Post Quantum Cryptography – Guidelines for Telecom Use Cases

Version 1.0

22 February 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

Table of Contents

1 Introduction 8
1.1 Overview 8
1.2 Scope 8
1.3 Intended Audience 9
2 Executive Summary 9
3 Planning: Timelines and Dependencies 11
3.1 Phases (High Level) 11
3.1.1 Capability and Skills Development 12
3.1.2 Cryptography Discovery and Analysis 12
3.1.3 Business Risk Analysis 12
3.1.4 Prioritisation, Planning and Governance 13
3.1.5 Remediation Execution 13
3.1.6 Operation and Ongoing Crypto-Governance 13
3.2 Post Quantum Government Initiatives by Country and Region 13
3.3 Preliminary Recommendations for Automation 13
3.4 Algorithm Standardisation: Asymmetric Cryptography 14
3.4.1 Key Establishment 14
3.4.2 Stateless Digital Signatures 15
3.4.3 Stateful Digital Signatures 16
3.5 Migration Options 16
3.5.1 Hybrid Schemes 17
3.5.2 Digital Signatures for Code Signing 17
3.6 Impact on Symmetric Cryptography 17
3.6.1 Symmetric Key Sizes 17
3.7 Impact on Hash Functions 18
3.8 Impact on Widely-used Protocols (TLS, IPSec) 19
3.8.1 Transport Layer Security Protocol (TLS) 19
3.8.2 Internet Key Exchange Protocol (IKE) 20
3.8.3 Cryptographic Inventory Implications 20
3.9 Zero Trust Architecture Framework Consideration 21
3.9.1 Zero Trust Architecture in the Context of Post Quantum Cryptography 21
4 Telco Use Cases: System Impacts and Guidelines 22
4.1 List of Use Cases 23
4.1.1 Internal to MNO Use Cases 23
4.1.2 Customer Facing Use Cases 23
4.2 Use Case: Protection and Configuration / Management of Link between Base Stations and Security Gateway 23
4.2.1 Scope 23
4.2.2 Sensitive Data Discovery 24
4.2.3 Cryptographic Inventory 24
4.2.4 Migration Strategy Analysis and Impact Assessment 26
4.2.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 26
4.2.6 Standards Impact (current and future) and Maturity 27

4.2.7 Stakeholders 28
4.2.8 PKI Implications 28
4.2.9 Legacy Impact 28
4.2.10 Potential Actions/Dependencies 29
4.3 Use Case: Virtualized network function integrity 29
4.3.1 Scope 29
4.3.2 Sensitive Data Discovery 30
4.3.3 Cryptographic Tools 30
4.3.4 Cryptographic Inventory 31
4.3.5 Migration Strategy Analysis and Impact Assessment 31
4.3.6 Implementation Roadmap (Crypto-Agility and PQC Implementation) 32
4.3.7 Standards (and Open Source) Impact 32
4.3.8 Stakeholders 32
4.3.9 PKI Implications 32
4.3.10 Legacy Impact 32
4.3.11 Potential Actions/Dependencies 33
4.4 Use Case: Cloud Infrastructure 33
4.4.1 Scope 33
4.4.2 Sensitive Data Discovery 33
4.4.3 Cryptographic Inventory 34
4.4.4 Migration Strategy Analysis and Impact Assessment 34
4.4.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 34
4.4.6 Standards and Open Source Impact 35
4.4.7 Stakeholders 35
4.4.8 PKI Implications 35
4.4.9 Legacy Impact 35
4.4.10 Potential Actions/ Dependencies 36
4.5 SIM Provisioning (physical SIM) 36
4.5.1 Scope 36
4.5.2 Sensitive Data Discovery 36
4.5.3 Cryptographic Inventory 37
4.5.4 Migration Strategy Analysis and Impact Assessment 37
4.5.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 37
4.5.6 Standards Impact (current and future) and Maturity 38
4.5.7 Stakeholders 38
4.5.8 PKI Implications 38
4.5.9 Legacy Impact 38
4.5.10 Potential Actions/ Dependencies 38
4.6 Remote SIM Provisioning 38
4.6.1 Scope 38
4.6.2 Sensitive Data Discovery 38
4.6.3 Cryptographic Inventory 39
4.6.4 Migration Strategy Analysis and Impact Assessment 41
4.6.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 42
4.6.6 Standards Impact (current and future) and Maturity 43

4.6.7 Stakeholders 43
4.6.8 PKI Implications 44
4.6.9 Legacy Impact 44
4.6.10 Potential Actions/ Dependencies 44
4.7 Firmware Upgrade / Device Management 44
4.7.1 Scope 44
4.7.2 Sensitive Data Discovery 44
4.7.3 Cryptographic Inventory 45
4.7.4 Migration Strategy Analysis and Impact Assessment 45
4.7.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 46
4.7.6 Standards Impact (current and future) and Maturity 46
4.7.7 Stakeholders 47
4.7.8 PKI Implications 47
4.7.9 Legacy Impact 47
4.7.10 Potential Actions / Dependencies 47
4.8 Concealment of the Subscriber Public Identifier 47
4.8.1 Scope 47
4.8.2 Sensitive Data Discovery 48
4.8.3 Cryptographic Inventory 48
4.8.4 Migration Strategy Analysis and Impact Assessment 49
4.8.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 49
4.8.6 Standards Impact (current and future) and Maturity 50
4.8.7 Stakeholders 50
4.8.8 PKI Implications 50
4.8.9 Legacy Impact 50
4.8.10 Potential Actions/ Dependencies 50
4.9 Authorization and Transport Security in 4G (MME-S-GW-P-GW) 50
4.9.1 Scope 50
4.9.2 Sensitive Data Discovery 51
4.9.3 Cryptographic Inventory 51
4.9.4 Migration Strategy Analysis and Impact Assessment 51
4.9.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 51
4.9.6 Standards Impact 52
4.9.7 Stakeholders 52
4.9.8 PKI Implications 52
4.9.9 Legacy Impact 52
4.9.10 Potential Actions/ Dependencies 52
4.10 Authentication and Transport Security in 5G: Quantum Safe TLS between Components of 5G Core Network (SBA) 53
4.10.1 Scope 53
4.10.2 Sensitive Data Discovery 53
4.10.3 Cryptographic Inventory 54
4.10.4 Implementation Roadmap (Crypto-agility and PQC Implementation) 56
4.10.5 Standards Impact (current and future) and Maturity 56
4.10.6 Stakeholders 57

4.10.7 PKI Implications 57
4.10.8 Legacy Impact 57
4.10.9 Potential Actions/ Dependencies 57
4.11 Use Case: Virtual Private Networks 58
4.11.1 Scope 58
4.11.2 Sensitive Data Discovery 58
4.11.3 Cryptographic Inventory 59
4.11.4 Migration Strategy Analysis and Impact Assessment 59
4.11.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 60
4.11.6 Standards Impact (current and future) and maturity 60
4.11.7 Stakeholders 61
4.11.8 PKI Implications 61
4.11.9 Legacy Impact 61
4.11.10 Potential Actions/ Dependencies 61
4.12 Software Defined Wide Area Networks (SD-WAN) 61
4.12.1 Scope 61
4.12.2 Sensitive Data Discovery 62
4.12.3 Cryptographic Inventory 62
4.12.4 Migration Strategy Analysis and Impact Assessment 62
4.12.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 63
4.12.6 Standards Impact (current and future) and Maturity 63
4.12.7 Stakeholders 63
4.12.8 PKI Implications 63
4.12.9 Legacy Impact 63
4.12.10 Potential Actions/ Dependencies 64
4.13 Privacy (Lifecycle) of Customer Personal Data 64
4.13.1 Scope 64
4.13.2 Sensitive Data Discovery 64
4.13.3 Cryptographic Inventory 65
4.13.4 Stakeholders 65
4.13.5 PKI Implications 65
4.13.6 Legacy Impact 65
4.13.7 Potential Actions/ Dependencies 65
4.14 Lawful Intercept (and Retained Data) 66
4.14.1 Scope 66
4.14.2 Cryptographic Inventory 66
4.14.3 Migration Strategy Analysis and Impact Assessment 66
4.14.4 Implementation Roadmap (Crypto-agility and PQC Implementation) 66
4.14.5 Standards Impact (current and future) and Maturity 67
4.14.6 PKI Implications 67
4.14.7 Legacy Impact 67
4.14.8 Potential Actions/ Dependencies 67
4.15 IoT Services 67
4.15.1 Smart Meters Connectivity 67
4.15.2 Automotive 70

4.16 Enterprise Data 72
4.16.1 Scope 72
4.16.2 Sensitive Data Discovery 73
4.16.3 Cryptographic Inventory 73
4.16.4 Migration Strategy Analyses and Impact Assessment 74
4.16.5 Implementation Roadmap (Crypto-agility and PQC Implementation) 74
4.16.6 Standard Impact (current and future) and Maturity 74
4.16.7 Stakeholders 74
4.16.8 PKI Implication 74
4.16.9 Legacy Impact 75
4.16.10 Potential Actions 75
5 Algorithm Testing and Implementation 75
Annex A Post Quantum Government Initiatives by Country and Region 77
A.1 Australia 79
A.1.1 PQC Algorithms 79
A.1.2 Published Recommendations 79
A.1.3 Timeline 79
A.2 Canada 80
A.2.1 PQC Algorithms 80
A.2.2 Published Recommendations 80
A.2.3 Timeline 81
A.3 China 81
A.4 PQC Algorithms 81
A.4.1 Published Recommendations 81
A.4.2 Timeline 81
A.5 European Commission 82
A.5.1 Published Recommendations 82
A.5.2 Timeline 82
A.5.3 A.4.3 Other Information 82
A.6 Japan 83
A.6.1 PQC Algorithms 83
A.6.2 Published Recommendations 83
A.6.3 Timeline 84
A.6.4 Other Information 84
A.7 The Netherlands 84
5.1.1 PQC Algorithms 84
5.1.2 Published Recommendations 84
A.8 New Zealand 84
A.8.1 PQC Algorithms 84
A.8.2 Published Recommendations 85
A.8.3 Timeline 85
A.9 Singapore 85
A.9.1 PQC Algorithms 85
A.9.2 Published Recommendations 85

A.9.3 Timelines 85
A.9.4 Other Information 85
A.10 South Korea 86
A.10.1 PQC Algorithms 86
A.10.2 Published Recommendations 86
A.10.3 Timeline 86
A.10.4 Other Information 86
A.11 France 86
A.11.1 PQC Algorithms 86
A.11.2 Published Recommendations 87
A.11.3 Timeline 87
A.12 Germany 88
A.12.1 PQC Algorithms 88
A.12.2 Published Recommendations 88
A.12.3 Timeline 88
5.1.3 Other Information 89
A.13 UK 89
A.13.1 PQC Algorithms 89
A.13.2 Published Recommendations 89
A.13.3 Timelines 89
A.13.4 Other Information 89
A.14 USA 89
A.14.1 PQC Algorithms 89
A.14.2 Published Recommendations 90
A.14.3 Timeline 90
Annex B Definitions, Abbreviations and References 91
B.1 Definitions 91
B.2 Terminology 92
B.3 Abbreviations 92
B.4 References 98
Annex C Document Management 103
C.1 Document History 103
C.2 Other Information 104

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.

The Zero Trust framework, briefly covered in this document in Section 3.9, encompasses Quantum safe cryptography. The Telco use cases in Section 4 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.

