Post Quantum Telco Network Impact Assessment Whitepaper

Version 1.0

17 February 2023

This is a Whitepaper of the GSMA

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2023 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

To address the security challenges presented by emerging quantum technologies, many countries have created national Post-Quantum Cryptography (PQC) initiatives. One example is the U.S. National Institute of Standards and Technology (NIST) announcement [54] in July 2022 announcing the first PQC algorithm standardisation candidates for the quantum computing era.

The telecom industry needs to mobilise to define guidelines and processes for the PQC adoption to secure networks, devices and systems, given that this affects the entire telecom supply chain and ecosystem: operators, network and IT vendors, integrators, regulators, standards and open source communities.

To date, significant work in the telecom industry has focused on Quantum Key Distribution (QKD) and Quantum Random number generation with limited concerted focus on PQC adoption.

1.2 Scope

Scope of this report is to analyse the dependencies and timelines for a responsible industry transition to Quantum-Safe technology.

This includes algorithms considered capable of resisting attacks by Cryptographically Relevant Quantum Computers (such as those selected by the NIST process) and how to introduce and maintain quantum resistance and/or crypto agility where applicable within the telco ecosystem. It considers a wide range of aspects such as PQC technology and standards, business processes, security, policy and regulation. The risk assessment will inform and guide a set of priority actions needed to mitigate the various risks and maintain defence capacity.

In this report “quantum computer” refers to a Cryptographically Relevant Quantum Computer.

Technologies out of scope of this document include quantum computing, quantum networking, Quantum-Safe mechanisms which rely on quantum properties such as QKD, quantum sensing, and quantum internet. While other architectures may be studied over time, this report focuses on 5G wireless architecture to provide a baseline.

1.3 Intended Audience

The audience for this document is the following: 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 message of this document is intended to be relevant for CEOs and Company Boards.

2 Post Quantum Cryptography – Executive Summary

This report assesses Post-Quantum Cryptography (PQC), Quantum-Safe market drivers, government initiatives, and implications for operators and their partners. In summary we highlight the following insights:

- **The transition to PQC is underway**
  - Governments and civil-society groups have started planning, and are recommending businesses start the planning process.
  - Standards groups have identified PQC algorithms and begun the standardisation process.

- **Prepare as an industry for the transition to PQC**
  - To address "Store Now, Decrypt Later" and other quantum attacks, overhauling existing PKI architectures is required as existing algorithms become obsolete.
  - Engage with industry groups, government and vendors on the roadmaps to implement PQC.
  - Prepare how to handle the legacy. Understand how to treat systems/services/products that may not be updated.
  - Consider how to reduce the creation of technical (cryptographic) debt e.g. assess available quantum-safe symmetric cryptography. In some cases where public-key cryptography is used, quantum-safe symmetric keys may be a secure alternative.
  - Adapt or account for impacts to key management systems.

- **Operator business and technology preparation**
  - Plan to establish a cryptographic inventory: e.g. currently used cryptographic algorithms and key-lengths; identify systems or vendor products dependent on cryptography.
  - Plan to perform a risk assessment of cryptography used in network systems.

- **Develop in-house expertise in PQC and security**
  - Support PQC standardisation and open-source projects.
  - Sponsor or support research on cryptographic agility.
  - Engage with customers on requirements and potential benefits.
  - Develop a PQC plan (see section 3.4).

Operators and industry partners should

- Plan for future implementation of the transition to Quantum-Safe.
- Deploy standardised Quantum-Safe algorithms (see section 6).

3 Post Quantum Telco Network – Market Drivers and Timelines

3.1 Market Driver – Network Security

A standard, ongoing activity of network operators is to evolve and adapt network security against risks. In this sense, the "quantum threat" is an intrinsic driver for the telco industry. This means completing risk assessments across the broad set of cryptographic applications in operations including the areas below, each area will be expected to have different timelines and dependencies to manage:

- Cryptographic technology, including cryptographic libraries, cryptographic protocols, cryptographic hardware.

- Cryptographic systems including Public Key Infrastructure, Certificate Authority, Hardware Security Modules, Identity/Access Management, and Privilege Access Management.
- Computing technology, e.g. servers, firmware, operating systems, virtualisation, cloud infrastructure, databases (column length), software (data structures), middleware, security systems).
- Networking equipment, e.g. Ethernet switches, IP routers.
- Telecom architectures, e.g. settlement, Telecom-specific network functions, Radio, Core, transmission, communication services (voice, messaging, mission critical), OSS/BSS systems.
- Telecom-specific business processes, e.g. device activation, roaming and settlement.

3.2 Market Driver – New Services

Post Quantum Cryptography is intended to secure communication networks from potential threats from quantum computers. Given the estimated high risk that these threats may materialise in the next decade, the question arises:

What is cost of doing business for telecoms service providers versus what can be *monetised* as a service for customers including enterprise customers, as a service that is new or upgraded due to a premium level of security?

The answer to the above question may relate to time and awareness of customers from the enterprise and government sectors, and the position service providers take.

For example, migrating to PQC to secure key network infrastructure and communication links of public networks may be considered a ‘must do’ by network operators and could be considered a cost of doing business. The goal post is set by the service providers themselves in the interest of managing reputation and brand value.

3.2.1 Customer Demand for Services

Different demand scenarios dictated by private and public sector clients may materialise.

The first possibility is that they could actively demand that networks and services become Quantum-Safe. While it is unlikely that enterprises from different sectors have sufficient market power to exercise effective influence on service providers, it could be very different regarding governments. Those could resort to mandating that service providers meet certain requirements and/or they may activate their national telecoms regulators.

The second possibility is that enterprise customers are slow in taking proactive action to mitigate any quantum threats. This could, for example, be the case for the SME sector. Companies may express little demand for Quantum-Safe telecoms services (like Quantum-Safe SD-WAN services) at least in the early phase of migration to PQC. In this transition phase, service providers could offer early Quantum-Safe service propositions to customer groups who, for certain reasons, would welcome a ‘premium level of protection’, premium at least for a transition period, until that level of protection becomes ‘standard’ for all.

Where service providers offer private mobile networks to enterprise customers (and operate those networks), certain customer groups who become early adopters of Quantum-Safe technology could well demand of their suppliers to render those networks quantum-ready. As long as technology that leverages PQC is not a commodity or commonplace yet, service providers could meet that market demand through extra features or ‘premium’ network service levels and aim to monetise those.

From the above discussion, timing appears important. An opportunity for monetisation of Quantum-Safe network services may arise during the migration to a quantum-ready status.

As opportunities to monetise Quantum-Safe services may arise, the interdependency on technology standards becomes an important factor to consider. To assist planning, this report analyses this in more detail within section 6.5.

Follow-up questions for those different scenarios are occurred:

- Under the assumption that there is a market for new (security-upgraded) services based on PQC at least during the multi-year long migration period, what kind of services might be of value to different customer groups?
- Could PQC be an enabler for completely new types of services?

3.2.2 Examples of New Services

Regarding security-upgraded *services*, the following are examples of potential new services:

- Quantum-Safe virtual private networks
- Quantum-Safe software-defined wide area networks
- Quantum-Safe connection of enterprise customers to telco cloud computing centres
- Quantum-Safe interconnection of telecoms edge cloud computing services and infrastructure to public and private clouds
- Quantum-Safe IoT connectivity
- Quantum-Safe satellite communication links for enterprises and governments
- Quantum-Safe (cloud) storage with telecoms service providers (e.g. to mitigate against Store Now Decrypt Later attacks).

The search for new services leveraging PQC could also be inspired by considering what might be most at risk from quantum attacks, when seen through the eyes of a hypothetical malicious actor, e.g. a state actor. Quantum attacks can be used for different purposes, ranging from spying on secret information and transactions (e.g. banking transactions) to disrupting services and infrastructure and enabling hacking of critical IT infrastructure. Based on areas of high vulnerability or areas of high attractiveness to malicious actors, one could consider new services that help to mitigate such risk in a pre-emptive way. An example might be the protection of a private mobile network if used for critical (national) infrastructure.

3.3 Market Driver – Business Verticals

As an operator market driver, interest from customers across multiple industries in Quantum-Safe communications is an important consideration while prioritizing PQC related-efforts.

Though all verticals are expected to benefit from the improvements from PQC, including the new services above, certain industries are also mentioned specifically with additional detail regarding their expressed interest in PQC.

3.3.1 Public Sector

Please refer to section 5 for details of global public sector interest related directly to PQC.

3.3.2 Financial Services

The Financial Services industry has started planning for PQC.

The Bank for International Settlements started a research program in its Innovation Hub on post quantum cryptography and payments in June 2022: "This project will investigate and test potential cryptographic solutions that can withstand the vastly improved processing power of quantum computers. The goal is to test use cases in various payment systems and examine how the introduction of quantum-resistant cryptography will affect their performance." [55].

The Depository Trust and Clearing Corporation (DTCC) published a white paper in September 2022 with recommendations for clearing bank members and the banking industry on the implication of PQC on inter-bank settlements and payments [56].

