protecting Critical Devices: Electrical Smart Meters
- Prepare automotive for quantum-safe cybersecurity
- More linked to privacy (vs security), but key as well regarding privacy preserving and associated regulation (GDPR, …)
- Lawful Intercept and Retained Data
- Cryptographic agility: migrating from PQC1 to PQC2

5.2 Use Case: Protection and Configuration / Management of Link between Base Stations and Security Gateway

5.2.1 Scope

In scope of this use case is the secure transport between the 4G/5G radio access network (RAN) and the security gateway (SecGW). IP traffic between RAN and core network is vulnerable to attacks when it travels over an unsecured or a third-party network. Even in secured operator-owned networks, transport links can be tapped (including by insiders). The use of SecGWs between RAN and network functions of the core network is not mandated by 3GPP standards but commonly deployed by operators.

Within the provider's RAN, base stations are typically grouped to ensure the appropriate RAN coverage. Within the architecture SecGWs are positioned accordingly, offering IPSec tunnels to base stations. IPSec tunnels provide authentication, data integrity and data confidentiality.

In addition, connectivity exists between base stations and OSS/OAM systems via SecGWs, as well as management connections to the SecGW itself. This connectivity is used e.g. for maintenance and upgrades of cryptographic parameters relevant for the connection between a base station and a SecGW.

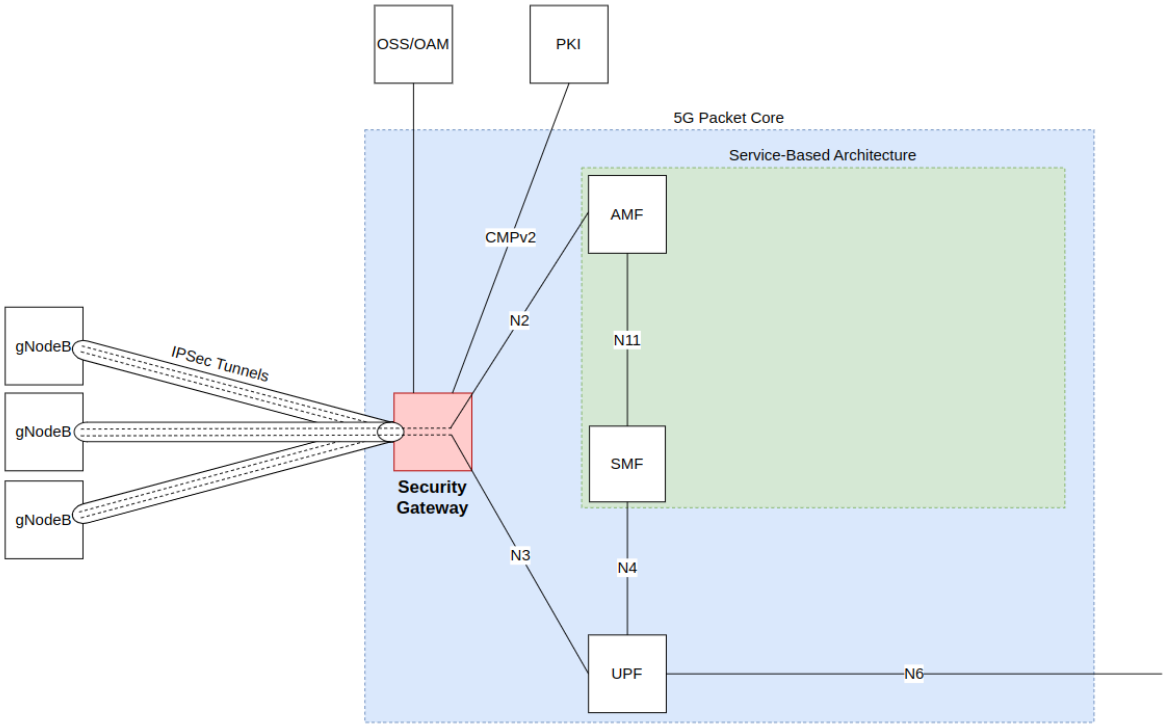
Authentication of base stations and SecGWs is typically done using X.509 certificates, distributed using a PKI system.

All of the above-mentioned connections (base station to SecGW, base station to its management system, SecGW to its management system) should be quantum-safe, and the PKI communications and certificates should use quantum-safe methods.

Finally, although this use case is focused on base station to SecGW, the guidelines here can also be applied to SecGWs used to secure the F1 interface between distributed units (DU) and centralised units (CU) in Open RAN architectures.

5.2.2 System Context

To further illustrate the above points, refer to the example below of a Security gateway protecting a 5G packet core:



The security gateway terminates IPSec tunnels from the gNodeBs, each of which encapsulates the N2 and N3 interfaces. Those interfaces are then forwarded in cleartext to their respective remote endpoints (AMF and UPF respectively) by the Security gateway.

Authentication of the gNodeBs is via X.509 certificates, preventing unauthorised entities from accessing the packet core. The IPSec tunnel then provides the integrity and confidentiality of N2 and N3 communications over the backhaul interface.

The security gateway typically does not interact in any way with the underlying protocols. The decrypted data is passed unchanged to the relevant control or user plane entities. Note however that some vendors may provide features such as provide protocol conformance checks or layer 4 firewalling on the decrypted data.

5.2.3 Sensitive Data Discovery

Quantum computing will break modern asymmetric cryptography and compromise the security of those connections which rely on such type of cryptography and carry user signalling and management traffic.

Due to the use of asymmetric cryptography, the following connections are considered not quantum safe:

- Connection between base station and SecGW due to the use of the IPSec protocol suite, specifically the IKE key establishment.
- Connection between base station (SecGW) and associated OSS/OAM system due to use of secure protocols like TLS.

Examples of sensitive data in this use case.

Data in transit:

- User data transferred between base station and SecGW
- Management data transferred between the network elements (base station, SecGW) and their OSS/OAM systems.

Data at rest:

- Sensitive credentials (like passwords, private keys, symmetric keys for data at rest encryption) stored in the network elements

Current protection of sensitive data

- Data in transit is currently protected by standardised security protocols like TLS, IPSec or MACsec.
- Data at rest (e.g., private key used by a network element) is protected through security environments built into the network elements by their manufacturers. A security environment may leverage e.g. a Trusted Platform Module or a Hardware Security Module. Protection is afforded through symmetric encryption of sensitive data at rest.

Asymmetric private keys, used to establish the secure connection, must also be securely stored and used, though this falls under the banner of PKI.

5.2.4 Cryptographic Inventory

Details of cryptographic assets to be used in a service provider's RAN/SecGW context are defined in guidelines and documents like backhaul security standards, cyber security baselines etc. Some details will be specific to service providers. Other details refer to 3GPP and IETF standards. Therefore, the discussion in this section is for illustration and not exhaustive.

5.2.4.1 Data at Rest

Sensitive data at rest in base station and SecGW will be encrypted. The symmetric encryption algorithm may be AES-256 or others. The corresponding encryption keys can be either fully managed by the machine hosting the network element (like the base station) or by the service provider.

5.2.4.2 Data in Transit between Base Station and Security Gateway

Data in transit over the base station/SecGW connection can be secured using the IPSec protocol suite (in line with 3GPP) which creates a secure IP tunnel. The IPSec Encapsulating Security Payload protocol (ESP) provides secure authentication and integrity via a message digest that uses a secret key of the sender, and confidentiality through encryption of IP network packets which carry user and network signalling data.

IPSec uses the Internet Key Exchange (IKE) protocol to negotiate security associations between base station and SecGW. A security association is a set of parameters agreed upon by base station and SecGW before they start communicating over the secure tunnel. IKE is used among others to negotiate (symmetric) keys and set up the authentication and encryption algorithms for both devices.

IKE version 1 and version 2 have minor differences with respect to phases and message exchanges.

IKE v2 uses several request/response exchanges between base station and SecGW. In the first exchange, it negotiates encryption for a security association for IKE messages and uses the Diffie-Hellman key exchange algorithm (a public key protocol) to establish a shared secret key between base station and SecGW over a still insecure connection. This key is for encrypting and decrypting IKE messages that follow. In a second exchange, base station and SecGW authenticate each other using digital certificates (or a pre-shared key). In addition, the two devices finally establish an IKE security association (for management purposes) and at least one child security association (for the mobile network user/signalling traffic). Thereafter, the two devices start exchanging user and signalling traffic over the secure tunnel.

Vulnerability to quantum attacks arises from the use of a non-quantum-safe public key protocol and traditional certificates. The certificates are issued through a public key infrastructure (PKI).

5.2.4.3 Data in transit between network elements and OSS/OAM systems

Configuration and management data in transit between network elements (base station, SecGW) and their associated OSS/OAM systems is protected through the use of (today) secure protocols which importantly also handle authentication. As long as authentication and creation of a secure tunnel (e.g., by the top-level application protocol or delegated to a lower-level protocol) is quantum-safe, all is good. Examples where vulnerabilities arise are: use of SSH (makes use of Diffie-Hellman key exchange itself), use of SFTP (which in turn uses SSH), or HTTPS (which uses TLS).

5.2.4.4 Role of PKI

The PKI issues network operator certificates to base station and security gateway. These certificates will have to be renewed from time to time (e.g. using automated renewal via the Certificate Management Protocol (CMP) or manual renewal) or revoked. The PKI certificate profiles follow 3GPP standards requirements [TS33.310].

The operator certificate acts as a ‘machine identity’ to identify the network component like base station towards the SecGW for the creation of the IPSec tunnel, and towards its OAM system. X.509 certificate formats are in use.

5.2.4.5 Cryptographic assets

For examples of what constitutes cryptographic assets as they are typically present for this use case in base station and security gateway, see section 4.7.

5.2.5 Migration Strategy Analysis and Impact Assessment

The way towards a quantum-safe solution involves the creation and later deployment of quantum-safe versions of TLS and IPSec and supporting PKI infrastructure.

- For new deployments of base stations that shall use a quantum-safe IPSec tunnel to the mobile core network, operators can request standards compliant PQC capabilities in protocol stacks. The same applies for new deployments of security gateways (physical or virtual ones).

- For upgrading legacy base stations and SecGWs to quantum-safe IPSec capabilities: vendors need to implement standards-compliant quantum-safe protocols into their products, then the relevant software needs to be remotely updated or installed.
- IPSec has two post-quantum vulnerabilities that need to be considered: the authentication mechanism used to identify the endpoints to each other (e.g. RSA, ECDSA), and the key exchange mechanism (Diffie Hellman).
- For authentication, operators need to evaluate the benefits of

    - aiming straightaway for introduction of hybrid certificates via corresponding upgrades or replacement of PKI systems, versus
    - using pre-shared keys (considering them quantum safe) for a transition period before upgrading the PKI infrastructure.

- For key exchange, using pre-shared keys may also be an option (via RFC8784) although since this standard is itself relatively new and may not be supported by all vendors, it may be preferable to migrate directly to quantum-safe hey exchange algorithms.

5.2.6 Stakeholders

Prime stakeholders for the RAN-SecGW scope are:

- Network operators
- Vendors of base stations
- Vendors of security gateways
- Vendors of PKI systems
- 3GPP
- IETF, with IRTF, CFRG and other working groups.

5.2.7 PKI Implications

Main impacts on PKI systems are as follows:

- PKI systems need to support hybrid certificates; thus, upgrades or replacements will be required.
- The goal of using PKI is to provide certificate-based authentication between network elements. This protects the network itself and, consequently, also customer data.
- This use case is based on 3GPP standards

5.2.8 Legacy Impact

The introduction of Post Quantum Cryptography into the RAN (base station) and Security Gateway areas can happen in multiple ways. Examples are:

a) through planned technology refresh cycles implementing PQC capabilities. This is applicable to legacy infrastructure if the new generation is scheduled to replace the legacy infrastructure.

b) through *activation of PQC features* in already deployed software or equipment via already implemented crypto-agility mechanisms, or through procurement of feature upgrades for existing software / hardware. This might work for legacy infrastructure.

Regarding the feasibility of option (b), service providers will have to consider multiple factors, e.g.

- whether suppliers consider the upgrade of legacy software components as technically feasible (e.g., regarding compute requirements from PQC algorithms) and commercially viable.
- whether the legacy product lines of vendors are nearing end-of-life, and whether the incorporation of PQC features for a short remaining lifespan is warranted at all.

From a service provider point of view, whether legacy infrastructure poses a big issue or not also depends on multiple factors, e.g.

- the proportion of the infrastructure assets (like base stations that are connected to SecGWs). Are 5% of assets considered legacy, or is it 30%?
- the quantum risk level assigned to the legacy assets as determined from a quantum risk assessment and business prioritisation assessment.

5.2.9 Dependencies

5.2.9.1 Standards

Within the scope of the SecGW use-case, the standardisation of the required post-quantum algorithms for both authentication and key exchange is ongoing via the NIST post-quantum cryptograhy standardisation process.

In addition, each protocol requires updates in order to integrate those algorithms. For all three areas discussed above, this standardisation is being managed by the IETF. For IPSec, the relevant working groups is ipsecme, for TLS it is the tls group, and for PKI it is the lamps group.

5.2.9.1.1 IPSec:

At the time of writing, there are two RFCs relevant to key exchange, RFC9370 and RFC9242, which extend the IKEv2 signalling protocol. RFC9370 enables up to seven additional key exchange algorithms to be used in the establishment of a security association (optionally including a classical Diffie Hellman exchange), and RFC9242 allows extra messages to be added to the initial exchange, to support those additional exchanges. Although RFC9242 is not strictly required for all possible post-quantum solutions, in practice it is expected that all vendors will implement them together, and in practice both should be considered as requirements to give the maximum flexibility and interoperability. For authentication, RFC9593 allows authentication methods to be negotiated in order to enable support of hybrid authentication schemes.

5.2.9.1.2 TLS:

For TLS, no official standard exists at the time of writing, but an IETF draft is under development in the IETF tls group covering hybrid classical/post-quantum key exchange.

5.2.9.1.3 PKI:

Many drafts are under development in the lamps IETF group covering authentication algorithms for signed data, data encryption, and the use of post-quantum authentication algorithms in x.509 certificates.

5.2.9.2 National Guidelines

The prevalence of security gateways varies between countries, and in addition, some countries are actively developing sovereign post-quantum algorithms. National guidelines should be consulted to ensure that any recommendations or regulations are followed appropriately.

5.2.9.3 Vendors

As standards begin to mature, equipment vendors will begin to provide support in their products. Roadmaps should be consulted to determine expected timelines and input into the overall migration planning. Vendors may also provide pre-standard protocols or algorithms, and this may be useful for initial proof of concept testing in preparation for a full migration towards a standards-based solution.

5.2.9.4 3rd-Parties

Generally, use-cases will involve communication between different entities, for example a Radio Access Network and a core network may be operated by two different network operators. In that case each will be dependent on the other to implement post-quantum algorithms. In some cases, protocols will allow a negotiation between entities to allow a fallback to classical methods if one of the parties does not support post-quantum protocols or algorithms. In other cases, the parties must work together closely to coordinate the migration timetable.

5.2.9.5 Performance

In IPSec, the data encryption uses symmetric protocols which are essentially unaffected by the quantum threat. Theoretical higher efficiencies of brute force searches using Grover's algorithm can be mitigated by using longer keys, but due to practical difficulties of implementing Grover's algorithm, NIST considers AES128 to retain level 1 security (128-bit equivalent)

For this reason, once an IPSec tunnel is established, the performance should be identical to the classical case. Any hardware offload or other acceleration will continue to be available, and throughput, latency and jitter should be unaffected. Similarly, it is unlikely that concurrent tunnel scaling will be significantly impacted, although this could be implementation dependent, and it is recommended to check with the vendor if the existing classical deployment is close to the scaling limits.

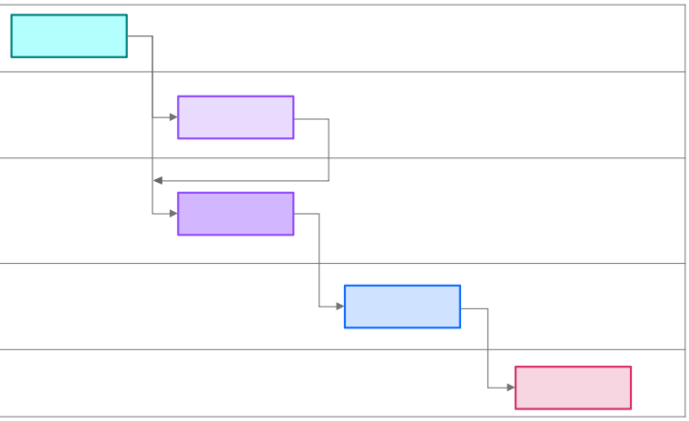
The area that will be impacted by the migration will be tunnel setup performance. Adding Post-Quantum key exchange steps will add some latency to the tunnel setups, both in terms of cryptographic processing, and in packet round-trips. The latter factor is determined by key sizes and the fragmentation of large keys into multiple packets.

Whilst a small increase in resource usage and set up time may not be a big issue for a single tunnel, it may become significant when a SecGW is terminating a large number of tunnels, and a network failure or other catastrophic event causes all tunnels to be re-established at once.

For management/OAM connections, as well as for PKI, the same issues will apply and increased processing load and latency should be expected, although there typically won't be the same parallel scale as for IPSec tunnels. In all cases it is recommended to work with vendors to understand the impact, as part of the migration process.

5.2.10 Gantt Chart for PQC Migration

Standards	*PQC Standards* • NIST PQC Standards • IETF IPSec/TLS standards
National Guidelines	*PQC guidance* • PQC for sectors • Sovereign crypto •
Vendors	*Update products for PQC* • Update Security Gateways • Update Base Stations • Update PKI
Operators	*Test and Deploy PQC products* • Test interoperability • Deploy updated RAN • Deploy updated SecGWs
Migration	*Migrate* • Migrate to PQC



5.2.11 PQC Migration process Description

Taking the example of a security gateway protecting a mobile packet core, the operator must first wait for post-quantum standards to be available, and then for the functionality to be made available from the security gateway vendor (or migrate to a vendor which does provide support). The choice of standard may also be influenced by applicable national guidelines. It is likely that the first available post-quantum offering will be support for a quantum-safe key exchange mechanism within IKEv2. The relevant standards (RFC9370 and RFC9242) allow for support of post-quantum algorithms to be negotiated between peers, which will allow the security gateway to support post-quantum tunnels to those base stations which already have support, whilst also allowing connections from legacy base stations which do not. It is important that vendors incorporate functionality to give visibility of which base stations are still using classical algorithms to allow the operator to manage the transition process.

The implementation of post-quantum key exchange in general should be possible independently from the PKI migration. As explained above, because of the "store now, decrypt later" problem, and depending on availability of standards, and on vendor roadmap, an operator may choose to migrate the key exchange first, keeping a classical PKI, then migrate the PKI later.

5.2.12 Synergy with Internal Programs

Within the operator environment, groups managing the security gateways and the PKI infrastructure will have to carefully coordinate the migration process. In addition, PKI will be

used in other areas, so there will be other dependencies to consider. Ideally a hybrid PKI approach will mean that all PKI consumers can benefit from the migration.

5.2.13 Synergy with External Programs

Post quantum migration may be planned as part of a general equipment refresh.

5.3 Use Case: Virtualized network function integrity

5.3.1 Scope

The virtualisation of network functions on private and public cloud infrastructure is now widely adopted within the networks of communications service providers. The initial focus was on Virtualise Network Functions (VNFs) running on infrastructure managers such as OpenStack and VMware. The industry is now progressing to deploy Cloud-native Network Functions (CNFs) running on container platforms and orchestration systems such as Kubernetes. Given the concentration of diverse VNF/CNF workloads (e.g. RAN, Mobile Core, Security gateways, IMS, SD-WAN, API gateways, etc) running on the private and public cloud infrastructure, security is a key concern and area of considerable previous and ongoing effort within the developer community and standards organisations. In discussing this Use Case within the context of the Post Quantum Cryptography, we will focus on the security and integrity of all types of workloads as they are deployed into the cloud infrastructure, and upgraded.

Note: Other areas of security within cloud systems are discussed in the “Cloud Infrastructure” Use Case.

The following diagram depicts a typical pipeline for the deployment of virtualised network functions.

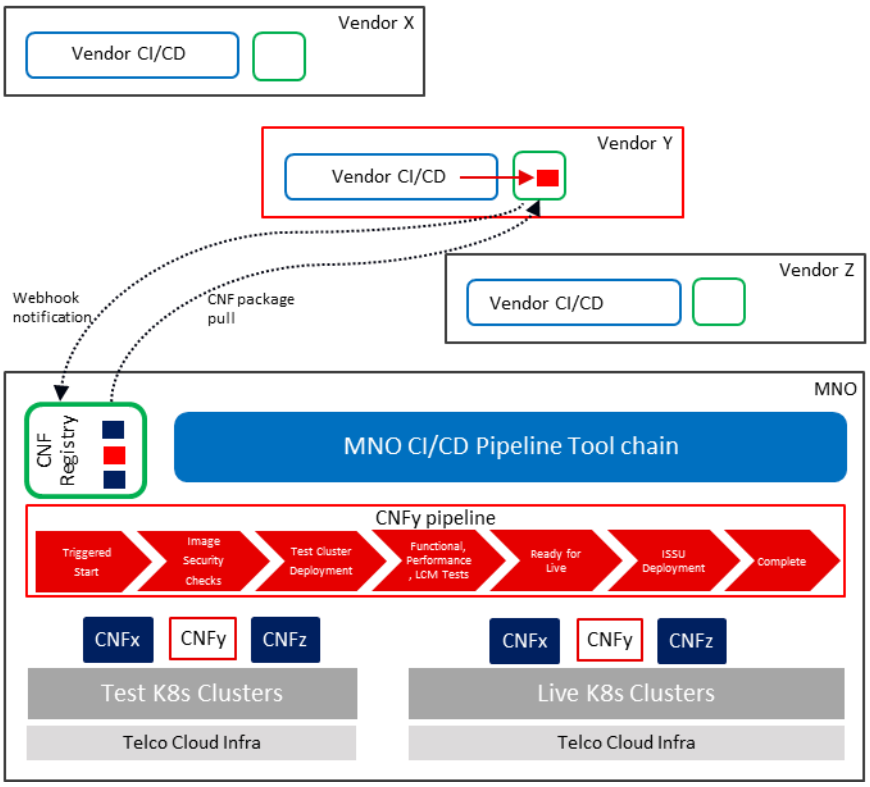


Figure 6: Typical Pipeline for the Deployment of Virtualised Network Functions**.**

Given the industry direction of embracing CNFs, the following discussion focusses on container-based systems. The prevalence of VNFs is such though that Virtual Machine based systems are also briefly considered.

Further information, in addition to the following sub-sections, can be found in NIST Special Publication 800-190, “Application Container Security Guide”. In particular, section 4.1.5 “Use of untrusted images” and section 5.3 “Running a Poisoned Image”. The Update Framework specification (https://theupdateframework.github.io/specification/latest/index.html) provides further context on this subject.

5.3.2 Sensitive Data Discovery

Arguably the most fundamental aspect of security within a cloud environment is ensuring that the workloads that are deployed and run can be trusted for authenticity and integrity. That is: *“you are running what you think you are running!”* and, with the rapid and automated software upgrades facilitated by continuous integration (including test), continuous delivery and continuous deployment pipelines (using Jenkins, Tekton, etc), a strong trust relationship must be established and maintained. Without such trust, a rogue, malicious or uncertified workload can be introduced into the network without the required level of oversight.

5.3.3 Cryptographic Tools

Various tools have been created to secure the deployment of workloads within Kubernetes environments. By way of example, two such tools used together to secure deployments are Cosign, part of the Sigstore project (https://github.com/sigstore/cosign), and StackRox (https://github.com/StackRox/StackRox).

Cosign is used to sign the image during development. A similar signing solution is Notary (https://github.com/notaryproject/notary, https://github.com/theupdateframework/notary)

StackRox is a security solution for Kubernetes that is used, in part, to verify the image during deployment (i.e. that it is validly signed) . An alternative tool for verification during deployment is Connaisseur (https://github.com/sse-secure-systems/connaisseur) – an admission controller for Kubernetes. Tools like these sit within the operator's CICD pipeline and deliver security attestation for the assets. That is, security validation and tamper detection.

Similar approaches are used within OpenStack (Virtual Machine) environments. Images are signed (e.g. with openssl) using keys stored in the OpenStack Key Manager (barbican) prior to being uploaded into the OpenStack Image Service (glance). During deployment, the OpenStack Compute Service (nova) requests the desired image from the OpenStack Image Service and performs verification.

5.3.4 Cryptographic Inventory

The prime cryptographic inventory components for this Use Case are the tools (and command line utilities) like Cosign which sign and verify the software images. These ensure the place of origin of the software is unequivocally known and the software remains unadulterated (I.e. not tampered with). Underpinning these tools are established cryptographic schemes. For example, Cosign supports RSA, ECDSA, and ED25519.

5.3.5 Migration Strategy Analysis and Impact Assessment

Communications Service Providers (CSPs) typically operate their mission-critical network workloads in highly secure, carrier-grade, closely monitored "cloud" environments. These cloud environments sometimes exist as virtual private clouds delivered by public cloud operators but are still predominantly dedicated, on-premises (in Data Centre) private clouds. Further, within these "closed" environments the CSPs also typically operate a private repository of images rather than relying on external repositories. This ensures they have a greater level of control over the images. And in addition, the majority of these private environments use a Kubernetes Distribution provided by a vendor, but owned and generally managed by the operator. This has two main implications:

Firstly, the migration of the base Kubernetes to being Post Quantum secure is highly dependent on the vendor of the Kubernetes Distribution and the vendor(s) of the related tools, repositories, components and libraries. Most Kubernetes Distributions from vendors come packaged with tools/components like StackRox, Connaisseur, etc. Hence, migration is at least partially handled by the vendor "pre-integrating" (i.e. certifying) the tools. In cases where the CSP integrates their own set of tools and a lean Kubernetes, the CSP is faced with a more extensive and complicated migration. Hence, "pre-integrated" distributions are likely to be foremost in most CPS's migration path.

Secondly, deployments of workloads – either generated via their own pipelines or delivered from vendors – are generally not exposed to direct public attack. That is, they operate a private repository of images. Hence, although image signing is a critical aspect of security the deployment process, it is generally not directly visible to external parties. This opacity

should not drive complacency within the CSP, but does provide a degree of flexibility for the operators. Hence, the “likelihood” of compromise due to Quantum attacks is lower than publicly exposed infrastructure.

5.3.6 Implementation Roadmap (Crypto-Agility and PQC Implementation)

The majority of the tools used in securing the integrity of workloads in Kubernetes systems use standard PKI and transport security procedures and implementations. The physical environments are generally not constrained either in terms of compute capacity, storage capacity or network capacity. Hence the implementation roadmaps for Communications Service Providers are primarily defined by the roadmaps of the constituent libraries and tools, and importantly the roadmap for the “pre-integrated” Kubernetes Distributions.

5.3.7 Standards (and Open Source) Impact

The majority of the tools used in securing the integrity of workloads in Kubernetes systems are developed as open-source projects. Some are overseen by de-facto standards bodies, and to a lesser extent full standards bodies. Given that cloud technology has been widely adopted by the CSP, there is a pressing need for these projects and bodies to map out a path and timeline to becoming Quantum Safe. The Post Quantum maturity at this time is relatively low.

Further, although there are some sets of popular cloud tools, there is far from one dominant collection used by the majority of CSPs. Hence, the maturity is likely to remain fragmented.

5.3.8 Stakeholders

The prime stakeholders are CSPs, open-source software tool projects (and their sponsoring bodies), Kubernetes Distributions (software vendors) and “pre-integrators” (software integrators/vendors).

5.3.9 PKI Implications

Standard PKI and transport security procedures and implementations underpin most of the tools used in ensuring image integrity. Enhancement to the software libraries and PKI infrastructure is a pre-requisite step for securing the cloud environments and hence the operator’s network functions.

5.3.10 Legacy Impact

CSPs typically operate their own private repositories, and on-premises or virtual private cloud infrastructure. As such legacy software images are to a degree shielded through lack of reachability. Of course, this breaks down with insider attacks though.

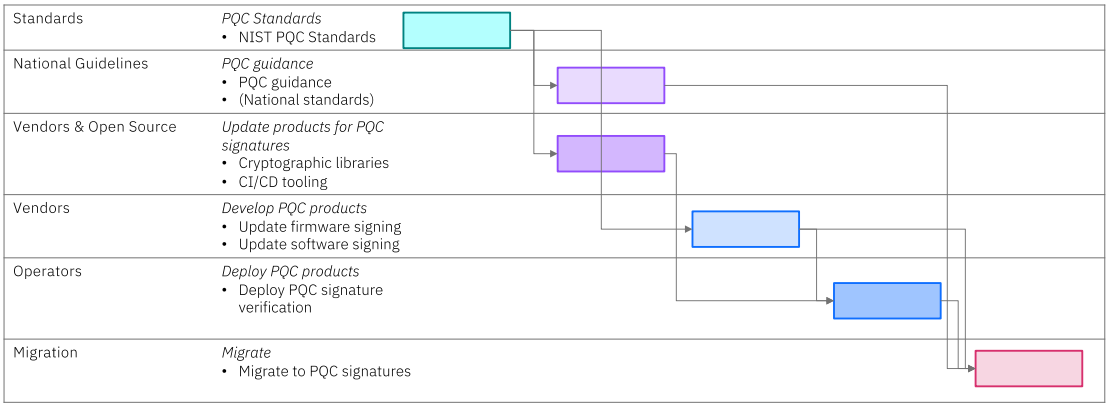
Software lifecycle times are sufficiently short these days that for the majority of software there will be multiple image (CNF/VNF) releases per annum. This relatively rapid turnover – at least in comparison to historical software cycle times – greatly increases agility. Upgrading the CI/CD pipeline to be PQC compliant has the follow-on effect that in fairly short order the images deployed become PQC verified. (Note: this doesn’t mean the images themselves are Quantum Safe, just that they are verified as authentic and unadulterated).

5.3.11 Potential Actions/Dependencies

As noted above, the virtualisation of network functions on private and public cloud infrastructure is now widely adopted within the networks of CSPs. Hence, CSPs are and will remain highly dependent on the broader “cloud” ecosystem (including the open source community) to ensure a smooth and timely transition to PQC. Although efforts are underway, at the time of writing, much remains in terms of the required coordination and timing across the “cloud” ecosystem.