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 first 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.

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

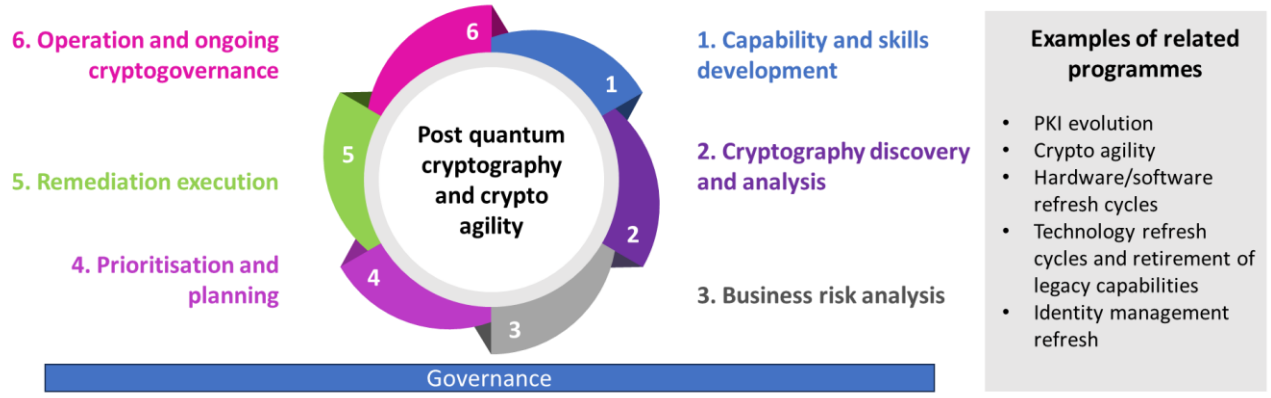

Figure 2: High Level Phases

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 Post Quantum Government Initiatives by Country and Region

Details on the Post Quantum Government initiatives are described in Annex A.

3.3 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.

3.4 Algorithm Standardisation: Asymmetric Cryptography

There are many ongoing efforts to select and standardize algorithms for key establishment and digital signatures that are intended to resist attackers with access to a cryptographically relevant quantum computer (CRQC). This subsection describes these standardization processes and the key features of the selected algorithms from the perspective of migration from traditional algorithms (that are vulnerable to CRQCs) based on elliptic curve cryptography and RSA.

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.

3.4.1 Key Establishment

New algorithms for Post Quantum key establishment are being defined by NIST and other national bodies.

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

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

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.

CRYSTALS-Kyber [Kyber] was selected by NIST as the only key encapsulation mechanism (KEM) in the third round of their PQC competition. NIST has released a draft standard under the name ML-KEM [NIST FIPS 203] and the final standard should be published as FIPS 203 in 2024. 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).

NIST chose to advance four other KEMs to their fourth round, though SIKE [SIKE] was shown to be insecure and has now been withdrawn. The remaining three algorithms are Classic McEliece [McEliece], BIKE [BIKE] and HQC [HQC], all of which based their security on computational problems in code-based cryptography. 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).

The BSI in Germany [BSI-TR-02102-1] and ANSSI in France [ANSSI22] are recommending the usage 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 (its design is based on *unstructured* lattices, which have received more cryptanalysis).

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].

3.4.2 Stateless Digital Signatures

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

CRYSTALS-Dilithium [Dilithium] was selected by NIST in the third round of their PQC competition as the primary digital signature candidate for standardization. NIST released a draft standard under the name ML-DSA [NIST FIPS 204] and the final standard should be published as FIPS 204 in 2024. Its 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).

In addition to ML-DSA, two further (non-primary) schemes were selected in the third round by NIST: Falcon [Falcon] and SPHINCS+ [SPHINCS+]. NIST released a draft standard for SPHINCS+ under the name SLH-DSA [NIST FIPS 205] and the final standard should be

published as FIPS 205 in 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).

The standards document for Falcon – which will be referred to as FN-DSA by NIST – will likely come after the 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, 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.

ML-DSA and FN-DSA are based on structured lattices, so in order 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.

3.4.3 Stateful Digital Signatures

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

The 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. 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 ensures that these one-time signature key pairs are only used once. The challenging 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. Conformance with NIST SP 800-208 [SP 800-208] even 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.

3.5 Migration Options

The migration from traditional cryptography to quantum resistant cryptography is not as straightforward as 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 will be underpinned by the cryptographic technologies and protocols that are standardised, then implemented in products, subsequently integrated and configured into solutions.

For telecommunication systems, operators must take an end-to-end solution view across the different systems to coordinate testing and deployment of quantum resistant solutions that consider crypto-agility, backward compatibility and interoperability. For this reason, we are strongly advocating the use of standardised algorithms, protocols and solutions as a way of facilitating migration and minimising cost.

As new products, protocols and solutions emerge, a key aspect to consider is around performance and reliability requirements related to the specific use cases.

For this reason, 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.

3.5.1 Hybrid Schemes

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). 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. This aspect is for further study.

3.5.2 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. Note that BSI only refer to XMSS/LMS for this standalone usage, while ANSSI also include SLH-DSA. As described above the stateful hash-based schemes have their own implementation challenges.

3.6 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.

3.6.1 Symmetric Key Sizes

Grover's algorithm provides a potential quantum advantage (compared to classical computers) for exhaustive key search on symmetric cryptography. 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. 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.

For example, ANSSI [ANSSI] recommends using 256-bits key size. Conversely, 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.

In 2022, the BSI [BSI-2022] recommendations read:

> *"However, when using keys with a length of 128 bits (or less), quantum computer attacks with Grover's search algorithm cannot be completely ruled out. Especially if long-term protection of data is important, a key length of 256 bits should therefore be provided for new developments in which a symmetric encryption algorithm is to be implemented."*

This statement therefore supported the use of 256-bit key without formally recommending it in general. However, in January 2023, the new 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.

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.

3.7 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. 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.

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

These protocols are developed and standardised by the IETF.

Relevant work in the IETF TLS working group:

- Hybrid key exchange in TLS 1.3: provides hybrid confidentiality, but not hybrid authentication
  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 a 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:

- Areas include:
  - 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 January 2024

Section 4 will present a number of use cases that are prevalent in the telco domain, and this section will describe some of the cryptographic protocols that are prevalent in multiple use cases in the context of migration to Post Quantum Cryptography.

3.8.1 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. 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.

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.

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.

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

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 draft [IETF-IKEv2-hybrid] has published in May 2023 for usage of the key exchange component of IKE v2 in hybrid mode. The idea is slightly different to 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].

3.8.3 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, DES
    - 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: e.g., DH-DSS-AES256-GCM-SHA384
  broken down into:
    - Key Exchange: DH (Diffie-Hellman)
    - Signature: DSS (Digital Signature Standard)
    - Cipher: AES256 (Advanced Encryption Standard)
    - Mode: GCM (Galois/Counter Mode), i.e., mode of operation for symmetric key cryptographic block ciphers
    - Digest/Used for PRN: SHA384

3.9 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).

3.9.1 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.

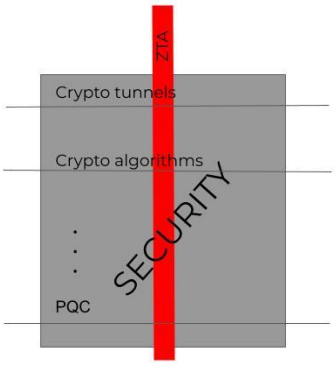

Figure 3: ZTA Framework within Security Realm

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

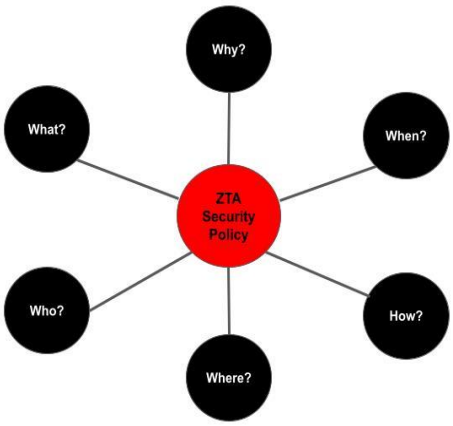

Figure 4: Kipling Method. Elements of ZT Security Policy

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 Telco Use Cases: System Impacts and Guidelines

4.1 List of Use Cases

4.1.1 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)

4.1.2 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

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

4.2.1 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. This connectivity is used e.g. for maintenance and upgrades of cryptographic parameters relevant for the connection between a base station and a SecGW.

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.

4.2.2 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.

4.2.3 Cryptographic Inventory

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

4.2.3.1 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.

4.2.3.2 Data in Transit between Base Station and Security Gateway

Data in transit over the base station/SecGW connection can be instead secured through the use of the IPSec protocol suite (in line with 3GPP) which creates a secure IP tunnel. The IPSec Encapsulating Security Payload protocol (ESP) can provide secure authentication and integrity via a message digest that among others also 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).

4.2.3.3 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: use of SSH (makes use of Diffie-Hellman key exchange itself), use of SFTP (which in turn uses SSH), HTTPS (which uses TLS), and SNMPv3 (which can use e.g., SSH or TLS/DTLS). In the case of TLS, all the public-key algorithms that are currently standardized for use in TLS are vulnerable to quantum attacks.

4.2.3.4 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 (c.f. 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.

4.2.3.5 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.

4.2.4 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.

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.

4.2.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

It is primarily the responsibility of network element vendors to implement new, quantum-safe capabilities for the given RAN/SecGW scope in line with new/upgraded standards released by standards defining organisations like IETF. Much or all of the network element software is closed and proprietary to the vendors. Network operators will need to manage the requirements for the introduction of quantum safe cryptography into base station and SecGW network elements as part of the implementation and monitoring of quantum safe solutions.

Any implementation roadmap to render the RAN backhaul to the core network quantum-safe can be decomposed into two parts:

1. A roadmap part which is agnostic of the particular mobile network domain (here backhaul between RAN and SecGW).

    a) This roadmap will be characterised by a sequence of milestones and deliverables (like new standards) to be achieved e.g. in standards

organisations like IETF and potentially 3GPP. This roadmap will be key for all 'downstream' uses of such deliverables, e.g. all network domains which make use of a quantum-safe version of IPSec, which includes the RAN/SecGW domain as well as others like VPNs for various purposes.

2. A roadmap part which is specific to the mobile network domain (here base station to SecGW connectivity including OAM). This roadmap has a partial dependency on the first roadmap. In addition, this roadmap must cater for:

    a. introduction of upgraded, quantum-safe PKI systems,
    b. development of network domain-specific crypto-agility requirements by network operators and issuance to their RAN and security gateway vendors,
    c. update of operator cryptographic requirements as relevant for the given scope including for at-rest and in-transit encryption, key management, PKI and certificate life cycle management,
    d. development and deployment of technical means to manage (understand, monitor, control, evaluate, configure) new cryptographic ciphers, protocols and supporting hardware devices.
    e. upgrades to base stations and security gateways depending on availability of quantum-safe feature implementations by vendors (e.g., for quantum-safe protocol stacks).

For reasons of cost efficiency, it is not recommended to introduce non-standardised quantum-safe technology or deploy pre-standard algorithms at scale.