The Banque de France (the French central bank) has tested the implementation of PQC in its innovation centre in September 2022 [57].

The World Bank includes PQC on the list of future technologies where banks need to act and on its education curriculum.

3.4 Timelines

Through assessment of the intrinsic/extrinsic market drivers, operators can determine the appropriate timeline for their business. We present below a generalised PQC transition timeline which can be adapted.

- Phase I: PQC research and algorithm standardisation
    - Algorithms selected for ongoing standardisation, e.g. NIST, KpqC.
    - PQC-enablement of protocols, including hybrid modes.
    - Partner with SDOs (e.g. 3GPP, ETSI) to standardise PQC as appropriate.
- Phase II: Operator architecture and planning
    - Update operator requirements to support PQC.
    - Collaboration with Telco vendors on roadmaps.
    - Collaboration with open-source communities e.g. Linux, OpenSSL.
    - Cryptographic inventory.
    - Crypto agility considerations.
- Phase III. Engineering
    - PQC enablement of cryptographic systems including PKI, CA and HSM.
    - Vendor products and open-source projects updated to support PQC.
    - Validate and test systems, network functions and processes are Quantum-Safe.
- Phase IV. Implementation (prioritised by operator-specific risk assessments and customer requirements)

  - Updating the mobile network itself to be Quantum-Safe. This is where we evolve devices and network to use PQC or other Quantum-Safe approaches according to industry standards.

- Phase V. Once the standards are updated, vendors have implemented the new standards and operators have deployed them, we can consider the end-to-end network to be Quantum-Safe.

4 Post Quantum Telco Network – Ecosystem

The following Ecosystem map provides a high-level view on quantum-specific standards and industry groups internationally. As this PQTN report focuses on PQC, we connect the activities in the top row (“Quantum Security”), to the broader Telco Networks context of standards and industry groups. This is not an exhaustive list.

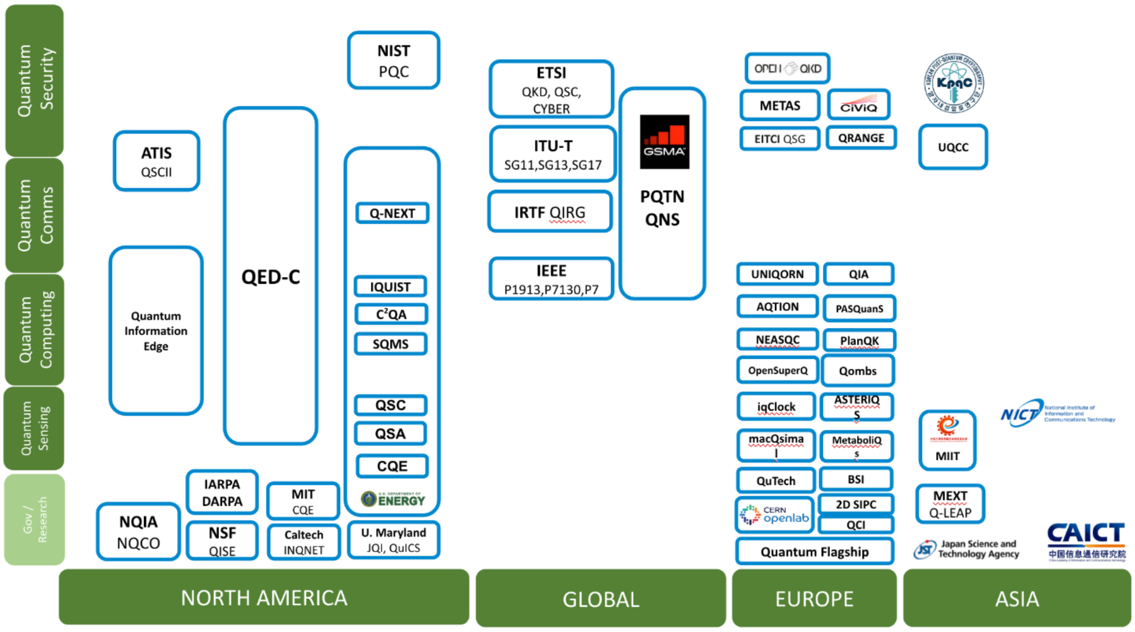

Figure 1: Quantum Standards and Industry Groups

4.1 Potentially impacted entities

The following table shows the list of potential entities impacted by the transition to PQC.

GSMA may collaborate with those entities as required.

Group Name	Subgroup(s)
TM Forum	ODA, OpenAPI
GSMA	FASG,. eSIMWG,. RCS,. QNS
3GPP	3GPP SA, CT and RAN (Entry Point SA3) (3GPP Architecture: USIM, RAN, Core, IMS and Service Aspects)
Open RAN	WG1 (Architecture) and WG11 (Security); nGRG

ETSI	TC-Cyber, TC-LI, TETRA, ISG-MEC, ISG-NFV, ISG-ZSM, OSG OSM, TC SET
Linux Foundation	Open Daylight, ONAP, ISRG, CNCF
NGMN	SCT 6G
ATIS	NGA and QSCII
ITU-T	SG11, SG13 and SG17
Open Quantum-Safe	https://openquantumsafe.org/ https://link.springer.com/chapter/10.1007/978-3-319-69453-5_2

Cross-industry open-source communities and standards bodies which are impacted by PQC

Open Source	Kubernetes, KVM, Linux, OpenSSL, OpenStack
IETF, IANA	SSH, TLS/SSL, HTTPS, DTLS, IPSec/IKE, OAuth, BGPSEC, DNSSEC, SIP, DIAMETER

5 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.

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2021)	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)	Start planning; Transition from 2025
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
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 (2020)	Start planning;
United States	NIST	NSA (2022)	Implementation 2023-2033

Country	Key References
Australia	Post-quantum Cryptography, Australian Cyber Security Center [59]
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]
Germany	BSI – Quantum Technologies and Quantum-Safe Cryptography (bund.de) [63]
Japan	Cryptography Research and Evaluation Committees (CRYPTREC) [64]
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	NCSC
United States	NIST

5.1 Australia

5.1.1 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.

5.1.2 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 published "Post-Quantum Cryptography", July 2022, and plans to update the Australian Information Security Manual to address PQC [67]

5.1.3 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.

5.2 Canada

5.2.1 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.

5.2.2 Published Recommendations

The Canadian Center for Cyber Security has published guidance on planning for the transition to PQC and Cryptographic Agility.

- 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

The Minister for Innovation, Science and Economic Development (ISED) Canada sponsored a working group to publish detailed industry recommendations on the transition. Canadian National Quantum-Readiness: Best Practices and Guidelines, Version 02 – June 17. 2022. published by the Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) [10.1]

- 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

5.2.3 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

- Preparation
- Discovery
- Quantum Risk Assessment

Stage II: Implementation. Starting in 2025

- Quantum Risk Mitigation
- Migration to new QSC
- Validation

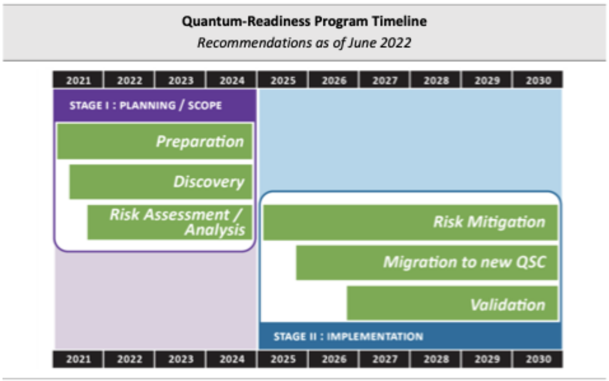
Quantum-Readiness Program Timeline
Recommendations as of June 2022
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
STAGE I : PLANNING / SCOPE
Preparation
Discovery
Risk Assessment / Analysis
Risk Mitigation
Migration to new QSC
Validation
STAGE II : IMPLEMENTATION

Figure 2: Quantum-Readiness Program Timeline [10.1]

5.3 China

5.3.1 PQC Algorithms

Starting in 2018, the Chinese Association for Cryptologic Research (CACR) held a one-round competition to select quantum-resistant algorithms. This competition was open only to teams that included at least one Chinese participant. The CACR [81] called for public key algorithms of three types: key exchange, digital signature, public key encryption schemes. The winners were announced in January 2020. 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).

5.3.2 Published Recommendations

CACR published recommendations for PQC algorithms in 2020 (available in Mandarin [80]).

5.3.3 Timeline

It was reported in 2018 that theoretical research of PQC in China has started, as well as a plan of prototype design, standardisation, and application in several stages.