A clear action is for additional focus in this respect, especially given the role that telecommunications plays as critical infrastructure and thus one of the first verticals required to move to PQC.

5.3.12 GANTT Chart for PQC Migration



GSMA PQ.03v2 VNF v02

5.4 Use Case: Cloud Infrastructure

5.4.1 Scope

CSPs use cloud infrastructure to run OSS/BSS and ERP systems and to host virtualized networks (both CNFs and VNFs). This cloud infrastructure can be a public cloud, a local instance of a public cloud, a private cloud, NFV infrastructure and edge clouds (MEC, TEC).

Cloud platforms typically enable CSP to benefit from economy of scale and common management tools.

Another key benefit is that Cloud platforms include security features such as Privilege Access Management, cryptographic key management, and a PKI.

Cloud platforms usually implement a shared-responsibility model for security. The cloud provider is responsible for the security of the cloud itself; the workload owner is responsible for the security of the workload, data and configuration.

Organizations using cloud infrastructure need to ensure that sensitive data is not publicly available on the cloud. Several security incidents have been discovered by scanning for unsecured data in cloud services, like EC3.

Cloud providers including Amazon, Google, IBM and Microsoft have deployed pre-production implementations of the NIST PQC algorithms designed for customers to get early experience of using the algorithms and to understand how workflows and workloads are affected.

5.4.2 System Context

Cloud infrastructure supports deployment and operation of workloads. The components of the cloud infrastructure include computer hardware, storage hardware, datacentre networking, virtualisation and containerisation, infrastructure monitoring.

Cloud processes include infrastructure management, workload management, infrastructure operation.

In addition, supporting security functions are required. These include PKI/CA, Identity and Access Management, Privilege Access Management, Security Monitoring, Log management, Firewalls, Cloud Key Management, and hardware security modules (HSM).

Zero trust - core principle at the heart of Cloud encryption & key management

5.4.3 Sensitive Data Discovery

Sensitive data within Cloud Infrastructure can be broken into categories:

1. Data related to the operation of the Cloud Infrastructure itself. e.g. user credentials and privileges.
2. Data related to common resources provided by the Cloud Infrastructure. e.g., sensitive data within databases or Platform-as-a-Service components provided by the Cloud operator.
3. Data related to the “workloads” (“virtual machines” or “containers”) that are deployed onto the Cloud Infrastructure by (external and internal) customers of the Cloud operator.

Further, with respect to 3, as within the Use Case “Protection and configuration / management of link between base stations and security gateway”, sensitive data resides not only within the workload itself (i.e. data at rest) but also within the communications between the workload and the other entities (i.e. data in-transit to/from the workload). This communication is further delineated into interactions between workloads within the same Cloud Infrastructure (e.g. between microservices implemented as workloads) and interactions between the workload and external clients and servers.

5.4.4 Cryptographic Inventory

The Cryptographic Inventory for the Cloud Infrastructure can be separated into three broad categories:

1. Attending to data in transit

2. Attending to data at rest

3. Attending to data in use

It is important to minimise secrets (passwords, cryptographic keys) stored in source-code repositories or memory dumps. These have been identified as the root cause for multiple security incidents. Scanning artefacts to identify secrets before they are uploaded to code repositories or cloud environments mitigates the impact of developer error. The use of hardware-based key management (HSMs, enclaves) mitigates the risk of in-memory keys.

5.4.5 Migration Strategy Analysis and Impact Assessment

As a generalisation, the focus of Cloud providers is currently on “attending to data in transit”; to a lesser extent “attending to data at rest” and “attending to data in use”.

“Attending to data at rest” is largely solved by using AES-256 and by not utilising AES keys wrapped in non-PQC (legacy) asymmetric public keys.

“Attending to data in use” is a problem solved by QSC-hardening of infrastructure up to the platform level. Attending to data in transit in Cloud Infrastructure initially involves deploying QSC-enabled versions of critical components:

- OpenVPN, OpenIKED (aka IPsec), TLSv1.3 for ingress controllers for Kubernetes (including intra-cluster QSC re-encrypt), Istio/Envoy Service Mesh, ssh/scp, gRPC, etc.

Additionally, a hybrid-PQC approach as outlined in the Legacy Impact section below is being adopted to smoothen the transition and provide a degree of early protection.

5.4.6 Stakeholders

The key stakeholders for this use case are: Cloud providers, cloud software providers, software package developers, xNF developers and national cybersecurity authorities providing security guidance (e.g. CISA).

5.4.7 PKI Implications

Cloud platforms often include dedicated PKI and CA. These should to be updated to support PQC.

5.4.8 Legacy Impact

Upgrading cloud native applications (i.e. workloads; CNFs and VNFs) to take advantage of PQC capabilities like TLSv1.3 will take some time. To assist their customers in this transition, Cloud Infrastructure providers are expected to take a hybrid approach.

Cloud native applications running in a container-based environment (e.g. Kubernetes) can use a quantum-safe proxy. This approach provides PQC (or hybrid-PQC) connections between clients and application without requiring changes to the application. It provides a migration option.

5.4.9 Dependencies

5.4.9.1 Standards

ISO 27001, NIST Cybersecurity Framework, CSA's Cloud Controls Matrix,

Dependency-PQC-std-kem

Dependency-PQC-std-sig

Dependency-TLS

Dependency-OAUTH

Update to OASIS PKCS #11 to support PQC

5.4.9.2 Open Source

Updates to Linux Kernel and hypervisor to implement PQC

Updates to open source virtulalisation (OpenStack) and containerisation (Docker, Kubernetes, OpenShift) software to implement PQC

Availability of open source implementations of PQC algorithms

Updates to open source TLS implementations to implement PQC

Updates to open source secret stores (Vault, Barbican) to support PQC

5.4.9.3 National Guidelines

Dependency-PQC-guidance

Dependency-PQC-std-national, if required

The publication of national guidance for cloud infrastructure for telecom and CNI.

5.4.9.4 Vendors

Updates to vendor cloud infrastructure to implement PQC for firmware signing, code signing, administrative access to the cloud, machine identity management, monitoring and logging, APIs, secret store, data at rest

Updates to security management to implement PQC (Security Monitoring, Firewall)

Availability of PKI/CA that supports PQC

Updated operational procedures for infrastructure supporting PQC (e.g. key rotation, certificate management, software signing, firmware validation).

5.4.9.5 Operators

Define updated operational processes to support PQC (e.g. code and firmware signing)

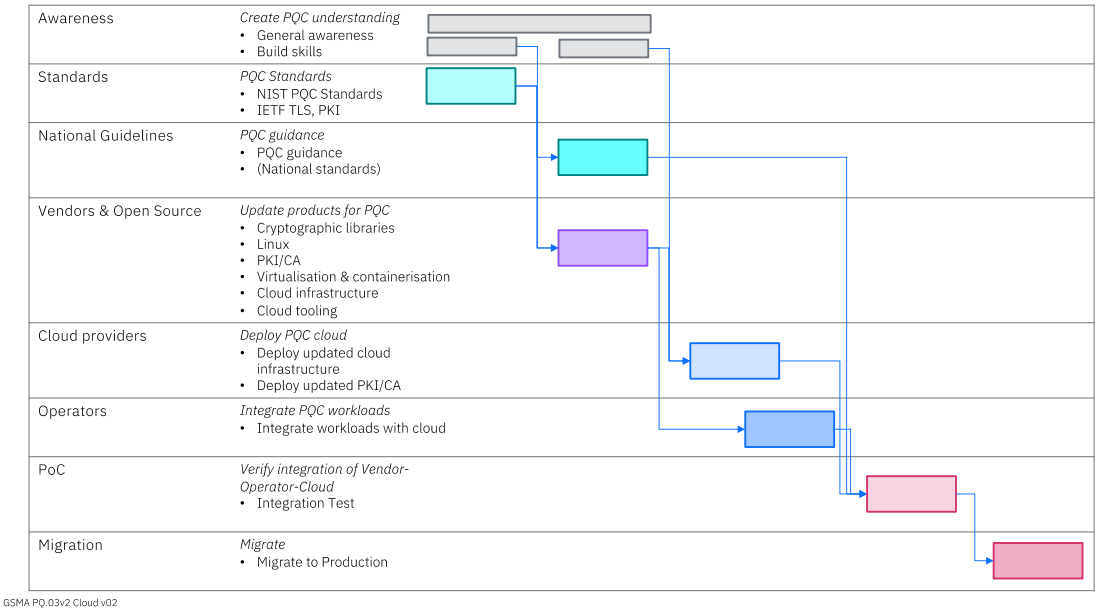
Define updated processes for key rotation including automated and manual rotation.

Migration to infrastructure (cloud, NFVi etc.) that uses PQC.

5.4.9.6 Performance

No impact. The implementation of the PQC algorithms on cloud infrastructure

5.4.10 Gantt Chart for PQC Migration



5.4.11 PQC Migration Process Description

Implement updated operational processes to support PQC (e.g. code and firmware signing)

Deploy infrastructure supporting PQC.

Deploy security products supporting PQC..

Deploy PKI/CA supporting PQC.

Integrate workloads with updated infrastructure, security products and PKI/CA.

Test workloads on updated environment.

Deploy to production.

5.4.12 Synergy with Internal Programs

Infrastructure refresh is a good opportunity to ensure the new infrastructure now supports PQC.

5.4.13 Synergy with External Programs

The updates to cloud infrastructure may be provided by vendors as regular functional enhancements.

5.5 SIM Provisioning (physical SIM)

5.5.1 Scope

This use case involves the transfer of sensitive data/UICC profile that includes cryptographic keying material between a mobile network operator (MNO) and a vendor of UICCs (SIMs) at the time of manufacturing. This means that the input data must be protected when transmitted from MNO to UICC vendor, when it is stored at the vendor's premises, and then the output data that is returned to the MNO must also be preserved. MNOs and UICC vendors are encouraged to follow the GSMA specifications for UICC profiles [GSMA-FS.27] and exchange of UICC credentials [GSMA-FS.28].

Trust between MNO and UICC vendor is often based on an initial shared secret, known as a Master Key. The transfer of the Master Key must be protected against Cryptographically Relevant Quantum Computer (CRQC) since its disclosure could allow decryption of any data transferred between the two entities.

The network links are often secured with TLS, while generation of cryptographic key material is often performed on a hardware security module (HSM). It is therefore necessary to migrate both the TLS configurations (and associated PKI) and the HSM infrastructure to support the PQC algorithms and their requirements.

In the event that the MNO and UICC vendor choose to transfer the profiles in a manner that is not fully compliant with the GSMA specifications then it is necessary for the pair of parties to agree on their migration strategy to PQC. Note that protocols to update the SIM profile [TS 102 225 and 102 226] while it is in the field are based on symmetric cryptography and are therefore less affected by the threats to asymmetric schemes (see Section 4.3)

5.5.2 System Context

This use case involves a communication channel between a UICC vendor and an MNO, where the channel requires confidentiality, authenticity and integrity. These features are provided by modern key establishment protocols such as TLS 1.3 and IKE v2, or by using modern symmetric encryption schemes (i.e. AEAD schemes) if using long-term symmetric pre-shared keys. For entity authentication the endpoints may use certificates in a PKI, with signatures that are also vulnerable to CRQCs. The physical devices performing these actions may be used for purposes beyond SIM provisioning.

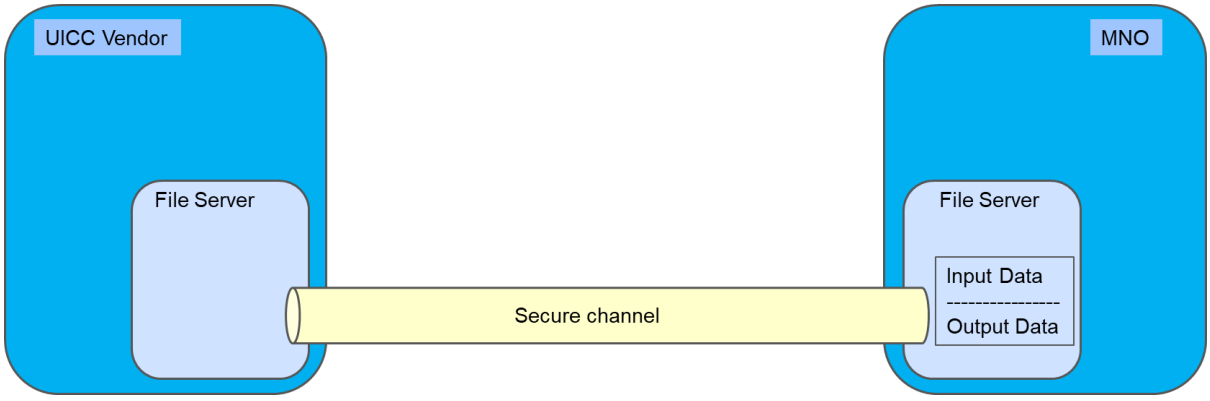


Figure 7: Conceptual diagram of SIM provisioning communication channel.

5.5.3 Sensitive Data Discovery

Due to the use of asymmetric cryptography, the following connections are considered not quantum safe:

- Connection between MNO file server and UICC vendor file server if it uses key establishment protocols such as TLS or SFTP (which uses SSH).
- Connection between MNO HSM and UICC vendor HSM if a key establishment protocol such as TLS/SFTP is used to transfer the Master Key.

Examples of sensitive data in this use case:

Data in transit:

- UICC input files transferred between MNO file server and UICC vendor file server
- UICC output files transferred between UICC vendor file server and MNO file server
- Master key transferred between MNO HSM and UICC vendor HSM

Data at rest:

- Sensitive UICC credentials (like Authentication keys, OTA keys) stored in the HSM

5.5.4 Cryptographic Inventory

The secure communication protocol chosen for the SIM provisioning, which is MNO/UICC vendor dependant (for instance, TLS, SFTP…), may vary.

Storage is based on the existing implementation and usually in the HSM, mainly symmetric encryption based on AES.

5.5.5 Migration Strategy Analysis and Impact Assessment

Migration in this use case is relatively straightforward insofar as the only components that require migration are:

1. the communication channels between MNOs and UICC vendors, which often run over TLS, and

2. the HSMs that generate keying material.

This second item is more straightforward if the HSM is only generating symmetric keys (for authenticated encryption schemes and message authentication codes), as migrating to longer keys requires generating more random bits. If the HSM is producing signing keys for DSA/RSA/ECDSA and/or encryption keys for RSA/Elliptic Curves and this needs to be migrated to algorithms that are Post Quantum secure, then the profile of the keys will be very different and may require new or upgraded hardware.

5.5.6 Stakeholders

UICC vendors and their subcontractors. MNOs and MVNOs.

5.5.7 PKI Implications

At the point of writing this document, there are no implications regarding PKI outside of the general implication of the necessity to upgrade TLS certificates for use in the transfer of UICC profile data.

5.5.8 Legacy Impact

At the point of writing this document, there are no legacy implications that are specific to this use case.

5.5.9 Dependencies

If using TLS or SFTP (SSH) then the migration process requires upgrading both endpoints to support configurations that include post-quantum algorithms, and making these configurations the default mode(s). The dependencies specific to this use case are therefore:

- the software at each endpoint supporting PQC algorithms for session establishment;
- potentially, replacement of hardware: if the current setup cannot support the throughput/data sizes required by the post-quantum algorithms being used under the hood;
- the PKI used by each endpoint.

Note that the first two dependences concern confidentiality of UICC data and therefore are vulnerable to harvest-now-decrypt-later attacks, while the PKI component requires a real-time attacker in possession of a CRQC to be vulnerable.

In addition to these, the use case has the usual dependencies for TLS/SSH: standardized algorithms, standardized variants of TLS/SSH (initially in a hybrid key exchange) that combine traditional cryptography and post-quantum cryptography in an interoperable way, and the requirement that both endpoints support the same post-quantum algorithms.

5.5.9.1 Standards

For TLS 1.3 the 'Hybrid Key Exchange in TLS 1.3' draft by the IETF [https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/] is in an advanced state and provides post-quantum confidentiality (but not authentication).

The migration of SSH depends on the software used by the endpoints. OpenSSH supports post-quantum confidentiality of channels by default since OpenSSH v9.0 [https://www.openssh.com/txt/release-9.0] was released in October 2022 but it should be noted that this uses Streamlined NTRU Prime [https://ntruprime.cr.yp.to/], which was a third-round candidate in the NIST KEM process but did not proceed further. If usage is required to use standardized post-quantum algorithms under the hood then the parties must wait for further work by the IETF. The Open Quantum Safe project has forks of OpenSSH and libssh, but these forks are inactive at the time of writing [https://openquantumsafe.org/applications/ssh.html].

5.5.9.2 National Guidelines

The MNO and UICC vendor may be required to follow the guidance of the national bodies in which their hardware resides (and if the UICC profile data is decrypted and processed in a third country along the way, then of course the guidance of this third country too). This

simply means that each point-to-point connection needs to agree on which asymmetric cryptography algorithms to use, however such processes are likely already in place using for example TLS ciphersuite negotiation.

5.5.9.3 Vendors

For UICC vendors to migrate to PQC, it is necessary to upgrade the software on the machines that connect to MNOs and/or upgrade the hardware if the demands of PQC (e.g. due to increased data packet sizes in KEM-based key establishment compared to ECDH) result in unsatisfactory throughput.

5.5.9.4 Operators

Similarly to the UICC vendors, the MNOs simply need to ensure that the hardware used to receive UICC data is capable of using PQC at the throughput required after a software update, and upgrade the hardware if this is not the case.

5.5.9.5 LEAs

Not applicable.

5.5.9.6 Performance

Performance requirements for the SIM provisioning use case mainly concern connection throughput, since the post-quantum cryptography usage is in the secure channel establishment component and not the transfer of data. Systems should therefore be tested regarding the expected number of connections for the endpoints, particularly if dedicated hardware such as HSMs have data throughput limitations that would be affected by the larger packet sizes involved in post-quantum key establishment.

5.5.10 Gantt Chart for PQC Migration

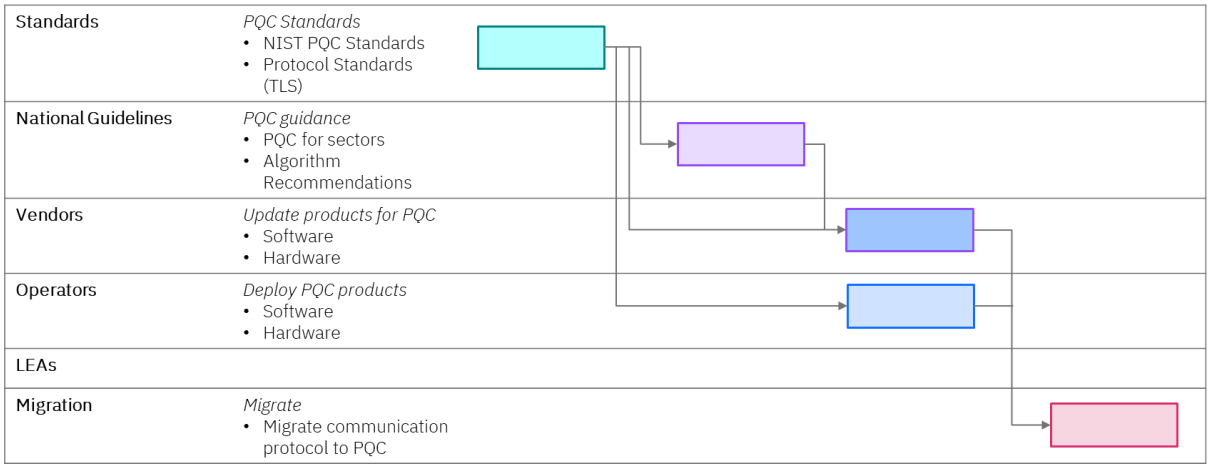


Figure 8: SIM Gantt Chart for PQC Migration

5.5.11 PQC Migration Process Description

The migration of the physical SIM provisioning use case is in many ways considerably simpler than the other use cases described in this document, because it describes point-to-point secure communication channels between entities with very few external dependencies. Further, the amount of data being transferred is likely to be easier to estimate than for other use cases. Security policies will already be in place for strengthening measures such as key

rotation and intrusion detection of physical hardware, which will map directly into the post-quantum setting. This makes the task of assessing viability of migration relatively straightforward, however there may be many legacy elements in the involved systems.

5.5.12 Synergy with Internal Programs

At the UICC vendor side and the MNO side, groups managing the security gateways and the PKI infrastructure will have to carefully coordinate the migration process. The PKI involved may be used in other areas at each endpoint.

5.5.13 Synergy with External Programs

There is no synergy with External Programs.

5.6 Remote SIM Provisioning

5.6.1 Scope

In this section, we consider the impact of quantum computing on the profile download and profile (State) management (e.g. Enable, Disable, …) procedures for the three existing specifications (M2M, Consumer and IoT) and discuss potential migration strategies for each of them.

5.6.2 System Context

The RSP procedure is secured by cryptographic protocols which differ according to the different generations of specifications (M2M, Consumer and IoT). They are briefly recalled below.

5.6.2.1 M2M (SGP.02)

Remote SIM provisioning is performed through secure channels involving three entities, the SM-DP, the SM-SR and the eUICC as illustrated on the figure below.

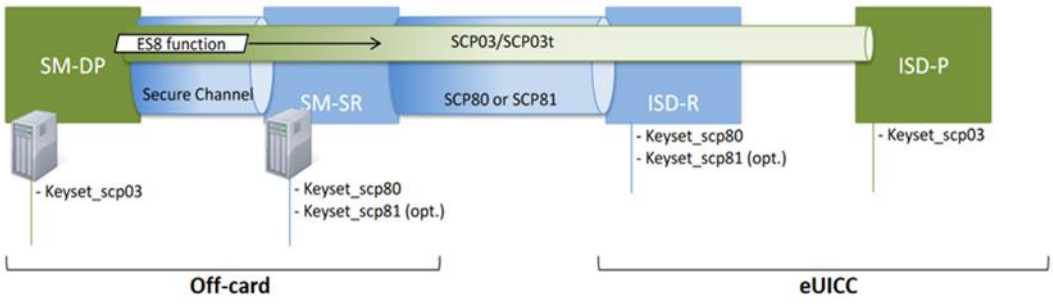


Figure 9: Secure Channles in eSIM M2M

More specifically, a SCP03/SCP03t logical channel between the SM-DP and the eUICC is sent through the SM-SR. A first physical tunnel is established between the SM-DP and the SM-SR and then a second physical channel using SCP80/81 is established between the

SM-SR and the eUICC. We need to consider each of these channels separately as they rely on very different cryptographic primitives.

5.6.2.1.1 SM-SR/eUICC Channel

SCP80 (binary SMS) and SCP81 (https) are secure channel establishment protocols that essentially rely on symmetric cryptographic algorithms. In the context of SGP.02, only AES-128 is used, in different modes.

These channels use secret keys that have been provisioned in the eUICC by the eUICC Manufacturer (EUM) in their SAS-UP certified environment before eUICC issuance unless a SM-SR change procedure has been triggered afterwards.

5.6.2.1.2 SM-DP/SM-SR Channel

SGP.02 does not specify which cryptographic protocols/schemes shall be used to secure the integration between SM-DP and SM-SR: “The procedure describing how the SM-DP establishes a link to the SM-SR (for example: business agreement or technical solution) is not covered by this specification.”

The requirements SR4 and SR6 from SGP.01 apply to this channel but they do not prescribe any cryptographic protocols.

5.6.2.1.3 SM-DP/eUICC Channel

The SCP03 and SCP03t protocols also exclusively rely on symmetric cryptographic protocols. However, these protocols require a shared key between the SM-DP and eUICC.

To establish such a shared key, each eUICC has been personalized with static long-term Elliptic Curve Diffie-Hellman key pairs along with a certificate authenticating them. The corresponding public keys and certificates are stored by the SM-SR. They are provided to the SM-DP at the beginning of the profile download procedure (Section 3.1.1. of SGP.02).

The key establishment protocol is described in Section 3.1.2 of SGP.02. It essentially consists in the generation of an ephemeral Diffie-Hellman key pair by the SM-DP which signs the corresponding public key and a challenge sent by the eUICC using its certified ECDSA private key. The signature and the associated certificate are checked by the eUICC so as to authenticate the SM-DP. At the end of the protocol, the SM-DP knows the static eUICC public key used for ECKA and the eUICC has received an authenticated Diffie-Hellman public key from the SM-DP, which allows to derive a common keyset that can be used for SCP03 or SCP03t. This optimized Diffie-Hellman key agreement protocol is known as ElGamal Key Agreement protocol where one of the participants (the eUICC in the M2M specifications) uses a static DH key pair.

5.6.2.2 Consumer Device (SGP.22)

The Consumer specifications removed the use of SM-SR. The SM-DP has evolved and is called SM-DP+. There is then a secure channel between the SM-DP+ and the eUICC to protect the Profile. The LPA (running on the Device or the eUICC) is responsible about the transport layer which is using HTTPS with server authentication only.

In the context of SGP.22, RSP follows a different approach involving three entities, the SM-DP+, the Device and the eUICC as illustrated in the figure below.

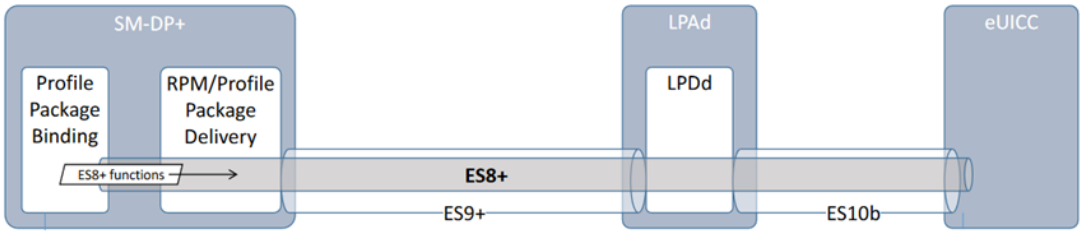


Figure 10: Secure Channles for eSIM Consumer

5.6.2.2.1 SM-DP+/Device Channel (ES9+ Interface)

The channel between SM-DP+ and the Device is secured using TLS with ECDHE key exchange and ECDSA or RSA signatures. The list of supported cipher suites can be found in Section 2.6.6 of SGP.22.

5.6.2.2.2 SM-DP+/eUICC (ES8+ Interface)

The protection of the profile package is done using keys derived from a shared secret derived from a Diffie-Hellman key exchange. Several initial steps are however required to establish such a shared secret involving many cryptographic computations.

First, the SM-DP+ and the eUICC initiates a so-called “common mutual authentication procedure” (described in Section 3.1.2 of SGP.22) where each of these entities generates a signature and authenticates the other party by verifying its signature and the corresponding certificates.

Once this stage is over, the SM-DP+ produces a signature on the transaction data which is sent to the eUICC. If the signature is valid, the eUICC generates its Diffie-Hellman key share which is signed by the eUICC along with some transaction data. The resulting elements are then sent to the SM-DP+.

If the signature is valid, the SM-DP+ generates its own Diffie-Hellman key share and can thus derive a shared secret used to generate the Bound Profile Package (BPP). This key share can thus be sent to the eUICC along with the BPP and a signature authenticating this material.

5.6.2.3 IoT (SGP.32)

As in the case of Consumer Device, in the IoT case, the profile provisioning involves the SM-DP+, the IoT Device (where the “IoT Profile Assistant” (IPA) replaces the SGP.22’s LPA) and the eUICC. Optionally, an intermediary entity called “eSIM IoT Remote Manager” (eIM) may be involved. The profile may consequently be downloaded into the Device either directly (first figure below) or indirectly (the package is then relayed by the eIM between the SM-DP+ and the Device, as illustrated in the second figure below).

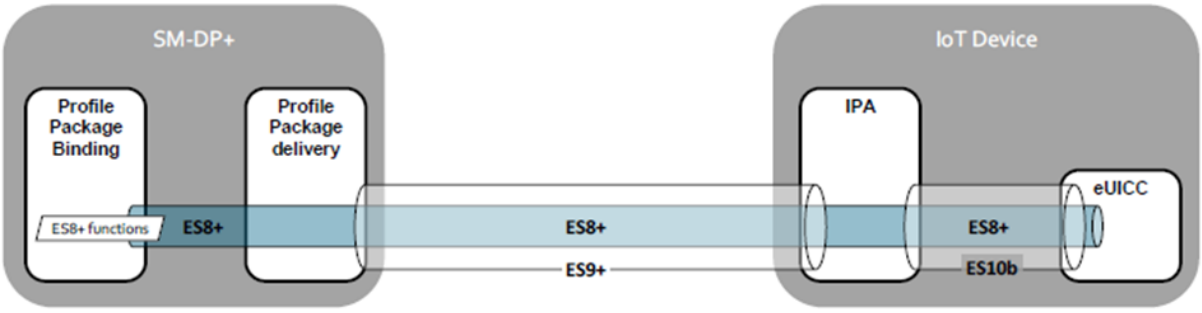


Figure 11: Secure Channles for eSIM IoT

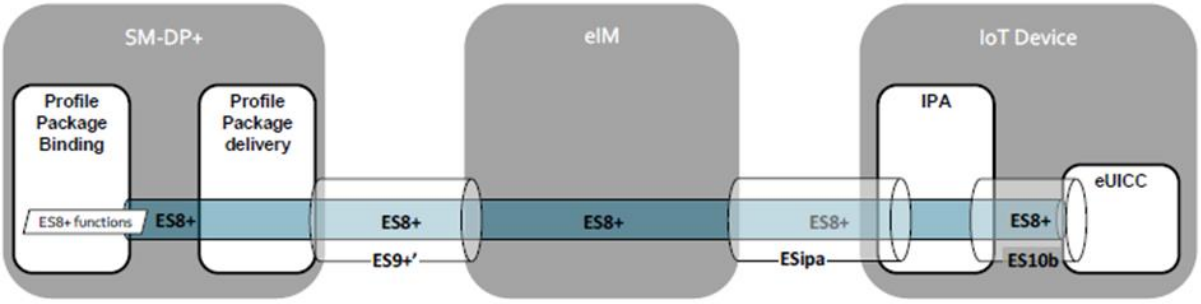


Figure 12: Secure Channles for eSIM IoT

5.6.2.3.1 SM-DP+/device Channel (ES9+ Interface)

This channel is protected the same way as in the Consumer Device case, where IPA plays the role of the SGP.22's LPA.