4.2.6 Standards Impact (current and future) and Maturity

Given the reliance on secure protocols like TLS, IPSec and IKE, quantum-safe versions of these protocols will become important. Where the protocols are standardised by a particular organisation (like IETF), availability of the corresponding specifications depends on the progress made in the relevant working groups of that organisation.

Within IETF, relevant quantum-safe work is ongoing in the Crypto Forum Research Group (CFRG). IETF working groups rely on CFRG to define new PQC mechanisms, monitor progress in NIST and make recommendations to IETF working groups. The Internet Research Task Force (IRTF) is involved in researching quantum-safe new protocol versions and feeds results into IETF working groups.

IETF is preferring hybrid schemes, combining Post Quantum and traditional mechanisms (the terminology used in IETF, in short PQ/T), to transition the deployed infrastructure and make TLS and IPSec quantum safe. IETF is progressing work on PQ/T Hybrid Confidentiality (to protect from Store Now; Decrypt Later threats) and PQ/T Hybrid Authentication (to protect against on-path attacks). IETF is also exploring the security properties of hybrid solutions, their performance impact, security levels, deployability, crypto-agility and other aspects.

The most relevant IETF working groups for the RAN/SecGW scope are:

- IPSECME: for IPSec protocol suite
- TLS: for the TLS protocol
- LAMPS: for X.509 certificates, CMP (certificate management protocol)

- PQUIP: for common terminology in IETF for hybrid PQC and baseline information for engineers

For more details regarding work in those IETF working groups, see Section 4.7.

4.2.7 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 aforementioned working groups.

4.2.8 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

4.2.9 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. 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.

4.2.10 Potential Actions/Dependencies

To prepare for migration to quantum-safe status, dependencies on Internet standards (e.g., for TLS, IPSec) need to be considered. Very likely this influences the commercially viable and technically feasible starting point of a migration (new infrastructure or upgrades) on the side of service providers.

4.2.10.1 Potential actions for service providers:

- To raise Quantum Safe awareness with relevant suppliers of base stations and security gateways and to set out technology and timeline requirements for procurement activities

- To include Quantum Safe requirements in Open RAN standards and vendor roadmaps. Relevant organisations include:

    - O-RAN Alliance (o-ran.org): In particular, the next Generation Research Group (nGRG) is considering security and has been working on a “Research Report on Quantum Security” (report ID RR-2023-04).

    - Telecom Infra Project (TIP), Project Group OpenRAN

4.3 Use Case: Virtualized network function integrity

4.3.1 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.

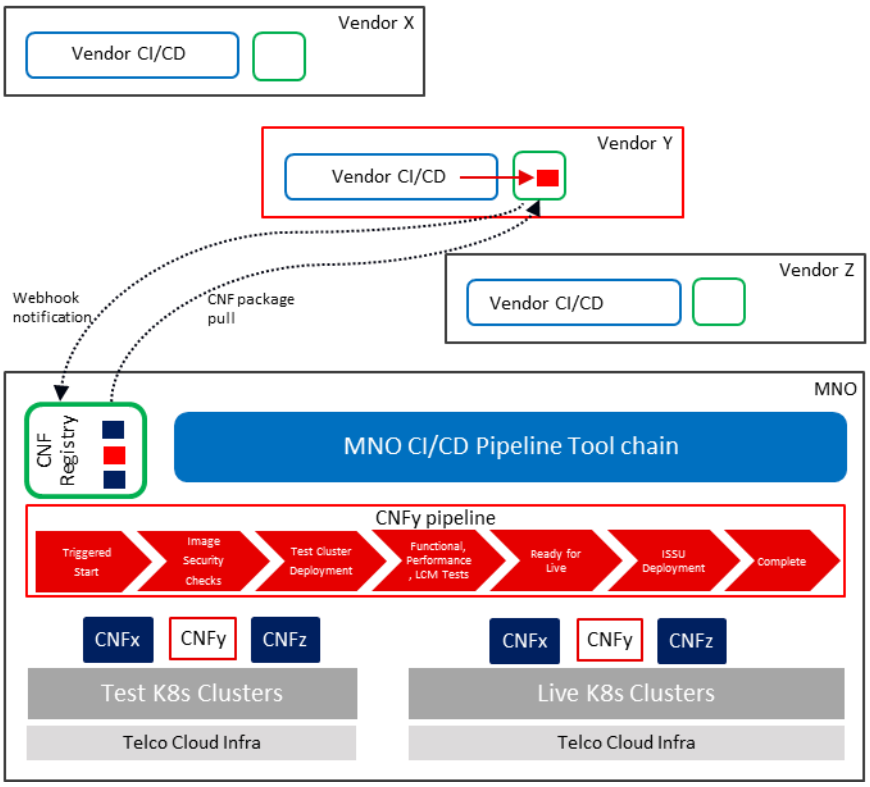

Figure 5: Typical Pipeline for the Deployment of Virtualised Network Functions**.**

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.

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.3.5 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.

4.3.6 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.

4.3.7 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.

4.3.8 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).

4.3.9 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.

4.3.10 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).

4.3.11 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 playes as critical infrastructure and thus one of the first verticals required to move to PQC.

4.4 Use Case: Cloud Infrastructure

4.4.1 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.

4.4.2 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.

4.4.3 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) appearing 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.

4.4.4 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 not utilising AES keys wrapped in non-QSC (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.

4.4.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

Cloud providers are making pre-standard implementations of PQC available so that cloud users can gain early experience with tools, workflow, and can test their workloads.

Cloud Provider	PQC Service
Amazon Web Services (AWS)	AWS Key Management supports pre-standard NIST PQC algorithms. AWS Transfer Family PQC support for SSH with hybrid keys.
IBM Cloud	PQC enabled TLS endpoints deployed in 2 regions for customer early experience. Support for both hybrid and pure PQC using pre-standard NIST algorithms.
Microsoft Azure	Microsoft has developed PQC enabled versions of OpenVPN, OpenSSL and OpenSSH
Google Cloud	Google Cloud is using Application Layer Transport Security with hybrid keys to secure internal traffic. Google Cloud Platform (GCP) have deployed TLS with pre-standard PQC to test interoperability.

Table 2: Cloud Providers & PQC Services

4.4.6 Standards and Open Source Impact

- 3GPP, ETSI ISG NFV, ETSI ISG MEC, IETF
- Open Infrastructure Foundation, Cloud Native Computing Foundation, Linux Foundation.

4.4.7 Stakeholders

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

4.4.8 PKI Implications

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

4.4.9 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.

4.4.10 Potential Actions/ Dependencies

Each cloud provider has different guidelines for customers migrating on-premises data to the cloud. Each cloud provider has unique services for cryptographic key management, (including support for BYOK, and HSM-as-service) and secrets management.

Developing and sharing best-practice for operators migrating IT and network workloads to cloud (and between clouds) is a potential action.

4.5 SIM Provisioning (physical SIM)

4.5.1 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 based on an initial shared secret, known as Master Key. The transfer of the Master Key must be protected against 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 3.4).

4.5.2 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 due to the use of the TLS/SFTP protocol.
- Connection between MNO HSM and UICC vendor HSM if the TLS/SFTP protocol 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

4.5.3 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 existing implementation in HSM, mainly symmetric encryption based on AES.

4.5.4 Migration Strategy Analysis and Impact Assessment

Migration in this use case is relatively straightforward insofar as the only components that requires 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.

4.5.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

Data transport that is conducted over a channel with TLS (or TLS-like) layer protection is subject to store-now-decrypt-later style attacks. The impacts are particularly acute in this use case because of the long-lived nature of the symmetric keys that are transmitted between MNOs and UICC vendors: using a CRQC to decrypt this data allows an adversary to decrypt network traffic between a UICC and base stations for the lifetime of the UICC. Moreover, via the OTA keys the attacker would get full access to the card content and card behaviour.

Furthermore, using a CRQC to compute a (TLS) certificate signing key for a UICC vendor would allow an adversary to impersonate that entity and thus receive UICC profiles for potentially millions of users.

This urgency means that communication channels between MNOs and UICC vendors should be migrated as soon as is feasible, at least initially in a hybrid mode [IETF-TLS].

4.5.6 Standards Impact (current and future) and Maturity

It will follow the evolution of TLS by IETF e.g.: IETF RFC: TLS 1.3, IETF Draft: Hybrid Key exchange in TLS 1.3"

HSM will evolve according to requirements of NIST certifications

Note: Algorithms leveraging symmetric keys within the UICC profile, such as TUAK, Milenage and the air interface confidentiality and integrity algorithms, are based on symmetric cryptography and are therefore less affected by the threats to asymmetric schemes (see Section 3.6). Moreover, these algorithms either already support longer key lengths (e.g. TUAK) or standardisation processes for variants supporting longer keys are under way.

4.5.7 Stakeholders

UICC vendors and their subcontractors. MNOs and MVNOs.

4.5.8 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.

4.5.9 Legacy Impact

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

4.5.10 Potential Actions/ Dependencies

At the time of writing this document, potential actions have not been identified.

4.6 Remote SIM Provisioning

4.6.1 Scope

In this use case, 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 the potential migration strategies for each of them.

4.6.2 Sensitive Data Discovery

A profile contains very sensitive data such as the long-term secret key K, the operator secret key OPc and the IMSI/SUPI. With such data, an adversary could authenticate to the operator on behalf of the legitimate user, impersonate the operator towards the user using this profile and even decrypt all their communications.

4.6.3 Cryptographic Inventory

As the cryptographic protocols present some differences between M2M, Consumer and IoT, we will consider each of them separately in what follows.

4.6.3.1 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 in the figure below.

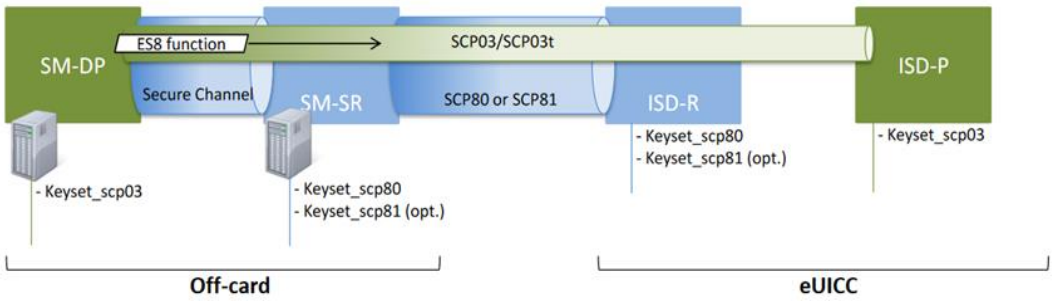

Figure 6: SM-DP/SM-SR/eUICC Channel

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.

4.6.3.2 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.

In all cases, 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.

4.6.3.3 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.

4.6.3.4 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.

4.6.3.5 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.