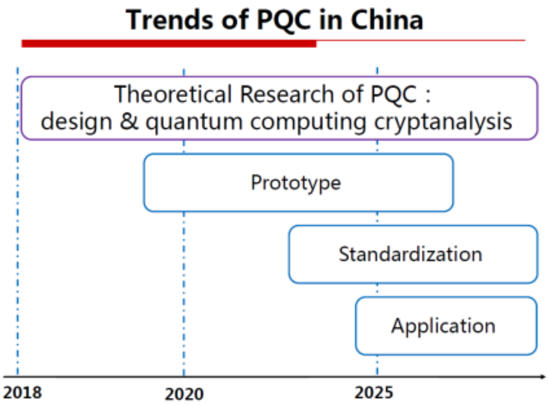
Trends of PQC in China
Theoretical Research of PQC : design & quantum computing cryptanalysis
Prototype
Standardization
Application
2018
2020
2025

Figure 3: Trend of PQC in China [81]

5.4 European Commission

5.4.1 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.

5.4.2 Timeline

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

5.4.3 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).

5.5 Japan

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.

5.5.1 PQC Algorithms

Japanese researchers have contributed to the NIST process.

5.5.2 Published Recommendations

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

5.5.3 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.

5.5.4 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

5.6 New Zealand

5.6.1 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.

5.6.2 Published Recommendations

The New Zealand Information Security Manual was updated 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.

5.6.3 Timeline

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

5.7 Singapore

5.7.1 PQC Algorithms

Singapore is monitoring the NIST process.

5.7.2 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.

5.7.3 Timelines

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

5.7.4 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.

“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.”

5.8 South Korea

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

5.8.1 PQC Algorithms

A Korean standardisation project for PQC (KpqC) was announced in 2021 [99]. This competition is a two-round process that aims at selecting three types of post-quantum algorithms: key exchange/key establishment, digital signature and public key encryption schemes. The first round finishes by the end of 2023 and the second round by the end of 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 [100]. Each proposal must specifically include a technical description of the algorithm, security proofs and a reference implementation in ANSI C.

5.8.2 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=

5.8.3 Timeline

Start competition first round (Nov.'22-Nov.'23).

5.8.4 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=

5.9 France

5.9.1 PQC Algorithms

ANSSI closely follows the NIST PQC process. Yet, ANSSI does not intend to limit the recommended post-quantum algorithms to the NIST winners and may consider additional algorithms. Thus, ANSSI deems Kyber, Dilithium, Falcon (future NIST standards) 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.

5.9.2 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)".

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

5.9.3 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 2025) “defence-in-depth” systems should consider the use of PQC within a hybrid framework.
- Phase 2: 2025-2030) 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.

5.10 Germany

5.10.1 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).

5.10.2 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 [12]. Additionally, BSI highlights the need for further research to address open questions concerning PQC.

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 AIS 20/31 [89].

5.10.3 Timeline

Further Information: BSI - Post-quantum cryptography (bund.de)

BSI - Quantum Technologies and Quantum-Safe Cryptography (bund.de)

5.11 UK

5.11.1 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). Current guidance, is that adoption of Quantum-Safe Cryptography (QSC) will provide the most effective mitigation for the quantum computing threat, supporting the work that NIST is pursuing to provide a set of standardised algorithms that will fulfil the requirements of different use cases for key agreements and digital signatures. The expectation is that commercial products and services will include a transition to Quantum-Safe Cryptography as part of their roadmap, based on

NIST and ETSI guidance, standards and protocols. Additionally, NCSC is not recommending the adoption of pre-standard QSC to mitigate security and business continuity risks linked to replacement of cryptographic components. For organisations that are managing their own cryptographic infrastructure a longer-term plan for Quantum-Safe transition that factors in priorities and dependencies should be prepared.

5.11.2 Published Recommendations

Preparing for Quantum-Safe Cryptography, Version 2, 11 November 2020, NCSC,

https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

5.11.3 Timelines

NCSC advises against early adoption of non-standardised QSC. More guidance will follow the outcome of the NIST process.

5.11.4 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.

5.12 USA

5.12.1 PQC Algorithms

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.

5.12.2 Published Recommendations

For software and firmware signing

- Algorithms are specified in NIST SP-800-208. https://csrc.nist.gov/publications/detail/sp/800-208/final

Symmetric-key algorithms

- Same as CNSA 1.0, but with the addition of SHA-512.

Public-key algorithms

- CNSA 2.0 has identified CRYSTALS-Kyber (key establishment) and CRYSTALS-Dilithium (digital signatures) as the candidate algorithms for the ongoing NIST standardisation process. When the NIST process is complete, the new algorithms will deprecate RSA, Diffie-Hellman, and elliptic curve cryptography.

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.

5.12.3 Timeline

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

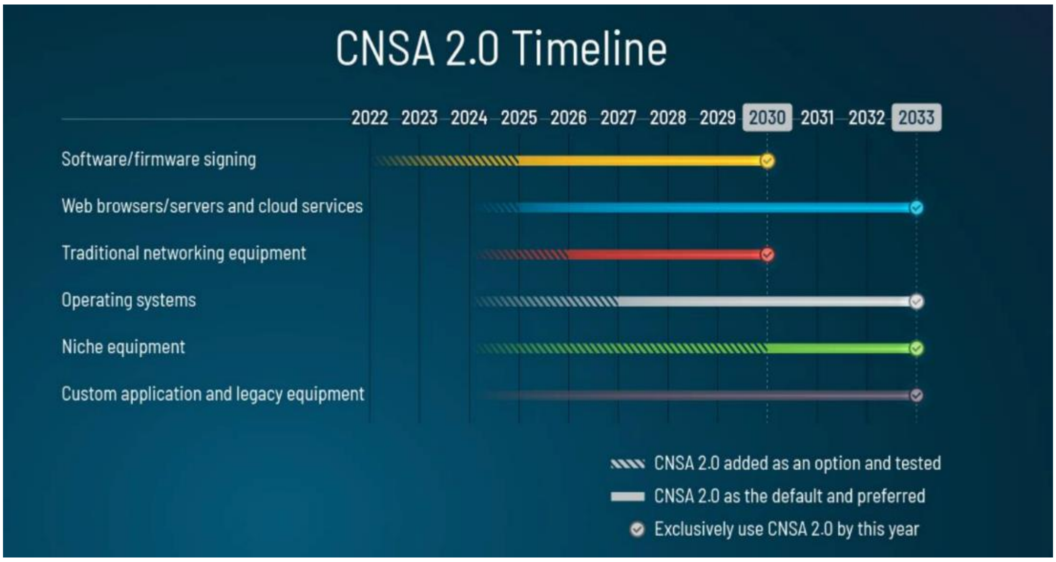

Figure 4: CNSA 2.0 Timeline from announcing the Commercial National Security Algorithm Suite [49]

6 Post Quantum Telco Network – Technology Analysis

6.1 The Quantum Threat – Technical Risk

The security of commonly employed cryptographic algorithms, such as RSA- and elliptic curve-based public key encryption and digital signature schemes, is reliant upon the hardness of solving certain underlying mathematical problems. RSA-based protocols rely on the hardness of finding the prime factors of large integers, while elliptic curve-based methods and Diffie-Hellman key exchanges rely on the hardness of the discrete log problem. Security of these asymmetric protocols is founded on the assumption that a compute- or time- bounded attacker is unable to efficiently compute the prime factors of large integers or solve the discrete log problem. The advent of quantum computing fundamentally changes our assumptions regarding the compute powers available to bad actors. Shor’s algorithm, for example, enables the efficient factorisation of large integers and allows attackers to efficiently solve the discrete log problem. Importantly, Shor’s algorithm can achieve an exponential speedup, relative to known classical methods, rendering it infeasible to simply increase key sizes. Consequently, a sufficiently large fault tolerant quantum computer poses a threat to systems and protocols that utilise public key cryptography and/or digital signatures, and large-scale changes are required to retain present-day security assurances in the face of this quantum threat.

In addition to the above-mentioned threat to asymmetric protocols, symmetric cryptographic protocols such as block ciphers may also require modification, owing to the quantum threat. Grover's quantum algorithm permits a quadratic speedup in unstructured data base searches, relative to classical methods, and may be employed to attack symmetric key protocols such as AES or hash functions. Note however that there is an ongoing line of work which aims at finding attacks more efficient than Grover's algorithm.

The timescale for the development of a large, fault-tolerant Quantum Computer that is capable of running crypto analytic algorithms that threaten modern day cryptography is uncertain. However, it is widely considered that there is a significant (>30%) [52] risk of such a computer emerging in the next decade (by 2032), and therefore, requires preparation, particularly because some forms of attack may be retrospective, as discussed below (e.g. store now, decrypt later).