5.6.2.3.2 SM-DP+/eUICC Channel (ES8+ Interface)

This channel is protected the same way as in the Consumer Device case.

5.6.2.3.3 SM-DP+/eIM Channel (ES9+' Interface)

This channel is protected the same way as the ES9+ interface in the Consumer Device case, with server (SM-DP+) authentication.

5.6.2.3.4 EIM/device Channel (ESipa Interface)

SGP.32 does not mandate any protocol between the eIM and the Device, but the protocol must provide at least the integrity and the confidentiality of messages.

SGP.32 suggests however the following protocols: HTTP over TCP with TLS, and CoAP over UDP with DTLS (optionally with session resumption). If any of these two protocols is deployed, then only the server (eIM) authentication is required. The protocol versions and ciphersuites required for TLS and DTLS are listed in Section 2.6.3 of SGP.32.

5.6.3 Sensitive Data Discovery

A profile contains very sensitive data, some of which serving as seeds to derive cryptographic keys, which makes the quantum risk assessment particularly intricate. Indeed, when evaluating the consequences of a profile leakage, one should not only consider the data contained in the profile but also the ones that are secured using those derived keys. In particular, one of the main subtleties of this use-case is that a profile leakage remains a

problem even when the associated device is discarded as it provides a way to decrypt all the data received and transmitted by this device during its lifespan. It is thus extremely important to perform a QRA for all applications, even those involving devices whose lifespan expires before the expected advent of CRQCs.

5.6.4 Stakeholders

- RSP server vendor (SM-DP, SM-SR, SM-DP+),
- eUICC manufacturer
- OEM for LPA (Local Profile Assistant) (agent in mobile phone)

5.6.5 Dependencies

5.6.5.1 Standards

The protocols for the M2M, Consumer Device and IoT architectures are respectively defined in the SGP.02, SGP.22 and SGP.32 specifications. Those documents themselves rely on other standards, and in particular on TLS, ECDSA and ECKA for security aspects.

All the migration strategies considered here require at some point to update TLS to at least support hybrid key exchange, as in the following draft by IETF:

draft-ietf-tls-hybrid-design-10 - Hybrid key exchange in TLS 1.3

In parallel, implementation of quantum resistant KEMs and signatures will be necessary. As of writing, there are no published standards on PQC algorithms (unless in the very specific cases of stateful signatures) but the NIST ML-DSA and ML-KEM drafts are in a very advanced state and thus constitute the most natural candidates for updating the SGP.02, SGP.22 and SGP.32 specifications.

We also note that these specifications are built upon several standards relying on symmetric key cryptography and in particular on the SCP03(t), SCP80 and SCP81 specifications. As the exact quantum resistance of symmetric cryptography is still under debate (see the “Technical Challenges for PQC Migration” section above), the need to update these standards will depend on the targeted recommendations related to symmetric key sizes.

5.6.5.2 Vendors

All the migration strategies considered below will affect RSP server vendors that will have to update their equipment to at least support quantum resistant key exchange for secure channel establishment.

Similarly, in the context of SGP.22 and SGP.32, the OEM will have to update their devices to at least support a post-quantum variant of TLS.

The impact on eUICC manufacturers will differ according to the considered migration strategies and we thus refer to the next sections for the details.

5.6.5.3 Operators

Operators are not directly involved in the RSP process but as the profiles contain some cryptographic keys used within their networks, they should check that the security level of RSP is consistent with the one of their own networks.

5.6.6 Performance

The impact of PQC migration on the performance differs according to the strategies described below and is thus discussed in the corresponding sections.

5.6.7 Gantt Chart for PQC Migration

We discuss in this section several migration strategies, with different options, which can hardly be reflected by a unique Gantt Chart.

5.6.8 PQC Migration Process Description

5.6.8.1 General Observations

As mentioned earlier in this document, the discrepancies among national recommendations are a significant problem for worldwide specifications such as those defining RSP. Nevertheless, we note that, in all cases, an implementation of the most conservative recommendations naturally defines a migration strategy which is ideal from the security standpoint. While we do consider this migration strategy in this section, we note that it comes with several practical challenges that may require to investigate alternative migration strategies. By essence, these alternative strategies are not optimal on some security aspects, but we believe they remain interesting because they appear to be easier-to-implement remediation measures or can even constitute one of the only solutions for legacy systems that could not support a full-fledged transition to post-quantum cryptography.

5.6.9 Transition Challenges for RSP

Legacy systems: eSIMs are massively deployed today, and more will come before an update of the current specifications, which raises the usual question of legacy management. Ideally, all the systems could be remotely updated to match the new version of the standards, but this seems unlikely, at least for eUICCs in some use-cases. We indeed recall that post-quantum public key mechanisms are very different from classical ones in the sense that they make use of different mathematical objects, involving different operations. In some cases, making eUICCs PQC-compatible might then not be possible through a mere software update, which dooms to failure a full PQC transition. Fortunately, the eUICCs are just one component of the different architectures which also include easier-to-update systems such as servers (e.g., SM-DP+) and devices (e.g., a smartphone). In one of our alternative migration strategies, we will then investigate how we can rely exclusively on such devices to mitigate the quantum risks.

Size Complexity: most of the future NIST standards are based on lattices, which requires to handle and transmit much larger elements compared to traditional elliptic curves. While this might seem insignificant at a time of widespread fast communications, it leads to a bottleneck at the Device/eUICC interface where communication channel is based on APDU (APDU size being 256 bytes). We can consider that payload size to download a typical 32KB profile is doubling due to signature and public key size for ML_DSA (Level3). Then APDU

bottleneck is leading to about 40% time increase for whole download process, which is impacting Use Experience.

In this regard, it might then be interesting to investigate alternative migration strategies that would minimise the communication complexity.

5.6.9.1 Full-Fledged Transition

The first migration strategy we consider in this section is the conventional one, where all the vulnerable algorithms would be replaced by their post-quantum counterparts or combined with them in a hybrid approach.

5.6.9.1.1 eUICC/SM-DP Interface

In the case of the eUICC/SM-DP interface, those vulnerable algorithms are essentially:

- the ECKA key exchange
- the ECDSA and/or SM2 signatures

The future NIST standards provide post-quantum alternatives to those schemes, although the case of key exchange is a bit subtle. In all cases, one could implement ML-KEM to ensure quantum resistance of the key exchange part. The case of signatures offers more options as one can choose between ML-DSA, SL-DSA, FN-DSA (in a near future) and even LMS and XMSS in some restricted cases, but is also more challenging as RSP procedures involve many signature generations/verifications. Moreover, transition of these signature schemes must be done consistently all along the certificate chains, which adds to the complexity of the whole migration process.

The table below, communicated by Thales, provides an estimation of the transcript size and corresponding timings in the classical and post-quantum settings.

	RSP Protocol	Certificates	Signatures	Key Exch	Midsized Profile	Total	Estimated Timing (due to data overhead)
ECDSA ECDH	4,8	3 (7,8 %)	0,384 (1%)	0,128	30	38,3 KB	≈ 30-35s
ML-DSA 3 ML-KEM 3	4,8	20,6 (26,5 %)	19,8 (25,5 %)	2,3 (3 %)	30	77,5 KB **(+102 %)**	≈ 45-50s
ML-DSA 5 ML-KEM 5	4,8	28,2 (30 %)	27,6 (29 %)	3,1 (3 %)	30	93,7 KB **(+145 %)**	≈ 52-57s

Table 2: an estimation of the transcript size and corresponding timings in the classical and post-quantum settings.

It clearly indicates that the part of the cryptographic elements in the RSP protocol that has been so far very moderate will considerably increase with PQC to account for more than half of the whole size. This evolution is also reflected by the timings which are expected to increase by 50 to 75%. Interestingly, it shows that this increase is mostly due to the certificates/signatures, which could plead for the phased transition presented in the next section.

Besides these sole complexity considerations, one must also consider the impact on the GSMA PKI, with a specific focus on the M2M case where certificates are in GP format instead of x509.

5.6.9.1.2 Device/SM-DP Interface (SGP.22/32)

As this interface is secured using the TLS protocol, the transition would essentially imply a migration to a post-quantum variant of TLS. We nevertheless note that the situation would be comparable to the eUICC/SM-DP interface as most of the allowed cipher suites involve Diffie-Hellman key exchange and ECDSA signatures.

Here again, the whole certificate chain would have to be updated consistently.

5.6.9.2 Phased Transition

The most pressing threat posed by CRQCs is arguably the so-called “Harvest Now Decrypt Later” which means that privacy of current data is already at risk. Conversely, data authenticity is ensured as long as CRQCs do not exist. Since CRQCs are not expected before 2030, it might be worth considering a phased transition where only the cryptographic materials vulnerable to “Harvest Now Decrypt Later” would be upgraded to PQC. More specifically, in a first phase, only key exchange and encryption mechanisms would be upgraded whereas migration of digital signature mechanisms would be postponed to a second phase whose date will be determined according to the advances of quantum computing.

The advantage of this solution is to limit the protocol modifications to what is strictly necessary at this stage. The impact on complexity and payload size (and thus on the cost or on the user’s experience) would thus be rather moderate (as detailed in the table above) without any compromise on security. Moreover, it avoids at this stage the very complex PKI considerations that are mentioned above, except in the specific case of certified long-terms keys (M2M).

The downside is that it does not fully address the quantum threat but only repels it to the Q-day. One must then continue to monitor the advances of quantum computers to initiate the second phase of the transition on time, which will require long-terms efforts from stakeholders.

5.6.9.3 Partial Transition

In this scenario which targets legacy systems, we assume that the eUICC itself cannot be updated to support PQC. Obviously, in this case, one cannot hope to ensure against quantum computers the same security properties as the ones enjoyed today against classical computers. However, as we will explain, one could still retain relevant security properties without modifying the eUICC by leveraging the security of the other channels. We will need to distinguish the M2M case from the other ones in what follows.

5.6.9.4 M2M

Although the key establishment protocol securing the SM-DP/eUICC channel cannot withstand quantum computing, attacking this channel requires to first strip off the SCP80/81 channel between the SM-SR and the eUICC or the secure channel between the SM-DP and the SM-SR. We consider each of them below.

- **SM-SR/eUICC channel: T**he SCP80/81 channel essentially relies on symmetric cryptography, with pre-provisioned key. If the AES key sizes used to secure SCP80/81 were to be increased to 256 bits, or if 128-bit AES is deemed sufficient to resist quantum computing, then this channel would achieve post-quantum security.
- **SM-DP/SM-SR:** The lack of precise specifications for this channel prevents any conclusion regarding its post-quantum security or general migration plan. We nevertheless note that :

    - In a situation where this channel is protected using symmetric cryptographic protocols (e.g. TLS in Pre-Shared Key mode), communication security could resist to quantum computers.
    - In a situation where this channel is protected by TLS (e.g asymmetric cryptography), a proposed migration path would be to upgrade TLS channel to PQC (e.g. hybrid key exchange - see draft-ietf-tls-hybrid-design-10 - Hybrid key exchange in TLS 1.3).

In the end, we note that the Profile Download procedure for M2M could remain secure in presence of an external adversary (that is, one that does not control the SM-SR) without major changes in the case where the SM-DP/SM-SR channel is already quantum resistant (or can be updated to achieve this level of security). We nevertheless stress that this approach would fundamentally change the security model as no post-quantum security would be achieved with respect to the SM-SR. However, in some cases, for example the one where the SM-DP and the SM-SR would be controlled by the same entity or would be deployed in the same premises, this could be considered as a reasonable compromise, at least for legacy systems.

5.6.9.5 Consumer Device

The situation here is quite different from the one of M2M as both the ES8+ and ES9+ interfaces are protected using classical public key cryptographic mechanisms and so none of them could resist quantum computing. However, since ES9+ (between the SM-DP+ and the device) is secured by using the TLS protocol, one could envision to implement an hybrid key exchange for the latter (see draft-ietf-tls-hybrid-design-10 - Hybrid key exchange in TLS 1.3). In such a case, we note that mounting a “Harvest Now, Decrypt Later” attack would be much more complex as the adversary could no longer merely eavesdrop communications. Concretely, it would essentially remain two options for mounting this kind of attack:

1. Either break the security of the TLS certificates to mount a man-in-the-middle attack on the ES9+ interface and therefore recover the classically encrypted data exchanged on ES8+
2. Or intercept the profile at the only place where it is not protected by post-quantum cryptography, namely at SM_DP server or device level.

While these scenarios are still plausible because the security level of the device is not as strong as the one of an eUICC and because the TLS certificate policy may be less stringent than the one defined by GSMA, it forces the adversary to control the device or to mount a man-in-the-middle attack at the time where the profile is downloaded which seems harder to perform at a large scale. Regarding SM_DP server, attack would be at WAF (Web Application Firewall) level, which is a security component.

In other words, updating ES9+ to achieve quantum resistance significantly increases the complexity of the “Harvest Now, Decrypt Later” attack and could thus constitute an interesting mitigation, at least for legacy systems whose eUICCs cannot be updated.

5.6.10 Practical Considerations

Leaving aside the particular case of legacy systems, all migrations strategies will require at some point to implement PQC on eUICCs which is a challenging task. However, PQC encompasses many cryptographic algorithms whose diversity could be leveraged to minimise impacts on performance. In parallel, some implementation choices specific to PQC can limit security risks. Those practical aspects are discussed below and should be considered regardless of the chosen migration strategy.

5.6.11 Mixing Algorithms

As mentioned above, one of the identified bottlenecks for eUICCs is the large size of the cryptographic elements associated to some PQC algorithms. At first sight, this could be addressed by resorting to algorithms yielding smaller elements. For example, one could replace Dilithium signatures by those generated by Falcon but this would essentially trade one problem for another as the latter algorithm has a rather complex signature generation procedure. In addition, Falcon is considered as much harder to protect against side-channels attacks.

However, here again, one could leverage the asymmetry between the different entities and procedures of RSP. For example, the mutual authentication procedure between the eUICC and the server could be done using different algorithms. More specifically, the server could authenticate itself using Falcon signatures whereas the eUICC would produce Dilithium signatures. This would ensure a low computational burden for the eUICC (as Falcon signature can be efficiently verified) while reducing the transcript size compared to a solution exclusively based on Dilithium.

Similarly, one could envision a solution where the CA root certificates would be issued with stateful signature schemes so as to benefit from their small sizes and time-tested security.

This approach mixing different algorithms allows thus to shift the bulk of the computational workload on the most powerful entity (namely, the server) while optimizing the size of the transmitted elements. This however comes at the cost of a greater implementation complexity as all the entities would have to support several different cryptographic protocols, with specific side-channel protection, etc. Moreover, as of writing, the NIST has not published a draft for FN-DSA which makes performance evaluation uncertain and may hamper broad adoption of this mechanism.

5.6.12 Implementation Choices

In the current versions of the SGP.02, SGP.22 and SGP.32 specifications, the key exchange procedure is implemented with the Diffie-Hellman protocol. As of writing, no exact post-quantum counterpart has been standardized or is in the process of being standardized. One must instead implement a Key Encapsulation Mechanism, such as ML-KEM, which introduces asymmetry between the two endpoints. Indeed, one is responsible of the secret

key encapsulation whereas the other one must decapsulate it. These two procedures are very different, in particular from the side-channel standpoint, and assigning the encapsulation (resp. decapsulation) to either of the endpoints has different consequences.

- Encapsulation performed at the server side.

This approach significantly simplifies the server management as it does not need to keep track of decapsulation keys but forces the eUICC to perform decapsulation, which raises the issue of side-channel protection. In the cases of SGP.22 and SGP.32, the keys are ephemeral which limits the risks of side-channel attacks, but it is still hard to completely rule out the need for SCA protection, at least for certification reasons. If the ML-KEM keys were to be static (as is currently the case for the Diffie-Hellman keys in M2M specifications), proper side-channels countermeasures would have to be implemented.

- Encapsulation performed at the eUICC side.

Conversely, performing the encapsulation at the eUICC side simplifies the implementation on this device but shifts the burden to the server side, which could create scalability issues.

5.6.13 Synergy with Internal Programs

There is no identified synergy at this stage.

5.6.14 Synergy with External Programs

There is no identified synergy at this stage.

5.7 Firmware Upgrade / Device Management

5.7.1 Scope

Firmware updates play a critical role in maintaining the security and functionality of devices. This use case considers code signing and the Root of Trust in the device.

Only authentic and authorized firmware update images shall be applied to devices. An update image is authentic if the source (e.g., the device, system manufacturer, or another authorized entity) and integrity can be successfully verified. In addition, confidentiality of the image shall be ensured through ciphering techniques.

Although we will introduce impacts and recommendation regarding transport protocol (secure communication channels), this use case will be focused on integrity and authenticity of the image, in order to ensure that no adversarial image could be loaded and activated.

In the subsequent sections, we explore how the current (classical) cryptographic mechanisms can be adapted to migrate to post-quantum security and several related challenges.

5.7.2 System Context

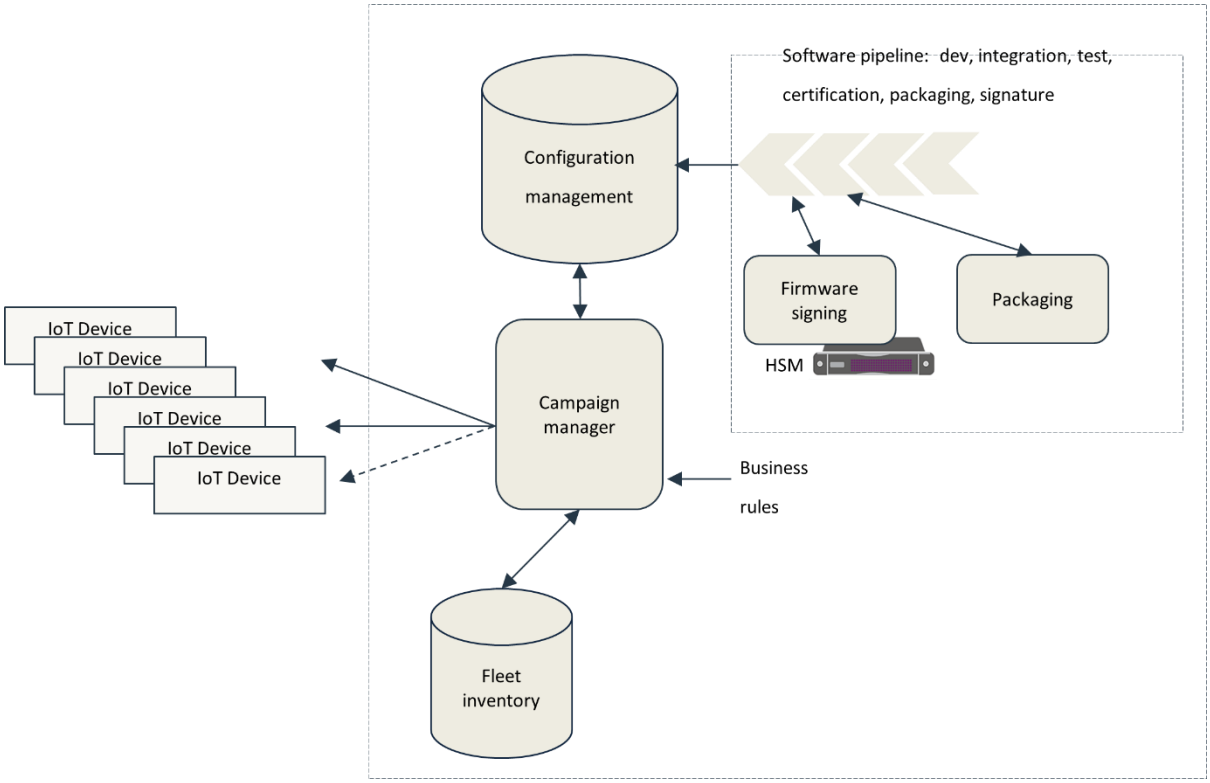


Figure 13: Schematic view of a firmware upgrade system

Updating a firmware onto a (constrained) end-device implies several steps, among which:

- Signing the new firmware.
- Transmitting the signed firmware to the end-device.
- Verifying the firmware signature.
- Deploying the firmware.

This use case focuses on the cryptographic operations involved during the signature generation and signature verification. However other components may have to be resistant to quantum attacks, in particular:

- the means to request new signatures from the signing entity (e.g., HSM),
- the schemes to establish a secure tunnel with the end-device (to transmit the signed firmware),
- the means to protect the integrity of the signature verification key stored onto the end-device.

5.7.3 Sensitive Data Discovery

Firmware code itself should be considered highly sensitive, as demonstrated by the following examples:

- Device Configuration: Firmware updates often include changes to device settings and configurations. This may include network settings, authentication credentials, access control lists, encryption keys, or other sensitive parameters that control the behavior and security of the device.
- Keys: Firmware updates may require the regeneration or reconfiguration of keys used for securing communications, data storage, or other cryptographic operations. These keys are highly sensitive as they protect the confidentiality and integrity of data, and their compromise could lead to unauthorized access or data breaches.
- System Logs and Audit Trails: Firmware updates may impact the system logs and audit trails maintained by the device. These logs record events, errors, user activities, or other relevant information for troubleshooting, compliance, or forensic purposes. Access to these logs could potentially reveal sensitive information or aid in reconstructing user activities.

In specific case of a UICC, sensitive Data include (for the exhaustive list – refer *GSMA FS.28 - Security Guidelines for Exchange of UICC Credentials*)

- Credentials that are unique to each UICC (e.g. subscriber keys, OTA keys, service provider keys, subscriber specific parameters), called **UICC unique credentials**

Credentials that are common to one or several batches of UICCs, such as MNO specific parameters (Milenage OP value or the TUAK TOP value)

5.7.4 Cryptographic Inventory

Physically embedded roots of trust are used to authenticate software and firmware updates.

Today, asymmetric algorithms, such as RSA or ECDSA), are widely used for digital signatures which are vulnerable to the quantum threat. In case symmetric cryptography is used (HMAC, CMAC), leveraging secret keys, impact will be lower and will be linked to key size.

Depending on the secure communication protocol chosen for the firmware update (which is manufacturer dependant) cryptographic keys, that could be linked to asymmetric or symmetric cryptography (pre-shared keys), will be embedded in the device. Options for the secure protocol include: Transport Layer Security (TLS), Global Platform Secure Channel protocol such as SCP11C, one that allows broadcast distribution.

5.7.5 Migration Strategy Analysis and Impact Assessment

The deployment of connected devices with quantum safe firmware signing and firmware update capabilities will be the foundation for cryptographic agility.

Update protocols shall also be updated to be quantum-safe. They may be proprietary, or standardized (e.g. TR-069 -CPE WAN Management Protocol).

Key management and firmware signing is usually managed using HSMs (Hardware Security Modules), which need to be quantum safe as well. (The HSM firmware update function shall be quantum safe. The HSM shall support the required quantum safe algorithms. The HSM shall provide the right level of entropy for quantum safe key generation).

Devices should support remote update of the embedded Root of Trust (the credentials used for firmware signing verification). If new devices do not have Quantum-safe firmware when deployed this allows update and avoids recall.

Remote update capability (server) shall also be available, with quantum resistant protocol (key agreement.)

5.7.6 Stakeholders

- HSM vendors
- Device management platforms
- Device vendors, including chipset and module suppliers

5.7.7 PKI Implications

In case integrity, authenticity, confidentiality are leveraging asymmetric cryptography, PKI plays a key role, and must be transitioned to quantum safe.

The detailed implications for PKI depend on whether hybrid schemes are adopted or if the classical algorithms are instead merely replaced by PQC variants.

5.7.8 Legacy Impact

For legacy devices that cannot support a firmware refresh to implement PQC a decision will need to be made to either recall and replace the devices or accept the risk.

5.7.9 Potential Actions / Dependencies

Complexity that is caused by careful state management is a topic highly discussed with NIST. This state management is the reason NIST does not allow key backup, in order to avoid any misuse or double usage of a private key.

NIST shall provide guidelines for operationalisation of LMS/XMSS, including the capability for transferring keys from one FIPS HSM to another FIPS HSM. Indeed, the time scale of the firmware update use case could be up to 15-20 years, and a HSM vendor is likely to need to transfer keys to a new HSM generation during this time.

Waiting for this guideline and SP 800-208 update, in case key generation should occur for LMS/XMSS, best practice would be to generate a lower level keys among several HSMs, considering generating extra number of keys to mitigate any problem during the life time of these keys (i.e. the failure or loss of an HSM).

5.7.10 Dependencies

5.7.10.1 Standards

NIST SP 800-208 for Stateful Hash-Based signature (HBS) algorithms [NIST SP 800-208]

NIST FIPS 205 for Stateless Hash-Based signature algorithms [NIST FIPS 205]

NIST FIPS 204 for Lattice-Based signature algorithms [NIST FIPS 204]

5.7.10.2 National Guidelines

The publication of national guidance on the use of PQC.

The publication of national standards for sovereign PQC algorithms, if required.

5.7.10.3 Vendors

- HSM
- PKI
- Devices
- Firmware update vendors

5.7.10.4 Operators

Firmware update supply chain update

5.7.10.5 LEAs

N/A

5.7.10.6 Performance

Generally, the signature verification operation (done by the end-device) is not a performance bottleneck contrary to signing key generation and signature computation (done by the HSM or an authority server).

Bigger concerns are verification code size and the length of the verification key (stored on the end-device).

Regarding the signature size, the latter is usually much higher for post-quantum schemes compared to classical schemes. However, the signature is sent together with the updated firmware which is usually already rather large.

5.7.11 Gantt Chart for PQC Migration

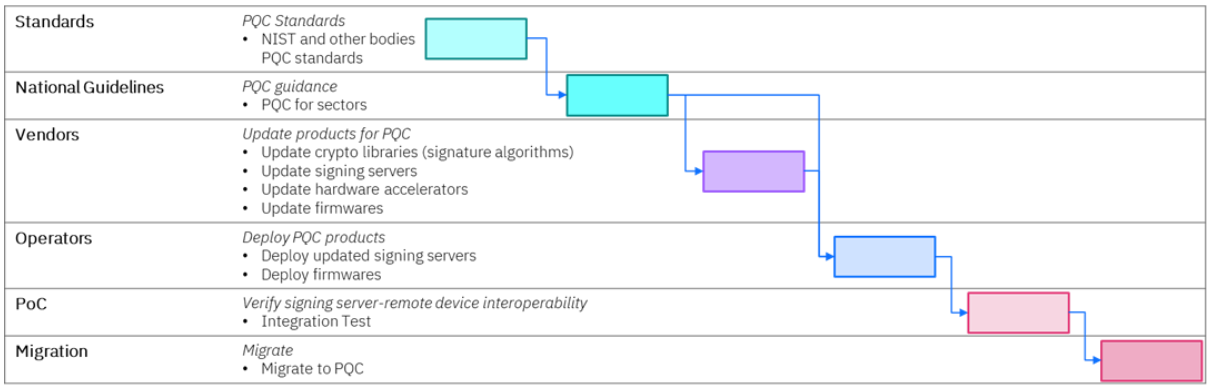


Figure 14: Gantt Chart for PQC Migration

5.7.12 PQC Migration Process Description

5.7.12.1 Migration strategies

For new devices, key first step is to physically embed quantum safe Root of Trust in the device now, to avoid costly, logistically challenging recalls in the future. A Secure enclave, such as Secure Element, is the ideal container, providing temper resistance.

Today, security agencies are recommending usage of stateful HBS algorithms (SP 800-208 from NIST), considering the limited number of signatures required during device life, the

limited resources on device (e.g., RAM) required for verifying signature, and the proven technology that is not requiring cryptographic hybridization.

Crypto-agility allows to embed both classic crypto based Root of Trust and PQC one, and switch when required. This would allow to migrate the whole Firmware update ecosystem asynchronously.

Crypto-agility is as well allowing to consider other PQC signature types, if device resources are sufficient. Indeed, to mitigate concerns raised to stateful HBS algorithms (e.g., no key back-up allowed), other PQC signature algorithm, such as ML-DSA, could be used. This is raising other challenges, such as hybridization required for ML-DSA-65 (NIST security level 3) and probable costly update of device to meet resource required for ML-DSA-87 (NIST security level 5).

For this first migration step (e.g., embedding quantum-safe Root of Trust), HSM shall be implementing the chosen algorithm(s), key generation, and for stateful HBS algorithms, state management. PKI shall be available. Root of Trust shall be embedded in devices at manufacturing.

Second migration step, before 2030, is updating rest of firmware update ecosystem, especially software pipeline.

For legacy devices, or devices that could not be updated to PQC before shipment to the field, the level of risk shall be appreciated during the Quantum Risk Assessment phase. If risk is not acceptable, then the devices shall be recalled once quantum computer capable to break classic asymmetric cryptography is available.

Some update systems are exclusively based on symmetric-key algorithms. As of writing, such algorithms are deemed quantum-safe assuming that adequate parameters size is used. Although there is no consensus among cybersecurity agencies on that matter, a conservative measure would consist in increasing the key size (e.g., from 128 to 256 bits) and other parameters (MAC tag length, hash output size, etc.).

If such measures would be enough for infrastructures already relying upon symmetric-key cryptography, note that switching from classical signature algorithms to symmetric-key algorithms would radically change the security perspective. If the symmetric authentication key is extracted from a device, this may allow impersonating the legitimate signing/MAC-ing entity to the device (depending on if additional security means are deployed, such as a secure tunnel, to transmit the firmware). If a distinct symmetric key is used per device, then this increases the complexity of the key management on the MAC-ing side. If one key is used for a set of devices, then the damages spread throughout the whole fleet of devices.

We can also observe that signature algorithms enjoy a property not provided by asymmetric key encryption schemes. That is, as long as we are confident that no efficient quantum computer is available, we can rely upon classical signature algorithms to safely load the new post-quantum public key into the end-devices (as authentication cannot be retroactively broken). Of course, this implies that the classical signature verification algorithm be deactivated onto the end-device before quantum computers be usable. In turn, the latter procedure is conceivable if the public key can be updated. However, the public keys are often burnt into fuses. Therefore, this kind of workflow may not be widely applicable.

5.7.12.2 Cryptographic resources

In this section we list the signature algorithms that may be considered to authenticate the firmware.