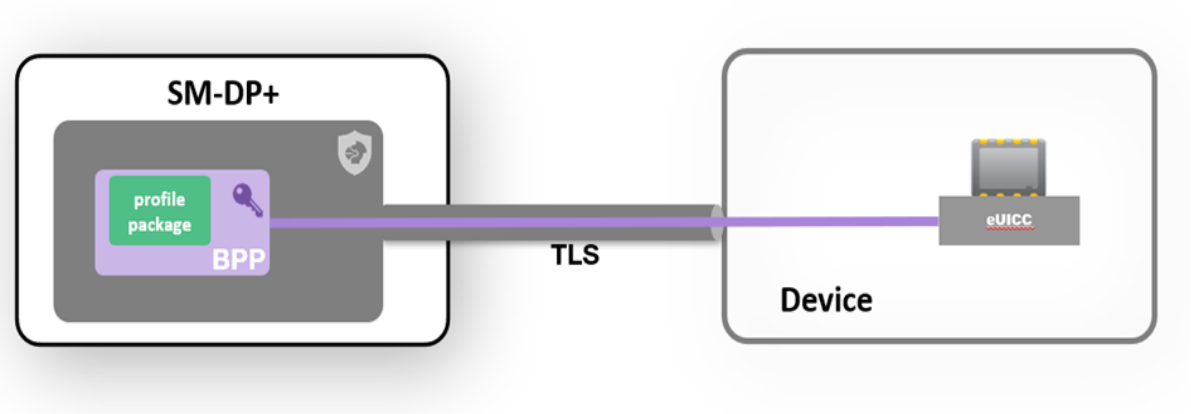

Figure 7: SM-DP+/Device Channel

4.6.3.5.1 SM-DP+/Device Channel

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.

4.6.3.5.2 SM-DP+/eUICC

The protection of the profile package is done using keys derived from a shared secret computed using 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 3.0.1 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.

4.6.3.6 IoT (SGP.32)

The security protocols for eSIM IoT are based on eSIM consumer specification. Therefore, section 4.6.3.5 applies in the eSIM IoT Context.

4.6.4 Migration Strategy Analysis and Impact Assessment

The very different nature of the M2M secure channels and the Consumer/IoT Device ones may lead to different strategies, depending on the security model considered.

4.6.4.1 M2M (SGP.02)

In the case of M2M, we consider the following two migration strategies with very different impacts on the system and the security model.

4.6.4.1.1 Strategy 1: Achieving Quantum Resistance for all Channels

This is the standard migration strategy which consists in upgrading each cryptographic primitive so as to achieve quantum resistance. The SM-DP eUICC channel will be highly impacted by this strategy as it would require implementing hybrid cryptography for every signature/certificate involved in the protocol described in Section 5.6.3.1 and to adapt this protocol to replace the current Diffie-Hellman key exchange by a hybrid key exchange mechanism.

The implementation efforts induced by this strategy are then very significant, but the security assurances would remain unchanged.

4.6.4.1.2 Strategy 2: Minimizing Changes

Another approach consists in leveraging the very different natures of the involved channels to retain some level of security without significant changes. The basic idea is that, although the key establishment protocol described in Section 4.6.3.1 cannot withstand quantum

computing, attacking the SM-DP/eUICC 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:** The 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 would prove more resistant to quantum computers than expected[1], 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.

The impact of Grover's algorithms on symmetric cryptography is discussed in Section 3.6.1.

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.

4.6.4.2 Consumer Device and eSIM IoT (SGP.22 and SGP.32)

In the case of SGP.22 and SGP.32, Profile Download is done through two channels but that essentially rely on the same cryptographic tools. An adversary able to break the security of one of them using a quantum computer would then have no difficulty in breaking the security of the other one. Any migration strategy should then consider updating these two channels at the same time.

4.6.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

Given that most of the symmetric primitives used in the cryptographic protocols are based on AES, one of the first modification could be to consider the use of 256-bit keys for this block cipher. As mentioned above, this could even act as a global risk mitigation in the case of M2M.

The case of asymmetric cryptography is more complex as we need to take three concrete issues in practice:

- There is no Post Quantum drop-in replacement for Diffie-Hellman key exchange in the future NIST/ISO standards and others.

- The protocols involve many signatures/certificates generation/verification, in particular in the case of SGP.22/SGP.32
- The eUICC has limited computational power and has a limited bandwidth.

The first item implies that any modification of the current specifications cannot be restricted to a mere substitution of the current algorithms by Post Quantum variants, although the necessary changes to use Key Encapsulation Mechanism (like ML-KEM) are not dramatic. In all cases, the replacement of the current Diffie-Hellman key exchange is the most pressing matter as this component is the key to prevent the so-called “store now, decrypt later” attack.

Together, the last two items also question the ability of simply replacing current digital signatures schemes with Post Quantum ones. A complexity evaluation should at least be performed before initiating such a replacement. One could note that the operations involving signatures or certificates are not at risk before the advent of computationally relevant quantum computers. For example, forging a signature for communications which happened in the past would be pointless. Migration to Post Quantum signatures could then follow a more gradual process. Concretely, the standards would have to be updated to support hybrid signatures, but the implementation and the use of such mechanisms could potentially differ according to the following criteria:

- Lifespan: a tentative date for the realisation of a CRQC could be determined based on the advances in this area. Any device which is not expected to be active after this date would then not need to implement hybrid signatures.

- Revocability: the other devices would support hybrid signatures but could still only use classical signatures as long as the corresponding certificates can be revoked before the advent of a CRQC. Once this revocation occurred, the devices would switch to the hybrid mode. The benefit of this solution is that the performances would not be affected in the period preceding the revocation. This does not take into account the possible option of using hybrid solutions, taking into consideration implementation constraints.

4.6.6 Standards Impact (current and future) and Maturity

SGP.02 [GSMA SGP.02]
SGP.22 [GSMA SGP.22]
SGP 32 [GSMA SGP.32]

4.6.7 Stakeholders

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

4.6.8 PKI Implications

In all the architectures considered, every entity owns a certificate in order to ensure authentication during secure channel establishment. All the certificates share the same root. Their migration should be planned in a consistent way, but several versions of the certificates could coexist, as explained in section 4.6.5..

4.6.9 Legacy Impact

In the case of the SGP 02, we have already noted that some level of security could be retained in some situations.

For all the other cases (and architectures), all security assurances are lost with respect to an adversary access to cryptographically relevant quantum computing. Worse, if the profile download procedure has been subject to a “store now, decrypt later” attack, then security of all past communications involving this profile would be compromised. From the security standpoint, continuing to support such legacy systems would therefore require assessing the plausibility of such a kind of attacks.

4.6.10 Potential Actions/ Dependencies

The GSMA eSIM Group has created a work item to generate a technical report to understand the impact of PQC in the context of eSIM.

4.7 Firmware Upgrade / Device Management

4.7.1 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.

4.7.2 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)

4.7.3 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.

4.7.4 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.)

4.7.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

One interesting option, in case asymmetric cryptography is used for firmware signature, is to use Stateful Hash-Based signatures. Two Stateful Hash-Based Signature schemes LMS and XMSS were published in 1995 and 2011. These two schemes were standardized by the IETF in RFC 8554 and RFC 8391. In October 2020, NIST finalized the PQC standard SP800-208 based on a subset of the parameters in the RFCs. Stateful Hash-Based Signature are quantum-safe, mature and trusted. Regarding their maturity, they don't require hybridization. Generally speaking, Stateful Hash-Based Signature have a couple of disadvantages, that are not applicable to firmware signing, making them a good option for the Use Case:

- Need to define upfront the maximum number of signatures
- Size of the signature is linked to the maximum number of signatures

Stateful Hash-Based Signature algorithms allow a finite number of signatures. For the firmware signing Use Case, assuming 1024 signatures over the lifetime of the key, the signature size is approximately 3kB signature size. This is a good match for the Use Case.The main concern is implementation of Stateful Hash-Based Signature is that itrequires careful state management. .essential, with any used private key being reliably deactivated before the corresponding signature is released. See Section 3.4 for a more detailed discussion on guidelines for usage of Stateful Hash-Based Signature algorithms.

The main concern regarding the implementation of Stateful Hash Based Signature is that it requires careful state management, with reliable deactivation of used private keysahead of the release of the corresponding signature. See section 3.4 for more details on Stateful Hash Based Signature algorithm usage.

On embedded devices, verification will generally not be a performance bottleneck, and time is dominated by hashing operations.

Key generation can take minutes or even hours, depending on the number of expected signatures, but it is generally done by an HSM, outside of the embedded device. Key generation may be significantly accelerated with cryptographic hash accelerator (around 85% of the compute time is performing hash compression computation).

4.7.6 Standards Impact (current and future) and Maturity

Stateful Hash-Based Signature are already specified:

- RFC 8391 XMSS (2018)
- RFC 8554 LMS (2019)
- NIST SP 800-208 approves the use of some but not all of the parameterr sets defined in the above RFCs, and also defines some new parameter sets

Although backup/restore operations of LMS/XMSS keys are currenlty not allowed in FIPS, some discussions are still active regarding “key transfer” between two FIPS certified HSMs in certain conditions.

4.7.7 Stakeholders

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

4.7.8 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.

4.7.9 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.

4.7.10 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).

4.8 Concealment of the Subscriber Public Identifier

4.8.1 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. The main problem of this solution, which has been pointed out in several papers[1][2][3], is that this backup procedure can easily be triggered by an adversary so as 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. In this section, we evaluate the impact of quantum computing on this procedure.

4.8.2 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.

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.

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.

4.8.3 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

[1] Another Look at Privacy Threats in 3G Mobile Telephony | SpringerLink

[2] Defeating IMSI Catchers | Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

[3] arxiv.org/pdf/1510.07563.pdf

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.

4.8.4 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 dramatically 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 is the most challenging one given the constrained nature of the device.

4.8.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

As any data whose confidentiality is protected using asymmetric cryptography, SUPI are subject to the "Store Now Decrypt Later" attack. Migrating to Post Quantum SUCI should then not wait for the advent of quantum computers powerful enough to break Diffie-Hellman.

As mentioned above, the current specifications allow 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 specifications.

4.8.6 Standards Impact (current and future) and Maturity

3GPP TS 33.501: Security architecture and procedures for 5G System

4.8.7 Stakeholders

- SIM card manufacturers
- SIM card vendors
- Network Operators

4.8.8 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.

4.8.9 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.

4.8.10 Potential Actions/ Dependencies

- 3GPP TS 33.501 will need to adopt a Quantum Safe mechanism for concealment of the SUCI as the current approach is vulnerable to attack. This creates a standards dependency for network operators choosing to implement the security procedures in 3GPP TS 33.501.
- However, the current standard also provides an option for operators to use their own protection scheme if desired. Operators choosing this latter path will need to ensure that their proprietary schemes are Quantum safe.

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

4.9.1 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 that can record encrypted traffic today and, in the future, holds a CRQC may run Shor's quantum algorithm to target the individual ephemeral Diffie-Hellman keys (i.e., a store now, decrypt later attack). Breaking a Diffie-Hellman key breaks 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.

4.9.2 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.

4.9.3 Cryptographic Inventory

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

4.9.4 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.

4.9.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

Once NIST PQC standards are published, IETF can standardize their usage in IKEv2, 3GPP can specify them in relevant profiles, and vendors can implement them as options for algorithm negotiation in the protocol. Key establishment is more straightforward as it depends only on IKEv2 and implementations. The IETF may need to standardize specifically how IKEv2 deals with the communication overhead of quantum-resistant key establishment regarding IP fragmentation (see e.g., https://datatracker.ietf.org/doc/draft-tjhai-ipsecme-hybrid-qske-ikev2/). Quantum-resistant authentication depends on supporting the new NIST

PQC digital signature algorithms also in PKI and X.509 certificates. PKI in turn depends on for example hardware security modules to support the new algorithms. Standardization work is ongoing in the IETF, discussing for example different options in supporting so-called hybrid signatures in certificates.