6.2 The Quantum Threat – Business Risk

The quantum threat presents multiple high impact risks for the telecom industry and its users. The table below gives an overview of some of these threats:

Risk	Description
Store Now, Decrypt Later	Prior to the availability of a Cryptographically Relevant Quantum Computer (CRQC), motivated bad actors may harvest data and store it, with the goal of decrypting it once quantum computing capabilities become available. This attack undermines the security of data with long-lived confidentiality needs, such as corporate IP, state secrets or individual bio-data. It is widely believed that some actors are already engaging in this type of attack.
Code-signing and Digital signatures	If algorithms become vulnerable, then service authentication can be attacked, and lead to vulnerabilities in software updates.
Rewriting history	If digital signature algorithms become vulnerable, the integrity of digitally signed data can be compromised e.g. audit records, call records, contracts, other data.
Key Management Attacks	It is possible that infrastructure is used to store symmetric keys using vulnerable wrappers. Keys used for such long-term storage can therefore become vulnerable by attacking the wrapping mechanisms.

The business consequences of the risks above are important to stakeholders as they may lead to privacy breach, reputational damage, network disruption or other impacts with significant financial implications.

6.3 Post-Quantum Cryptography

PQC refers to a category of cryptographic protocols aiming to provide security against quantum-empowered adversaries by using classical (i.e. non-quantum) techniques. Since the quantum-threat to symmetric algorithms posed by Grover's algorithm is less severe, the pathway to a post-quantum status is perhaps more straight-forward for symmetric protocols. Namely, it remains feasible to retain similar cryptographic methods, in the presence of a quantum-empowered adversary, by employing a higher level of security. For example, in some cases increasing the bit-size of keys under the correct design paradigm may be sufficient to retain an adequate level of security in the face of Grover's algorithm. Such changes can elevate symmetric protocols from quantum-vulnerable to post-quantum secure.

The transition to post-quantum status is more complex for asymmetric algorithms. Since Shor's algorithm permits an exponential speedup, it is not feasible to simply increase the security level of current methods. Instead, one must replace existing asymmetric techniques with alternative methods that provide security assurances against quantum adversaries. Note that asymmetric protocols such as commonly deployed public key encryption schemes and digital signature schemes found favour due to the increased functionality and utility they afford. Since the quantum threat impacts these commonly deployed asymmetric cryptographic protocols, one must either forego this additional functionality or replace the vulnerable algorithms with new algorithms that provide the same functionality but are believed secure against a quantum attack.

One may retain the functionality offered by presently deployed public key encryption and digital signature algorithms by implementing replacement algorithms that are believed secure against quantum attacks. Algorithms in this category are referred to as post-quantum asymmetric cryptographic algorithms, meaning they are plausibly secure against quantum attacks. PQC is expected to play the dominant role in addressing the quantum threat and is recommended for adoption by agencies such as NIST, though standardisation remains ongoing. Such replacement algorithms are not as trivial as they may sound, since even when the desired cryptographic functionality and quantum protection is achieved, the algorithm may incur a compute or failure rate or key-size cost that is incompatible with given use-case constraints.

Research in the fields of quantum computing, quantum algorithms and quantum-related cryptography continues to rapidly evolve. Consequently, the notions *of plausible quantum security* and *provable quantum security* remain as distinct but related categories. New attacks, new algorithms or other technological advances may illuminate vulnerabilities in cryptographic algorithms that otherwise appear plausibly quantum secure; i.e. PQC is not synonymous with "provably Quantum-Safe". An ongoing NIST PQC standardisation project is one of the leading projects currently aimed at standardising a set of post-quantum secure encryption/key exchange algorithms and digital signature algorithms. During this standardisation project, new attacks and cryptanalyses of purportedly quantum secure algorithms, such as Rainbow and SIKE, were uncovered, demonstrating the relative infancy of this field. Nonetheless there are strong motivations for expecting candidate PQC algorithms to be quantum secure. Moreover, plausible quantum security is the next best alternative currently available. Confidence in cryptographic algorithms grows with the test of time and it is the latter that will ultimately determine which PQC algorithms remain viable.

Post-quantum asymmetric algorithms typically rely on new hardness assumptions that are plausibly quantum secure. Below, some key categories of PQC algorithms are briefly summarised. Since the NIST PQC standardisation process is currently the most advanced such project, the discussion references the NIST project.

6.3.1 Pre-shared keys

As an example of foregoing the functionality of asymmetric protocols, one possibility is to use keys established only using symmetric key methods. This approach forgoes some of the flexibility afforded by key exchange protocols that employ quantum-vulnerable algorithms, such as public key encryption and digital signature schemes. Both symmetric and asymmetric methods require pre-established, secure, authenticated communication channels either for pre-sharing secret keys or root certificates for PKI. Using pre-shared keys, to avoid the quantum threat, may be feasible in certain use cases. Indeed, SIM-based mobile communications already rely upon pre-shared keys to achieve key agreement and authentication between user equipment and the network. In Internet standards, the TLS1.3 protocol supports key establishment based on pre-shared keys. Additionally, the IKEv2 key establishment scheme used in IPsec typically uses pre-shared keys for authentication and allows pre-positioned keys to add quantum safety to key exchanges per RFC8784 [23]. Use of pre-shared keys may therefore form part of the solution to the quantum threat but this approach appears unlikely to replace all present-day use cases of quantum-vulnerable asymmetric algorithms. Note that any pre-shared keys must themselves be used within protocols that can withstand the quantum threat, meaning key lengths need to be sufficiently long and symmetric protocols using the keys must themselves be post-quantum secure.

6.3.2 Code-based approaches to PQC

Code-based cryptography utilises the mathematics of error-correcting codes, leveraging the hardness of problems such as correcting errors in random linear codes. Code-based techniques have been studied for many decades, dating back to foundational work by McEliece [42]. Nonetheless, despite pre-dating Shor's algorithm and the interest in PQC, these well-studied techniques did not initially find widespread adoption owing to superior performance characteristics of leaner techniques such as RSA- and elliptic curve-based methods. Code-based methods typically require a much larger public key and incur associated compute costs, for example. The discovery of quantum attacks on RSA- and ECC-based techniques rekindled interest in both well-studied code-based protocols and the design of newer code-based methods.

Multiple code-based algorithms were submitted to the NIST PQC project. However, all submitted digital signature schemes leveraged newer code-based assumptions that were ultimately broken. Similarly, NIST deselected some code-based encryption schemes, owing to cryptanalysis that emerged during the standardisation process. Ultimately no code-based methods were selected by NIST in the third round. Nonetheless, the remaining code-based schemes for key establishment, namely Classic McEliece, HQC and BIKE, all progressed to the fourth round. HQC and BIKE are newer code-based approaches that aim to reduce the public key size. Classic McEliece has a large public key and small ciphertexts, making it less useful for, e.g., ephemeral TLS key exchange. NIST may select a code-based encryption/KEM method for standardisation in the next round, to compliment the lattice-based algorithm selected in the third round. Standardising algorithms which rely on different (i.e., non-lattice-based) assumptions would provide diverse options in case future cryptanalysis reveals vulnerabilities in one method.

6.3.3 Lattice-based approaches to PQC

A lattice is a repeating structure of points in a multi-dimensional module (mathematical space). For lattices residing in many dimensions, it may be (computationally) hard to determine certain properties of points and lines in the space, relative to the structure of the lattice. This hardness provides the basis for lattice-based cryptography and hence mitigates the risks posed by Shor's algorithm.

6.3.3.1 Lattice-based analysis

Lattice-based techniques date back to 1996 [91] and are relatively well-studied, compared to some newer PQC methods. Lattice-based algorithms submitted to the NIST standardisation project rely on lattice-based hardness problems such as Module Learning with Errors (LWE), Module Learning with Rounding (LWR), and the NTRU problem [92]. Informally, the LWE problem involves solving a set of noisy linear equations [93]. The LWR problem can be considered a variant of the LWE problem [94]. Confidence in the hardness of the LWE problem stems from the fact that, for some lattice-based problems, the average-case hardness of solving the problem is provably as hard as the worst-case hardness for solving a related well-studied lattice problem. However, questions exist regarding the concrete security assurances provided by these reductions for the LWE problem [95]. Moreover, such reductions between problems are not known for all lattice-based hardness problems of cryptographic interest, including the NTRU problem. In short, cryptanalysis in this domain provides strong arguments that both the LWE problem and the NTRU problem are plausibly post-quantum secure, but existing analysis is perhaps insufficiently mature to unambiguously preference LWE-based algorithms versus NTRU-based algorithms based solely on security claims [96].

6.3.4 Hash-based approaches to PQC

A hash function is a standard cryptographic primitive that maps input strings to seemingly random output strings, such that it is hard to invert the output (of an unknown input) and hard to find two inputs that produce colliding (i.e. identical) outputs. Generic quantum attacks on hash functions rely on Grover's algorithm and are therefore less severe, making hash functions a suitable building block for the construction of quantum secure algorithms. Hash functions are routinely leveraged as part of commonly employed signature schemes, to handle messages of arbitrary length; for example, a signer may sign the hash of a message, rather than the actual message. However, hash functions can also be used to construct signature schemes, rather than merely being used within a scheme. Hash-based signature schemes do not rely on, e.g., number-theoretic or other mathematically structured hardness assumptions, and instead rely on the security of the underlying hash function, meaning the hash function must sufficiently well approximate a truly random oracle.