5.7.12.2.1 Stateful hash-based signature (HBS) algorithms

NIST SP 800-208 describes LMS and XMSS signature schemes. It approves the use of some but not all the parameters sets defined in RFCs 8391 (XMSS) and 8554 (LMS). It also requires that key and signature generation be performed in hardware cryptographic modules that does not allow secret keying material to be exported. This means as well that no back up is allowed, which is a concern if we consider HSM possible loss or migration to new HSM generation. NIST will publish SP 800-208 update in the course of 2024 to mitigate this concern.

These schemes are regarded as conservative because their security only relies on the properties of hash functions. The understanding of these properties is much more mature than that for lattice- and code-based cryptography.

LMS and XMSS have a number of parameters that affect performance, so it is difficult to give concrete numbers that make for useful comparisons, however in general XMSS has slightly smaller signature sizes while LMS is more performant.

Nevertheless, stateful HBS schemes have several advantages that make them a good option for the use case:

- The size of the signature depends on the maximum number of signatures that can be generated. This implies that, for typical end-device lifetime, the number of signatures, hence the size of the latter, can be reasonably low and easily manageable by a constrained end-device (1.5-3 KB allowing at most 1024 signatures).
- Generally, the signature verification operation (done by the end-device) is not a performance bottleneck contrary to signing key generation and signature computation (done by the HSM or an authority server).
- The size of the verification key (used by the end-device) is rather low (56-128 bytes).
- Several cybersecurity agencies (ANSSI, BSI, NSA) do not require hybridization when these signature schemes are implemented.

In turn, we can mention the following downsides:

- Stateful HBS schemes require a careful internal state management. The internal state is required during the signing procedure and handled by the signer entity (HSM). Such a burden does consequently not rely upon the end-device.

5.7.12.2.2 Stateless HBS algorithms

NIST FIPS 205 describes the stateless HBS scheme SPHINCS+ (slightly modified) under the name SLH-DSA. SLH-DSA is more conservative than the lattice schemes (see below) and is based on the security properties of hash functions with small key sizes (32-128 bytes), but is much slower and has larger signatures (8-50 KB). Most of the advantages of stateful HBS schemes mentioned above apply also to SLH-DSA. Notable differences are:

- The signature verification is slower.

- The signature size is significantly increased (8-50 KB). Note however that proposals exist aiming at lowering the number of maximum signatures (equal to 2^64 with the current parameters sets) which would in turn reduce the signature size. NIST is planning to create an SP for this.
- An additional advantage is that no internal state needs to be managed, which is appealing because the signing infrastructure is less complex to safely maintain.

5.7.12.2.3 Lattice-based signature algorithms

NIST released a draft standard (FIPS 204) of the signature scheme Dilithium (slightly modified) under the name ML-DSA. Its security is based on lattice-based cryptography, ML-DSA presents balanced properties: relatively fast key operations, medium-sized keys (1312-2592 bytes verification key, 2528-4864 bytes signing key) and medium-sized signatures (2420-4595 bytes).

NIST intends also to release a draft standard of the signature scheme Falcon under the name FN-DSA (after the current review process for ML-DSA and SLH-DSA has concluded). FN-DSA is also based on lattice assumptions and is generally slightly more performant than ML-DSA (in particular regarding the signature public key and the signature verification operation), however it requires double precision floating-point arithmetic which comes with challenges on embedded platforms and fragility in terms of vulnerability to side-channel attacks (the latter, however, is instrumental when it comes to signature computation whereas the end-device is expected to perform signature verifications).

The downside with these signature schemes is that several cybersecurity agencies recommend hybridization (e.g., ML-DSA+ECDSA) which increases the requirements in bandwidth, code footprint, computation time, and possibly RAM.

5.7.12.2.4 Benchmarks

Table 1, from [PKLN22], provides some figures regarding different signature schemes. Note that this is a mere illustration of what these schemes offer since benchmark may vary significantly depending on the trade-off between performance, RAM, use of non-volatile memory and hardware (not speaking of countermeasures to mitigate side-channel attacks when required). Moreover, several parameter sets are available (corresponding for some schemes to the same security level, e.g., XMSS, LMS) which enable different trade-offs.

The device considered is a Raspberry Pi 3 Model B equipped with an ARM Cortex-A53 quad-core processor running at 1.2 GHz and 1 GB of RAM (similar to end-devices deployed in typical IoT settings). Code is software only. Note that this does not allow a comparison between classical algorithms in hardware and post-quantum schemes possibly in software only. In that regard, refer to Table 3.

Regarding the computation time, we report only the verification time since signing is done on the server side. As firmware updates happen rather rarely, one can size HBS schemes (when such schemes are used) such that a few signatures only need to be output. This allows also lowering the size of the signature. That said, bigger concerns are verification code size and the length of the verification key rather than verification time and signature size. Moreover, the signature is sent together with the updated firmware which is usually rather large.

L: NIST security level (or equivalent). Sk: secret key. Pk: public key. Sg: signature. Verif: verification operation.

NB: In Table 1 and Table 2, Dilithium corresponds to the NIST PQC Round 3 version. XMSS is not part of NIST PQC standardisation process, hence it does not have an official NIST security level.

Algoritm	L	Sk (byte)	Pk (byte)	Sg (byte)	Verif (ms)
ECDSA (secp256r1)	n/a	32	64	64	4.85
Dilithium-2	2	2528	1312	2420	2.21
Falcon-512	1	1281	897	666	0.44
SPHINCS+-SHA-256-128s-simple	1	64	32	7856	3.53
SPHINCS+-SHA-256-128f-simple	1	64	32	17088	10.02
XMSS-SHA2-10-256	n/a	36	64	2500	6.49

Table 3: Benchmarks on target platform (raw figures)

Algoritm	L	Sk	Pk	Sg	Verif
ECDSA (secp256r1)	n/a	1	1	1	1
Dilithium-2	2	~x79	~x21	~x38	~/2
Falcon-512	1	~x40	~x14	~x10	~/11
SPHINCS+-SHA-256-128s-simple	1	~x2	~/2	~x123	~x1
SPHINCS+-SHA-256-128f-simple	1	~x2	~/2	~x267	~x2
XMSS-SHA2-10-256	n/a	~x1	x1	~x39	~x1

Table 4: Benchmarks on target platform (ratio with baseline ECDSA)

Algoritm	L	Sk+Pk+Sg	RAM	Code	Verif
ECDSA 256 (HW accelerated)	n/a	1	1	1	1
ML-DSA-65 (full SW)	3	~x58	~x8	~x3	~x1

Table 5: Benchmarks on Cortex-M4 (ratio with baseline ECDSA)

5.7.12.3 Challenges

In this section, we list some challenges towards transitioning to post-quantum cryptographic algorithms.

Cryptographic algorithm specificities – First of all, the selected signature scheme will impact the whole update process, starting with the signature generation and verification operations (code footprint, RAM), the storage of the public key (memory) and the private key (management: storage, update, export), and the transmission of the signature (possibly at a massive scale over a wireless network). It is likely that the heavier burden will lie upon the verification side (e.g., a constrained end-device). However, the signing entity may also be deeply affected (e.g., management of the private key).

5.7.12.3.1 Hardware support

Leveraging a hardware accelerator for the main cryptographic operations involved in the signature scheme facilitates both the computation and the verification of the signature. The different schemes mentioned above (Dilithium, Falcon, SPHINCS+, XMSS, LMS) all make (an extensive) use of hash functions. Most of these algorithms rely upon widely deployed hash functions (but, maybe, Haraka for SPHINCS+). Therefore, such a hardware support should be available. However, the choice of the signature scheme must be done with this aspect as well into consideration.

5.7.12.3.2 Hybridization

This technique is required by several (not all) cybersecurity agencies if lattice-based schemes (Dilithium, Falcon) are deployed. On the one hand, such a mitigation to compensate for the lack of maturity will not be needed anymore once one gets more confidence on these signature schemes. On the other hand, the fast pace that this use case might require may not allow avoiding such a combination method. Hybridization implies in particular on the signature verification side more memory for code footprint (multiple verification algorithms) and storage of several public keys.

5.7.12.3.3 Secret internal state

The choice of stateful HBS algorithms impacts the signing infrastructure and the verification device. Stateful HBS schemes imply that a secret state must be protected and carefully updated on the signing entity side. Moreover, per NIST recommendation (SP 800-208), exporting the private keys is forbidden. As a consequence:

- on the signing side: this may lead to operational issues in case the private keys become unavailable for some reasons (e.g., HSM loss, server crash, …). This problem can be mitigated with proper deployment architecture, leveraging for instance an HSM cluster (more private key leafs than estimated need) on several sites (server crash);
- on the verification side: the solutions proposed by NIST imply either an increase of the length of the public key material, or to regularly update the latter. Another possibility could lie in sizing the algorithm to afford an extra number of private keys (in order to compensate for possible losses). But this results also in an increase of the signature size. All these methods may be problematic for constrained end-devices

due to their limited memory, or if the public key is embedded in immutable ROM or fuses for security reasons.

Note however, as already said above, that NIST will publish an SP 800-208 update to mitigate this concern.

5.7.12.3.4 Data immutability

For a lot of devices, the verification key for the signature scheme is in fuses. Although this immutability can be viewed as a security feature (as it restricts potential attack vectors associated with over-the-air updates), this means that there would be no real way to properly update to post-quantum algorithms the devices that are already in the field or being deployed in the near future. This impacts primarily the legacy systems.

5.7.13 Synergy with Internal Programs

Similar migration strategies can be applied to use cases that involve code or security parameter updates (e.g., constrained devices in IoT, automotive).

5.7.14 Synergy with External Programs

Similar as with internal programs.

5.8 Concealment of the Subscriber Public Identifier

5.8.1 Scope

Security of mobile communications essentially relies on a symmetric key K shared by the user equipment (UE) and the home network (HN). For the home network, selecting the right shared key K requires a first step where it unambiguously identifies the UE. In 3G and 4G networks, the UE sends either its permanent identifier, called IMSI, or a temporary one called TMSI or GUTI to allow such an identification. Ideally, UE would almost exclusively use TMSI but there are several reasons (such as a loss of synchronization between the UE and the HN) which may lead a TMSI-based identification to fail. In such cases, an alternative procedure consists in requesting the UE to send the IMSI directly. This backup procedure can easily be triggered by an adversary to trace UE owners.

This family of tracing attacks (usually referred to as “IMSI-catchers”) are prevented in 5G networks by the concealment of the UE permanent identifier (called SUbscription Permanent Identifier – SUPI) as defined in 3GPP TS 23.501 and 33.501. This concealment/de-concealment of subscriber Identity is today managed thanks to asymmetric cryptographic for key agreement, to derive secret key used for symmetric encryption of the ID.

This SUCI generation process, put in place in 5G, is then vulnerable to quantum threat. In this section, we evaluate the possible migration path to quantum resilience.

5.8.2 System Context

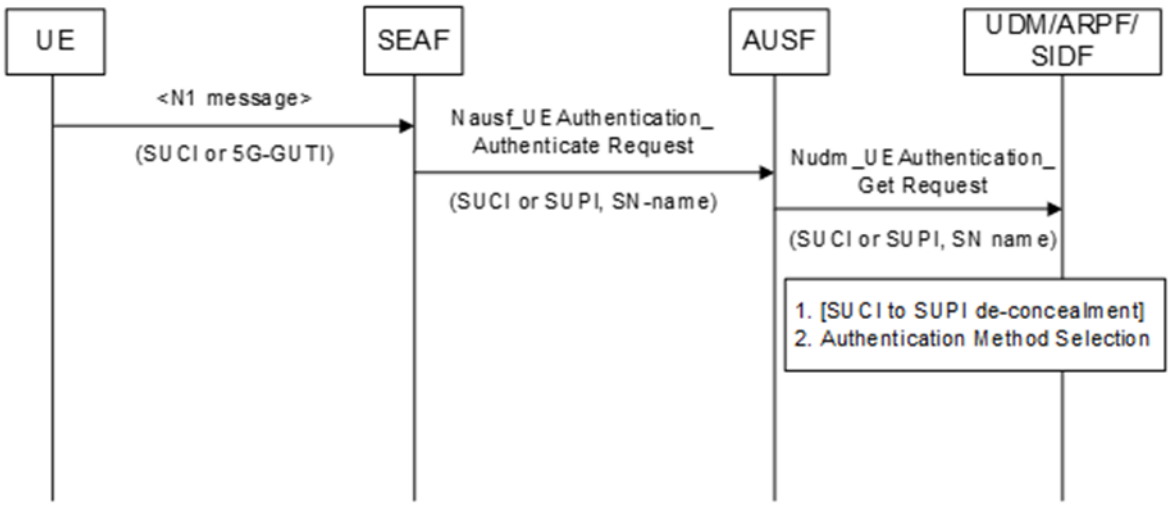


Figure 15: Initiation of authentication procedure and selection of authentication method (source 3GPP TS 33.501)

The UE does not transmit the SUPI in clear and is concealed to SUCI, a temporary identifier. The UE generates the SUCI and transmits to UDM for initial registration. Upon receipt of a SUCI, the subscription identifier de-concealing function (SIDF) located at the ARPF/UDM performs de-concealment of the SUPI from the SUCI. Based on the SUPI, the UDM/ARPF chooses the authentication method according to the subscription data

5.8.3 Sensitive Data Discovery

As specified in clause 5.9.2 of 3GPP TS 23.501, a SUPI may contain:

- an IMSI as defined in TS 23.003, or
- a network-specific identifier, used for private networks as defined in TS 22.261.
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316.
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316.

In 5G AKA the UE generates a SUCI using a protection scheme based on a home network public key. If the public key encryption scheme used were broken a user could be deanonymized. An attacker in possession of a HN public key could calculate the private key in advance of a connection, allowing immediate calculation of the SUPI encryption key when the UE public key is seen. In this case, the encryption scheme would offer no privacy protection for the subscriber.

An adversary able to un-conceal the SUbscriber Concealed Identifier (SUCI) is thus able to track the user in a similar approach to previous generations of Mobile Networks.

5.8.4 Cryptographic Inventory

As specified in clause 6.12.2 of 3GPP TS 33.501, the SUCI is generated using a protection scheme with the Home Network public key. This protection scheme is either the “Elliptic Curve Integrated Encryption Scheme” (ECIES) or one specified by the home network. In this document, we will only consider the case of ECIES.

The ECIES scheme is specified in [ECIES] but the Annex C of TS 33.501 introduced some minor modifications. From the cryptographic standpoint, this is a Diffie-Hellman key exchange between the UE (which generates an ephemeral key pair) and the home network (which uses a long-term public key already provisioned on the UE). The Diffie-Hellman key share is then used as an input to a key derivation function so as to generate an encryption key EK and a MAC key MK. Two profiles (profile A and profile B) are defined whose main difference lies in the elliptic curve parameters (curve 25519 vs secp256). In all cases, EK is used as an AES-128 key in CTR mode whereas MK is a 256-bit key used for HMAC-SHA-256.

5.8.5 Migration Strategy Analysis and Impact Assessment

Regarding the symmetric components of the ECIES protocol, we note that migration should be rather easy as MAC are already generated using 256-bit keys (which are deemed sufficient to withstand quantum computing) and as AES inherently supports 256-bit keys. Moving from AES-128 to AES-256 would then be the main change in this part of the specifications, along with the necessary adaptations of the key derivation function.

The main vulnerability of the ECIES protocol with respect to the quantum threat is actually the Diffie-Hellman key exchange step, regardless of the used profile. Although there is no drop-in Post Quantum replacement for this protocol, it is well-known that a Key Encapsulation Mechanism can achieve the same goal, namely share a common secret. In this respect, the future NIST standard ML-KEM seems to be the most suitable solution to protect SUPI against quantum computers.

The main remaining question is thus the one of the performances as moving to Post Quantum cryptography will increase the ciphertext size and change the nature of the computations. As the current version of the specifications allows the operator to decide whether the SUCI computation should be performed within the USIM or within the Mobile Equipment, there is no unique answer to this question. Arguably, the case where the USIM performs this computation may be the most challenging one given the constrained nature of the device.

5.8.6 Stakeholders

- SIM card manufacturers
- SIM card vendors
- Network Operators

5.8.7 PKI Implications

In the context of the concealment of the SUPI, there is only one public key, the one of the home network that is used in the ECIES protocol. This public key has been provisioned in the USIM and is not authenticated by any certificate. The way it is bound to the home network identity thus does not rely on usual cryptographic means but on the properties of the

provisioning and the updating procedures. As mentioned in clause 5.2.5 of TS 33.501, these procedures are out of scope of these specifications. Therefore, there is no direct PKI implications for this use-case, but one must obviously ensure that the procedures mentioned above are consistent with the targeted Post Quantum security of SUCI.

5.8.8 Legacy Impact

Interestingly, the situation of 5G networks in presence of an adversary equipped with a CRQC is extremely similar to the one of previous generations of networks. Put differently, a CRQC simply reinstates IMSI-catchers in 5G networks.

The threat of IMSI-catchers has not led to modifications of legacy systems (the generations of networks prior to 5G). Back then, the risk was accepted, and remediation was postponed to 5G. It is therefore likely that the quantum threat will not lead to changes in current systems using ECIES.

5.8.9 Dependencies

5.8.9.1 Standards

3GPP TS 23.501 and 33.501

The publication of NIST standards to define PQC algorithms. In practice these are being treated as FS dependencies by many other groups

5.8.9.2 National Guidelines

The publication of national guidance on the use of PQC.

The publication of national standards for sovereign PQC algorithms, if required.

5.8.9.3 Vendors

ME and USIM vendors. We note that for legacy UEs, there is no SUCI mechanism. Therefore, the permanent identifier hiding only affects 5G and future terminal devices.

UDM with associated HSM vendors if HSM is involved in deployment

5.8.9.4 Operators

As 3GPP specifications may take time to be updated, and as it allows the operator to select its own protection scheme (which implies that PQC implementation does not depend on the evolution of the 3GPP TS 33.501 specification), a transition path for operators can be to agree on Post Quantum protection scheme and security profile, and ask vendors to implement it in UDM and UE or USIM sides

5.8.9.5 LEAs

LEAs need to know SUCI/SUPI association. SUPI de-concealment is managed by UDM. There’s no direct dependence with LEAs

3GPP 33128 – Security, Protocol, and procedures for Lawful Interception specifies the handover interface with LEA, for SUCI/SUPI association

5.8.9.6 Performance

There is no requirement, in 3GG standard, on SUPI concealment/De-concealment performance.

5.8.10 Gantt Chart for PQC Migration

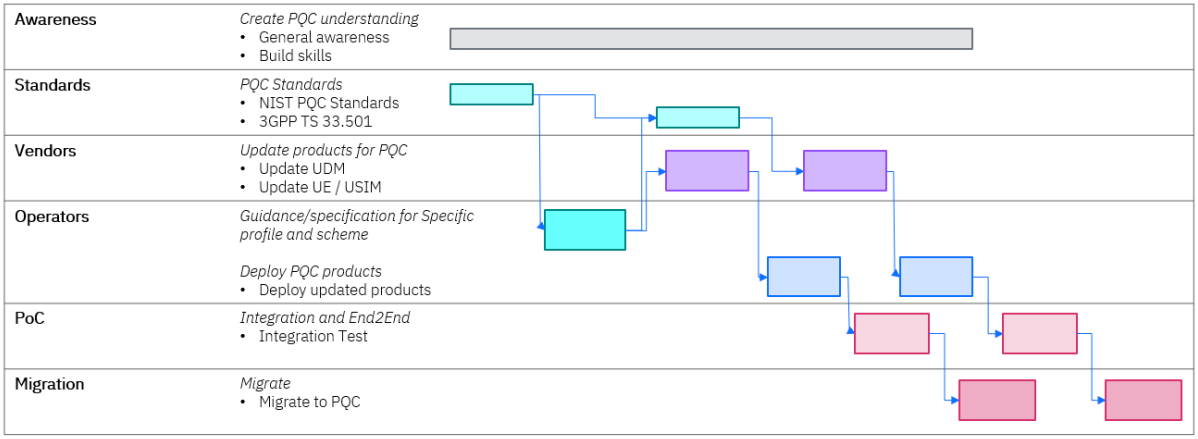


Figure 16: Gantt Chart for PQC Migration

5.8.11 PQC Migration Process Description

Ultimate target is the implementation of new updated 3GPP TS 23.501 and 33.501 specifications. 3GPP is then expected to standardize new protection scheme, with updated Profiles.

These new 3GPP specifications may be issued in steps:

1. Considering Hybridization between PQC and classic ECC based key exchanges algorithms. This step is allowing to mitigate maturity level of new PQC algorithms and keep same protection level against classic computers
2. Considering Full PQC replacement of classic ECC based cryptography for Key exchange, once PQC algorithm maturity will have been proven.

Let's figure out what could be step 1 above (which is described in gant chart above):

3GPP standard may have a first step with hybridization, and then specifying a security profile, derived from Profile A or Profile B (described in annex C 3.4.1 of 3GPP TS 33.501), with following updates:

- 'Post Quantum Cryptography' field for specifying a KEM algorithm. ML_KEM (Level 3 for matching embedded resource constraints, and which is recommended by security agencies such as ANSSI or BSI, with hybridization with classic asymmetric key exchange) would be, at the time we write the document, the proposed option. NIST is expected to standardized other KEM algorithms out of NIST round#4 but that will be likely standardized in coming years.

  This update would allow to tackle the main vulnerability of the ECIES protocol regarding quantum threat, which is the Diffie-Hellman key exchange step. Indeed

hybridization for key exchange, leveraging a KDF (Key Derivation Function), between Diffie-Hellman key exchange and KEM key exchange.

- Passing encryption to AES_256 for 'ENC' field, and then specifying 'maclen' and 'enckeylen' to 32 bytes

This conservative update would allow to tackle potential risk with respect to quantum computer against AES_128.

To illustrate specification proposed update, we focus below on UE/USIM side.

From the cryptographic standpoint, this is a Diffie-Hellman key exchange between the UE (which generates an ephemeral key pair) and the home network (which uses a long-term public key already provisioned on the UE). The Diffie-Hellman key share is then used as an input to a key derivation function so as to generate an encryption key EK and a MAC key MK

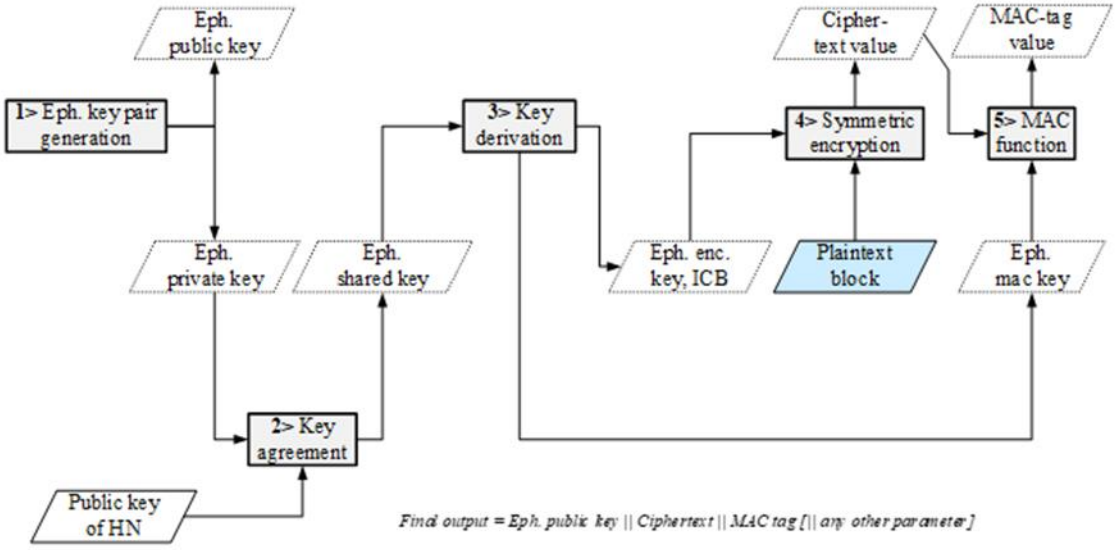


Figure 17: 3GPP TS 33.501 current key agreement procedure

Proposed update for Post Quantum resilience:

PQC key encapsulation is performed and hybridization with ECC based key exchange is performed thru Key Derivation Function. Note that security level enhancement could be done by providing cipher texts from PQC KEM and classic Key agreement as inputs to Key Derivation Function.

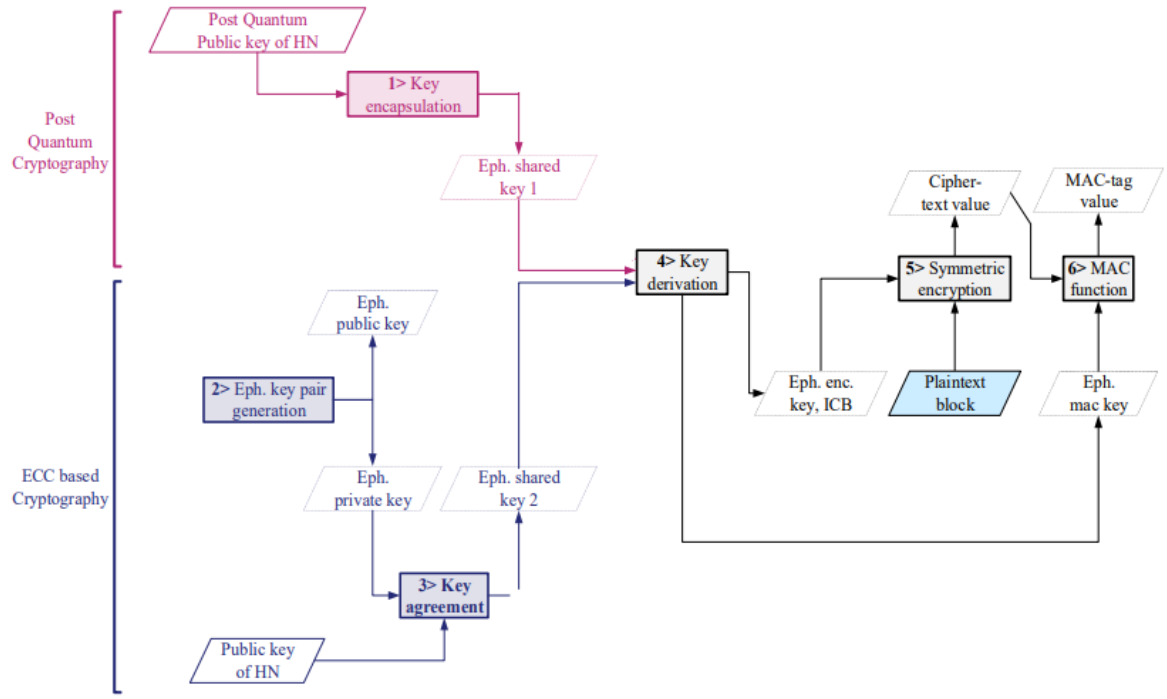


Figure 18: 3GPP TS 33.501 key agreement procedure update option

As 3GPP specifications may take time to be updated, and as it allows the operator to select its own protection scheme (which implies that PQC implementation does not depend on the evolution of the 3GPP TS 33.501 specification), a transition path for operators can be to agree on Post Quantum protection scheme and security profile, and ask vendors to implement it in UDM and UE or USIM sides, leveraging hybridization. This intermediate potential path is described in Gantt chart above, prior to 3GPP standardization.

NIST incoming standard FIPS 203 in 2024 will allow to define a PQC security scheme, either for 3GPP TS 33.501 specification update, or to define a specific protection scheme and profile outside 3GPP TS 33.501.

The proposal above requires no change to the traditional SUPI encryption method and infrastructure. An alternative path forward is to update the traditional component to HPKE [RFC 9180] (in its unauthenticated version), which provides stronger and more modular security properties and uses more modern underlying primitives than ECIES. This approach would then enable a smoother transition to hybrid PQC via use of hybrid components inside HPKE [HPKE-Kyber-draft], and furthermore this approach would allow a smoother transition from hybrid PQC to pure PQC in the future.

5.8.12 Synergy with Internal Programs

Other programs requiring PQC KEM capabilities implementation, that could be on back-end side (e.g leveraging HSM upgrade with KEM capability if HSM is involved) or UE/USIM side (e.g leading to need for PQC KEM at the far edge)

In this Use Case, there's no dependency with PKI, which simplifies the migration process.

5.8.13 Synergy with External Programs

The most likely synergy is with national cybersecurity initiatives including PQC.

5.9 Authorization and Transport Security in 4G (MME-S-GW-P-GW)

5.9.1 Scope

IPsec (NDS/IP) may be used to protect IP-based control plane signaling and to support the user plane protection on the backhaul link (see 3GPP TS 33.401). The IKEv2 protocol is used to perform authentication and key establishment for IPsec.

Key establishment in IKEv2 is done using ephemeral (elliptic curve) Diffie-Hellman key exchange, and the result is an ephemeral session key that can be used for data protection in IPsec. Best practices recommend re-running Diffie-Hellman key exchange to generate fresh ephemeral session keys frequently (e.g. every 100GB or every hour). The 3GPP data protection profiles in IPsec uses symmetric cryptography such as AES-128 and SHA-256. However, the exact quantum security of AES-128 is still under debate; see Section 3.6.

> NOTE: Their security strength against quantum (and classical) attackers is used to define the relevant security levels in the NIST PQC standardization.

Authentication in IKEv2 is done using digital signatures, directly in the protocol and in certificates.

An attacker can target the individual ephemeral Diffie-Hellman keys (i.e., a harvest now, decrypt later attack) and breaking the keys would impact the confidentiality of the recorded session data protected under that key. The risk and impact thus depend on for example the feasibility of encrypted traffic being collected today, the risk of session keys being targeted by such an attacker, and the confidentiality protection lifetime of the data. If we instead consider authentication, then if the IKEv2 protocol or underlying PKI is still accepting currently deployed digital signatures (e.g., ECDSA, RSA), an attacker who holds a CRQC can break digital signature keys and for example impersonate the respective nodes in NDS/IP.

5.9.2 System Context

In order for the NE, to be able to authenticate one another before a secure connection can be established, digital certificates will have to be mutually authenticated and validated. For RSA certificates, the public key length must be at least 2048-bit. For ECDSA certificates, the public key length must be at least 255-bit. A public key length of at least 384-bit may be supported as well.