4.9.6 Standards Impact

As explained above, affected standards include NDS/IP in 3GPP (e.g. 33.210 and 33.310) and IKEv2 standards in the IETF. For the authentication, the impact is also broader, including standards for X.509 certificates and PKI.

4.9.7 Stakeholders

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

4.9.8 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].

4.9.9 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.

4.9.10 Potential Actions/ Dependencies

- Equipment 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.
- Cloud Infrastructure:
    - The next-generation algorithms should be supported by the virtualization cloud-based infrastructure providers where cryptographic processing has hardware dependencies (e.g. Hardware Security Modules, remote attestation).
- Operators:
    - alignment with equipment infrastructure procurement cycles to ensure adoption of PQC capabilities.

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

4.10.1 Scope

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 the intra and inter-PLMN components of the 5G SBA.

The 5G SBA is designed based on virtualization and container technologies that helps to deploy scalable and flexible architectures. The NF service providers provide service to the NF service consumers. An example of interactions between the NF service producers and consumers are request/response or subscribe/notify. The communication between the NFs has to be secure and service APIs for producers and consumers must be authorized. The following diagram shows the service-based interface (SBI) between the different network functions and the N32 interface between different network operators. The N32 interface must also be secured and mutually authenticated. According to [TS 33.501], the N32 security could be achieved using mutual-TLS for direct operator interconnectivity, or PRINS when there are intermediaries between operators.

[3GPP TS 23.501] depicts the 5G system architecture with SBI. Figure 1. shows a simplified representation of the roaming 5G system architecture.

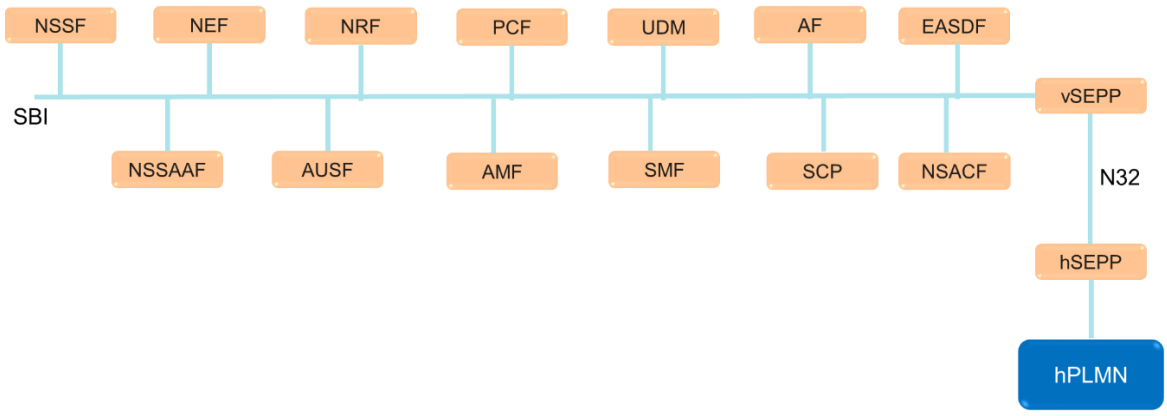

Figure 8: 5G SBA showing SBI and N32 interface

4.10.2 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 Management (UDM) NF. 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.

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

4.10.3 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 For DHE: Diffie-Hellman groups of at least 4096 bits should be supported	AES 128 (possibly weak), ECDHE, DHE, ECDSA, RSA, SHA256
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 3: 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.

4.10.3.1 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.

4.10.3.2 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.

4.10.4 Implementation Roadmap (Crypto-agility and PQC Implementation)

The implementation roadmap process involves standardization bodies and equipment manufacturers, infrastructure providers who are required to implement the protocol and algorithms. The process includes the following 4 steps:

- Step 1: Standardization of algorithms (NIST): [NIST-PQC] has been in the process of standardizing the PQC algorithms and after multiple rounds of evaluation, NIST has announced ML-KEM and ML-DSA as primary KEM and digital signature algorithms. More details of the NIST standardisation process is provided in Section 3.4. NIST plans to complete standardisation of these algorithms by 2024.
- Step 2: Standardization of protocol: The working group of ETSI as Cyber Quantum-Safe Cryptography (QSC) group [ETSI QSC] has been actively working on Post Quantum Safe algorithms. QSC focuses on architectural consideration for specific applications, implementation capabilities, performance, etc. The Crypto Forum Research Group (CFRG) [IETF-CFRG]] is working on the protocols that are complaint with the PQC such as hybrid Post Quantum KEM.
- Step 3: Implementation of protocol and algorithm: Generally cryptographic libraries that are verified and validated are commonly used rather than coding from the scratch. If implemented it is necessary to code the cryptographic algorithms correctly so as to avoid introducing security flaws such as side channel attacks. Limited open source libraries exist that are Post Quantum Safe. Open Quantum Safe [Open-QS] is an open-source project consisting of liboqs which is a C library for quantum-safe cryptographic algorithms and prototype integrations into protocols and applications, including the widely used OpenSSL library.
- Step 4: Real deployment in products: Replacing the existing products with quantum-safe algorithms will be a challenging task. With reference to previous migration deployments the process shall be time and resource consuming. For instance, though the specifications were released for SHA-256 the migration process happened for more than 5 years from SHA-1 to SHA-256 [Missing Reference - was 13 ?].

The crypto-agility of hybrid key exchange procedures in the SBA architecture between the NF server and NF client should be able to support multiple pair of algorithms so that when a pair of algorithms is found to be vulnerable, the switching to a new pair happens automatically. The NF server or client can come to a consensus for newer algorithms, or even agree to the old algorithms when appropriate.

In order to design a crypto-agile digital signature, it may not be mandatory for either the clients or the servers to implement all the component signature algorithms in the composite signature. A minimum set of component signatures can be verified by the client to proceed with the verification. Incorporating such a migration strategy will help for a smooth migration and provide time for all the clients or servers to implement the all specified component signatures. Another approach is to use the X.509 extensions to include the additional signature schemes and public keys. Only for critical extensions the clients must process both the traditional and alternative signature schemes part, however for non-critical extensions the clients may ignore the alternative signature schemes.

4.10.5 Standards Impact (current and future) and Maturity

Following are the standards that can impact the migration:

- NIST. Draft FIPS 203, 204 and 205
- IETF Draft: Hybrid Key Exchange TLS 1.3
- IETF Draft: Composite Signatures for Use in Internet PKI

Following are the standards that may be impacted:

- 3GPP TS 23.501: System architecture for the 5G System (5GS)
- 3GPP TS 33.501: Security architecture and procedures for 5G System
- 3GPP TS 33.210: Network Domain Security (NDS); IP network layer security

4.10.6 Stakeholders

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

4.10.7 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

4.10.8 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

4.10.9 Potential Actions/ Dependencies

- Equipment 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 5G 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.

- Cloud infrastructure providers:
    - Support for the use of Post Quantum algorithms by 5G SBA workloads. Performance testing of 5G SBAworkloads to ensure the resources are available to provide transport level security for all TLS connections.

- Operators:

- alignment with equipment infrastructure procurement cycles to ensure adoption of PQC capabilities.

4.11 Use Case: Virtual Private Networks

4.11.1 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.

4.11.2 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.

4.11.3 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.

4.11.4 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.

4.11.5 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.

4.11.6 Standards Impact (current and future) and maturity

VPNs execute according to protocols such as TLS and IPSec, which are specified by standardisation bodies. The use of hybrid modes, combining traditional and PQ cryptography, can help ensure compliance with existing (traditional) standards prior to

finalisation of PQC standards. This approach is suggested by NIST, to ensure e.g. FIPS compliance in the interim; see the NIST Post Quantum Cryptography FAQ (available at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs). Attention is also drawn to the NIST Special Publication 800-77 Revision 1, Guide to IPsec VPNs.

Regarding TLS, RFC 8784 [IETF-IKEv2-mixing] describes the mixing of pre-shared keys into IKEv2. Furthermore, IETF draft [IETF-TLS-hybrid] has been proposed to standardise the methods of hybrid key exchange used in TLS 1.3. Similarly, an IETF draft [IETF-IKEv2-hybrid] describes the use of hybrid key exchange methods in IKEv2, as used to established shared keys in IPSec VPNs.

4.11.7 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.

4.11.8 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.

4.11.9 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.

4.11.10 Potential Actions/ Dependencies

Operators and vendors should remain abreast of evolving standards.

4.12 Software Defined Wide Area Networks (SD-WAN)

4.12.1 Scope

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

An SD-WAN includes multiple nodes, typically spread across distinct sites, and control and orchestration elements. Initiation or termination points of SD-WAN VPNs are sometimes referred to as edge elements, and SD-WAN gateways are edge elements that allow sites

connected by the SD-WAN to also connect via other technologies (e.g. MPLS VPNs). The precise function of the control/orchestration elements can vary among products offered by distinct vendors but, in general, a key role is played by the security controller elements, which ensure that nodes behave according to specified security policies. Nodes are configured by the security controller, usually in accordance with a Network Configuration Protocol. Internode communication initially proceeds via a security controller, which can enable nodes to establish a direct VPN connection, subsequently allowing direct secure internode communication. Hence, SD-WANs are systems for dynamically establishing and evolving networks, within which internode communication can be secured by VPNs. 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. With regard to quantum safe considerations, the SD-WAN use case may be conceptualised primarily as a type of application of the VPN use case, with additional identity and authentication processes to manage the identities and authentication of multiple nodes and control/orchestration elements. These VPN-related cryptographic elements are within scope of a quantum safe analysis.

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. The public key cryptography and PKI methods employed for establishing secure connections are also within scope of a quantum safe analysis.

4.12.2 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.

4.12.3 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.

4.12.4 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.

4.12.5 Implementation Roadmap (Crypto-agility and PQC Implementation)

SD-WANs are somewhat complex systems that typically involve multiple components, often produced and/or operated by distinct organizations, to provide secure connectivity services. For example, an SD-WAN deployed by an enterprise may rely on different organisations who are responsible for aspects of the PKI, the cloud-based orchestrating/controlling components, and other elements in the system. These organisations could include an MNO, who sells the SD-WAN service to enterprise customers, a vendor, who retains cloud-based control over certain key elements in the system, and a third party, who operates the PKI. Achieving PQ security for SD-WANs is therefore dependent on the cooperative efforts of multiple parties, including the vendors, who sell SD-WAN products (and often retain control over some elements) and the PKI providers. These interdependencies could elongate the time required to migrate such systems to PQ status, suggesting that vendors and operators may benefit from earlier planning initiatives, to assure coordination among pertinent organisations and facilitate a timely migration.

4.12.6 Standards Impact (current and future) and Maturity

The standards relevant for VPN connections are relevant for VPN connections maintained and used by SD-WAN services.

4.12.7 Stakeholders

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

4.12.8 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.

4.12.9 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.

4.12.10 Potential Actions/ Dependencies

To achieve quantum safety, SD-WAN vendors will need to incorporate PQC enabled connections and processes into their products, presumably after PQC algorithms are standardised and protocol standards are upgraded. In particular, PQC migration of SD-WANs may have a dependency on quantum-resistant VPN service definitions.

4.13 Privacy (Lifecycle) of Customer Personal Data

4.13.1 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. IP address allocation) is maintained within the network for operational reasons. Other personal data (e.g. call records) is processed in mediation systems and stored in 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.