Within the hash-based category of algorithms, it's helpful to differentiate between *stateful* and *stateless* signature schemes. A stateful signature scheme requires users to keep track of some information since, e.g. re-using the same values may compromise security. NIST already released standards [101] for two hash-based stateful signature schemes, namely XMSS [102] and LMS [103]. Stateless signature schemes do not require users to keep track of a "state" (i.e. additional information) and therefore offer additional flexibility, relative to stateful schemes. In the third round of the PQC standardisation project, NIST selected the stateless hash-based signature scheme SPHINCS+ [104], promoting the algorithm from the

Alternatives category. note: all other signature schemes described in this section are also stateless.

6.3.5 Multivariate-based approaches to PQC

The security of multivariate-based crypto-systems relies on the hardness of solving systems of multivariate quadratic equations over finite fields. Efficient constructs typically employ seemingly random systems of equations which actually possess hidden structure, owing to the existence of a trapdoor. Multivariate-based constructs progressed as far as the third round of the NIST PQC project but were not ultimately selected after new attacks were discovered on the remaining candidates [105; 106]. Further analysis is required to determine whether potential efficiencies offered by multivariate-based schemes remain valid after the newly discovered attacks are addressed.

6.3.6 Isogeny-based approaches to PQC

Two elliptic curves are said to be isogenous if there is a mathematical map between them, called an isogeny, that preserves their underlying algebraic and geometric properties. Isogeny-based cryptosystems rely on problems relating to the hardness of finding isogenies [106.1]. SIKE is a key exchange mechanism based on supersingular isogenies that progressed to the third round of the NIST process. It has very small key and ciphertext sizes but is computationally more expensive than other candidate key exchange schemes. However, recent cryptanalysis uncovered a devastating key recovery attack on supersingular isogeny-based protocols [107]. Accordingly, the authors of SIKE currently state that SIKE is insecure and should not be used (see: https://sike.org/).

6.3.7 Hybrid approaches for PQC

A hybrid mechanism (key establishment or signature) combines the computations of a recognised pre-quantum public key algorithm and an additional algorithm that is post-quantum secure. This makes the mechanism benefit both from the strong assurance on the resistance of the first algorithm against classical attackers and from the expected resistance of the second algorithm against quantum attackers. For key establishment, one can perform both a pre-quantum and a post-quantum key establishment and then combine both results, e.g. using a Key Derivation Function (KDF). Alternatively, one may use for some specific applications a KDF on a pre-shared key and a shared key obtained from a classical scheme. For signature schemes, hybrid signatures can be achieved with the concatenation of signatures issued by a pre-quantum and a post-quantum scheme and the requirement that both signatures be valid in order for the hybrid signature to be valid. Given that most post-quantum algorithms involve message sizes much larger than the current pre-quantum schemes, the additional message size of a hybrid scheme remains low in comparison with the cost of the underlying post-quantum scheme.

For additional details on Hybrid Scheme, please refer to section 7.1.2.1

6.4 Relationships to other Quantum technologies

6.4.1 Quantum Key Distribution

Quantum Key Distribution (QKD) aims to leverage the quantum properties of matter to enable secret key exchange. For this reason, QKD falls into the category of quantum cryptography, meaning the protocol itself utilises the quantum properties of matter. Security derives from quantum physical properties, in particular the no-cloning theorem in quantum mechanics, which asserts the impossibility of making a perfect copy (i.e. a clone) of an unknown quantum state without altering the original state in some observable way. An adversary who intercepts an in-transit quantum state is therefore unable to both simultaneously learn all information within the state and send the state onwards to the intended recipient, undisturbed. Accordingly, QKD leverages the laws of physics to provide the basis for cryptographic security, avoiding the need for a hardness assumption. Nonetheless, implementations typically require additional security ingredients to ensure secure secret key establishment, such as pre-authenticated communication channels. Given these limitations, QKD is presently not recommended for adoption within certain scenarios by multiple agencies, including for use within U.S. and UK government applications. However, QKD has certain strengths, including complete invulnerability to computational and mathematical breakthroughs, and as such may support key refresh in symmetric cryptography over ultra-secure links. Industry and research institutes continue to actively explore and develop the potentialities of QKD.

The second solution, Quantum Key Distribution (QKD), represents a new way to distribute these random numbers and generate secure keys between different locations. That is because it rests on fundamental physical principles rather that specific mathematical assumptions. QKD can establish such a key remotely between two distinct parties, and it is essentially immune to hacking by both conventional hackers and quantum computers. This is because if anyone tries to tamper with the data, the two QKD parties (normally called Alice and Bob) will immediately know. The security of a complete cryptographic protocol is certainly no more secure than the weakest of all cryptographic elements used, but the key exchange element need not be the weakest link, but the strongest. In short, QKD is the only known method for transmitting a secret key over long distance that is provably secure in accordance with the fundamental properties of quantum physics. QKD can be used standalone to provide secure symmetric keys between parties; QKD can also be used with PQC. There are several activities on hybrid approaches for migration towards quantum-safe algorithms or protocols. Hybrid approaches for key exchange consist in generating a key exchange functionality by combining at least two different key exchange methods.

There are several activities of various SDOs on hybrid approaches for key exchange mechanisms such as ITU-T X.1714 [71], ETSI TS 103 744 [72], NIST Special Publication 800-133 Revision 2 [73], NIST Special Publication 800-56C Revision 2 [74] IETF RFC 8784 [23], IETF draft-ietf-ipsecme-ikev2-multiple-le-08 [76].

6.4.2 Quantum Random Number Generation

A random number is one that is both unpredictable and unbiased [97]. Random numbers are essential to network security because all forms of cryptography require a strong source of entropy. Examples of applications for Random Number Generators: in symmetric cryptography the generation of the key (and possibly also the initialisation vector); in PQC the choice of noise vector in the LWE problem; in QKD the choice of bit values and basis values.

- Pseudo-random number generators (PRNGs) are deterministic. PRNGs may be acceptable for security applications when using a seed containing sufficient entropy.

- Quantum Random Number Generators (QRNGs) are non-deterministic. QRNGs use the randomness of quantum physics to generate true random numbers used for encrypting messages and for other cryptographic applications. The selection of a QRNG requires characterisation and assurance of the entropy source and its implementation, e.g. for operating temperature, aging effects and correlation.

6.5 Standardisation of PQC Algorithms

There are ongoing programs to standardise PQC algorithms from NIST and the Chinese Academy of Science and national programs to adopt PQC in many countries.

6.5.1 NIST

In April 2016, NIST published a report on PQC and announced a competition to standardise post-quantum digital signature algorithms and public key encryption/key encapsulations mechanisms. The deadline for the first round submission was in November 2017. At that time, 69 propositions were submitted. The majority of these submissions were based on lattices, illustrating the potential of this mathematical tool to resist quantum computers.

For more than 4 years, the different candidates have been extensively studied by the cryptographic community. Several attacks were considered serious enough to lead to the non-selection of the concerned algorithms for the second round of the NIST competition.

In January 2019, the NIST announced the candidates selected for the second round of the competition. In July 2020, the list of candidates was narrowed down to 15 candidates entering the third round of the competition but not with the same status. Seven of them were indeed selected as “finalists”, meaning that they will continue to be reviewed for potential standardisation at the end of the round. The eight others were only selected as “alternate” candidates, meaning that they might be standardisation in the future but not at the end of the competition.

In July 2022, the NIST announced a first list of algorithms to be standardised: one key encapsulation mechanism and three digital signatures. Moreover, a fourth round was launched to diversify the KEM portfolio. In addition to new proposals that are expected, four key establishment candidates from the third round have been retained as alternative candidates to be considered for future standardisation (in the meantime, one of them (SIKE) has been fully broken and has been discarded).

NIST estimates* draft of PQC standards in 2023.

*https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

6.5.1.1 Summary of Algorithm Standardisation Process

To summarise, the third round of the NIST PQC project selected the lattice-based encryption/KEM algorithm CRYSTALS-Kyber for standardisation in the encryption/KEM category. Further candidate algorithms also progressed to the next round and may ultimately be selected for standardisation. In the digital signatures category, the lattice-based CRYSTALSs-Dilithium was selected as the primary recommendation, the NTRU lattice-based scheme FALCON was selected owing to efficiencies that may be preferred in some use-cases, and the hash-based algorithm SPHINCS+ was also selected, giving a non-lattice-based option.

In addition, NIST announced a new call for further PQC digital signature submissions. The analysis and design of PQC digital signatures has developed considerably since the NIST PQC standardisation project first began. In addition to analyses revealing weaknesses in some submissions, it became clear that other promising algorithms may exist. The Picnic digital signature scheme serves as an illustrative example to help understand the motivation for inviting new submissions. Picnic is a modular protocol that utilises both a hash function and a block cipher. The scheme, which progressed to the third round of the NIST PQC project, is therefore hash-based but security also depends on the security of the particular block cipher employed. Picnic also has the somewhat novel property of leveraging non-interactive zero knowledge proofs. To achieve efficiencies, the Picnic submission to NIST used a newer block cipher called LowMC [113] but cryptanalysis subsequently found security weaknesses in LowMC [114, 115]. Accordingly, Picnic did not progress beyond the third round. However, it may be possible to construct variants of Picnic that employ a better-trusted block cipher such as AES [106]. The new call for PQC digital signature submissions allows algorithm designers to utilise the lessons learnt already through the NIST project, to submit candidate algorithms whose performance and/or security assurances compliment the schemes already selected for standardisation.