Certificate Management Protocol v2 (CMPv2) is the protocol of choice for providing certificate lifecycle management capabilities for the SEG, and the NE.

Secure connections between NDS/IP end entities are established using IKE on the Za interface. The certificates used is expected to support ecdsa-with-sha256 and may support ecdsa-with-sha384, or support RSASSA-PSS with SHA-256.

5.9.3 Sensitive Data Discovery

As discussed in TS 33.401 Section 11, S3, S6a and S10 interfaces may carry sensitive subscriber specific data that requires confidentiality protection. Store now, decrypt later attacks may thus be a relevant threat for this data. TS 33.401 does not specify specific time frames for which the data must be protected. Authenticity and integrity of control plane signaling is critical for network operations.

5.9.4 Cryptographic Inventory

All public-key cryptography that is currently standardized for use in IKEv2 is vulnerable to CRQCs.

5.9.5 Migration Strategy Analysis and Impact Assessment

As implementations start supporting PQC according to the implementation roadmap in the next section, new nodes can negotiate to use the new quantum-resistant algorithms. Legacy nodes will need to be updated to support negotiating the new algorithms.

5.9.6 Stakeholders

- Network operators
- Vendors of transport equipment
- Vendors of security gateways
- Vendors of PKI systems
- 3GPP
- IETF

5.9.7 PKI Implications

As discussed in Section 4.9.5, quantum-resistance for this use case requires migration to quantum-resistant PKI. For more information about quantum-resistant PKI, see the planned [PKI implications document].

5.9.8 Legacy Impact

Legacy nodes will need to be updated to support negotiation of new algorithms. Any legacy node that is not updated to support PQC in a timely manner suffers the risks that are discussed in Section 4.9.6.

5.9.9 Dependencies

5.9.9.1 Standards

Relevant standards include, PKI and certificate life-cycle management protocols, such as Certificate Management Protocol (CMPv2), that uses X.509 certificates as described in RFC 4210. IP Security (IPsec) provides confidentiality, data integrity, and data source

authentication to IP datagrams. Establishing a shared state in a manual fashion does not scale and therefore a protocol that is used to establish the shared state dynamically was needed. The Internet Key Exchange (IKEv2) protocol, specified in IETF RFC 7296 is used for performing mutual authentication and establishment of that shared state, also referred to as Security Associations (SA).

5.9.9.2 National Guidelines

There may be efforts carried out by Alliance for Telecommunications Industry Solutions (ATIS) in addition to NIST guidelines for using PQC/ Hybrid schemes for IPSec, IKE interactions and the PKI infrastructure.

5.9.9.3 Vendors

Based on the evolution of IKEv2 / IPSec standards to support PQC algorithms within IETF, and further inclusion of those standards within 3GPP, would enable vendors to implement PQC support.

5.9.9.4 Operators

As the use of 4G systems reduces over time, and complete migration to 5G happens, the return-on investment for PQC support within 4G will have to be justified. The interfaces, that carry 4G subscriber data as well as security keys will have to be protected to mitigate against “harvest now decrypt later” type attacks that could potentially compromise a 4G subscriber’s privacy. In the near-term, operators may choose to use Hybrid schemes for only those interfaces that are deemed to have a higher risk profile (e.g. eNodeB to SEG).

5.9.9.5 LEAs

The LI interfaces (e.g. from the operator network to the LEA) is generally protected using SEG via IPSec. A migration plan needs to be in place in order that the relevant interfaces are protected from tampering as well as eavesdropping type attacks. To that extent, PQC capable PKI that is a mutually trusted third-party will have to be used as a trust anchor.

5.9.9.6 Performance

The main impact would be on the SEG to be able to request and manage the PQC certificates. The SEG would have to implement ML-KEM as well as ML-DSA and therefore impacts performance during the IKE/IPSec SA setup process. Since symmetric cryptography based on AES-256 and SHA-256 are used for encryption and integrity protection of the control and user plane traffic respectively, there is not going to any additional impact.

5.9.10 Gantt Chart for PQC Migration

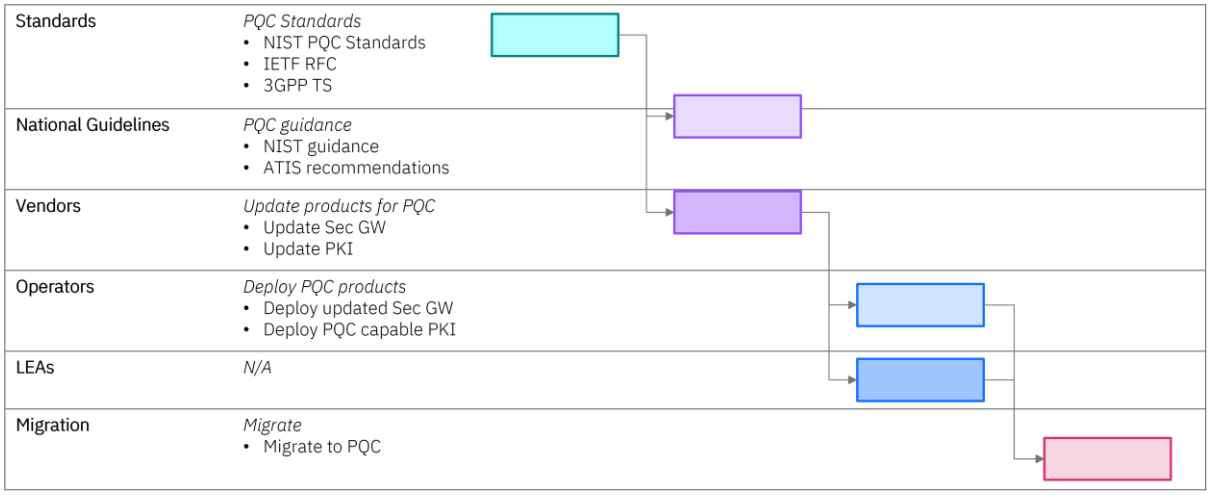


Figure 19: Gantt Chart for PQC Migration

5.9.11 PQC Migration Process Description

Protecting site-to-site communications (4G core to 4G RAN as well as core to core) and between core networks will have to be carried out using IPSec SEG that support PQC algorithms for digital signatures, as well as for key agreement. PQC capability within IKE will have to be leveraged to setup the IPSec connections. Initially supporting hybrid schemes and later on solely using PQC mechanisms.

Initially, a hybrid PKI that is set up with non-backward-compatible hybrid certificates (composites) and then a dedicated PKI that is capable of issuing and managing PQC certificates that are issued to SEG as well as to network entities (e.g. eNodeB / base station) will have to be in place. Post-Quantum / Traditional composite key signature algorithms suitable for use within X.509 protocols. These composite algorithms combine ML-DSA with RSA, and ECDSA.

Similarly, PQC support within IKEv2 will have to be standardized in order that PQC / Hybrid certificates can be used for mutual authentication using either ML-DSA or using composite signatures respectively. Using ML-KEM for key agreement for establishing the IPSec SAs, like the approach in the IETF draft proposal: draft-kampanakis-ml-kem-ikev2-03.

5.9.12 Synergy with Internal Programs

Internals synergies include efforts for securing site-site connections within an operator network as well as enterprise network connectivity using Security Gateways / VPNs.

5.9.13 Synergy with External Programs

IETF PQC standardization.

5.10 Authentication and Transport Security in 5G: Quantum Safe TLS between Components of 5G Core Network (SBA)

5.10.1 Scope

5G core network SBA stands for service-based architecture, where network functions (e.g. AMF) within the Control Plane enables other authorized network functions to access their services. This representation also includes point-to-point reference points where necessary [3GPP TS 23.501]. For security of 5G Core Network (SBA), According to [TS 33.501], all network functions shall support mutually authenticated TLS and HTTPS. The identities in the end entity certificates shall be used for authentication and policy checks. Network functions shall support both server-side and client-side certificates. TLS client and server certificates shall be compliant with the SBA certificate profile specified. The N32 security between PLMNs could be achieved using mutual-TLS for direct operator interconnectivity, or PRINS when there are intermediaries between operators.

The scope of this use case focuses on the Control Plane of the 5G system and analyses the approach of quantum-safe transport layer security (TLS) between different network functions of 5G service-based architecture (SBA). It covers both the intra and the inter-PLMN components of the 5G SBA.

5.10.2 System Context

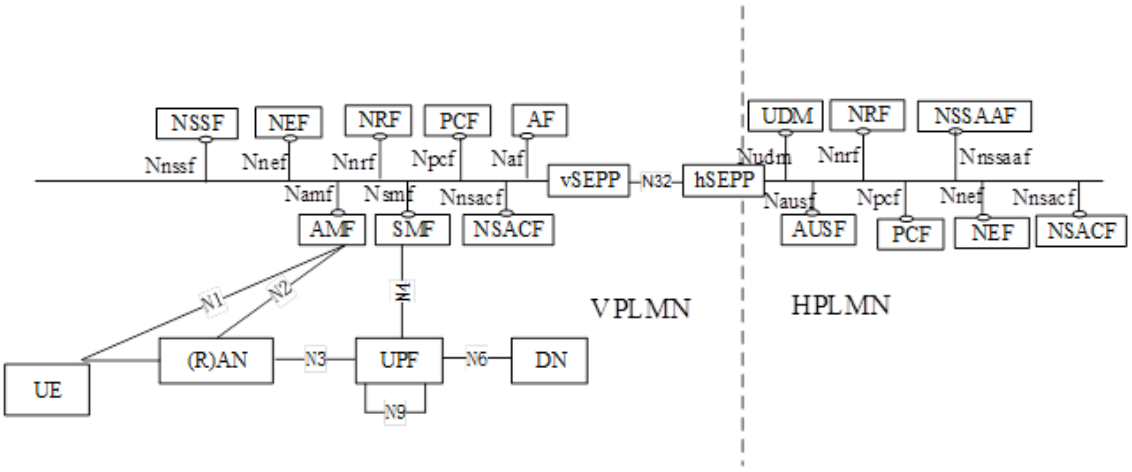


Figure 20: 3GPP Roaming 5G System architecture- local breakout scenario in service-based interface representation

Above Figure shows a typical architecture of 5G core with the VPLMN and HPLMN. The TLS is required to be adopted in all SBI between the network functions inside the PLMN as well as the N32 interface between vSEPP and hSEPP. And It is up to operator's implantation, TLS may be also adopted for non-service-based interface such as N4 and N9.

For the preceding interfaces, the quantum-safe TLS protocol needs to be used. As mentioned in the overview, the main vulnerability of TLS is the key exchange protocol. Because of network functions is relatively fixed, pre-shared keys may be used to solve this problem by operators implantation, but additional management costs may be required.

For interfaces between the gNodeB and the 5G core network, using the N2 interface with the AMF or the N3 interface between the gNodeB and the UPF, the links are protected using IPSec or DTLS. Similarly, the interfaces between the 5G core components as well as the 4G

core components are expected to be protected using IPSec. The N26 interface is used between the MME in the 4G core and the AMF in the 5G core when performing a 4G/5G handover. The N26 is expected to be protected using IPSec.

5.10.3 Sensitive Data Discovery

All mandatory and recommended TLS cipher suites use ECDHE or DHE for key agreement. An adversary can decrypt, spoof or tamper with the sensitive data communicated over the SBI or N32 interfaces by following a store-now-decrypt-later attack.

An example of sensitive data is the subscription information that is stored in the Unified Data Repository (UDR). UDM offers services that provide subscriber's information to other network functions such as AUSF, AMF, SMF, SMSF when requested. The UDM services transmit subscriber's SUPI/SUCI, Access and Mobility Subscription Data, SMS Subscription Data, Slice Selection Subscription Data, Location services (LCS) Privacy Data etc. [3GPP TS 23.502], to the NF consumers over the interface.

The N26 interface between the MME and the AMF carries the Non-Access Stratum (NAS) security context including the KNASint and KNASenc keys that are used for providing integrity protection and encryption respectively to the NAS messages.

The N2 interface is used by the AMF to carry the Access Stratum (AS) security context of the UE to the gNodeB. The security context carries the key KgNB, out of which derivative keys (e.g. RRC and UP integrity and encryption) keys are generated by the gNodeB.

Hence, it is necessary to secure the interfaces from next-generation attacks.

5.10.4 Cryptographic Inventory

Network Functions in the 5G architecture support TLS. Within a PLMN, TLS shall be used unless network security is provided by other means [3GPP TS 33-501]. Both client and server-side certificates are supported by the Network Functions. The certificates shall be compliant with the SBA certificate profile specified in clause 6.1.3c of [3GPP TS 33.310]. The Table 1 shows the profiles for the TLS used in the N32 and SBI interface.

No	Interface	Secure communication	TLS Profiles	Quantum vulnerable algorithms
1.	N32 (hSEPP - vSEPP)	N32-c: TLS1.2\1.3	TLS 1.2 cipher suites (mandatory): TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 signature algorithms (supported): ecdsa, rsa_pss_rsae, ecdsa_secp384r1_sha384 Diffie-Hellman groups: For ECDHE: secp256r1, secp384r1	AES 128 (possibly weak), ECDHE, DHE, ECDSA, RSA, SHA256

			For DHE: Diffie-Hellman groups of at least 4096 bits should be supported	
2.	SBI (NF - NF)	TLS1.2\1.3	TLS 1.3: signature algorithms (supported): ecdsa_secp384r1_sha384 Diffie-Hellman groups: Key exchange with secp384r1 should be supported	

Table 6: TLS Profiles for SBA interfaces (as specified in [TS 33.210])

We focus on migrating the latest version of TLS 1.3 [RFC 8446] to PQC in this section.

5.10.4.1 Key Exchange

There are several options for quantum secure key establishment listed as follows:

- Pre-shared key (PSK): The pre-shared keys are symmetric keys that are shared between the parties prior to communication. The size of Pre-shared key may be at-least 256-bit to be quantum-safe [ANSSI22, BSI-2023] and avoid the store-now-decrypt-later attack. If more than two parties are involved in communication then key distribution and key management is a tedious and complicated task that requires several interaction for peer-to-peer key establishment.
- Stand Alone PQC: Employing cryptographic algorithms that are secure against a quantum computer attack. NIST has been in the process of standardizing these algorithms and they are in the early stages of implementation. Hence, implementation experience is currently limited.
- Hybrid Key Exchange: Hybrid approach is defined as using more than one key exchange algorithm (two or more) and combining the result of these multiple algorithms [IETF-TLS-hybrid]. The PQC, or ECC can be combined to achieve a hybrid key exchange. so that security is achieved even if one of the algorithms is insecure.

Note: The Hybrid key exchange with PQC+ECC is most suitable and widely accepted solution, as it provides better security compared to stand alone PQC. Standard bodies like ETSI and Information Security Office, like BSI of Germany [BSI-2023], and ANSSI of France [ANSSI-23] support the use of Hybrid Key Exchange algorithms.

In addition to providing security, use of hybrid approach in TLS 1.3 must also satisfy the following performance features:

- Compatibility: The network components in the SBA that employ hybrid approach must also be compatible with components that are not hybrid aware. If both the NF service producer and NF service consumer are hybrid aware then they generate hybrid shared secret key. If either of them is not hybrid-aware i.e., either NF-producer or NF service consumer then the entities must generate a traditional shared secret. If either

of them are non-hybrid entities then the other should be able to downgrade to establish a shared secret using a single key exchange algorithm.

- Latency: The hybrid key exchange algorithms should not increase the latency while communicating with the entities. Latency should fulfil the requirements of specific scenarios. If the scenario is sensitive to latency then hardware accelerators can be used.
- Round Trips: The use of hybrid algorithms should not lead to additional round trips for negotiation or protocol communication.

5.10.4.2 Digital Signature

One of the approaches of digital signature to migrate to Post Quantum Cryptography is employing the composite signature [IETF dr-ounsworth] that comprises of multiple signature schemes i.e., one may be based on traditional cryptography e.g., RSA and another on Post Quantum Cryptography e.g., ML-DSA. The composite signature generation process uses private keys of each of the signature component algorithm to generate a component signature value on the input message. The individually generated signatures are then encoded as per the corresponding algorithm component specification to obtain the final Composite Signature Value. The verification process of the final Composite Signature Value consists of applying each component algorithm's verification process according to its specification using the public keys.

5.10.5 Stakeholders

- Equipment manufacturers
- Virtualization cloud-based infrastructure providers
- Operators

5.10.6 PKI Implications

The SBA certificate profile depends on the end-point of the communication entities and whether the communication is inter-domain or intra-domain, direct or indirect . The end points may be NF producer, NF consumer, SCP, or SEPP.

The root CAs and intermediate CAs generating and managing the keys and certificates need to be migrated to a Quantum Safe solution, taking into consideration aspects such as backward compatibility and interoperability

5.10.7 Legacy Impact

For the hybrid modes of the key exchange and the digital signature the clients and servers should be compatible with the end entities that are yet to migrate to employing multiple protocols and quantum-safe algorithms.

5.10.8 Dependencies

5.10.8.1 Standards

TLS 1.3 specified in RFC 8446 [X3 supports three basic key exchange modes, which processes cryptographic negotiation by the client in its ClientHello. Three key exchange mode is as following:

- (EC)DHE (Diffie-Hellman over either finite fields or elliptic curves)
- PSK-only (Pre-shared key only)
- PSK with (EC)DHE

During the key exchanges, TLS has two post-quantum vulnerabilities that need to be considered: (EC)DHE mode and PSK with (EC)DHE.

For quantum security, the standard for TLS may need to be updated, for example by adding to support quantum-safe key exchange mechanism.

5.10.8.2 National Guidelines

National guidelines should be consulted to ensure that any recommendations or regulations are followed appropriately.

5.10.8.3 Vendors

Vendors should consider a plan for products upgrade route according to the timeline of the quantum-safe TLS protocol and 3GPP profile of protocols standardization, to ensure the smooth upgrade towards quantum-safe capabilities.

5.10.8.4 Operators

Core network (SBA) may need be scanned any vulnerabilities of the equipment/network function with penitential quantum risks.

Identified quantum vulnerabilities shall be analysed or classified to determine whether they arise from specifications or from inherent product functionalities or configurations (i.e., unrelated to standards)

Based on the above vulnerabilities' analysis and classification, any potential tasks can be identified and developed a PQC migration plan such as the timeline and the strategy to influence relevant standard bodies, product upgrade requirements to integrate protocol (e.g., TLS, Oauth2.0) and multi-vendor products interoperability testing, etc.

5.10.8.5 Performance

The security establishment performance of the TLS may be affected. However, the performance impact may be minimal because Quantum migration mainly affects the TLS connection establishment phase and NF connections on the core network are not frequently updated. In terms of transmission phase, currently the 128-bit symmetric key algorithm is used for TLS transmission encryption. If the key length is increased to a larger value (e.g., 256 bits), the TLS transmission performance may be affected.

5.10.9 Gantt Chart for PQC Migration

The purpose of the Gantt chart is to communicate how dependencies interrelate.

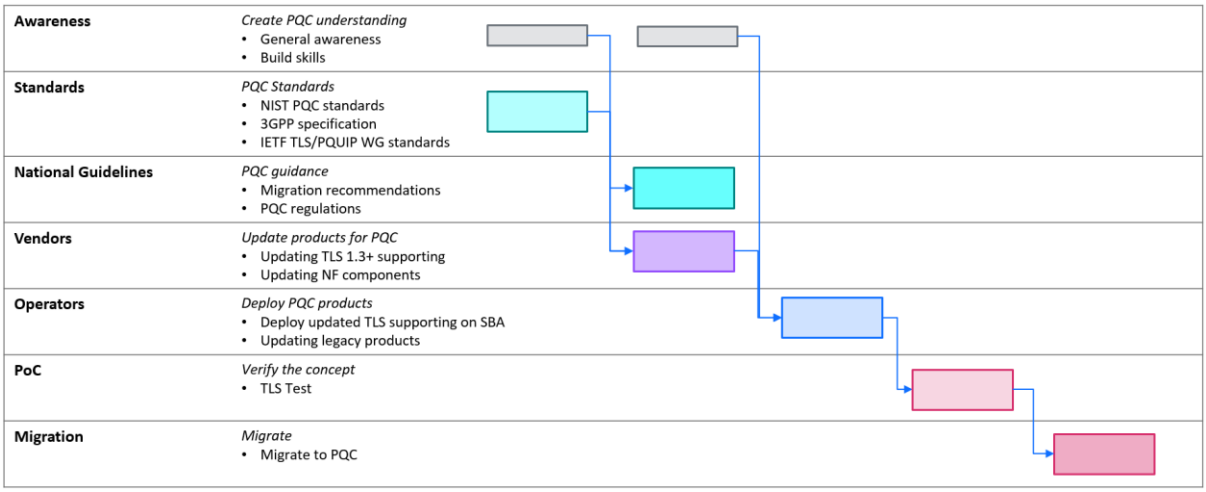


Figure 21: Gantt chart for TLS PQC Migration

5.10.10 Description

As mentioned in the overview, the main vulnerability of TLS is that the symmetric key exchange before the TLS security establishment. Therefore, in TLS1.3, non-exchange key has been considered in TLS process, i.e., using PSK-mode for key negotiation. From the current view of perspective, operators may need to consider using PSK-mode as the security establishment between the TLS client and server in SBA architecture to give quantum resilience. It should be noted that PSK-mode may require additional key management and processing costs to pre-configure TLS keys. Also, the PSK mode is not supported in some earlier TLS versions. Therefore, operators may need to upgrade the TLS to a newer version (for example, TLS 1.3) to support the PSK-mode.

Beyond the existing TLS specifications, Operator can also consider post-quantum cryptography after the product provided by the vendor supports post-quantum algorithms. New TLS extension specifications are also under discussion. For example, the key exchange protocol in the TLS protocol may be replaced with an algorithm that resists a quantum attack. The potential algorithm could be a hybrid mechanism. For example, the key encapsulation mechanism (KEM) could use to replace the key exchange protocol in TLS in SBA. These tasks have been mentioned in the IETF draft [X3].

5.10.11 Synergy with Internal Programs

Within the operator environment, Fine-grained coordination is required between groups regarding coordination of TLS version upgrades and new version for TLS. In particular, scan all the places where TLS maybe deployed in the 5G core, because TLS may be widely used in all SBI and part of non-SBI interfaces in 5G core.

5.10.12 Synergy with External Programs

Synergy with national cybersecurity initiatives and recommendation including PQC.

Synergy with IETF PQUIP, coordinate and discuss to avoid any conflicts about the migration plan.

Synergy with vendors about the operator migration plan, which will affect the product development of vendors in advance.

5.11 Use Case: Virtual Private Networks

5.11.1 Scope

Virtual private networks (VPNs) enable secure private communication channels over public networks. These private networks are widely deployed in mobile telecommunication networks, forming a core component of the security apparatus utilised across many contexts. For example, VPNs are used to secure connections between base stations and security gateways, to securely connect different network functions within the 5G service-based architecture (SBA), during remote SIM provisioning, to facilitate firmware updates and device management, to secure data in transit when using Cloud infrastructure and to enable secure connections for customers.

There are different protocols for creating virtual private networks, depending, for example, on whether the security association occurs at the network layer, the transport layer or the application layer. Common elements in VPN operation include:

- a handshake, during which authentication occurs and a shared secret is established
- data exchange, which provides confidentiality by leveraging the shared secret to symmetrically encrypt the data to be shared.

The precise details of the protocol depend on the VPN type and the usage context. For example, a VPN established at the transport layer via TLS for an https session may only require the user to authenticate the server, whereas a VPN between two corporate sites typically requires mutual (i.e., two-way) authentication. As concrete example, VPN protocols such as IPSec use IKE, which commonly uses a Diffie-Hellman exchange to establish a security association, and RSA or EC digital signatures for authentication. The security assurances of DH exchanges and digital signature schemes such as RSA and ECDSA, both rely on the assumed mathematical hardness of the discrete log problem or finding prime factors. Both problems are vulnerable to quantum attacks via Shor's algorithm. Accordingly, VPN protocols leveraging such algorithms are quantum vulnerable and are within scope of the present work.

5.11.2 Sensitive Data Discovery

VPNs carry encrypted data which may have long-lived security needs. This in-transit data constitutes a primary source of potentially sensitive data for the VPN use case. Although the symmetric encryption method employed to encrypt the data may not be particularly sensitive to quantum attacks, the methods used to establish a shared secret key may be vulnerable. Hence, an adversary could harvest and store VPN traffic now and leverage a quantum computer in the future to access the shared secret key. Once this key is attained, the transmitted data can be decrypted. Accordingly, it is important that telcos identify where VPNs are used internally to transmit sensitive data with long-lived security needs and offer VPN products which meet the needs of customers with long-lived data security requirements. Private keys, used to establish the secure VPN connection, must also be securely stored and used, though this falls under the scope of PKI.

5.11.3 System Context

VPNs are a key component of modern electronic communications and enable confidential, authenticated communication between devices. Accordingly, VPNs are widely deployed; for example, VPNs provide secure communication channels between corporate offices, achieve connectivity for remote workers, enable the remote provisioning of servers, and avail secure connections for online customers. Due to their ubiquity, the migration of VPNs will be a major component of the larger migration to quantum safety. As example, in a telco context, VPNs enable secure connections between base stations and security gateways, so migrating the underlying VPNs will be a key component of migrating the BS-SecGW link.

5.11.4 Cryptographic Inventory

VPNs typically use cryptographic methods for authentication, establishing a shared secret, and encrypting transmitted data. A cryptographic inventory should cover each of these aspects, describing properties such as the protocols used, the digital signature options used/available for authentication, and available options for sharing a secret and encrypting the data. The primary quantum vulnerabilities for VPNs relate to the authentication and secret-sharing procedures. For the purpose of planning a migration to PQC, it is therefore important that these aspects are covered by the inventory. Although symmetric encryption algorithms are less vulnerable to quantum attacks, they typically have different security options, relating to choice of key-size, which is influenced by the security demands of the context. Including this information in the inventory may also prove useful.

With regard to the most pressing security threat posed by quantum computers, namely the harvest now, decrypt later attack, identifying the methods used for establishing shared secrets may be considered the highest priority. Accordingly, a cryptographic inventory should, as a minimum, identify such mechanisms, as used by the VPN protocol.

Unlike the mechanism of shared secret establishment, which directly impacts the future security properties of a VPN session (i.e., after the session has ended), authentication protocols may only need to remain secure for the duration of a session. Hence, the consequences are typically less severe if an adversary attacks an authentication protocol after the session terminates. Signature schemes used during authentication will ultimately need to be migrated to a quantum safe status. Consequently, it will be beneficial to include both authentication and secret establishment data in the cryptographic inventory, even if an organisation decides to transition key establishment mechanisms to quantum safe status prior to transitioning digital signature schemes.

Operators will also benefit from determining where pre-shared secrets are employed in VPNs since symmetric encryption keys that derive from such pre-shared secrets are not expected to be vulnerable to attacks using Shor’s algorithm.

5.11.5 Migration Strategy Analysis and Impact Assessment

Sensitive long-lived data reliant on the confidentiality assurances of a VPN will remain susceptible to the harvest now, decrypt later attack if the VPN protocol is not upgraded to quantum safe status. As mentioned, VPNs are widely deployed in the telco context, including internal usage for enterprise purposes (e.g. connecting corporate offices to each other and

to remote workers), usage for establishing secure network services (e.g., connecting base stations to security gateways), and usage by enterprise customers to facilitate business functioning. Since confidentiality is a key security function offered by VPNs, and VPNs are so widely deployed in the telco context, the impact of breaking this confidentiality assurance by a quantum attack could be significant, both to telcos themselves and their customers. Migrating to a quantum safe method of establishing shared keys used within VPNs therefore has strategic importance for both an organisation and any customers who rely on confidentiality assurances provided by the organisation's products and services.

5.11.6 Implementation Roadmap (Crypto-agility and PQC Implementation)

VPNs operate according to protocols such as IKEv2/IPSec, TLS and SSH. These protocols are typically specified by standards bodies and vendors are responsible for providing hardware and software that enables the execution of these protocols.

An early priority for VPN migration is to ensure that VPN protocols use a quantum secure mechanism to establish shared secret keys. This means migrated VPN protocols should either rely on pre-shared secrets or leverage a PQC KEM selected by a standardisation body such as NIST. Two important aspects for consideration in this migration are crypto-agility and the use of hybrid modes.

Crypto-agility refers to the ability of an implementation to easily replace or switch algorithms when required. The need for such a replacement in the VPN context may arise if, e.g., a security flaw is discovered in a less mature PQC algorithm. Adhering to a principle of agility ensures that disruptions caused by such security breaks are minimised and more easily managed.

Hybrid cryptographic modes combine PQC cryptography with a traditional method. For example, hybrid establishment of a shared secret in a VPN context could involve generating two shared secrets, one via a PQC KEM such as ML-KEM, the other via a traditional Diffie-Hellman exchange. These two secrets can be jointly employed to derive the shared symmetric key, perhaps via a key derivation function. This approach ensures that, even if a security flaw is discovered in the PQC algorithm, the data remains protected by the traditional approach (though it would lose its PQC security assurance). It also facilitates the early implementation of PQC algorithms while maintaining compliance with existing standards – since the traditional method is also used, compliance with pre-PQC standards remains assured.

Telcos and their customers employ VPNs in a variety of contexts and across many devices and components. For example, remote access VPNs, used by remote workers to connect to corporate networks, may connect many different device types. Similarly, VPNs connecting base stations to security gateways may involve many different base stations. Consequently, the implementation roadmap for the large-scale cryptographic transition required to achieve Post Quantum Safe may involve staged rollouts. During such a staggered transition, it is important that newer or updated systems can function properly when communicating with older or yet-to-be-upgraded systems. Namely, when establishing a shared secret, upgraded PQC-capable systems should be able to negotiate a shared secret via a non-PQC/traditional mechanism when communicating with non-upgraded components/devices. Accordingly,

backwards compatibility is an important consideration during the migration process and when planning the implementation roadmap.

As noted, the use of pre-shared secrets can also form a viable part of a VPN migration strategy. Such an option may be preferable when the more-flexible functionality of a KEM is not essential or when PQ security is essential, but it is not yet possible to implement a PQC KEM.

5.11.7 Stakeholders

The common usage of VPNs means they are relevant for stakeholders including standards bodies, vendors and operators. Standards organisations such as IETF and NIST will continue to evolve their standards to include PQC. Vendors and operators will, in turn, likely seek to develop products and offer services to customers that protect against the quantum threat.