4.13.2 Sensitive Data Discovery

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

4.13.2.1 Sensitive Data Retention and Destruction

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

4.13.3 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 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.

4.13.4 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.

4.13.5 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.

4.13.6 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.

4.13.7 Potential Actions/ Dependencies

Many operators implement a data-lake which allows federated access to multiple databases for data science and analytics. As part of the cryptographic discovery process, operators need to ensure the inventory includes the protocols used within the data lake.

4.14 Lawful Intercept (and Retained Data)

4.14.1 Scope

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 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 requirements on 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.

There are a separate set of 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.

4.14.1.1 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.

4.14.2 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.

4.14.3 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.

4.14.4 Implementation Roadmap (Crypto-agility and PQC Implementation)

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

4.14.5 Standards Impact (current and future) and Maturity

ETSI TC LI defines the architecture and interfaces for LI and RD systems. Stakeholders

- LI and RD management function vendors
- Network function vendors
- MNOs
- Law enforcement agencies
- National cybersecurity authorities and national privacy regulators

4.14.6 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

4.14.7 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.

4.14.8 Potential Actions/ Dependencies

At the time to write this document, potential actions have not been identified.

4.15 IoT Services

Post Quantum 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.

4.15.1 Smart Meters Connectivity

4.15.1.1 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

4.15.1.2 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

4.15.1.3 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.

4.15.1.4 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

4.15.1.5 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.

4.15.1.6 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.

4.15.1.7 Stakeholders

- Smart Meter manufacturers
- MNOs
- SIM Manufacturers/ EUM

4.15.1.8 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.

4.15.1.9 Legacy Impact

The migration to PQC Smart Meters will be under time pressure, given the criticality of those devices.

4.15.1.10 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

4.15.2 Automotive

4.15.2.1 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.

4.15.2.2 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

4.15.2.3 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.

4.15.2.4 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.

4.15.2.5 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

4.15.2.6 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

4.15.2.7 Stakeholders

- Automotive component manufacturers
- Automotive TIER 1 vehicle manufacturers
- MNOs
- SIM Manufacturers/ EUM

4.15.2.8 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.

4.15.2.9 Legacy Impact

Accept the risk.

Propose pluggable workaround.

4.15.2.10 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

4.16 Enterprise Data

4.16.1 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 9: the data lifecycle management process

4.16.2 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

4.16.3 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.

4.16.4 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.

4.16.5 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.

4.16.6 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

4.16.7 Stakeholders

OEM providers of Information Protection services and software, Open Source Information Protection providers, Standards Authorities.

4.16.8 PKI Implication

All related vendors or OEM providers will include PKI support with CA.

4.16.9 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.

4.16.10 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 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 attempts to categorize 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 most simple 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 (to-be-)standardized algorithms are generally very performant in terms of execution time on server-grade devices, meaning that speed is unlikely to cause issues when migrating. However, even in this case, 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 (to-be-)standardized 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.

Furthermore, 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 showed (https://www.chromium.org/cecpq2/), it is possible that buggy middleware is causing issues with larger than expected keys, whereby “expected” relates to non-PQC implementations. [https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html] 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.
Another challenging use case is that software/firmware updates (Section 4.7) 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.

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 (Section 4.6), IMSI encryption (Section 4.8), VPNs (Section 4.11) and IoT Services (Section 4.15), however this list is almost certainly not exhaustive for the service portfolio of an MNO. 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 (to-be-)standardized 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.

Annex A Post Quantum Government Initiatives by Country and Region

The scope of this section is to provide a summary of countries with active PQC programs as context for the Post Quantum Telco analysis. This is not an exhaustive list and is intended to be indicative only. Given the rapidly evolving area for governments globally, ongoing monitoring will be required to ensure consistency with strategic plans and roadmaps.

Note: This section has been updated (to 27 Nov 2023) include the latest guidance from the listed countries. For ease of reference countries have been included even if there is no update since Dec 2022.

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2023)	Start planning; early implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Start planning; impl. from 2025
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022, 2023)	Start planning; Transition from 2024
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
Netherlands	AES, monitoring NIST, SPHINCS-256 and XMSS	NCSC (2023)	Draft action plan with timeframes
New Zealand	NIST	NZISM (2022)	Start planning
Singapore	Monitoring NIST	MCI (2022)	No timeline available
South Korea	KpqC	MSIT (2022)	Start competition First round (Nov.'22-Nov.'23)
United Kingdom	NIST	NCSC (2023)	Start planning; impl. from 2024
United States	NIST	CISA (2021, 2022, 2023) NIST (2023) NSA (2022, 2023) White House (2022)	Implementation 2023-2033

Table 4: Summary of Guidelines provided by the Countries

Country	Key References
Australia	Planning for Post-quantum Cryptography, Australian Cyber Security Center (May 2023) https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Planning%20for%20Post-Quantum%20Cryptography%20%28May%202023%29.pdf
Canada	Canadian Center for Cyber Security [60]
China	CACR [80]
EC	PQC – Integration Study – ENISA [61]
France	ANSSI VIEWS ON THE POST-QUANTUM CRYPTOGRAPHY TRANSITION [62] Follow up position paper on Post-Quantum Cryptography
Germany	BSI – Quantum Technologies and Quantum-Safe Cryptography (bund.de) [63]
Japan	Cryptography Research and Evaluation Committees (CRYPTREC) [64]
The Netherlands	Post-Quantum Cryptography: Protect today's data against tomorrow's threats (October 2023), Nationaal Cyber Security Centrum, Ministerie van Justieie en Veiligheid https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-post-quantum-cryptography
New Zealand	Security Manual (Version 3.6, September 2022) Te Tira Tikai - New Zealand Government Communications Security Bureau
Singapore	MCI Response to PQ on Assessment of Risk and Impact of Quantum Computing Technology and Efforts to Ensure Encrypted Digital Records and Communications Networks Remain Secure [65]
South Korea	KpqC
United Kingdom	Migrating to post-quantum cryptography, NCSC, 03 Nov 2023 https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc And Next steps in preparing for post-quantum cryptography, 03 Nov 2023, NCSC https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
United States	Preparing for Post-Quantum Cryptography, CISA, October 2021 Preparing for Post- Quantum Cryptography Infographic (dhs.gov) https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf National Security Memorandum 10, White House, May 2022 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national- security-memorandum-on-promoting-united-

	states-leadership-in-quantum-computing- while-mitigating-risks-to-vulnerable-cryptographic-systems/ Preparing Critical Infrastructure for Post-Quantum Cryptography, CISA , August 2022 CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography Commercial National Security Algorithm Suite 2.0, NSA, 7 September 2022 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov) Quantum Computing Cybersecurity Preparedness Act, Public Law, 21 December 2022 https://www.congress.gov/bill/117th-congress/house-bill/7535/text Quantum-Readiness: Migration to Post-Quantum Cryptography, CISA/NSA/NIST, 21 August 2023 Quantum-Readiness: Migration to Post-Quantum Cryptography (cisa.gov) https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

Table 5: Key Reference by Country

A.1 Australia

A.1.1 PQC Algorithms

The Australian Cyber Security Centre (ACSC) is the Australian Government agency for cyber security. ACSC is not developing PQC algorithms, ACSC has not selected PQC algorithms, the selection will be informed by the NIST process.

A.1.2 Published Recommendations

The Australian Government Department of Industry, Science and Resources published national policy on PQC.

- Action Plan for Critical Technologies: Post-Quantum Cryptography, Oct 2021 [59.1]
- CSIRO (the Australian Government's national science agency) published a white paper: "The quantum threat to cybersecurity: Looking through the prism of Post-Quantum Cryptography", April 2021, CSIRO [66]
- ACSC updated "Planning for Post-Quantum Cryptography" in May 2023, and plans to update the Australian Information Security Manual to address PQC [67]

A.1.3 Timeline

Policy recommends early adopters in the commercial sector should implement PQC in the period 2024-2027. Beyond 2027 PQC should be implemented in all applications. Summary of the October 2021 Australian national policy for PQC.

Readiness Level – 2021

- Implementation of pre-standardised PQC for classified networks.
- Cyber security companies providing pre-standardised PQC services.
- Laboratory testing of hardware accelerators for pre-standardisation PQC algorithms.
- Readiness Level – 2–5 years (2023-2026)
- Early adopters in the commercial sector (e.g. financial institutions) may implement PQC for critical networks.

Readiness Level – Beyond 5 years (2027 on)

- PQC algorithms are incorporated in all consumer, commercial and industrial devices and software that need to store, send or receive sensitive data.
- Dedicated hardware for increasing the speed of PQC.

A.2 Canada

A.2.1 PQC Algorithms

The Canadian Centre for Cyber Security (the Government of Canada's authority on cyber security) is not developing its own PQC algorithms, it works with NIST on PQC.

A.2.2 Published Recommendations

The Canadian Center for Cyber Security has published guidance on planning for the transition to PQC and Cryptographic Agility. The Ministry for Innovation, Science and Economic Development (ISED) established the Canadian Forum for Digital Infrastructure Resilience (CFDIR) in 2020, a public private partnership to support Canada's National Strategy for Critical Infrastructure. The Quantum-Readiness Working Group (QRWG), one of five working groups part of the CFDIR, released a third version of the Canadian National Quantum-Readiness: Best Practices and Guidelines in 2023. The document outlines three PQC use cases (Authentication via KERBEROS, PKI/Cas, sFTP) as well as a PQC inventory checklist, cryptoagility use cases and a PQC vendor roadmap and 3rd party assessment checklist.

Source [cfdir-quantum-readiness-best-practices-v03.pdf (canada.ca)]

Addressing the quantum computing threat to cryptography, ITSE.00.017 May 2020, Canadian Center for Cyber Security

Preparing your organization for the quantum threat to cryptography, ITSAP.00.017 Feb 2021, Canadian Center for Cyber Security.

Guidance on becoming cryptographically agile, ITSAP.40.018 May 2022, Canadian Center for Cyber Security

Quantum-Safe Canada Initiative Quantum-Safe Canada – Quantum-Safe Canada Desktop Website aligned to NIST standardisation process.

The Canadian Government specifications for cryptography do not yet include PQC algorithms.

- Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information (Version 2), IT.SP.40.111 August 17, 2022. Canadian Centre for Cyber Security

A.2.3 Timeline

The Quantum Readiness Working Group (QRWG) defines the following timeline:

Stage I: Initial Planning and Scoping to be underway before new PQC standards completed in 2024

- Phase 0: Preparation
- Phase 1: Discovery
- Phase 2: Quantum Risk Assessment

Stage II: Implementation. Starting in 2025

- Phase 3: Quantum Risk Mitigation
- Phase 4: Migration to new QSC
- Phase 5: Validation

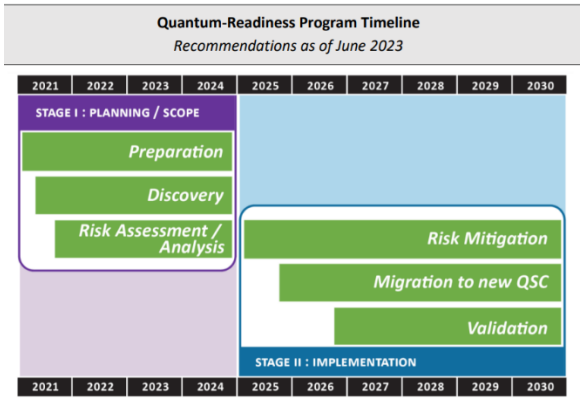

Figure 10: Quantum-Readiness Program Timeline

A.3 China

A.4 PQC Algorithms

Starting in 2018, the Chinese Association for Cryptologic Research (CACR) held a two round competition for symmetric and asymmetric key algorithms CACR is not a standardisation body, it is an academic body e.g., IACR. The motivation for the competition was to encourage cryptographers in China to pay attention to the design of new generation cryptographic algorithms. The competition was not limited to Post Quantum algorithms, public key algorithms like authenticated key exchange were also acceptable. The winners were announced in January 2020 [80]. Three algorithms have been ranked first (two key encapsulation mechanisms and one digital signature scheme). The second and third ranks include eleven other algorithms (three key exchange schemes, five key encapsulation mechanisms and three digital signature schemes).