In the third round, NIST selected CRYSTALS-Kyber as an encryption/key exchange algorithm, motivated in part by Kyber’s smaller key size and speed of operation (in relative terms). As a key encapsulation mechanism, Kyber derives from an underlying encryption algorithm whose security relies on the hardness of the module LWE problem.

NIST also selected CRYSTALS-Dilithium as the primary digital signature scheme in the third round. Dilithium is also based on the hardness of lattice problems over module lattices and was selected in part for its relatively high efficiency. NIST also selected the lattice-based digital signature scheme FALCON, due to its efficiency and smaller signature size. Security of FALCON relies on hardness assumptions relating to NTRU lattices, enabling signatures that are considerably shorter, relative to other lattice-based signature schemes, with the same security assurance. Public keys remain around the same size. Note, however, that FALCON requires fast constant-time double-precision floating-point arithmetic to provide acceptable signing performance. Deviation from this constant-time requirement can avail new attack vectors. Though most PCs have fast constant-time double-precision operations, not all devices do, meaning particular care must be taken when considering FALCON deployment. Dilithium is considered easier to safely implement and has better signing performance, though it incurs larger public keys and signatures. In short, Dilithium is currently recommended as a generalist type algorithm by NIST, whereas FALCON may be preferred for particular use cases with greater sensitivity to public key and signature size. SPHINCS+ is an alternative to lattice-based that has much larger signature sizes but significantly smaller public and private keys sizes.

Owing to their relative infancy, it is anticipated that asymmetric PQC algorithms may initially be deployed in a hybrid approach, in combination with classical algorithms. For example, by encrypting shared keys with both a PQC algorithm and a classical technique, one provides fallback security in case the newer PQC algorithm is subsequently found to be insecure. As confidence grows in the PQC algorithms, a transition from hybrid methods to solely PQC methods would follow.

To conclude this section, PQC aims to provide security against the quantum threat and the transition to a post-quantum future poses a challenge for the telco industry. With regards to symmetric protocols, achieving post-quantum security is perhaps more straight-forward since one may adopt similar methods with stronger security levels. Addressing the threat to asymmetric protocols will likely involve a combination of mitigation techniques, such as replacing quantum-vulnerable algorithms with their PQC counterparts or reverting to pre-shared keys. Other techniques such as QKD may find a role in some use cases though PQC is expected to play a dominant role, particularly as standards emerge. The viability of each approach depends on the needs of the particular use case and the performance characteristics of the given approach. Several PQC algorithms have already been chosen for standardisation by NIST and more will follow in the years ahead. As noted below, related standardisation processes are being pursued by similar bodies in other jurisdictions and contexts, ushering in the era of PQC.

6.5.2 ISO/IEC

Following the selection by NIST of the 4 future standards in PQC, the Working Group 2 of the Sub-Committee 27 of ISO/IEC has decided, during its meeting on 6 October 2022, to initiate a Preliminary Work Item “Inclusion of key encapsulation mechanisms for PQC in ISO/IEC standards”.

As this title suggests the specificity of the ISO/IEC initiative is that it only concerns, so far, key encapsulation mechanisms whereas the NIST competition also considered digital signature mechanisms.

Another specificity of the ISO/IEC initiative is that they are willing to consider candidates that were dismissed by the NIST such as FrodoKEM. More specifically, the report mentions three potential targets for standardisation, namely Kyber (future NIST standard), Classic McEliece (which is still under consideration by NIST in its fourth round) and FrodoKEM. The last two schemes suggest that ISO/IEC will favor conservative designs over performance, which would result in an alternative list of standards, somewhat complementary to the NIST ones.

6.5.3 IETF

IETF has multiple workstreams of activity related to PQC.

In terms of post-quantum algorithms, a new working group is under scrutiny to focus on the algorithms selected by NIST (post-quantum symmetric-key algorithms and other post-quantum asymmetric algorithms are out of the scope of this working group). The transition of existing protocols to post-quantum variants is still to be done in the relevant working groups. As such, the Crypto Forum Research Group of the Internet Research Task Force (IRTF) is tasked with providing long-term advice to the IETF on cryptographic algorithms for communication protocols such as TLS, SSH or IPsec. In particular, the design of hybrid key exchange (i.e., a protocol mixing a time-tested standard cryptographic algorithm with a post-quantum one) for TLS is discussed, and several drafts have been published [108,109]. Mechanisms based on symmetric pre-shared keys have also been proposed to authenticate the communication parties in TLS 1.3 [75] or to perform a key exchange in IKEv2 [23]. Other drafts have also been published. For Instance, [110] and [111] aim at adapting X.509

certificates and certificate revocation lists (CRL) respectively to the post-quantum key encapsulation mechanism Kyber and the signature algorithm Dilithium (two algorithms selected by NIST). [112] describes how to use the post-quantum signature SPHINCS+ (also selected by NIST) with the Cryptographic Message Syntax (CMS).

6.5.4 ETSI

ETSI has created the TC Cyber Working Group, and within this, the ETSI Quantum-Safe Cryptography (QSC) group, aimed at assessing and making recommendations for Quantum-Safe cryptographic primitives and protocols.

The group has surveyed all third round NIST candidates for post-quantum digital signatures and key encapsulation mechanisms, resulting in two technical reports, [12] and [14] respectively. All these technical reports are informative only as ETSI, so far, does not plan to support specific candidates.

In parallel, ETSI has issued a technical report [14] defining migration strategies to achieve post-quantum security. More specifically, this report presents a framework of actions that an organisation should take to anticipate transition to post-quantum systems. This increases awareness among organisations about the practical consequences of the advent of quantum computers, but this report remains high-level and does not promote concrete cryptographic solutions.

Finally, the TC Cyber Working Group has published in December 2019 a technical report [98] on “Quantum-Safe Identity-Based Encryption”, an advanced application that seems to fall outside the scope of this whitepaper.

6.5.5 ITU

ITU has published security guidelines for the application of quantum-safe symmetric and asymmetric algorithms to mobile telecommunication systems as well as the alignment of security levels between quantum-safe symmetric and asymmetric algorithms [85].

7 Application of Post Quantum Crypto to Telco Networks

7.1 Technology

In this section we address high level technology and infrastructure implications for network operators applying PQC, such as:

- What is the likely scope of technical change relevant for network operators?
- How are existing Public Key Infrastructures impacted?
- What is the likely nature of change and actions required to be undertaken by network operators and vendors?
- What technology may network operators need to assist with change management and migration to Quantum-Safe?

7.1.1 Scope of technical change

PQC is expected to be wrapped into various communications protocols to make those Quantum-Safe. Since fixed and mobile networks, including devices like customer premises equipment (CPE), smartphones or IoT devices with SIM cards, management systems and value-adding services often represent distributed systems with a large variety of hardware and software components all using communication protocols to communicate to each other, a very large number of components will benefit from Quantum-Safe versions of such communication protocols.

Any component that today uses a protocol which is vulnerable to future quantum attacks *and* is deemed to be sufficiently exposed to potential attacks (because it is not part of a very trusted network) should be considered in-scope. This includes network components which use protocols like IPsec, TLS, HTTPS, authentication mechanisms based on public/private keys, public key infrastructure (PKI) and digital certificates. The scope extends across different 'planes', like user plane, control plane and management plane.

The list of network components (fixed and mobile), network functions, service components (e.g., for SD-WAN), and management components is large and very long, so there is no point in trying to exhaustively list them here. It is more useful to provide a few examples.