5.11.8 PKI Implications

The application of PKI to VPNs should be considered an important use case since PKI can play an important role in authentication processes during the establishment of secure VPN connections. In transitioning to PQC VPNs, the detailed implications for PKI depend on whether hybrid schemes are adopted or if the classical algorithms are instead merely replaced by PQC variants. For hybrid schemes, the impact on PKI may depend on whether pre-shared secrets are used or a PQC KEM is employed.

5.11.9 Legacy Impact

The migration to PQC VPNs will likely be staggered and take considerable time, given the widespread usage of VPNs in the telco sector. A key issue relating to legacy devices and components will be the need to ensure backwards compatibility between upgraded and non-upgraded components.

5.11.10 Dependencies

5.11.10.1 Standards

The widely used TLS and IPsec protocols are developed and standardised by the IETF and MACsec protocols pertaining to Ethernet are developed by IEEE. These security related standards are closely watched by national security agencies to ensure secure operations.

TLS

The Transport Layer Security (TLS) [TLS-1.3-RFC] protocol enables a client and server to establish a secure communication channel at the application layer and provides one-sided or mutual authentication using certificates. The most recent version, TLS 1.3, is standardized as an IETF RFC [TLS-1.3-RFC] but earlier versions such as TLS 1.2 [TLS-1.2-RFC] and TLS 1.1 [TLS-1.1-RFC] remain widely used. Many web domains and browsers no longer support TLS 1.1 however servers may be required to accept incoming connections that only use version 1.1 due to remaining legacy devices and components.

In anticipation of cryptographic attacks to established key-exchange mechanisms, the IETF TLS working group published RFC 4279 in 2009. This document describes how to use symmetric keys (later called pre-shared keys or PSKs), shared in advance among the communicating parties, to establish a TLS connection. By relying on PSKs, the need for public key operations which are considered vulnerable to CRQC attacks can be avoided and provide a quantum-safe TLS connection.

The IETF TLS working group authored a draft on hybrid key exchange in TLS 1.3. This draft proposes that the key exchange phase be conducted two or more times using the regular TLS 1.3 key exchange message exchange process with different underlying algorithms in a side-by-side manner. For example, combining a traditional algorithm such as ECDHE and a Post Quantum secure algorithm such as ML-KEM, by concatenating the resulting keys into the key-derivation function that provides session keys to the record layer. This ensures security provided at least one of the component algorithms remains secure. Since this document migrates the key exchange component and not on the digital signature component of TLS, store-now-decrypt-later attacks (decryption of session traffic) are prevented but authentication attacks (an adversary acquiring the signing key for a certificate and impersonating the server) are not yet covered.

IKE / IPsec

The Internet Key Exchange protocol enables communicating parties to establish a secure channel at the internet layer and is part of the IPsec suite. Like TLS, certificates are used for entity authentication. The key exchange protocol at the heart is based on Diffie-Hellman. IKE v1 [IKE-v1-RFC] has been replaced by IKE v2 [IKE-v2-RFC], which is widely used in VPN applications.

The IETF-RFC [IETF-IKEv2-mixing] published in June 2020, describes an extension of IKEv2. Shared symmetric keys between peers, known as a Post-quantum PSKs (PPKs), are used as additional input to the key derivation function used for establishing security associations in IKEv2 and IPsec. By leveraging PPKs, IKEv2 becomes resistant to attacks involving CRQCs.

Another IETF draft [IETF-IKEv2-hybrid] published in May 2023 for usage of the key exchange component of IKE v2 in hybrid mode. The approach is slightly different to the TLS hybrid draft: an initial secure channel is created using Diffie-Hellman key exchange, and then a second (and perhaps a third) key exchange is done 'inside' this channel with a Post Quantum secure key exchange mechanism such as ML-KEM as an IKE_INTERMEDIATE extension [IKE-INT].

The IETF LAMPS group is performing additional relevant work in domains such as:

1. Usage and handling of PQC algorithms in certificates and the Certificate Management Protocol (CMP):
   - Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS
2. Defining identifiers for PQC algorithms; see:
   - Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA

- Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
- Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA

3. Improving crypto agility, in preparation for PQC inclusion:
   - Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)

Status: Drafts released and work continues in related domains

MACsec / MKA

MACsec (IEEE 802.1AE) was already published by IEEE in 2006 to secure Ethernet traffic. Later, IETF took inspiration from IEEE's work and developed complementary standards including those outlined before. Furthermore, 802.1X specifies how the Extensible Authentication Protocol (EAP) is encapsulated over wired Ethernet and wireless 802.11 networks, also known as "EAP over LAN" or EAPOL. In a nutshell, the Key Server periodically generates and distributes fresh symmetric keys to the MACsec peers, allowing the data encryption keys to be updated securely.

MACsec and EAPOL perform similar operations on Ethernet level (Layer-2) as IPsec and IKE do for the Internet Layer (Layer-3). Because MACsec is bound to Layer-2, it is typically used to protect infrastructure and established configuring PSKs. However, extensions exist to operate using public/private keys. Like IPsec, MACsec is considered quantum-safe if operating with PSKs.

Optical Transfer Networks / FlexOsec

Analogous to the use of MACsec to provide security at layer 2 (in the Open System Interconnection (OSI) model), layer 1 security methods may be employed in Optical Transfer Networks (OTNs). In particular, *FlexOsec* is a layer 1 security mechanism that uses systems and structures defined in G.709.1 : Flexible OTN common elements**.** Depending on the architecture for the connections between customer premises and operator premises, FlexOsec may provide security assurances for varying portions of the communications made by customers (see, e.g., ITU-T Series G Supplement 76). However, the ITU G.709.1 standard *does not* specify a key-agreement protocol to operate within the security limits of NIST SP 800-38D. Hence, to assure quantum safety for OTNs, the combination of standard FlexOsec and bespoke key-agreement protocols need to be considered. Vendors/operators offering products will need to ensure that all protocols become quantum-safe by either leveraging pre-shared keys or PQC methods.

5.11.10.2 National Guidelines

Quantum safe VPN products that use PQC cryptographic algorithms should employ algorithms that conform with national guidelines around PQC for the countries of deployment. For example, some countries may develop and/or mandate sovereign post-quantum algorithms and national guidelines should be consulted to ensure the cryptographic functionality of quantum safe VPNs aligns with national recommendations/requirements.

Some National guidelines target the use of symmetric PSKs to render their infrastructure quantum-safe. I.e. The Commercial Solutions for Classified (CSfC) established by the National Security Agency (NSA) enables U.S. government agencies to leverage commercial off-the-shelf (COTS) information and communications technology (ICT) products to protect classified national security systems (NSS) data. It is widely regarded as a reference for commercial system implementations worldwide. Currently, CSfC approved two protocols enabling quantum resistant confidentiality protection of data:

4. Internet Protocol Security (IPsec) with Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784-compliant implementations of Internet Key Exchange (IKEv2)
5. Media Access Control Security (MACsec).

In addition, the CSfC program office plans to approve TLS 1.3 for use with PSKs in future and is looking forward to add PQC to their list of approved protocols.

5.11.10.3 Vendors

As standards mature, it is anticipated that vendors will increasingly support quantum-safe services in their products. Vendors may find that providing pre-standard protocols or algorithms for testing may help facilitate the full migration towards standards-based solutions. Such advantage needs to be balanced, with the risk of integrating potentially vulnerable and not fully mature protocol implementations in a security relevant environment. The risk/benefit balance depends on applications and customer context. Vendors and operators need to jointly develop roadmaps for the transition, to illuminate expected timelines, assist migration planning and manage security risk during migration.

5.11.10.4 Operators

Operators who sell secure VPN services will need to identify products requiring an upgrade/migration to quantum safe status and communicate these needs to vendors/suppliers in requests for products/services. Early identification of anticipated cryptographic upgrades in product lines, and subsequent communication of these needs to vendors, will help coordinate operator and vendor expectations around timelines for providing PQC-enabled VPN offerings.

5.11.10.5 LEAs

(not clear its relevant here)

5.11.11 Gantt Chart for PQC Migration

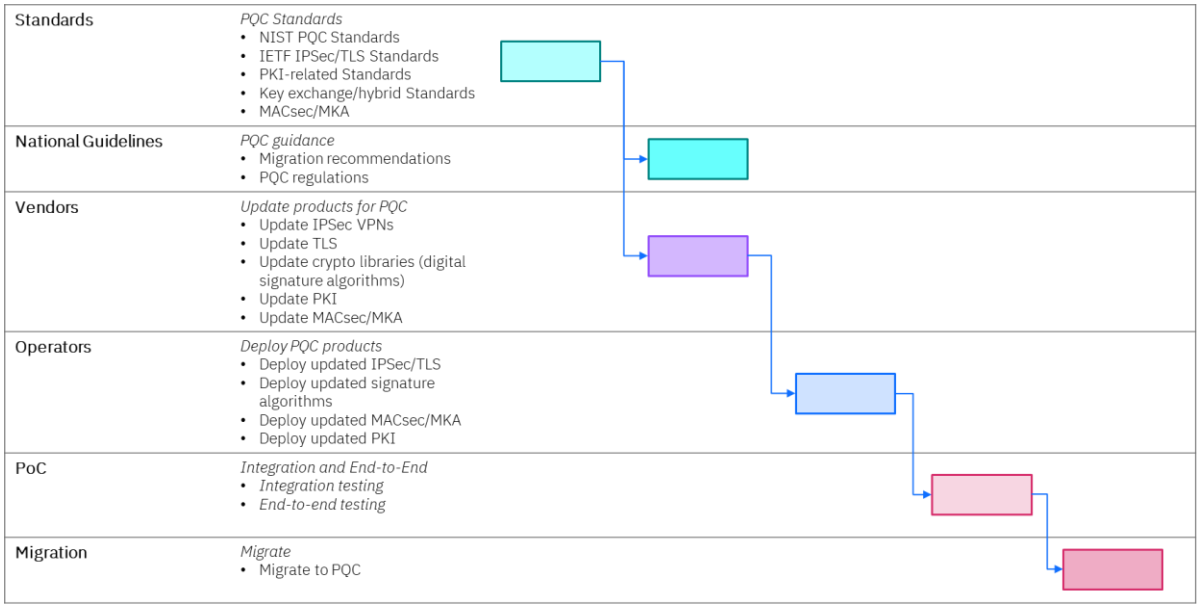


Figure 22: Gantt Chart for VPN PQC Migration

5.11.12 Description

At high level, full migration to PQC-VPNs first requires the release of PQC algorithm standards, such as those produced by the NIST PQC competition. Next, these algorithms will be incorporated into protocol standards release by, e.g., IETF working groups, such as those described above. Then, it is anticipated that vendors will incorporate PQC-enabled protocols into products that operators can deploy in relevant use-case contexts.

Note, however, that post-quantum security can be achieved in multiple ways. Anticipating that some organisations may wish to ensure post-quantum security prior to the finalisation/release of PQC standards, the IETF RFC 8784 standard can be used to mix pre-shared keys with IKEv2 keys (generated via traditional algorithms), to provide quantum safe VPNs prior to the release of PQC standards, albeit at the expense of incurring additional overhead to distribute and manage pre-shared keys.

RFC 8784 can already be used today to, e.g., secure critical site-to-site links without implementing a full-scale migration to PQC. However, the use of pre-shared keys may not be optimal or viable for many use cases, in which case PQC algorithms, standardised or otherwise, may be preferred or needed.

Even if pre-shared keys are not adopted, there are multiple ways to migrate to PQ key exchange for VPNs, depending on whether an immediate transition to PQC *only* is preferred or a hybrid approach, that mixes traditional and PQ keys is favoured. As example of the latter case, RFC 9242 (Intermediate Exchange in the Internet Key Exchange Protocol Version 2) and RFC 9370 (Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2) can be used to combine a traditional IKEv2 key with (up to) seven keys generated via PQ methods, producing a final hybrid that depends on (up to) eight keys that may be produced by different cryptographic approaches. The traditional key provides security against traditional/present-day attacks while the additional PQ keys provide security against harvest now, decrypt later attacks, while also providing redundancy to ensure PQ security in case of an unexpected

breaks of (any subset of) the PQ methods. In short, RFC 9242 allows the use of larger keys in the IKEv2 context and RFC 9370 facilitates the incorporation of multiple distinct keys. This approach avails significant redundancy in the PQ methods, reducing the risk involved with using any single PQ KEM prior to standardisation (or even as an early adopter, post standardisation).

More generally, migration to PQC will involve the release of vendor products that comply with protocol standards to implement standardised PQC algorithms. Once available, organisations such as telco operators can incorporate such products and, at a policy level, specify that PQC methods should be prioritised (or in some contexts, required) over traditional methods, perhaps with an allowance for the use of traditional methods in legacy contexts for which the PQC migration is not yet (or cannot be) complete.

5.11.13 Synergy with Internal Programs

VPNs are a core method of establishing secure communication channels. Accordingly, the migration of VPNs to quantum-safe status will naturally synergize with programs transitioning domains that apply VPNs, such as the BS-SecGW connection, authentication and transport connection between components in 5G core networks. In such domains, the matter of transitioning the cryptography deployed in the underlying VPNs is a main ingredient required to achieve quantum safety.

5.11.14 Synergy with External Programs

Commercial Solution for Classified (CSfC) [Source]:
The use of RFC8784 for IPsec and MACsec are approved by the CSfC program office. In order for CSfC solutions using IPsec on one or both layers to incorporate quantum resistant protection, RFC 8784-compliant implementations of IKEv2 must be used.

5.12 Software Defined Wide Area Networks (SD-WAN)

5.12.1 Scope

Software Defined Wide Area Networks (SD-WANs) are a type of dynamic overlay network architecture used by enterprises and governments to manage complex, evolving networks of interconnected sites requiring secure connectivity. Secure access service edge solutions (SASE) can be incorporated into SD-WANs to securely connect distributed elements/nodes to applications or services distributed in cloud infrastructure or data centres.

The underlay network infrastructure may consist of different technologies, such as ADSL, fibre, MPLS or 4G/5G, and the principal goal of SD-WAN is to match individual application requirements to the properties of each underlay technology.

Thus, for example, VoIP applications may be steered over MPLS in order to leverage the low latency and jitter, whereas general browsing can be steered over a fibre internet link to minimise costs. In addition, the control logic can provide additional functions such as load-balancing and resilience. Load balancing can be used to extend the available bandwidth beyond the capabilities of a single link, whilst a link failure can be handled by routing the affected data over an alternative link.

In order to route the traffic through the various WAN links, an overlay network is constructed, generally using a VPN technology such as IPSec. This also provides a layer of security, adding authentication, data integrity and confidentiality to the user data.

The steering of application traffic over the appropriate overlay may be done by a centralised controller, or alternatively, the nodes themselves may make the control decisions based on local policy.

Accordingly, the main impact of quantum computing attacks on SD-WANs likely relates to the cryptographic ingredients employed to establish and maintain these VPN connections. In this sense, regarding quantum safe considerations, SD-WANs may be conceptualised roughly as an application of VPNs, with additional identity and authentication processes to manage the identities and authentication of multiple nodes and control/orchestration elements.

The secure connections between components in an SD-WAN architecture may be IPSec VPNs, TLS connections or SSH tunnels, depending on the particular product and the particular connection. For example, connections between nodes may employ IPSec VPNs negotiated via a security controller, TLS connections may be used during onboarding or between security controllers and SSH may be used to access admin servers. Digital signature algorithms are also employed to enable downloads and installation of images during onboarding.

5.12.2 Sensitive Data Discovery

Similar to the VPN use case, the near-term primary threat from quantum computers relates to data in transit through the SD-WAN system. The SD-WAN itself may contain additional log data though this is typically short-lived (perhaps a year) and therefore not susceptible to the timelines necessary for SNDL attacks. Nonetheless, the VPNs employed in SD-WANs may carry encrypted data with long-lived security needs, potentially susceptible to SNDL attacks. This in-transit data constitutes a primary source of sensitive data for the SD-WAN use case.

5.12.3 System Context

SD-WANs are overlay networks for dynamically establishing and evolving networks, within which inter-node connections may be secured by VPN connections. Typically, SD-WANs are not tasked with storing sensitive user data but rather they facilitate transmission of data between nodes/sites. The main exception is that system/user log information may be retained, though this data is typically short lived (e.g., it may be retained for a year, say) and is therefore less relevant for harvest now, decrypt later attacks. Consequently, the main quantum computing threat relates to sensitive long-lived data transmitted between sites.

5.12.4 Cryptographic Inventory

Mirroring the discussion of VPNs, SD-WANs, as applied systems of VPNs, typically rely on cryptographic methods for authentication and identity management, establishing a shared secret, and encrypting transmitted data. A cryptographic inventory could cover each of these aspects, describing properties such as the protocols used, the digital signature options

used/available for authentication, and available options for sharing a secret and encrypting the data, as per the VPN use case.

5.12.5 Migration Strategy Analysis and Impact Assessment

SD-WANs are used by a variety of enterprises and government organisations. The data transiting through VPN connections orchestrated by SD-WAN controller elements may therefore contain long-lived sensitive information. For organisations solely reliant on confidentiality assurances provided by such VPN connections, there is a risk that SNDL attacks could compromise long-lived sensitive data. Sophisticated users of long-lived data are likely to employ their own cryptography and security protocols within the VPN tunnels. Nonetheless, the security assurances provided by VPNs employed in today's SD-WANs are dependent on quantum-vulnerable cryptography that will need to be upgraded in some way to retain these security assurances and enable PQ security. An absence of such upgrades could extirpate the long-term confidentiality assurances offered by SD-WAN products, impacting organisations and customers, and thus motivating a migration to PQ status.

5.12.6 Stakeholders

Stakeholders include standards bodies, who design protocols and standardise algorithms deployed by the VPNs used in SD-WANs, vendors and operators.

5.12.7 PKI Implications

PKI plays an important role in establishing secure connections and facilitating communication between elements in SD-WANs. The usage is similar to that of VPNs, with PKI commonly used to generate and store asymmetric keys, and communicate certificates. In an SD-WAN context, this may involve the PKI communicating certificates to an orchestrating element which, in turn, communicates them to specialised on-premise elements that distribute them to devices/nodes in the network. Hence the orchestrating element facilitates communication between the PKI and the on-premise equipment, which may not communicate directly.

5.12.8 Legacy Impact

Migration of SD-WANs to quantum-safe status involves the incorporation of quantum-safe VPN protocols. There are multiple SD-WAN vendors and products on the market and vendors will likely bear primary responsibility for upgrading SD-WAN products to PQ status. A risk for operators, relating to currently deployed legacy SD-WAN products, is to ensure that vendors intend to migrate all SD-WANs currently used by the operator. In the event that vendors do not intend to migrate certain older SD-WAN products, plans for transitioning legacy SD-WANs to alternative SD-WANs, that are either already PQ secure or are intended to be migrated to PQ status in an appropriate timeline, will be needed, to ensure the secure connectivity assurances within SD-WANs are maintained in the face of the quantum threat. In this regard, it is important that operators communicate with vendors to attain visibility over their SD-WAN PQ migration strategies and ensure currently deployed products do not become obsolete/insecure.

5.12.9 Dependencies

5.12.9.1 Standards

SD-WANs typically utilise IPSec VPNs so there is a clear dependency on the standards for VPN protocols relating to IPSec/IKE. Similarly, there is a dependency on the standards for the underlying PQC algorithms to be employed in the VPNs. The use of TLS for (e.g.) onboarding or connecting security controllers in SD-WAN contexts also give a dependency on TLS standards. PKI-related standards and key exchange/hybrid standards, as described in the VPN use case, are also relevant.

5.12.9.2 National Guidelines

National bodies provide recommendations around approved cryptographic algorithms and security levels. Such guidelines impact products/services like SD-WANs, which utilise cryptographic algorithms to ensure secure connections between sites and facilitate the transmission of sensitive data. Knowledge of national guidelines relating to cryptographic algorithms and security levels relevant for countries in which SD-WAN services are deployed will help ensure compliance with local requirements.

5.12.9.3 Vendors

It is anticipated that vendors will increasingly support post-quantum algorithms in their products as standards mature. Vendors may find that providing pre-standardised protocols or algorithms for testing may help facilitate the full migration towards standards-based solutions. Moreover, by providing roadmaps for the transition, to illuminate expected timelines, vendors can assist migration planning.

5.12.9.4 Operators

Operators who sell or use SD-WAN services can identify services requiring migration to quantum safe status and communicate these needs to vendors/suppliers. Early identification of anticipated cryptographic upgrades in product lines, and subsequent communication of these needs to vendors, will help coordinate operator and vendor expectations around timelines for providing PQC-enabled offerings. Of particular importance for operators is the possibility that vendors may not plan to upgrade all currently used SD-WAN services, in the case of e.g. older product lines. Operators will benefit from acquiring such information early, to enable sufficient time for planning (e.g., to transition customers to alternative product lines).

5.12.10 Gantt Chart for PQC Migration

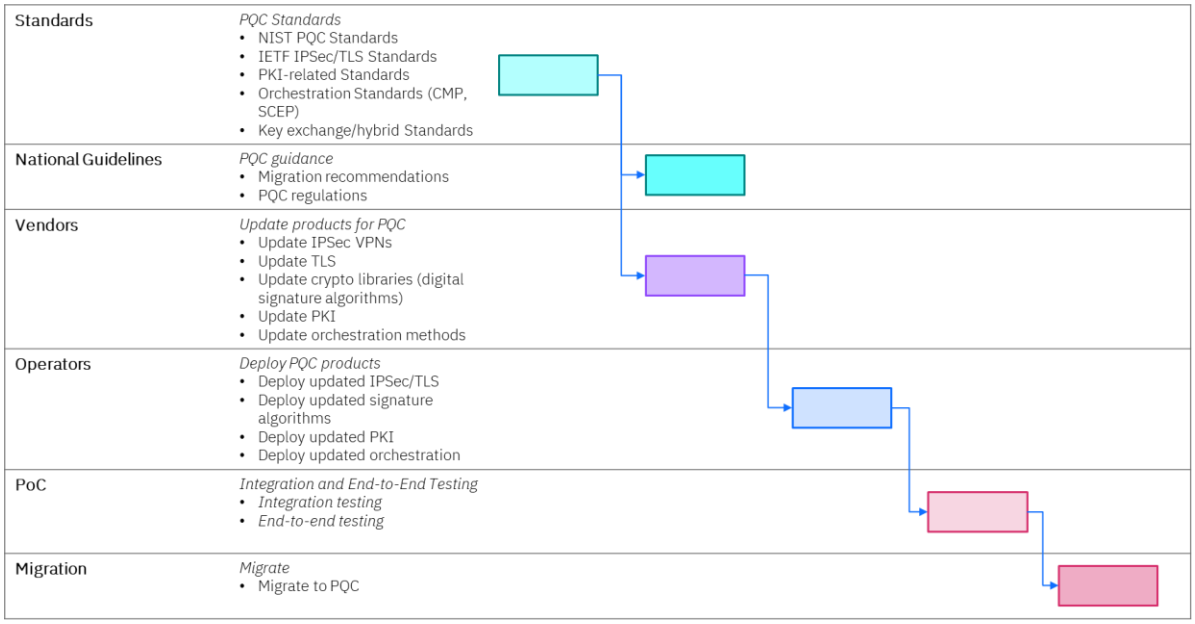


Figure 23: Gantt Chart for SD-WAN PQC Migration

5.12.11 PQC Migration Process Description

The following domains are relevant for SD-WAN operation and require migration to achieve PQ status:

- **PKI:** Some cryptographic capabilities of an SD-WAN are dependent on the public key certificates generated by the PKI.
- **Orchestration methods:** These orchestrate behaviour between devices on the network and may distribute certificates from the PKI to the devices, via protocols such as CMP (Certificate Management Protocol, RFC 4210) or SCEP (Simple Certificate Enrolment Protocol). When the PKI/certificates migrate to PQC, the certificate distribution methods (such as SCEP) must be able to handle the new certificates.
- **IPSec/IKE:** Information in transit between network devices is typically protected by IPSec VPNs.
- **SSH/TLS:** Used for securely accessing administrative servers (SSH) or protecting data in transit when onboarding devices (TLS).
- **Digital signing algorithms:** Used for signing (e.g.) downloadable images to be installed on devices.

Evidently SD-WANs incorporate multiple familiar cryptographic domains that possess quantum-vulnerabilities owing to their reliance on asymmetric cryptography. In particular, SD-WAN migration to PQ status requires migration of the cryptographic (VPN) methods used to generate secure connections between devices. At high level, migration to PQC VPNs first requires the release of PQC algorithm standards and the incorporation of the standardised algorithms into protocol standards (as released by, e.g., IETF working groups). Vendors may then incorporate standardised PQC-enabled protocols into products that operators can deploy. Related matters were described in the VPN use case. Similarly, the

need to transition PKI (and related protocols, such as SCEP) is directly relevant for the SD-WAN use case.

More generally, migration to PQC will involve the release of vendor products that comply with protocol standards to implement standardised PQC algorithms, for both PKI and key generation/VPN methods. Once available, operators can incorporate such products and, at a policy level, specify that PQC methods should be prioritised (or in some contexts, required) over traditional methods, subject to legacy constraints.

5.12.12 Synergy with Internal Programs

The quantum threat to SD-WANs relates mainly to their use of IPSec VPNs. Consequently, there can be synergies with other internal use cases deploying IPSec VPNs. For example, organisation-wide policy decisions relating to IPSec VPNs and migration timelines can readily apply to both SD-WAN VPNs and remote access VPNs, even if some dependencies (such as vendor support) may differ.

5.12.13 Synergy with External Programs

No external synergies yet identified

5.13 Privacy (Lifecycle) of Customer Personal Data

5.13.1 Scope

Personal data about subscribers is protected by legal safeguards (the EU GDPR and similar frameworks in other countries). To protect personal data at rest it is encrypted when stored, given the lifetime of the data the encryption used must be quantum safe. To protect personal data in transit it is encrypted when transmitted between systems, in this case the encryption used should be quantum safe.

Personal data is stored in operators' business support systems (BSS) and customer relationship management (CRM) systems. These applications typically use commercial or open source databases.

Copies of personal data also exist in the network, e.g. in the UDM, HSS and HLR. Network function typically use proprietary, commercial or open source databases.

Personal data is also generated in the network. Some personal data (e.g. International Mobile Subscriber Identity) is maintained within the network for operational reasons. Other personal data may be processed in mediation systems and stored such as billing and charging systems. These systems typically use proprietary, commercial or open source databases.

Database systems use symmetric encryption to secure stored data. Ensuring that symmetric encryption is quantum safe means checking key lengths provide the required security. Database systems use asymmetric encryption to protect the symmetric keys, usually implemented using a PKI.

Database systems also rely on encryption for identity and access management (IAM) for administrative and program access to data. This is usually implemented in a corporate IAM system, but some standalone databases may have a dedicated PKI.

5.13.2 System Context

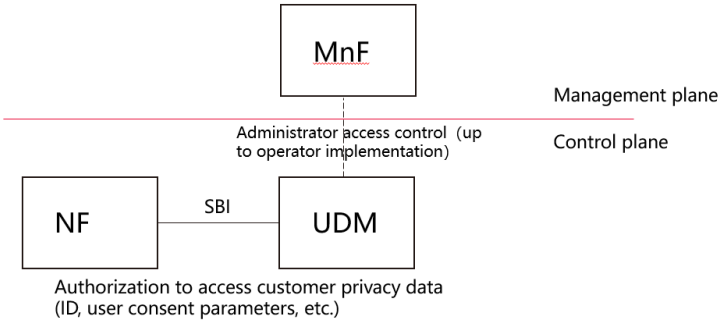


Figure 24: Example of accessing user privacy data in 5G system

Core NFs can be authorized to access the UDM to obtain customer privacy data. Include the subscriber ID and user consent parameter (on processing the related user data). Generally, the OAuth 2.0 protocol is used for authentication, which should consider PQC migration.

The administrator can access the privacy data of the UDM through the management plane NF (for example, IAM, up to the operator's implementation). Password authentication and usually requires an authentication protocol, such as Extensible Authentication Protocol (i.e., EAP) , which should consider PQC migration as well.

5.13.3 Sensitive Data Discovery

One of the reasons to secure subscriber databases is that the data access will expose personal information, e.g. call history, location history and financial information.

5.13.3.1 Sensitive Data Retention and Destruction

Scope is data lifetime, data retention policy, secure data destruction (for on-premise and cloud infrastructure and workloads).

5.13.4 Cryptographic Inventory

Database systems typically use symmetric cryptography to secure stored data, and asymmetric cryptography to secure the symmetric keys. Each vendor, or open source project, publishes documentation describing database encryption.

There are databases that may use fully homomorphic encryption (FHE), which is Quantum-Safe (since, as of this writing, all practical FHE schemes are based on hard problems not susceptible to efficient quantum attacks), to secure data and allow database operations to be performed on encrypted data. These are not yet widely deployed in production.

5.13.5 Stakeholders

IT systems, including BSS, CRM and the underlying databases are the domain of the CIO. Network systems, including UDM/HSS and the underlying databases are the domain of the CTO. Updates to the two sets of databases are independent and may proceed independently. Privacy regulators define requirements all businesses, including operators, must meet.

5.13.6 PKI Implications

Many database systems rely on a PKI. This can be a standalone PKI used just for one purpose, or an enterprise-wide PKI.

Database systems also rely on an identity and access management system. IAM is used to secure administrative access to the database by the DBA. It is also used to secure database access by programs running on other systems. In this case the IAM (or PKI) manages the technical identities. The underlying IAM/PKI are dependent on cryptography, which will need to be updated. From an implementation perspective the database may be integrated with an enterprise-wide identity management or may be a standalone implementation.

5.13.7 Legacy Impact

Databases and applications that store and process personal data need to be updated based on the lifetime of the data.

If the database uses weak symmetric encryption the database may need to be re-encrypted. The challenge is updating the asymmetric encryption used to secure the symmetric keys. If the database uses an external PKI, this may be resolved by updating the PKI. If the database uses its own asymmetric encryption this will require a vendor update or an update to the underlying open source technology.

5.13.8 Dependencies

5.13.8.1 Standards

According to 3GPP TS 33.501, the following general requirement are specified:

- The long-term key(s) used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM/ARPF unprotected.