A.4.1 Published Recommendations

No published recommendations yet.

A.4.2 Timeline

No official timeline released.

A.5 European Commission

A.5.1 Published Recommendations

The EC, through ENISA (the European Union Agency for Cybersecurity) has published multiple reports on PQC. The most recent report [60] focuses on technical changes required to update existing systems using cryptography to use PQC.

The EC has launched a collective risk assessment call in October 2023, an exercise which all member states will contribute to. The scoping phase is scheduled to conclude by the end of 2023 and the results have not been published prior to this reports' publication. The risk assessment will not be country-specific and risks impacting the entire EU will have priority. Source [C_2023_6689_1_EN_ACT_part1_v8.pdf (europa.eu)

A.5.2 Timeline

The ENISA reports do not include a timeline for the transition.

A.5.3 A.4.3 Other Information

The European Commission has launched a call on "Transition towards Quantum-Resistant Cryptography" (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03;callCode=HORIZON-CL3-2022-CS-01)

The European Commission closed a new call on 16 November 2022, entitled "Transition towards Quantum-Resistant Cryptography" (HORIZON-CL3-2022-CS-01). This new call is part of the Horizon Europe Framework Programme.

The European Union recognises the potential and opportunities that quantum technologies will bring and understands their significant risk to the security of the society. The European Union has also recognised the need to advance in the transition to quantum-resistant cryptography. They argue that many companies and governments cannot afford to have their protected communications/data decrypted in the future, even if that future is a few decades away.

In this context, European Commission launched this call with the following expected outcomes:

- Measuring, assessing and standardising/certifying future-proof cryptography.
- Addressing gaps between the theoretical possibilities offered by quantum-resistant cryptography and its practical implementations.
- Quantum resistant cryptographic primitives and protocols encompassed in security solutions.
- Solutions and methods that could be used to migrate from current cryptography towards future-proof cryptography.
- Preparedness for secure information exchange and processing in the advent of large-scale quantum attacks.

Participants are expected to develop cryptographic systems which are secure against attacks using quantum computers and classical computers (i.e. secure against both types of

attacks). They should equally look at the implementation of quantum-resistant algorithm on software as well as specific hardware, and provide different migration strategies by deploying pilot demonstrators in relevant use cases.

This call recognises not only the importance of the entire ecosystem but also the importance of cross-disciplinary cooperation. Participants are encouraged to take stock of and build on the relevant outcomes from other research fields (such as mathematics, physics, electrical engineering) and actions (e.g. H2020 projects, NIST PQC competition, efforts in ETSI), they are also encouraged to plan to engage and cooperate with them as much as is possible.

It is worth pointing out that the security of PQC depends on the computational hardness of certain mathematical problems. There are many established theorems and results that may have an impact on PQC. For instance, SIKE (Supersingular Isogeny Key Encapsulation), one of the finalists in the NIST competition third round, was cracked by researchers from KU Leuven using a single core process. The mathematics underlying the attack was based on a relatively old theorem dated in 1997 by the mathematician Ernst Kani. Involving people from other research fields into the study of PQC would bring new perspectives and thus accelerate the development.

Finally, this project demands not only an analysis of how to develop combined quantum-classical cryptographic solutions in Europe, but also an analysis taking in to account relevant actions in quantum cryptography (e.g. H2020 Open QKD project, EuroQCI).

A.6 Japan

A.6.1 PQC Algorithms

Japanese researchers have contributed to the NIST process.

A.6.2 Published Recommendations

Led by Japan’s Cabinet Office, the National Institute of Information and Communications Technology (NICT) is researching quantum secure cloud technology and has developed systems featuring quantum cryptography, secret sharing, and next-generation Post Quantum public key infrastructure.

Japan CRYPTREC (Cryptography Research and Evaluation Committees) is a NICT project to evaluate and monitor the security of cryptographic techniques used in Japanese e‐Government systems. The goal of CRYPTREC is to ensure the security of Japanese e‐Government systems by using secure cryptographic techniques and to realize a secure IT society.

In 2019, CRYPTREC set up a task force to follow the research trends regarding quantum computers and discuss how to deal with PQC.

The Cryptography Research and Evaluation Committees (CRYPTREC) has evaluated [82] the impact of quantum computers on current cryptographic algorithms and considered the adoption of PQC in the future.

CRYPTREC LS-0001-2012R7 (Japan e-Government Recommended Cipher List, last update: 2022/3/30) [83] has not been updated to cover PQC.

A.6.3 Timeline

The Bank of Japan's Institute for Monetary and Economic Studies published:

- Recent Trends on Research and Development of Quantum Computers and Standardisation of PQC, Discussion Paper No. 2021-E-5 [84]
- "On mitigation to PQCs" (in Japanese) includes a proposed timeline.

A.6.4 Other Information

Japan has significant national and commercial research and development activities on Quantum-Safe networks, QKD, and PQC. In 2020, a programme to build a global QKD network was announced, with 100 nodes. This will include fibre and satellite communication. Sumimoto, Toshiba and NICT are among the leading national organisations in Quantum-Safe communication development.

- Paper on Quantum Network. Building an International Hub for Quantum Security [87]
- Toshiba to Lead Joint R&D Project Commissioned by Japan's MIC to Develop Global Quantum Cryptography Communications Network -Aiming at deploying world's first wide-range and large-scale quantum cryptography communication networks- | Corporate Research & Development Center | Toshiba
- Press Release | World's First Demonstration of Space Quantum Communication Using a Microsatellite | NICT-National Institute of Information and Communications Technology

A.7 The Netherlands

5.1.1 PQC Algorithms

The Nationaal Cyber Security Centruum (part of the Ministry of Justice) recommends AES-256 for symmetric cryptography, SPHINCS-256 [*sic*] for stateless digital signatures, XMSS for stateful digital signatures.

5.1.2 Published Recommendations

The Nationaal Cyber Security Centruum (part of the Ministry of Justice) recommends that organizations draft a plan of action and a timeline to deal with the digital signatures and data security with the availability of quantum computers.

The Netherlands National Communications Security Agency published (with TNO and CWI) "The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography" in March 2023.

https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook

A.8 New Zealand

A.8.1 PQC Algorithms

The New Zealand Government Communications Security Bureau (GCSB) will review the outcome of the international standardisation program for PQC run by NIST before selecting PQC algorithms.

A.8.2 Published Recommendations

The New Zealand Information Security Manual was updated (to Version 3.6) in September 2022 to give recommendations on planning for the transition to PQC.

Recommendations include creation of cryptographic inventory, identification of systems using Public Key cryptography which are vulnerable to attack from a quantum computer, and creation of an inventory of datasets and the time for which the data must remain secure.

The final recommendation is the development of a transition plan.

A.8.3 Timeline

Prepare to transition away from classical cryptographic algorithms possibly from 2024-2027.

A.9 Singapore

A.9.1 PQC Algorithms

Singapore is monitoring the NIST process.

A.9.2 Published Recommendations

The Ministry of Communications and Information, the Cyber Security Agency of Singapore and the Information and Media Development Authority are working with other relevant agencies to develop Quantum-Safe approaches for the continued security of digital communications and records.

A.9.3 Timelines

The timeline for Singapore is not available at the time of writing this document.

A.9.4 Other Information

29 Nov 22 Minister for communications and information response to parliamentary question on assessment of risk and impact of quantum computing technology and efforts to ensure encrypted digital records and communications networks remain secure.

Singapore announced [88] that it will build a National Quantum-Safe network, consisting of 10 nodes initially, and encompassing both PQC and QKD. Frauenhofer Singapore and AWS are among the companies contributing to use-cases. SPTel and quantum firm SpeQtral to build the National Quantum-Safe Network Plus (NQSN+) network.

“The network will provide the following technologies:

- i) Quantum key distribution – a hardware approach to Quantum-Safe communication requiring the installation of devices to create and receive quantum signals; and
- ii) Post Quantum Cryptography – upgrading software to run new cryptographic algorithms perceived to be resistant to attacks by quantum computers.”

An initial quantum key distribution pilot between two data centres in Singapore was successfully completed by the NQSN (National Quantum Safe Network) and STT GDC (ST Telemedia Global Data centres) via a quantum secured link

A.10 South Korea

Quantum Cryptography is included in the Ministry of Science and ICT, 6th Science and Technology Forecast (Nov 2022)

A.10.1 PQC Algorithms

A Korean standardisation project for PQC (KpqC) was announced in 2021 [https://www.kpqc.or.kr/competition.html]. This competition is a two-round process that aims at selecting Post Quantum algorithms for digital signatures and key establishment/public key encryption. The first round concluded in December with four algorithms progressing in each of the two categories. The second (and final) round is expected to conclude in September 2024.

The procedure is similar to that of the NIST competition. The proposals must be published in the proceedings of a high-rank international conference or journal, or at least appear on the IACR Cryptology ePrint Archive [https://eprint.iacr.org/]. Each proposal must specifically include a technical description of the algorithm, security proofs and a reference implementation in ANSI C.

A.10.2 Published Recommendations

The Ministry of Science and ICT has published a work plan indicated as follows:

https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=610&searchOpt=ALL&searchTxt=

A.10.3 Timeline

The KoreaPQC competition is not expected to conclude before the end of 2024.

A.10.4 Other Information

The Ministry of Science and ICT initiated a Quantum-Safe communication infra project with QKD as part of ‘the Digital New Deal’ initiative in 2020. The Quantum-Safe communication infra demonstrated its potential to be commercialised as pilot-types of quantum cryptography networks have been deployed across the 26 public and private institutes in South Korea.

https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=627&searchOpt=ALL&searchTxt=

A.11 France

A.11.1 PQC Algorithms

ANSSI closely follows the NIST PQC process but recognizes that there are other alternatives which could prove valuable provided they are thoroughly tested. Yet, ANSSI does not intend to limit the recommended Post Quantum algorithms to the NIST winners and may consider additional algorithms. Thus, ANSSI deems ML-KEM, ML-DSA, FN-DSA but also FrodoKEM (not selected by NIST) as “good options for first deployments” [1] of quantum-resistant solutions. Moreover, ANSSI advises the security level of these asymmetric algorithms to be as high as possible, that is, level 5 in the NIST scale.-XMSS and SLH-DSA (stateless variant of XMSS) are considered conservative options by the French agency but, provided additional criteria are met, they are considered acceptable.