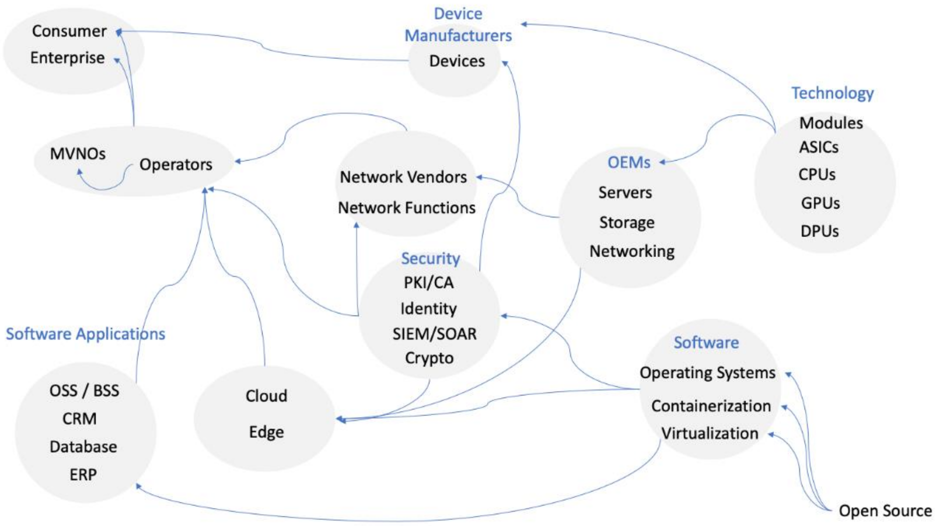

Figure 5*:* PQ Ecosystem Dependencies Structure

<u>SD-WAN services:</u> A workhorse to achieve secure communication tunnels between network devices is the IPsec protocol which is often used to tunnel across internet connections. Network endpoints may use RSA-based public key certificates and use a Diffie-Hellman key exchange mechanism to establish a common secret key for data encryption. This process is quantum-vulnerable. RFC 8784 [23] outlines a method to provide quantum security using pre-poistioned keys. Additional standards that support other Quantum-Safe versions of IPsec are expected to be elaborated by IETF. IPsec network endpoints will then have to support new standards as part of their communication protocol stacks.

<u>Base station to security gateway connection:</u> The connection from RAN to Core network can optionally use the IPsec protocol as well. Similar to the previous example, the setup is quantum-vulnerable unless RFC 8784 [23] methods are used. Thus, both components' protocol stacks are impacted in network deployments where such IPsec tunnels are used.

Service provider e-commerce portals: Customers access those portals over the Internet via HTTPS and TLS protocols to subscribe to services, shop for devices, check their account etc. The current version of TLS is quantum-vulnerable due to its reliance on certificates based on public key cryptography and Diffie-Hellman key establishment. It means that IT components that support protocols and application layer cryptography need to be made Quantum-Safe (e.g. load balancers, HTTP servers, JWT etc.).

IoT and CPE devices: Often software is remotely installed on such devices by downloading software images. These images are protected through digital signatures using e.g. the digital signature algorithm DSA. Since DSA is based on discrete logarithm, the whole process of signing software images to avoid malicious code installation is quantum-vulnerable. This implies that the digital workflow for image signing and decoding needs to be replaced or upgraded to render the architecture Quantum-Safe.

Another aspect to take into account is that some IoT devices will be constrained in terms of processing and memory: PQC implementation will need to consider any limitations of the device to ensure that PQC algorithms are able to run efficiently.

SIM cards and devices: In 5G networks, an encrypted version of the Subscription Permanent Identifier (SUPI) is used, which is called the Subscription Concealed Identifier (SUCI). The latter can be generated by the user equipment or the SIM. On the device-side, the SUCI is generated with a public key provisioned by the home network. Again, as the encryption scheme is based on discrete logarithm, the process is quantum-vulnerable and calls for a Quantum-Safe version.

Systems for Remote SIM provisioning: Mutual authentication between the application on a eUICC and the system which network operators use to securely encrypt operator credentials for over-the-air installation in the eUICC is based on classical asymmetric cryptography and is therefore quantum-vulnerable. As a consequence, protocol changes on protocols within Remote SIM provisioning have to be made.

Operator administrative access to network components: Often, the SSH protocol is used by operational staff to log into remote components for OAM purposes. SSH also uses classical public key cryptography and is therefore quantum-vulnerable. Again, the protocol stacks on both endpoints are impacted, including laptops and PCs used by operations personnel of the network operator and engineers from vendors.

Software modifications:

- Software developers may need to review data structures and field lengths (for keys)
- Database developers may need to consider database column width (for keys)

The examples mentioned illustrate the broad scope of where Quantum-Safe cryptography is relevant to telecoms and IT systems and technology.

7.1.2 Cryptography Management

Most of the current application of cryptography in telecommunications networks are related to the use of *Public Key Infrastructures* (PKI), supporting digital signatures, authentication and the agreement and distribution of the symmetric session keys applied for encrypting data exchange. The evolution of the stack of Internet protocols (the one traditionally known as TCP/IP) towards the generalised use of TLS, and the use of service-based architectures has made this trend even stronger in the last years.

With the exceptions of the use of a shared secret or some kind of security controller), the secure handshake, including peer authentication, and the session key negotiation phase for secure communication rely on the use of a PKI.

Whatever the symmetric algorithms in use, whenever they are the only mechanism used to secure communications, proper key and shared secret rotation intervals and the appropriate crypto material distribution mechanisms must be in place. The transition to Quantum-Safe algorithms does not preclude the possibility of side attacks, most notably via social engineering.

There can be variations in the scope of a PKI (from global ones to those circumscribed to a single site), but the structure based on acknowledged authorities vouching for the validity of a particular public key and its association to a particular identity is the method used in the vast majority of the application of cryptographic procedures in telecommunications.

Taking into account that most of the vulnerabilities and security issues related to PKI have been caused by poor key and identity management, it becomes critical to analyse the implications for these procedures from the PQC transition. The main fields to take into consideration include:

- Algorithm and parameter identifiers, to describe available algorithms and their configuration in security session negotiations and signatures.
- Public and private key formats, to be included in the distribution of crypto materials, especially in certificates.
- Revocation mechanisms, to verify the status of the certificates.

It is necessary to have standardised identifiers and key formats available, to avoid unintended leakage of crypto materials or unintended impersonations in identity management procedures, such as certificate requests and responses. An assessment of revocation mechanisms must be performed, in the light of the computational costs of new algorithms. Revocation verification is one of the most sensitive aspects even in current PKI environments.

7.1.2.1 Cryptographic Agility

Cryptographic Agility is the ability to rapidly update the cryptography used in deployed networks and applications without requiring a major effort to redesign and update the underlying systems, infrastructure and supporting processes.

We know there will be a significant effort involved in the transition to PQC. Cryptographic Agility means designing and implementing both the systems that use PQC and the systems that provide PQC so they can support the proposed NIST PQC algorithms but can be rapidly extended to support other PQC algorithms. If a weakness in a PQC algorithm is discovered, we have the option to transition to a new PQC algorithm after suitable review. Cryptographic agility requires an inventory of all the cryptography in use so we know what is affected (the Cryptographic Bill of Materials), Cryptographic Agility requires updates to the cryptographic libraries to support new PQC, and PQ/T hybrid schemes, and configuration interfaces so we can define the cryptography we are using (algorithms and schemes) by policy and configuration not re-engineering. In practice, Crypto Agility also means that in addition to the possibility of patching, products could include an extra surface for allowing potential updates in order to react to upcoming cryptographic recommendations and standard updates.

7.1.3 Nature of change and required actions

Introduction of PQC will occur over time through system upgrades, replacement of legacy components, and deployment of new components which have already been designed with crypto-agility in mind. To render the migration process economical, network and service providers will have to consider the natural refresh cycles as opportunities to lift components up to a Quantum-Safe status.

New hardware and software components should meet requirements related to cryptographic agility. The latter refers to practices and software architectures that allow to adapt e.g., to an alternative cryptographic standard or a secret key length quickly and thus with agility (should the need arise, because an existing mechanism gets broken) without the need for costly infrastructure changes and long extra development and procurement lead times.

Network operators will also have to decide on a most appropriate strategy to migrate from current status to a Quantum-Safe network and services environment. An example is the potential introduction and use of hybrid certificates, which are traditional ones with additional Quantum-Safe components added to them that can be used by IT or network systems which are quantum-aware, while legacy equipment may ignore the new Quantum-Safe components. This is a way to introduce more flexibility for an operator’s migration strategy.

7.1.4 New technology to assist operators in the journey to Quantum-Safe

A first step in the journey to Quantum-Safe is an analysis to understand vulnerability and prioritisation. Network operators and service providers therefore face a fundamental first challenge: to discover the detailed security configurations used in production across many technical domains as a snapshot at any time during the migration journey; to assess the current levels of risk, remaining vulnerability to quantum attacks and any level of accidental non-compliance to updated corporate security policies.

Given the size of the challenge, such discovery and the inferencing on top of it should ideally benefit from automation. An example is the auto-discovery of security-relevant configuration settings of network components retrievable from network element systems. Automation is expected to reduce the otherwise required operational expense for network operators. However, in above scenario of “security configuration crawling” the question arises, whether any interface or API aspects should be standardised or harmonised across network components to render this feasible and to truly harvest the benefits of automation.

7.2 Business Processes

The PQTN Task Force have assessed the quantum threat landscape and summarize at risk areas below. Along with these risk areas, risk assessment frameworks are presented which can help inform business processes impacted along with mitigation strategies.

7.2.1 Areas Vulnerable to Attacks – Macro View

International organisations such as NSA in USA [49], ENISA in Europe [60,61], and NCSC in the UK [10.3] have identified areas vulnerable to the quantum threat.