The following requirements are specified for Subscriber privacy related requirements for UDM and SIDF:

- The SIDF is responsible for de-concealment of the SUCI and shall fulfil the following requirements:
    - The SIDF shall be a service offered by UDM.
    - The SIDF shall resolve the SUPI from the SUCI based on the protection scheme used to generate the SUCI.
- The Home Network Private Key used for subscriber privacy shall be protected from physical attacks in the UDM.
- The UDM shall hold the Home Network Public Key Identifier(s) for the private/public key pair(s) used for subscriber privacy.
- The algorithm used for subscriber privacy shall be executed in the secure environment of the UDM.

here is also the test specification 3GPP TS 33.514 [Y1] about 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class.

Moreover, user consent can be required for 3GPP features depending on local regulations for user privacy. The user consent checking is as follows:

6. Any NF that is deemed an enforcement point for user consent shall support to retrieve the user consent parameters from the UDM.
7. Any NF that is deemed an enforcement point for user consent shall not accept any services or requests for data processing unless user consent is granted.
8. Any NF that is deemed an enforcement point for user consent shall determine the purpose of data processing prior to the data processing. If the purpose of data processing is not implicitly known from the service request, the user consent enforcement point shall request it or otherwise deny the service.

NFs obtaining or checking the user consent parameters shall consider the user consent parameters as effective until revoked.

5.13.8.2 National Guidelines

National guidelines should be consulted to ensure that any recommendations or regulations are followed appropriately.

5.13.8.3 Vendors

Products, such as the UDM, need to support quantum-safe database access control. The detail specification may be out of 3GPP specification scope. But products may need to prevent quantum-enabled adversaries from forging signatures during the authentication and accessing the database to obtain the user privacy data without permission over management plane.

5.13.8.4 Operators

Databases such as UDM that store customer privacy data may necessarily support quantum-safe authentication mechanisms implementing the access control. For example, quantum-safe signature algorithms during authentication procedure may consider to be implemented for new network function as well as existing legacy network function.

5.13.8.5 Performance

For permanent UE identity concealment, the performance of both the UE and UDM may be affected due to the introduction of quantum-safe algorithms. However, it usually occurs when the user is accessing for the first time without an existing security context.

For NF obtaining user consent parameters from UDM, the performance impact may be minimal because the user consent parameters can be transmitted over the existing SBI interface with protection.

The performance of administrator login (for example, IAM) on the management plane may be related to the operator's implementation and policies, such as the frequency of management login and authentication.

For some privacy related data that has been encrypted stored in database, there is an impact because the data may require to re-encrypt with quantum-safe algorithms. This is related to the database storage policy. Typically, encrypted storage uses mature symmetric cryptography. The performance impact can be predictable.

5.13.9 Gantt Chart for PQC Migration

The purpose of the Gantt chart is to communicate how dependencies interrelate.

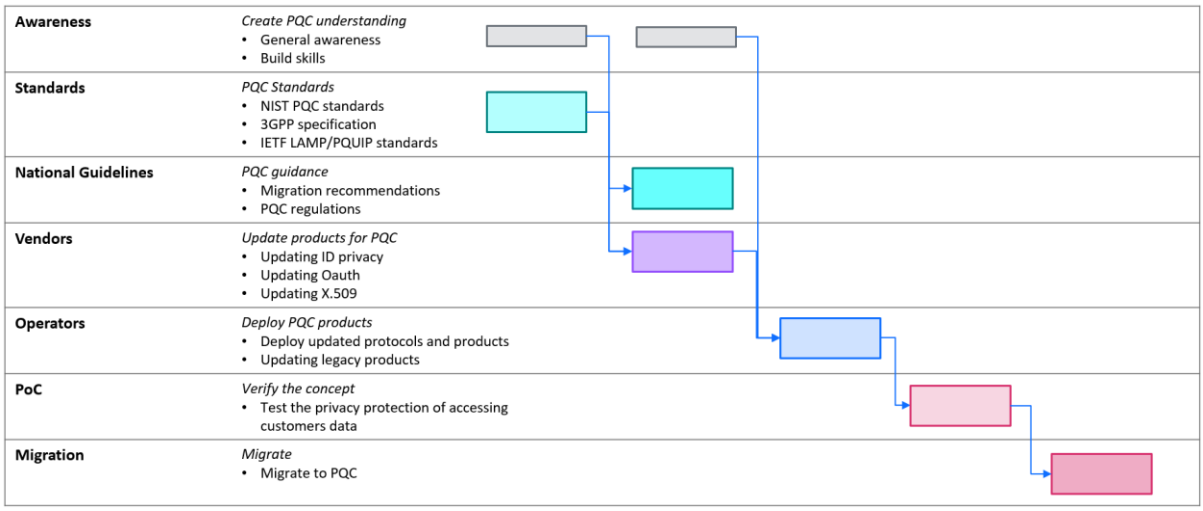


Figure 25: Gantt Chart for customer data privacy migration.

5.13.10 Description

According to the existing 5G privacy data storage requirements, customer/subscriber privacy data (e.g., permanent ID, subscription information, user consent parameters, etc.) needs to be stored in a physically secure location or area, for example, the UDM. This may not be affected by quantum attacks. Therefore, the main consideration regarding the migration process should be access control of customer privacy data.

First, for the access control of privacy data between different NFs, the 5G network uses the OAuth 2.0 authorization mechanism to authorize by verifying tokens before the data access. Usually, the token uses the signature algorithm of the asymmetric cryptography (i.e., RSA). These algorithms should be considered to replace with quantum-safe signature algorithms. IETF drafts are discussing mechanisms such as using hybrid signature mechanisms to provide quantum resilience [Y2].

Second, for privacy data accessed through the management plane. For example, administrators access ongoing devices such as the UDM and OAM through SSH. Specific requirements may be out of the scope of the communication specification. However, vendors and operators should consider support the authentication mechanism for network function login. Generally, the login system of the management plane uses signatures and certificates for authentication. These certificates and signatures need to be replaced with quantum-safe algorithms or mechanism as well. Some mechanisms are being discussed in the IETF draft. For example, PKI with quantum security extensions [Y3]. detail migration description may refer to other use case dedicated to SSH and PKI.

In future network with the increasing specification of network services, other network function may also storage and process user privacy data, and new algorithms and requirements may be introduced with additional quantum risks. One needs to continuously focus on the quantum resilience and migration for new requirement in the communication network.

5.13.11 Synergy with Internal Programs

Within the operator environment, Fine-grained coordination is required between groups regarding coordination of protocol updating on SBI (e.g., support for PQC migration of Oauth2.0) Administrators need to be notified to improve login security, for example, by using updated quantum-safe certificates.

5.13.12 Synergy with External Programs

Synergy with national cybersecurity initiatives and recommendation including PQC.

Synergy with IETF PQUIP, coordinate and discuss to avoid any conflicts about the migration plan.

Synergy with vendors about the operator migration plan, which will affect the product development of vendors in advance.

5.14 Lawful Intercept (and Retained Data)

5.14.1 Scope

Lawful Intercept and Retained Data (LI/RD) systems are implemented within operator's networks to provide information required by Law Enforcement Agencies (LEAs).

Lawful interception (LI) is the action of a network operator, access provider or service provider (based on lawful authority) of accessing and delivering in real-time certain current information from the Lawful Intercept Management Function/System (LIMF/LIMS to a Law Enforcement Monitoring Facility (LEMF), for a specific target identity(s). This information includes Intercept Related Information (IRI) and Content of Communications (CC).

The updates required to make LI/DR systems quantum safe are to update the Warrant and Handover interfaces.

In this use case we focus on the migration of the system interfaces, and the migration of the underlying systems.

- The first requirement to make LI/DR systems quantum safe is to update the Warrant and the handover interface between the LEA (the LEMF) and the operator (the LIMF). This covers confidentiality of access to LI systems, confidentiality of LI requests, confidentiality of LI data and integrity of LI data. These are defined in the HI interfaces specified by ETSI TC-LI or in national guidance.
- The implementation of the LI/RD systems must also be updated to be quantum safe. This covers the LIMF/LIMS and the LEMF platforms including identity management, infrastructure.
- Finally, there are additional requirements within the operator's domain. These cover the interfaces between the LIMF and the network functions. These are defined in the X interfaces specified by ETSI TC-LI or in national guidance.

These considerations apply equally to Retained Data.

In all cases these interfaces are secured by cryptography, and the cryptography must be updated to be Quantum-Safe.

5.14.2 System Context

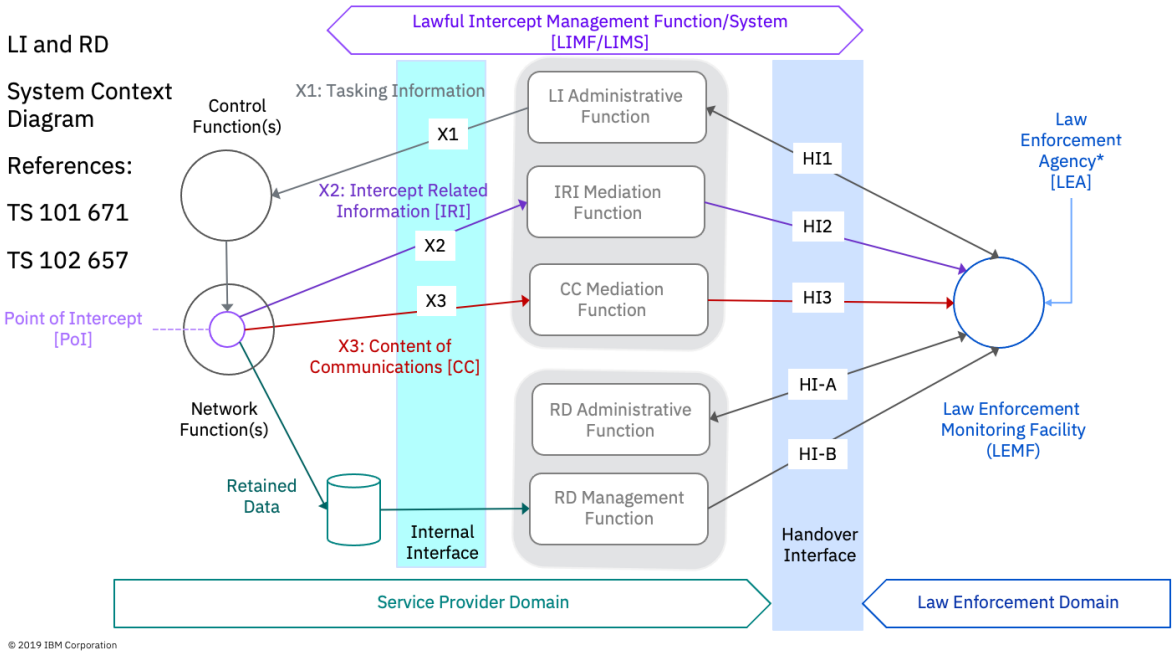


Figure 26: Sstem Context

The LEMF (Law Enforcement Monitoring Facility) provides a service for Law Enforcement Agencies (LEAs). The LEMF sends requests to the Lawful Intercept Management Function/System (LIMF/LIMS) within the operator and receives responses and data from it. The LIMF/LIMS in turn interfaces with the operator network to get the required data.

LEMF (Law Enforcement Monitoring Facility) and LI Management Systems (LIMS) are usually implemented by specialist vendors. Some national authorities have specific security requirements for network functions and the LI/RD systems [Hoffmann-2005, ETR-311, ETR-330].

5.14.3 Sensitive data discovery

Lawful interception data is exceptionally sensitive data that needs to be protected at all times and must never be altered. Therefore, it is necessary to secure access to LI elements and LI data.

5.14.4 Cryptographic Inventory

Physically embedded roots of trust are used to authenticate new LI elements and the process is often performed manually.

Asymmetric algorithms, such as RSA or ECC, are widely used for digital signatures

Symmetric cryptography is used (HMAC, CMAC), leveraging secret keys.

5.14.5 Migration Strategy Analysis and Impact Assessment

As LI elements are mostly part of other network elements the migration strategy is strongly connected to those network elements. Therefore, the strategy for the LI elements will follow the strategy of the Virtualized network functions use case.

5.14.6 PKI Implications

The ETSI specifications for Lawful intercept recommend the use of X.509 certificates for authentication [ETSI-LIHI1]. Updating LI to be Quantum Safe requires:

- IETF updates to the algorithm identifiers used in X.509 certificates. This work is underway in the IETF lamps working group.
- Definition (by national authorities) of which algorithms are acceptable in the certificates used to secure LI interfaces.
- Deployment of updated PKI that supports the selected algorithms
- Deployment of support for new algorithms in products supporting the handover interfaces.
- Use of quantum-safe certificates

5.14.7 Legacy Impact

Updates to the cryptography of the handover interfaces requires support from both LIMF (LIMS) vendors (typically network vendors) and also LEMF suppliers (often specialist vendors). The LEMF is outside the control of the operator, so there may be a period of time where the LEMF does not support PQC.

5.14.8 Dependencies

5.14.8.1 Standards

The publication of NIST standards to define PQC algorithms. In practice these are being treated as FS dependencies by many other groups.

The LI/RD system architecture is defined by ETSI TC CYBER and published by ETSI. The standards for the LI handover interfaces (HI1, HI2, HI3) must be updated to use PQC algorithms. The standards for the RD handover interfaces (HI-A and HI-B) must be updated to use PQC algorithms.

5.14.8.2 National Guidelines

The publication of national guidance on the use of PQC.

The publication of national standards for sovereign PQC algorithms, if required.

The publication of national guidance on the use of PQC (algorithms, key-sizes) for PQC for handover interfaces (HI1, HI2, HI3) for LI systems.

The publication of national guidance on the use of PQC (algorithms, key-sizes) for PQC for handover interfaces (HI-A, HI-B) for RD systems.

5.14.8.3 Vendors

The availability of vendor implementations of Law Enforcement Monitoring Facility (LEMF) supporting PQC.

The availability of vendor implementation for Lawful Intercept Management Function/System (LIMF/LIMS) supporting PQC.

The availability of vendor implementations for control functions and network functions supporting PQC.

5.14.8.4 Operators

Implementation of Lawful Intercept Management Function/System (LIMF/LIMS) supporting PQC for handover interfaces and internal interfaces.

Implementation of control functions and network functions supporting PQC.

5.14.8.5 LEAs

Implementation by LEA of updated LEMF supporting PQC for handover interfaces.

5.14.8.6 Performance

At the point of writing this document, there is no performance described.

5.14.9 Gantt Chart for PQC Migration

The purpose of the Gantt chart is to communicate how dependencies interrelate.

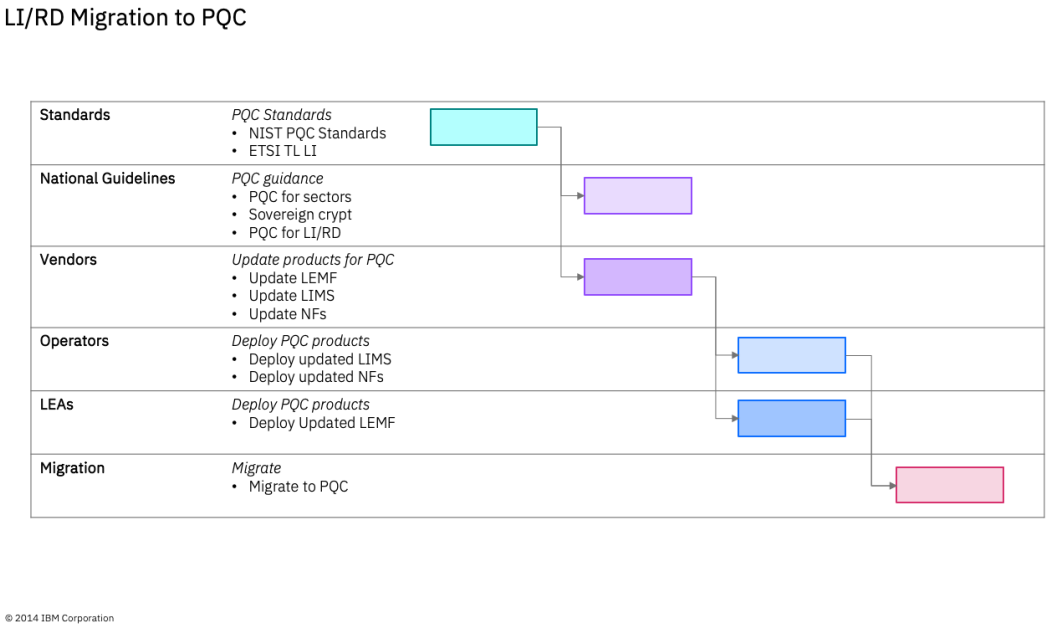


Figure 27: Gantt Chart

5.14.10 PQC Migration process Description

First we need LI PQC standards. Then we need vendor products for both operators and LEAs. These products must be verified in a test environment. The tested products must be

deployed. Then we can start the migration process, using new cryptographic algorithms between the LEMF and LIMF.

5.14.11 Synergy with Internal Programs

Editor's Note: Are there other programs within the operator with potential for synergy?

The required updates to network functions may be provided by vendors as regular functional enhancements.

5.14.12 Synergy with External Programs

Editor's Note: Are there programs external to the operator with potential for synergy?

The most likely synergy is with national cybersecurity initiatives including PQC.

5.15 IoT Services

Post Quantum Cryptography is not limited to telecom industries or telecom use cases. All industries managing sensitive data or requiring secure communications will be impacted. This section describes, through two examples, how Mobile Operators and Telecom industrials could leverage their Post Quantum implementation to offer value added services to their business customers.

5.15.1 Smart Meters Connectivity

5.15.1.1 Scope

In this use case we will focus on how to leverage Post Quantum telecom infrastructure, including (e)SIM card, as an asset for Root of Trust in a Smart Meter infrastructure (Post Quantum Root of Trust with eSIM, integration with operating system, secure remote services).

Electricity Smart Meters can affect electricity distribution networks. Successful attacks can lead to mass black outs, issues on network load balancing (wrong forecast), wrong billing.

The Department of Homeland Security, in the US, recognises Electricity Distribution as a high priority sector for Post Quantum migration, with high complexity and high need for support. https://www.rand.org/pubs/research_reports/RRA1367-6.html

5.15.1.2 Sensitive Data Discovery

There are several large-scale quantum attacks possibilities for connected Smart Meters:

- Take control of concentrators, or infect them
- Insert new authenticated devices on Broadband over power lines
- Take control of smart meters, or infect them
- Take over the identity of field technicians to administer equipment
- Change index & information in the public network
- Neutralize any equipment

5.15.1.3 Cryptographic Inventory

Roots of trust are used to authenticate software and firmware updates.

Asymmetric algorithms, such as RSA or ECDSA, are widely used for digital signatures.

Communication with devices is usually based on standardized secure communication protocol, such as TLS.

5.15.1.4 Migration strategy analysis and impact assessment

A quantum-safe solution involves the creation and later deployment of quantum-safe versions of Standard transport protocols.

For new deployments of Smart Meters that will be quantum-safe shall implement the capacity to upgrade their Software in a Quantum Safe manner. Smart Meters manufacturers can request standards compliant PQC capabilities in protocol stacks. The same applies for new deployments of concentrators. This could be achieved through integration of SIM/eSIM root of trust in the Smart Meter Operating Systems.

Operators need to evaluate the benefits of

- Offering Quantum-Safe Root of Trust to Smart Meters OEM
- Proposing Remote Quantum-Safe protocols for Firmware Upgrade based on those Root of Trust

5.15.1.5 Implementation roadmap (crypto-agility and PQC implementation)

One possible Migration strategy for Smart Meters migration is to leverage the connectivity of Secure Element (i.e. eSIM or SIM) and use it as a Root of Trust for the device.

By definition, Smart Meters are connected devices. They may be directly connected to a cellular network or through a concentrator.

The Post Quantum implementation in the eSIM/SIM can be used as a Root of Trust for the whole Smart Meter, securing Post Quantum credentials. By integrating the use of SIM/eSIM Root of Trust in the Smart Meter operating System, Post Quantum protocols can then be used to update safely the operating system of Smart Meters to any Quantum safe protocol.

5.15.1.6 Standards Impact (current and future) and maturity

Post Quantum cryptography migration might become mandatory as soon as 2025 [CNSA 2.0].

In the US, CISA, NIST and NSA have released migration plan for critical systems to Post Quantum cryptography. Migration shall start as soon as 2025 [CNSA 2.0], and shall be finalized by 2030-2035 for critical infrastructure.

5.15.1.7 Stakeholders

- Smart Meter manufacturers
- MNOs
- SIM Manufacturers/ EUM

5.15.1.8 PKI Implications

In case integrity, authenticity and confidentiality are leveraging asymmetric cryptography, PKI is playing a key role, and has to be quantum safe.

The detailed implications for PKI depend on whether hybrid schemes are adopted or if the classical algorithms are instead merely replaced by PQC variants.

5.15.1.9 Legacy Impact

The migration to PQC Smart Meters will be under time pressure, given the criticality of those devices.

5.15.1.10 Potential Actions/ Dependencies

- Smart Meters manufacturers:
    - While many Post Quantum algorithms (including ML-KEM and ML-DSA) will be comparable to traditional algorithms (ECDH and ECDSA) in terms of speed on the platforms used for 4G core, they may need a higher allocation of memory and throughput/bandwidth. Equipment manufacturers are therefore encouraged to take these constraints into account for the next generation of hardware devices.
    - Define a solution for crypto-agility to support migration of long-lasting device to Quantum safe cryptography
- Operators:
    - alignment with equipment infrastructure
    - Technical solution to leverage their PQ implementation for their IoT customers

5.15.2 Automotive

5.15.2.1 Scope

This use case focuses on protecting vehicle access and data communication, by protecting vehicle access through V2X connectivity unit, leveraging PQ ready eSIM as secure element to protect connectivity unit, and integrating eSIM services in unit OS for in depth Post Quantum security.

Increasing connectivity and automation of vehicles in combination with new regulations and standards like UN Regulation 155 and ISO/SAE 21434 require car manufacturers to monitor incidents and risks of their vehicle fleets over the entire life cycle.

Users' expectations are that car continue to ensure their security and their passenger's security. With the emergence of autonomous or automated cars, cars shall also ensure security of the environment. In addition, connected cars will generate additional user data.

5.15.2.2 Sensitive Data Discovery

The following is at risk:

- Firmware of electronic components, in particular the one which have an impact on safety, are sensitive to any modification.
- User data generated by entertainment connectivity.
- Any car monitoring data that could give away sensitive information about the car or the customer.

If Certificates and digital signatures are compromised, there are:

- Risk on secure boot
- Risk on mutual authentication
- Risk on software update
- Risk on transaction signature

If Asymmetric key exchange is compromised, then:

- TLS / VPN connectivity is compromised
- There are risks on stored or exchanged confidential data, if encryption key is transported through asymmetric protection
- Car Digital key

5.15.2.3 Cryptographic Inventory

Roots of trust are the basis of software authentication and firmware updates.

Asymmetric algorithms, such as RSA or ECDSA, are widely used for digital signatures.

Communication with devices is usually based on standardized secure communication protocol, such as TLS.

5.15.2.4 Migration Strategy Analysis and Impact Assessment

A quantum-safe solution involves the creation and later deployment of quantum-safe versions of automotive transport protocols.

For new deployments of automotive that will be quantum-safe, they shall implement the capacity to upgrade their Software in a Quantum Safe manner (see section 4.7). Automotive manufacturers can request standards compliant PQC capabilities in protocol stacks. The same applies for new deployments of concentrators. This could be achieved through integration of SIM/eSIM root of trust in the Smart Meter Operating Systems.

5.15.2.5 Implementation Roadmap (Crypto-Agility and PQC Implementation)

A first step could be to protect access and communication to the car, by implementing the protection in the communication unit of the car.

- Implementing Post Quantum communication between a cloud server and the car communication unit, leveraging the eSIM for asymmetric cryptography. Expose eSIM cryptographic capabilities to this communication unit operating system for critical operations (Secure boot, TLS, Software update…)

On a second step, automotive architecture based on international standards will need to evolve to integrate quantum safe protocols.

- Those standards will have to evolve to manage topics such as:
- Implementation of a distributed root of trust, able to handle crypto-agility.
- Securing each operating system with a quantum safe root of trust
- Maintaining certification

5.15.2.6 Standards Impact (current and future) and Maturity

Automotive industry uses numerous international standards, such as ISO, SAE, 5GAA, IATF, and local or regional regulations.

Car Connectivity Consortium (CCC) for digital keys

5.15.2.7 Stakeholders

- Automotive component manufacturers
- Automotive TIER 1 vehicle manufacturers
- MNOs
- SIM Manufacturers/ EUM

5.15.2.8 PKI Implications

In case integrity, authenticity and confidentiality are leveraging asymmetric cryptography, PKI is playing a key role, and has to be quantum safe.

The detailed implications for PKI depend on whether hybrid schemes are adopted or if the classical algorithms are instead merely replaced by PQC variants.

5.15.2.9 Legacy Impact

Accept the risk.

Propose pluggable workaround.

5.15.2.10 Potential Actions/ Dependencies

- Car manufacturers/Tier 1:
    - While many Post Quantum algorithms (including ML-KEM and ML-DSA) will be comparable to traditional algorithms (ECDH and ECDSA) in terms of speed on the platforms used for 4G core, they may need a higher allocation of memory and throughput/bandwidth. Equipment manufacturers are therefore encouraged to take these constraints into account for the next generation of hardware devices.
    - Define a solution for crypto-agility to support migration of car/ECUs to Quantum safe cryptography
- Operators:
    - alignment with car infrastructure
    - Technical solution to leverage their PQ implementation for their connected car customers

5.16 Enterprise Data

5.16.1 Scope

Mobile Network Operators have a range of business functions that create, harvest, process, store, and sanitise sensitive data for the enterprise to facilitate business operations. Some key examples include the legal, human resources, risk and regulatory, mergers and acquisition, fraud and strategy and innovation business areas.

The extent of enterprise data within each business function and their sensitivity, is required to be classified by the business owner based on its criticality to the overall business. A data classification and retention policy are established to govern how this strategic information is securely stored, exchanged within the organization, or shared with strategic partners externally and then finally sanitised or destroyed when the data is no longer required.

This follows the data lifecycle management process in the below figure. In general terms, most enterprises would be subject to the requirements that stem from the policy, however, for MNOs, this is pertinent as well, in the context of Post Quantum Cryptography. The related sensitive or critical information is managed and governed by specific information protection controls, including securing data at rest, either structured or unstructured, data leakage prevention (i.e. either intentional data sharing or unauthorised data sharing) and data whilst in transit.

Figure 28: the data lifecycle management process

5.16.2 Sensitive Data Discovery

Various systems of record and systems of insight exists within the business function that contain critical or sensitive information that support the mobile business operations, and these include but is not exhaustive for the following areas. The risk related to each, emanates from the disclosure of the data that is subject to cryptographic attack.

- Mobile Network critical information, including site or network roll-out plans
- Strategic mergers and acquisition contracts or due diligence artifacts
- Human resource personally identifiable information of employees
- Risk and regulatory information, covering aspects of spectrum license acquisition
- Legal contracts and supplier agreements
- Financial records, financial results, budgeting plans

- Intellectual property, Patents or Innovation ideas

Various strategic plans covering technology strategy, customer acquisition and retention strategies, business growth strategies

5.16.3 Cryptographic Inventory

Symmetric algorithms employed to secure, sensitive information on data storage, both on-prem or in the cloud, are potentially subject to cryptographic attack from quantum computing (Section 3.5 as noted has reference on the current impact and debate on AES128 from quantum computing). Asymmetric algorithms, such as RSA and ECDSA, which are widely used for digital signatures to secure data in transit and to assure only designated, authenticated and authorised persons can receive, and decrypt confidential information are also subject to cryptographic attack from quantum computing. The related cryptographic algorithms employed, where there is business justification based on the classification policy (i.e. highest encryption is employed for sensitive data that has the highest impact to the business operations to the organisation if disclosed or altered) made to encrypt sensitive data with the appropriate algorithms is the cryptographic inventory for this use case. There can be various encryption algorithms thus employed for the range of sensitive information stored or transmitted. Some examples of Tools that encrypt data at rest include Bitlocker (Windows end point disk encryption), File Vault (full disk encryption for MacOS), IBM Guardium (Database security and protection tool), Varonis Data Security Platform (data security and protection, access control and auditing) and tools that encrypt data in transit include, Cisco AnyConnect Secure Mobile Client or Microsoft Azure VPN Gateway.

5.16.4 Migration Strategy Analyses and Impact Assessment

The migration strategy requires that the OEM vendors providing these related tools, provide protection from quantum attacks primarily from organisations sharing data across public internet infrastructure for the purpose of their business operations. The extent of impact will primarily depend on the classification policy employed and the extent to which data leakage prevention tools are used.

5.16.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

The implementation roadmap approach is to assess and address areas with the highest risk of sensitive data stored or transmitted, and then to focus on adopting a quantum safe protections for this data. As a first step, it is recommended that operators along with OEM Information protection vendors work together to experiment and test new tools sets that are quantum safe to be adopted in the enterprise environment. This plan will allow more seamless adoption, reducing the impact on business operations.

5.16.6 Standard Impact (current and future) and Maturity

GSMA (GSM Association):

- GSMA Security Guidelines
- GSMA Fraud and Security Group (FASG)
- GSMA Network Equipment Security Assurance Scheme (NESAS)
- GSMA IoT Security Guidelines

3GPP (3rd Generation Partnership Project):

- 3GPP Security Standards
- 3GPP TS 33 Series
- 3GPP Network Domain Security (NDS) Framework
- 3GPP IMS Security

Other Relevant Standards:

- ETSI (European Telecommunications Standards Institute)
- ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)
- ISO/IEC 27001

5.16.7 Stakeholders

OEM providers of Information Protection services and software, Open Source Information Protection providers, Standards Authorities.

5.16.8 PKI Implication

All related vendors or OEM providers will include PKI support with CA.

5.16.9 Legacy Impact

The primary process invoked to reach a target state, will depend on various phased or roll-out programs to upgrade, OEM products that support information protection within the enterprise and can include complete replacement of toolsets or introduction of specific features into existing software packages.

5.16.10 Potential Actions

As mentioned previously, awareness of the impact of quantum computing and the requirements associated to a quantum safe enterprise, starts with vendor engagement both at a strategic, tactical, and operational level, expressing the urgency and impact of related capability required. Identifying and assessing within the enterprise key risk area, and working closely with interested stakeholders, to craft strategic and detailed plans early, will reduce impact to business operations and a need for hastened impactful changes to the enterprise.