A.11.2 Published Recommendations

In 2022, the French cybersecurity agency (ANSSI) issued a position paper “ANSSI views on the Post-Quantum Cryptography transition” [1] providing its views on the Post Quantum transition. In this document, ANSSI clearly states its support for PQC (PQC) that is presented as “the most promising avenue to thwart the quantum threat”. Conversely, they dismiss Quantum Key Distribution (QKD) as an unsuitable countermeasure, “except for niche applications where QKD is used for providing some extra physical security on top of algorithmic cryptography (and not as a replacement)”.

In October 2023 ANSSI published two addenda to the 2022 paper and one of the updates is regarding a speeded up adoption timeline as now the first French security visas for products implementing hybrid Post Quantum Cryptography (end products as well as intermediate products) are expected to be delivered around 2024-2025

ANSSI also confirmed its position on symmetric key sizes, namely that they should be increased to 256 bits although it acknowledged that this is a more conservative position than those of NIST and BSI.

2022: https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

Addendum to 2023 paper - https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

https://cyber.gouv.fr/sites/default/files/document/pqc-transition-in-france.pdf

A.11.3 Timeline

This support for PQC must however be qualified as the ANSSI clearly acknowledges the lack of maturity of such solutions. They therefore propose a gradual transition consisting of three stages. In the first two stages, no standalone PQC will be recommended except in the very particular case of hash-based signatures. That is, any system targeting quantum-resistance will have to be based on hybrid solutions.

- Phase 1: to 2024) “defence-in-depth” systems should consider the use of PQC within a hybrid framework.
- Phase 2: 2024-2030) ANSSI will consider quantum resistance as optional but intends to recommend it for products claiming long-term security. ANSSI also makes recommendations that “Post Quantum security could become a mandatory feature” for the latter type of products.
- Phase 3: 2030 and beyond) ANSSI considers standalone PQC solutions can be deployed.

A.12 Germany

A.12.1 PQC Algorithms

BSI has been involved in supporting the US NIST PQC Project and actively promoting preparation for a Quantum-Safe Cyber-security strategy that is based on a working hypothesis that Cryptographically Relevant Quantum Computers will be available early 2030 (timeline for risk assessment).

A.12.2 Published Recommendations

The Federal Government objective is to use quantum technology to secure IT systems. BSI has published a set of recommendations regarding accelerating preparation, the implementation of crypto-agility and interim protective measures and the implementation of PQC [BSI-2022]].

BSI considers FrodoKEM and Classic McEliece and is involved in the standardisation of the quantum-safe procedures. “In October 2022, a preliminary work item for the project "Inclusion of key encapsulation mechanisms for PQC in ISO/IEC standards" was launched in ISO/IEC SC27 WG2 following a proposal by the BSI.” [BSI link below – to be added in references]

Additionally, the BSI has updated studies on random number generation to include quantum sources. Their position is “QRNGs are a special type of random number generator that is not necessarily superior to conventional physical generators”. This is relevant for PQC algorithms deployments, since implementations must ensure entropy sources are effectively chosen. Details of this assessment may be found within draft AIS 20/31 [dBIS AIS 20/31 draft].

A.12.3 Timeline

2026 goals

- Development of a federal government strategy for the migration to Post Quantum Cryptography in Germany.
- Continuation of the migration to Post Quantum Cryptography for the high-security sector.
- Initiate the migration to Post Quantum Cryptography in other security-critical areas.
- Integration of Post Quantum Cryptography methods into practical IT security solutions.
- Further Information:

Entwicklungsstand Quantencomputer (Deutsche Zusammenfassung), 13 Nov 2023, BSI-Projektnummer: 477
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand_QC_Zusammenfassung_V_2_0.pdf

BSI - Quantum Technologies and Quantum-Safe Cryptography (bund.de) – latest update 9.01.2023

Federal Ministry of Education and Research - April 2023

5.1.3 Other Information

- quantum technology for satellite navigation (optical clocks that fulfil the requirements of the next generation of Galileo clocks and and inertial navigation)
- implementation of a nationwide fibre optic backbone for quantum communication and time and frequency distribution.
- Demonstration of the first quantum repeater test tracks.
- Launch of the first test satellites for quantum key distribution.

A.13 UK

A.13.1 PQC Algorithms

The National Cyber Security Centre (NCSC) is the UK's national authority for cyber threats. It is part of the Government Communication Headquarters (GCHQ).

Updated NCSC guidance (Nov 2023) is that symmetric cryptogaphy is unaffected by the tranistion to PQC. The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases. Users should wait for the availability of implementations based on the final NIST standards before deploying production systems.

A.13.2 Published Recommendations

Next steps in preparing for post-quantum cryptography, 03 November 2023, NCSC

https://www.ncsc.gov.uk/pdfs/whitepaper/next-steps-preparing-for-post-quantum-cryptography.pdf

A.13.3 Timelines

NCSC recommends organisations wait for the standardisation of PQC by NIST, planned for 2024.

A.13.4 Other Information

Additionally, the UK has significant ongoing research activities both in the development of PQC, and the implementation of quantum communication networks. One example is a QRNG assurance project at the National Physical Laboratory (117). British Telecom and Toshiba have implemented a pilot Quantum-Safe QKD Metro-network (118) in London, and is trialling the service for high bandwidth dedicated links between large sites such as corporate offices and datacentres.

A.14 USA

A.14.1 PQC Algorithms

PQC migration plans following varying paths depending on system type – federal National Security Systems (NSS), federal non-NSS, and non-federal.

In September 2022 CNSA (Commercial National Security Algorithm Suite) 2.0 was announced which includes PQC algorithms, timelines and usage recommendations. The PQC algorithms selected are based on the NIST standardisation process.

Federal non-NSS migration will utilize NIST standardized algorithms. When the PQC algorithm specifications are finalized, NIST will publish guidance to deprecate RSA, Diffie-Hellman, and elliptic curve cryptography.

Programs are being developed to educate and engage non-federal entities in the development of sector specific adoption plans aligned with the NIST process.

A.14.2 Published Recommendations

For National Security Systems (NSS), CNSA 2.0 applies. NSS are defined in NIST Special Publication 59.

1. Stateful hash-based digital signature schemes are required for software and firmware signing; specifically, LMS or XMSS as defined in NIST SP-800-208.
2. Symmetric-key algorithms are specified as the same as CNSA 1.0, but with the addition of SHA-512.
3. Public-key algorithms are specified as ML-KEM-1024 (key establishment) and ML-DSA-87 (digital signature).
4. Other algorithms selected for standardization by NIST, such as SLH-DSA and FN-DSA, are not approved for use in NSS.

For non-NSS, guidelines for PQC migration will be forthcoming from NIST and CISA, pursuant to the following directives:

The US Federal Government in May 2022, in alignment with the NIST PQC standardisation activities (described in section 6.5.1), issued a National Security Memorandum [69] directing federal agencies to begin “the multi-year process of migrating vulnerable systems to quantum-resistant cryptography”.

The US Executive Branch issued on November 18, 2022, additional guidance for Departments and Agency heads to assist compliance with NSM-10. [70]

In December 2022, the US Executive Branch also signed the bi-partisan Quantum Computing Cybersecurity Preparedness Act as Public-Law 117-260 (formerly H.R.7535) which mandates planning for PQC across US Government within 15 months.

A.14.3 Timeline

The CNSA 2.0 timeline is provided below as reference and can be considered an effective baseline for US operators.

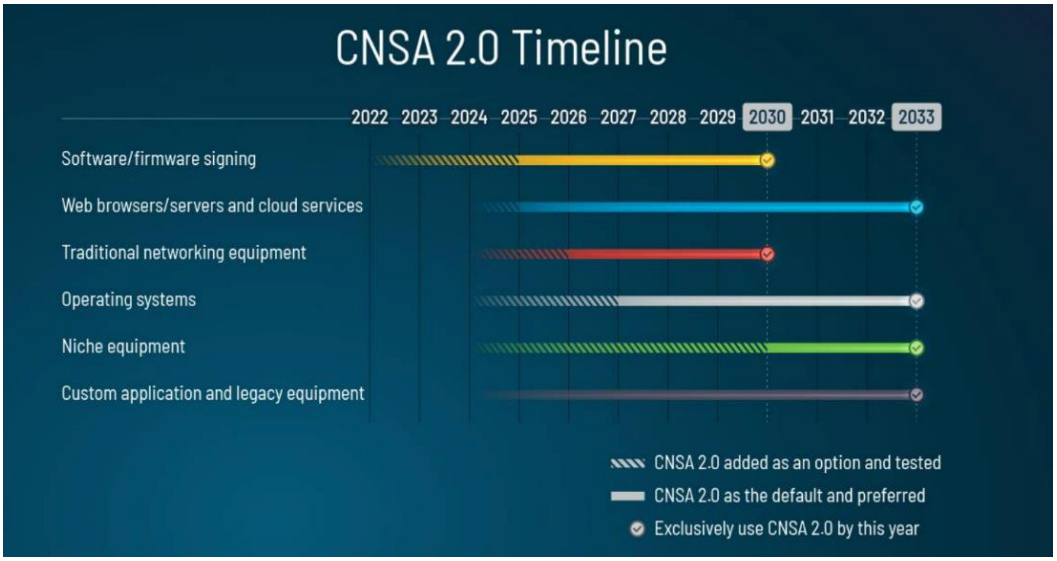

Figure 11: CNSA 2.0 Timeline from announcing the Commercial National Security Algorithm Suite

Annex B Definitions, Abbreviations and References

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 documents remotely. 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 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.

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 documents remotely. 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 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.
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 are expected to be published in 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, 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

Term	Description
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
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
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

Term	Description
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
FHE	Fully Homomorphic Encryption
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

Term	Description
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
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

Term	Description
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
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

Term	Description
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
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

Term	Description
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

B.4 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)"
3GPP TS 33.501	3GPP TS 33.501	"Security architecture and procedures for 5G system"
3GPP TS 33.310	3GPP TS 33.310	"Network Domain Security (NDS); Authentication Framework (AF) "
3GPP TS 33.210	3GPP TS 33.210	[] “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

Ref	Doc Number	Title
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
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
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

Ref	Doc Number	Title
EQCSAISC		An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography | SpringerLink
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
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
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
HQC	HQC	Hamming Quasi-Cyclic (HQC) https://pqc-hqc.org/download.php?file=hqc-specification_2023-0430.pdf
IETF-TLS-hybrid	IETF-TLS-hybrid	Hybrid key exchange in TLS 1.3 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

Ref	Doc Number	Title
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
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
MoodyETSI	MoodyETSI	The first NIST PQC Standards https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/NIST_MOODY.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
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

Ref	Doc Number	Title
		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
On-Ramp	On-Ramp	Post-Quantum Cryptography: Digital Signature Schemes https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals
Open-QS	Open-QS	Open Quantum Safe: https://openquantumsafe.org

Ref	Doc Number	Title
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
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
TDFZSS	TDFZSS	Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices https://eprint.iacr.org/2023/506
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

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
PQ.03 version 1	22/02/2024	First version of PQ.03 Post Quantum Cryptography Guidelines for Telecom Use	TG	Yolanda Sanz, GSMA

C.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 Thomas Davies, NXP – Loïc Ferreira, Orange – Olivier Sanders, Orange – Galina Pildush, Palo Alto Networks – Anthony Bord, Thales – Diego Lopez, Telefonica – Michaela Klopstra, Utimaco – Darshan Lakha, Vodacom – Luke Ibbetson, Vodafone – Guenter Klas, Vodafone – Kristian McDonald, Vodafone –

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.