5.17 Network Function Authorization

5.17.1 Scope

Authorization between network functions is carried out using OAuth 2.0 tokens over the SBI interfaces. Since the OAuth tokens are digitally signed by the NRF using its signing key based on ECC, it may be vulnerable to quantum adversaries. Therefore, the signature algorithm (e.g. ECDSA) used in the token will need to be replaced with a quantum-safe algorithm (e.g. ML-DSA). For example, a hybrid mechanism. Some mechanisms are being discussed in IETF drafts [X4]. When the algorithms and mechanisms mature, they can be introduced into token-based protocols to replace existing signature algorithms, such as OAuth 2.0 and Client Credential Assertion (CCA) token-related authorization protocols.

5.17.2 System Context

A producer NF (NF-P) provides services to a consumer NF (NF-C) based on an access token presented by the NF-C. The NF-C obtains the token from an authorization server (NRF), which issues the token to the NF-C based on authorization policies (defined by the NF profile using operator policies). The access token provided by the NRF includes the claims encoded as a JSON object (JSON Web Token). The JWT is integrity and authenticity protected using JSON Web Signature (JWS). The digitally signed access token is then converted to the JWS Compact Serialization encoding as a string as specified in RFC 7515. The JWT may be optionally encrypted within a JSON Web Encryption (JWE) object.

A PKI infrastructure that is capable of issuing and managing the life cycle of signing certificates isued to the NRF, where the certificate management protocol of choice may be CMPv2 or other protocols (e.g. SCEP, EST) that are dependent on the operator deployment.

5.17.3 Sensitive Data Discovery

Due to the use of asymmetric cryptography, the following connections are considered not quantum safe:

Connection between the NRF and the NF that is used for carrying the token request, NF discovery uses TLS 1.2 / 1.3.

Connections between the NF-C and the NF-P uses SBI interface secured using TLS 1.2 / 1.3 to carry the OAuth 2.0 tokens as well as the CCA.

Examples of sensitive data in this use case:

Data in transit:

OAuth 2.0 token containing the digital signatures of the NRF

CCA that contains the digital signature of the NF consumer

Data at rest:

Private Key associated with the NRF for signing the access tokens

Private Key of the NF-C for signing the CCA.

5.17.4 Cryptographic Inventory

The digital signatures within the OAuth 2.0 tokens and CCA may be based on ECDSA using Elliptic Curve public key certificates.

The NRF and NF public key signing certificates and associated private keys may be protected for integrity and confidentiality using data-at-rest cryptography generally based on AES.

5.17.5 Migration Strategy Analysis and Impact Assessment

The digital signatures used by NRF and the NF consumer for signing the OAuth 2.0 token as well as the CCA respectively will have to be migrated to ML-DSA or Hybrid schemes.

Ensure that the public key signing certificates at-rest is protected using AES with longer keys (128 or greater).

5.17.6 Stakeholders

NF and PKI vendors

5.17.7 PKI Implications

The PKI system will have to migrate to performing life-cycle management (provision, update, revoke) of ECC/ECDSA based signing certificates to ML-DSA or Hybrid signing certificates.

5.17.8 Legacy Impact

No legacy impact.

5.17.9 Dependencies

5.17.9.1 Standards

3GPP TS 33.501 and TS 33.210 defines JWS and JSON Web Encryption (JWE) profiles. JWT, JWS and JWE are specified in IETF RFC 7519, 7515 and 7516 respectively and the cipher-suites are described in RFC 7518. The algorithm (“alg”) parameter that has been specified to be used for signing the access token is ES256 (ECDSA using P-256 curve with SHA-256). If JWE is used, then ECDH may be used as one of the key agreement mechanisms.

Other relevant standards include, PKI and certificate life-cycle management protocols, such as Certificate Management Protocol (CMPv2), that uses X.509 certificates as described in RFC 4210, as well as the extended key purpose 5G network functions described in RFC 9509. Certificate validation and certificate revocation lists may also be used.

5.17.9.2 National Guidelines

There may be efforts carried out by Alliance for Telecommunications Industry Solutions (ATIS) in addition to NIST guidelines for securing OAuth 2.0 tokens, that would recommend the use of PQC based digital signature schemes for JWS.

5.17.9.3 Vendors

Standards development will enable vendors to implement PQC crypto support. The NRF vendor as well as NF-C vendor must build capability to support PQ / Traditional hybrid schemes for OAuth token signing as well in certain cases, for PQC key encapsulation.

5G NF-P vendors must have the capability to validate signatures within OAuth 2.0 tokens and CCA using PQ / Traditional hybrid schemes and in some cases the ability to perform PQC key decapsulation capabilities.

5.17.9.4 Operators

Based on risk profile, operators may use PQC when available from the vendors or PQ/T hybrid schemes for certain use cases where the risk is higher especially when using JWE in order to mitigate against “harvest now decrypt later” type attacks. For most of the use-cases, where only JWS is used the threat is not imminent and therefore a migration to PQC signatures schemes may be undertaken in a phased manner.

5.17.9.5 LEAs

N/A

5.17.9.6 Performance

The greatest performance impact is going to be on the NRF to generate ML-DSA signatures for the OAuth 2.0 tokens and the impact is going to be even higher on the NRF if hybrid schemes are used to sign those tokens. There is going to be some impact on the NF-P to validate the digital signatures in the tokens.

Even though, the CCA has been specified it is not expected to be used for a lot of use-cases unless end-to-end security is a requirement and therefore the overall impact on the system may be minimal. However, in those use-cases, where CCA is used, there is going to be impact on the NF-C to generate the CCA and for the NF-P to validate the digital signature(s) in the CCA.

5.17.10 Gantt Chart for PQC Migration

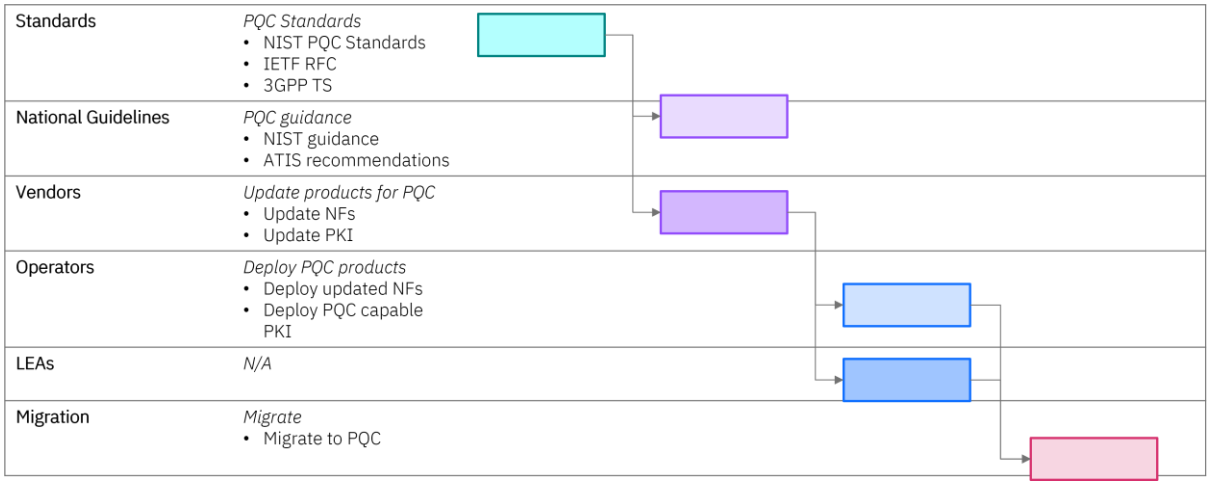


Figure 29: Gantt Chart for PQC Migration

5.17.11 PQC Migration Strategy

The digital signature within a JWS object will have to be updated with the ML-DSA (Crystals-Dilithium) or any other standardized PQC digital signature algorithm. Firstly, the ML-DSA will have to be specified in the IETF and based on such a specification, a mechanism that uses the IETF specs will have to be described and specified within the 3GPP TS 33.210 specs. In the interim, a hybrid scheme for digital signature that combines ECDSA and ML-DSA can be used if there is a near-term availability of a viable quantum computer. Algorithms that are being standardized within the IETF, that includes generating composite signatures (e.g. draft-ounsworth-pq-composite-sigs) may be good candidate schemes. It must be noted that “harvest now, decrypt later” type attacks are less of a concern when only JWS is being used which may be the case for almost all of the use-cases.

There may be some use cases where encrypted JSON objects are needed, e.g. when confidentiality or privacy related data needs to be shared within a token. If key agreement is being used, then one of the standardized ML-KEM (e.g. Crystals-Kyber) should be used. The “harvest now, decrypt later” type attacks are a genuine concern when JWE is used and

therefore quickly pivoting to PQ/Traditional hybrid key agreement mechanisms and later to ML-KEM type schemes when PQC matures.

In a hybrid environment, the certificate life-cycle management must include certificates that are used for both ML-DSA as well as for the traditional algorithms (e.g. ECDSA, ECDH). The certificates used for the NRF signature generation / verification by the NF-P must be provisioned and managed by PQ PKI systems and that also has the ability to support hybrid schemes. Also, PQ compliant capabilities within the certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP) must be developed and standardized.

5.17.12 Synergy with Internal Programs

The following are projects where there could be synergies:

- Single-Sign-On (SSO) systems within an enterprise that uses Open Id Connect and leverages OAuth 2.0 tokens for human / machine authorization.
- API security

5.17.13 Synergy with External Programs

Synergy with national cybersecurity initiatives and recommendation including PQC.

Synergy with IETF PQUIP, LAMPS, OAuth working groups coordinate and discuss to avoid any conflicts about the migration plan.

Synergy with vendors about the operator migration plan, which will affect the product development of vendors in advance.

Annex A Post Quantum Government Initiatives by Country and Region

This section will be described in a separate document.

Annex B Definitions, Terminology and Abbreviations

B.1 Definitions

Term	Description
FN-DSA	FFT over NTRU Lattice Based Digital Signature Standard. Designed to protect the digital signatures used when signing documents remotely. Based on the FALCON submission. To be standardised by NIST.
ML-DSA	Module-Lattice-Based Digital Signature Standard. Designed to protect the digital signatures used when signing data objects. Based on the CRYSTALS-Dilithium submission. One of three replacements for the DSA and EC-DSA algorithms for digital signatures. The other signature algorithm is SLH-DSA (and in future FN-DSA). Standardised in FIPS-204.
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism Standard. Designed for general encryption purposes such as creating secure websites. Based on the CRYSTALS-Kyber submission. The replacement for the RSA-KEM and (EC)DH algorithm in public key cryptography. Standardised in FIPS 203.
Quantum Safe	Quantum Safe secures sensitive data, access, and communications for the era of quantum computing.
Post Quantum Cryptography	The goal of Post Quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. (NIST definition.) Synonyms include Quantum Resistant Cryptography, Quantum Secure Cryptography.
SLH-DSA	Stateless Hash-Based Digital Signature Standard. Designed to protect the digital signatures used when signing documents remotely. Based on the SPHINCS+ submission. One of three replacements for the DSA and EC-DSA algorithms for digital signatures. The other signature algorithm is ML-DSA (and in future FN-DSA). Standardised in FIPS-205.

B.2 Terminology

In August 2023 NIST released initial public draft standards for Post-Quantum Cryptography as part of the Post-Quantum Cryptography Standardization Project. The initial public drafts introduced formal names for the standardised PQC algorithms.

The final standards were published in August 2024.

This document uses the new names for the PQC algorithms: ML-KEM, ML-DSA, SLH-DSA and FN-DSA. This ensures commonality with the standards, and reduces confusion. The historic names (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, Falcon and variants) are only used when referring to information about the original submissions.

B.3 Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
5GAA	5G Automotive Association
5G AKA	5G Authentication and Key Agreement
5G-CRG	5G Control Risks Group
5GS	5G System
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
AF	Application Function
AH	Authentication Header
AMF	Access and Mobility Management Function
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	Application Programming Interface
ARPF	Authentication Credential Repository and Processing Function
AUSF	Authentication Server Function
BPP	Bound Profile Package
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Business Support Systems
BYOK	Bring Your Own Key
CA	Certificate Authority
CACR	Chinese Association for Cryptologic Research
CAICT	China Academy of Information and Communications Technology
CBC	Cypher Block Chaining
CC	Content of Communications
CCC	Car Connectivity Consortium
CEO	Chief Executive Officer
CFDIR	Canadian Forum for Digital Infrastructure Resilience
CFRG	Crypto Forum Research Group
CI/CD	Continuous Integration Continuous Deployment
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMAC	Cipher Message Authentication Code
CMP	Certificate Management Protocol

Term	Description
CNF	Cloud native Network Function
CNSA	Commercial National Security Algorithm Suite
CPE	Customer Premises Equipment
CRM	Customer Relationship Management system
CRQC	Cryptographically Relevant Quantum Computer
CRYPTREC	Cryptography Research and Evaluation Committees
CRYSTALS	Cryptographic Suite for Algebraic Lattices
CSP	Communication Service Provider
CTO	Chief Technology Officer
DBA	Database Administrator
DES	Data Encryption Standard
DH	Diffie-Hellman
DHE	Diffie-Hellman key Exchange
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTLS	Datagram Transport Layer Security
EASDF	Edge Application Server Discovery Function
EC	European Commission
EC3	Elastic Cloud Computing Cluster
ECC	Elliptic-Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encrypted Scheme
ECKA	Elliptic Curve Key Agreement
EK	Encryption Key
ERP	Enterprise Resource Planning
eSIM	Embedded Subscriber Identity Module
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
ETSI GR ETI	ETSI Group Report Encrypted Traffic Integration
ETSI ISG	ETSI Industry Specification Group
ETSI TC	ETSI Technical Committee
eSIM	Electronic Subscriber Identity Module
eUICC	embedded Universal Integrated Circuit Card
EUM	eUICC Manufacturer
FAQ	Frequently Asked Questions
FASG	Fraud and Security Group

Term	Description
FIPS	Federal Information Processing Standards
FN-BRG	Fixed Network – Broadband Residential Gateway
FN-CRG	Fixed Network Cable Residential Gateway
FN-DSA	Falcon Digital Signature Algorithm
FTP	File Transfer Protocol
GCHQ	Government Communication Headquarters
GCI	Global Security Index
GCM	Galois/Counter Mode
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GLI	Global Line Identifier
GSMA	Global System for Mobile Communication Association
GUTI	Global Unique Temporary Identity
HI	Handover Interface
HLR	Home Location Register
HMAC	Hash-based Message Authentication Code
HN	Home Network
HQC	Hamming Quasi-Cyclic
HSS	Home Subscriber Server
hPLMN	home Public Land Mobile Network
hSEPP	home Security Edge Protection Proxy
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IATF	International Automotive Task Force
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPSec	Internet Protocol Security
IPSECME	IP Security Maintenance and Extensions
IRI	Intercept Related Information
IRTF	Internet Research Task Force
ISC2	International Information Systems Security Certifications Consortium
ISG	Industry Specification Group
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission

Term	Description
ITU-T	International Telecommunications Union Telecommunication Standardisation Sector
KEM	Key Encapsulation Mechanism
LAMPS	Limited Additional Mechanisms for PKIX (Public Key Exchange) and SMIME (Secure/Multipurpose Internet Mail Extensions)
LCS	LifeCycle Service
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Intercept
LIMF	Lawful Intercept Monitoring Facility
LMS	Leighton-Micali Signature
LPA	Least Privilege Access
M2M	Machine to Machine
MD5	Message Digest Method 5
MEC	Multi-access Edge Computing
MK	MAC Key
ML-DSA	Module-Lattice Digital Signature Algorithm
ML-KEM	Module Lattice based Key Encapsulation Mechanism
MNO	Mobile Network Operator
MME	Mobility Management Gateway
MVNO	Mobile Virtual Network Operator
NCCOE	National Cyber Security Center of Excellence
NCSC	National Cyber Security Centre
NDS	Network Domain Security
NEF	Network Exposure Function
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualisation
NICT	National Institute of Information and Communications Technology
NIST	National Institute of Standards and Technology
NIST-SP	(NIST) Special Publication
NPL	National Physical Laboratory
NQSN	National Quantum Safe Network
NRF	Network Repository Function
NSA	National Security Agency
NSACF	Network Slicing Admission Control Function
NSS	National Security Systems
NSSAAF	Network Slice Specific Authentication and Authorization Function

Term	Description
NSSF	Network Slice Selection Function
OAM	Operation Administration Management
OEM	Original Equipment Manufacturer
O-RAN Alliance	Open RAN Alliance
OS	Operating System
OSS	Operations Support System
OTA	Over-The-Air
PCF	Policy Control Function
P-GW	Packet Gateway
PFS	Perfect Forward Security
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
PQ/T	Post Quantum/ Traditional
PQTN	Post Quantum Telco Network
PQUIP	Post-Quantum Use in Protocols
PRINS	PRotocol for INterconnect Security
PSK	Pre-Shared Key
RSP	Remote SIM Provisioning
QKD	Quantum Key Distribution
QRM	Quantum Risk Management
QRNG	Quantum Random Number Generation
RAN	Radio Access Network
RD	Retained Data
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RSP	Remote SIM Provisioning
SAE	System Architecture Evolution
SBA	Service-Based Architecture
SBI	Service-Based Interface
SCP	Secure Copy Protocol
SCP	Service Communication Proxy (5G related)
SD-WAN	Software Defined Wide Area Network
SecGW	Security Gateway
SEPP	Security Edge Protection Proxy
SIDF	Subscriber Identity De-concealing Function
SFTP	Secure File Transfer Protocol
S-GW	Serving Gateway

Term	Description
SHA	Secure Hash Algorithm
SIKE	Supersingular Isogeny Key Exchange
SIM	Subscriber Identity Module
SLH-DSA	Stateless Hash-based Digital Signature Algorithm
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager Secure Routing
SMF	Session Management Function
SMS	Short Message Service
SNDL	Store Now, Decode Later
SSH	Secure Shell Protocol
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TEC	Telco Edge Cloud
TMSI	Temporary Mobile Subscriber Identity
TIP	Telecom Infrastructure Project
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
VNF	Virtualized Network Function
VPN	Virtual Private Network
vSEPP	visitor Security Edge Protection Proxy
WAN	Wide-Area Network
XMSS	EXtended Merkle Signature Scheme
ZT	Zero Trust
ZTA	Zero Trust Architecture

Annex C References

Ref	Doc Number	Title
3GPP TS 23.501	3GPP TS 23.501	System Architecture for the 5G System
3GPP TS 23.502	3GPP TS 23.502	"Procedures for the 5G System (5GS)"

Ref	Doc Number	Title
3GPP TS 33.501	3GPP TS 33.501	"Security architecture and procedures for 5G system"
3GPP TS 33.310	3GPP TS 33.310	UMTS; LTE; 5G; "Network Domain Security (NDS); Authentication Framework (AF) "
3GPP TS 33.210	3GPP TS 33.210	UMTS; LTE; 5G; “Network domain security; IP network layer security”
ANSSI22	ANSSI22	ANSSI Technical postion papers Post Quantum Cryptography Transition https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf
ANSSI23	ANSSI23	Follow Position Paper Post Quantum Cryptography https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography
BIKE	BIKE	Bit Flipping Key Encapsulation https://bikesuite.org/files/v5.0/BIKE_Spec.2022.10.10.1.pdf
BSI-TR-02102-1	BSI-TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile
BSI-2022	BSI-2022	Quantum-safe cryptography – fundamentals, current developments and recommendation https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6
BSI-2023	BSI-2023	Cryptographic Mechanisms: Recommendations and Key Lenghts, BSI TR-02101-1, 9 January 2023, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf
BSI-2023	BSI-2023	Cryptographic Mechanisms: Recommendations and Key Lenghts, BSI TR-02101-1, 9 January 2023, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

Ref	Doc Number	Title
BSI AIS 20/31 draft	BSI AIS 20/31 draft	A Proposal for Functionality Classes for Random Number Generators Version 2.35 - DRAFT, 02 September 2022. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Zufallszahlengenerator/zufallszahlengenerator_node.html
CCS 2022		Güneysu et al.; "Proof-of-Possession for KEM Certificates using Verifiable Generation", ACM CCS 2022. https://dl.acm.org/doi/10.1145/3548606.3560560
CNSA 2.0	CNSA 2.0	Commercial National Security Algorithm Suite 2.0 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
cr.yp.to: 2017.10.17		cr.yp.to: 2017.10.17: Quantum algorithms to find collisions
Dilithium	Dilithium	Dilithium Specification Round 3 https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf
ECIES	ECIES	SEC 1: Elliptic Curve Cryptography http://www.secg.org/sec1-v2.pdf
EQCSAI SC		An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography | SpringerLink
ETR 311	ETSI ETR 311	"Security Techniques Advisory Group. Definition of user requirements for lawful interception of telecommunications" (1996-12)
ETR 330	ETSI ETR 330	"Security Techniques Advisory Group; A guide to legislative and regulatory environment"
ES 201 158	ETSI ES 201 158	"Telecommunications security; Lawful Interception (LI); requirements for network functions" (2002-02)
TR 103 308	ETSI TR 103 308	TC CYBER: Security baseline regarding LI and RD for NFV and related platforms" (2016-01)
ETSI LI HI1	ETSI TS 102 232-1	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery
ETSI GR ETI 002	ETSI GR ETI 002	ETSI GR ETI 002 Encrypted Traffic Integration (ETI); Requirements definition and analysis https://www.etsi.org/deliver/etsi_gr/ETI/001_099/002/01.01.01_60/gr_ETI002v010101p.pdf

Ref	Doc Number	Title
ETSI QSC	ETSI QSC	ETSI Quantum-Safe Cryptography (QSC) https://www.etsi.org/technologies/quantum-safe-cryptography
Falcon	Falcon	Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU https://falcon-sign.info/falcon.pdf
Frodo	Frodo	FrodoKEM: Learning With Errors Key Encapsulatio https://frodokem.org/files/FrodoKEM-standard_proposal-20230314.pdf
G-CECPQ2		The Chromium Projects: CECPQ2 https://www.chromium.org/cecpq2/
G-Hybrid		Chromium Blog: Protecting Chrome Traffic with Hybrid Kyber KEM https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html
GSMA-PQ.01	GSMA-PQ.01	Post Quantum Telco Network Impact Assessment Whitepaper Version 1.0 17 February 2023
GSMA-PQ.02	GSMA-PQ.02	Guidelines for Quantum Risk Management for Telco Version 1.0 22 September 2023
GSMA-FS.27	GSMA-FS.27	FS.27 Security guideliens for UICC Profileshttww.gsma.com/security/resources/fs-27-security-guidelines-for-uicc-profiles/
GSMA-FS.28	GSMA-FS.28	FS.28 Secuirty Guidelines for Eschange of UICC Credentials https://www.gsma.com/security/resources/fs-28-security-guidelines-for-exchange-of-uicc-credentials/
GSMA SGP.02	GSMA SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
GSMA SGP.22	GSMA SGP.22	eSIM Consumer Technical Specification
GSMA SGP.32	GSMA SGP.32	eSIM IoT Technical Specification
GSMA Landscape	N/A	GSMA Mobile Telecommunications Security Landscape, Feb 2024 https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/02/Security-Landscape-2024-Issue-1.0.pdf
HQC	HQC	Hamming Quasi-Cyclic (HQC) https://pqc-hqc.org/download.php?file=hqc-specification_2023-0430.pdf

Ref	Doc Number	Title
IETF-TLS-hybrid	IETF-TLS-hybrid	Hybrid key exchange in TLS 1.3 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
IETF-draft-flo	IETF-draft-flo	IETF Draft "Terminology for Post-Quantum Traditional Hybrid Schemes" https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/
IETF dr-ounsworth	IETF dr-ounsworth	IETF Draft: "Composite Signatures For Use In Internet PKI https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/
IETF-CFRG	IETF-CFRG	IETF Crypto Forum Research Group (CFRG): https://datatracker.ietf.org/rg/cfrg/documents/
IETF PQUIP	IETF PQUIP	Post-Quantum Use In Protocols https://datatracker.ietf.org/wg/pquip/documents/
IKE-v1-RFC	RFC-2409	The Internet Key Exchange https://datatracker.ietf.org/doc/html/rfc2409
IKE-v2-RFC	RFC-7296	Internet Key Exchange Protocol Version 2 https://datatracker.ietf.org/doc/html/rfc7296
IETF-IKEv2-hybrid	RFC-9370	Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 https://datatracker.ietf.org/doc/rfc9370/
IETF-IKEv2-mixing	RFC-8784	Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 https://datatracker.ietf.org/doc/html/rfc8784
IKE-INT	RFC-9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 https://datatracker.ietf.org/doc/html/rfc9242
IETF-x.509		IETF Hackathon: PQC Certificates https://github.com/IETF-Hackathon/pqc-certificates
ISO 18033-2	ISO 18033-2	Encryption algorithms — Part 2: Asymmetric ciphers https://www.iso.org/standard/37971.html
ISO/SAE 21434	ISO/SAE 21434	ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering
KPQC	KPQC	Selected Algorithms from the KpqC Comptetion round 1 https://kpqc.or.kr/
Kyber	Kyber	Algorithm Specifications And Supporting Documentation https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf
McEliece	McEliece	Classic McEliece: conservative code-based cryptography: cryptosystem specification https://classic.mceliece.org/mceliece-spec-20221023.pdf
NCSC 2023	NCSC 2023	Next steps in preparing for post-quantum cryptography https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

Ref	Doc Number	Title
NIST PQC	NIST PQC	Post-Quantum Cryptography Standardization https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
NIST 800-56A	NIST 800-56A	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final
NIST 800-56B	NIST 800-56B	Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography https://csrc.nist.gov/publications/detail/sp/800-56b/rev-2/final
NIST 800-56C	NIST 800-56C	Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final
NIST SP 800-207	NIST SP 800-207	Zero Trust Architecture https://csrc.nist.gov/pubs/sp/800/207/final
NIST-FAQ	NIST-FAQ	Post-Quantum Cryptography FAQs https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs
NIST FIPS 203	NIST FIPS 203	(Draft) Module-Lattice-based Key-Encapsulation Mechanism Standard https://doi.org/10.6028/NIST.FIPS.203.ipd
NIST FIPS 204	NIST FIPS 204	(Draft) Module-Lattice-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.204.ipd
NIST FIPS 205	NIST FIPS 205	(Draft) Stateless Hash-Based Digital Signature Standard https://doi.org/10.6028/NIST.FIPS.205.ipd
NIST On-Ramp	NIST On-Ramp	Request for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process https://csrc.nist.gov/News/2022/request-additional-pqc-digital-signature-schemes
NIST SP 800-56A	NIST SP 800-56A	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, https://doi.org/10.6028/NIST.SP.800-56Ar3
NIST SP 800-56B	NIST SP 800-56B	Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography, https://doi.org/10.6028/NIST.SP.800-56Br2
NIST SP 800-190	NIST SP 800-190	Application Container Security Guide, https://doi.org/10.6028/NIST.SP.800-190
NIST SP 800-208	NIST SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes, https://doi.org/10.6028/NIST.SP.800-208

Ref	Doc Number	Title
Open-QS	Open-QS	Open Quantum Safe: https://openquantumsafe.org
PKLN22		Paul, Y. Kuzovkova, N. Lahr, R. Niederhagen. “Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3”. AsiaCCS 2022
RFC 2986	RFC 2986	PKCS #10: Certification Request Syntax Specification https://datatracker.ietf.org/doc/html/rfc2986
RFC 4210	RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) (2005-09)
RFC 7296		Internet Key Exchange Protocol Version 2 (IKEv2) (2014-10)
RFC 8391	RFC 8391	XMSS: eXtended Merkle Signature Scheme https://www.rfc-editor.org/rfc/rfc8391
RFC 8446	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3"
RFC 8554	RFC 8554	Leighton-Micali Hash-Based Signatures https://www.rfc-editor.org/rfc/rfc8554
RFC 9242	RFC 9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) (2022-05)
RFC 9370	RFC 9370	Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) (2023-05)
SP 800-208	SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes https://csrc.nist.gov/publications/detail/sp/800-208/final
SPHINCS+	SPHINCS+	SPHINCS+ https://sphincs.org/data/sphincs+-r3.1-specification.pdf
TLS-1.3-RFC	RF C 8446	TLS-1.3 https://datatracker.ietf.org/doc/html/rfc8446
TLS-1.2-RFC	RFC 5246	TLS-1.2 https://datatracker.ietf.org/doc/html/rfc5246
TLS-1.1-RFC	RFC 4346	TLS-1.1 https://datatracker.ietf.org/doc/html/rfc4346
UK TSA		Telecommunications (Security) Act, 2021 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
PQ.03 version 1	21/02/2024	First version of PQ.03 Post Quantum Cryptography Guidelines for Telecom Use	TG	Yolanda Sanz, GSMA
PQ.03 v2 Draft 0	03/07/2024	First draft with the merge of the migration use cases Post Quantum Cryptography Migration Plan.docx using the template: 2024-07-02 LI Example Marked up v03.docx	PQTN	Yolanda Sanz, GSMA
PQ.03 v2 Draft 1	08/08/2024	Merged content of original PQ.03 and migration Use Case documents	PQTN	Zygmunt Lozinski, IBM

D.2 Other Information

Type	Description
Document Owner	Post Quantum Telco Network Task Force
Editor, Company	Catherine White, EE – Erik Thormarker, Ericsson – Taylor Hartley, Ericsson – Chitra Javali, Huawei – Jamie Chard, IBM – Lory Thorpe, IBM – Zygmunt Lozinski, IBM – Jerome Dumoulin, IDEMIA – Gert Grammel, Juniper Networks – Saïd Gharout, KIGEN – Gareth T. Davies, NXP – Loïc Ferreira, Orange – Olivier Sanders, Orange – Anthony Bord, Thales – Diego Lopez, Telefonica – Michaela Klopstra, Utimaco –

	Darshan Lakha, Vodacom – Luke Ibbetson, Vodafone – Guenter Klas, Vodafone – Kristian McDonald, Vodafone – Gabriela Radu, Vodafone Ryan Parker, Vodafone Simon Bryden, Fortinet Ivo Rodrigues, Nokia Vinod Choyi, Verizon

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.