CNSA 2.0 groups the areas as follows:

- Software and firmware signing
- Web browsers/servers and cloud services
- Traditional networking equipment (e.g. virtual private networks, routers)
- Operating systems
- Niche equipment (e.g. constrained devices, large public-key infrastructure systems)
- Custom applications and legacy equipment

7.2.2 Risk Assessment Frameworks

The Quantum Threat has created an evolution of cryptographic algorithms and technology; additionally researchers have provided security risk assessment frameworks to help business and strategic planning related to the considerable trade-offs in managing a cryptographic upgrade. Two methodologies are described briefly for reference. This is not comprehensive and should not be considered a specific endorsement.

7.2.2.1 Mosca's Theorem

As first described in 2015 and later elaborated (IEEE, 2018), Michele Mosca [78] from the University of Ottawa proposes an assessment method based on three quantities:

(x) the security shelf life of information and assets

(y) the migration time to PQC

(z) time remaining before the quantum threat is realised (ie. Real-world application of Shor's Algorithm)

In summary, "If x + y > z, then worry"

7.2.2.2 CARAF

CARAF is a proposed "Crypto Agility Risk Assessment Framework", which is grouped into five stages:

1. organisations must determine the specific threat vector that is driving the crypto agility risk assessment.
2. identify the assets impacted by that threat vector.
3. evaluate the expected value of impacted assets being compromised.
4. identify the appropriate mitigation strategy based on the expected value of the compromised asset.
5. develop a roadmap that outlines how to implement the distinct mitigation strategies for the different classes of assets differentiated by risk.

Full details of CARAF have been published in the Journal of Cybersecurity (2021). [49]

8 Post Quantum Telco Network – Impact Assessment

Cryptography provides the building blocks that are used to secure networks, devices and systems. Examples of the uses of cryptography in telecom cover multiple domains.

Domain	Confidentiality	Identification	Integrity	Non-Repudiation
Device	Secure user-to-network registration	Identify the user (IMSI) and device (IMEI) to the network.	Critical software (RF baseband) is unaltered	Emergency call origin
SIM/eSIM	Secure user-to-network communication against casual eavesdropping	Identify the user. (The root of trust for user identity).	Data on SIM is unmodified.	Call origin and billing
Network	Secure network signalling	Limit access to network functions to privileged users	Network Function software is not modified	Control plane and routing changes
Systems (OSS)	Secure network topology and configuration	Limit access to management plane to privileged users	Network configuration is not modified	Origin of critical network changes
Systems (BSS)	Keep subscriber account data and call records confidential	Limit access to subscriber data	Ensure subscriber call records cannot be altered	Inter-operator transactions (roaming, unbundled orders) cannot be revoked
ERP	Ensure employee records are confidential	Limit access to unannounced financial results	Ensure financial records (ledger) are not altered	Payments cannot be revoked
Infrastructure (Cloud)	Ensure data-at-rest is confidential	Limit access to cloud control plane to privileged users	Ensure workloads and configuration are not modified	Origin of workload deployment and updates

8.1 Domains

8.1.1 Device

Post quantum security carries implications for user equipment (UE), such as mobile phones, smart devices, mobile IoT and personal computing devices, with mitigations eventually being required at multiple points in the stack.

For the devices supporting PQC algorithms, the impact is: new code signing, new device firmware, new application software.

8.1.1.1 Operating System Software

Device operating systems generally provide cryptographic software API frameworks. These frameworks are generally proprietary and need to be updated by OS providers before application developers (including browsers) can become Quantum-Safe.

8.1.2 UICC, eSIM/eUICC

8.1.2.1 SIM/UICC

SIM/UICC is defined in ETSI and 3GPP specifications. SIM/UICC implements cryptography, both symmetric and asymmetric for various use cases.

SIM/UICC is used for network authentication. MILENAGE and TUAK are based on symmetric encryption, respectively AES 128 bits and KECCAK/SHA-3 128 to 256 bits. Additionally, 5G SIM/UICC (i.e. 3GPP rel 15 and beyond) introduce IMSI encryption, which used a combination on symmetric (AES) and asymmetric (Elliptic Curves) algorithms. This IMSI encryption may be executed on the SIM/UICC or on the device. A quantum computer would break confidentiality of the user identity.

Those functionalities are defined in 3GPP specifications. It should be a 3GPP SA and CT group responsibility to ensure that the mechanisms are updated to reach quantum safety.

SIM/UICC content is managed through Remote File/Application Management (RFM/RAM), using an OTA (Over The Air) platform. RFM/RAM is defined in ETSI, 3GPP and GlobalPlatform specifications. There are two ways to do this management: SMS-based or HTTPS based. In both cases, security is based on symmetric pre-shared keys. Key compromise would give attackers access to most of the SIM/UICC content.

Review and updating of those protocols are under the responsibility of ETSI SET, 3GPP CT and GlobalPlatform SE committee group.

Besides, SIM/UICC can be accessed through a point-to-point communication. This communication might be secured through Secure Channel Protocols (SCP) defined in GlobalPlatform specifications. These SCP may be use in several use cases, including SIM/UICC personalisation. SCP are based on various protocols, symmetric (DES, 3DES, AES) or asymmetric (RSA, ECC). Update of those SCP and deprecation of the vulnerable ones falls under the responsibility of the GlobalPlatform Secure Element Committee.

Some SIM/UICC can be used as a Java Card platform for application. This platform can provide support of a wide range of symmetric and asymmetric algorithms to applications loaded on the SIM/UICC. Algorithms usage is applications specific. SIM/UICC Java Card platform will have to provide to the applications a Quantum-Safe solution. Update of the Java card specification will be the responsibility of the Java Card Forum.

In addition to the functionalities above, there are also various exchanges of assets between operators and SIM/UICC manufacturers. Those assets include, but are not limited to, master key (from which other secrets may be derived through a Key Derivation Function (KDF)), transport key, input files from operator to SIM vendors and output files from SIM vendors to operators. Some of those data have a lifespan of several years. If some of those data are compromised, it can lead for example to SIM/UICC cloning. All those exchanges are purely proprietary and specific to each pair of operator/SIM vendors. Therefore, it is the duty of each actor to review their exchange mechanism in the light of quantum computing. More specifically, all computer-based exchanges relying on some public key cryptography need to be assessed.

8.1.2.2 eSIM/eUICC Architecture

The analysis made for the SIM in chapter 8.1.2.1 applies in the eSIM context as well.

In the context of eSIM Consumer and M2M, remote SIM Provisioning mandates the use of TLS 1.2 or 1.3 to secure communication over the interfaces between the Remote SIM provisioning Servers (SM-DP+, SM-DS) and between the Remote SIM provisioning Servers (SM-DP+ and SM-DS) and the Device (LPA). In all cases, the use of Diffie-Hellman key exchange is required, with unilateral or mutual authentication based on digital signatures. As a consequence, both confidentiality and authenticity of the communication will be broken by a quantum computer, regardless of the key size used for the symmetric components of the cipher suites.

In the context of eSIM Consumer and M2M, the use of TLS is not mandatory for the Operator and Remote SIM provisioning Server (SM-DP+, SM-DP) but SGP.22 [120] /SGP.02 [119] require a level of security “equivalent to TLS”, which is likely to lead to the use of the same algorithms and therefore to the same vulnerabilities.

In the context of eSIM Consumer, the interface between the Remote SIM provisioning Server (SM-DP+) and the eUICC is secured using a procedure different from TLS but still relies on the same asymmetric components (namely Diffie-Hellman Key Exchange and Digital Signatures) and will thus have the same vulnerabilities.

In the context of eSIM Consumer, the interface between the Operator and the eUICC is protected either by 3DES or AES, in different modes, or by the use of the TLS protocol in Pre-Shared Key (PSK) mode. In the former case, the protocol should withstand quantum computing in the case where AES with enough key length is used.

In the context of eSIM M2M, the SGP.02 cryptographic mechanisms used for 1) Operator and eUICC interface and eUICC are essentially the same as the ones used for Operator and eUICC Interface in the eSIM Consumer paragraph above, which leads to the same conclusions. The eUICC and Remote SIM provisioning Server (SM-DP) interface relies on AES in CBC or CMAC modes, with keys ranging from 128 to 256 bits.

The same document, SGP.02, also mandates the support of the following cipher suites for TLS:

- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CBC_SHA256

with a pre-shared key having at least 128 bits of entropy.

Those interfaces are defined by the GSMA eSIM WG. It should be GSMA eSIM WG responsibility to update those interfaces.

8.1.3 5G Network

Mobile communications between the user equipment and the home/serving network are secured using the Authentication and Key Agreement (AKA) protocol whose purpose is to allow user equipment and network to authenticate each other and establish shared keys that will be used to protect confidentiality and integrity of the communications. The fact that most of the cryptographic mechanisms involved in this process are associated to “symmetric cryptography" reduces the impact of the post-quantum transition on the network but this transition cannot be reduced to a mere doubling of the keys size, as we explain below.-But first we note that 5G introduced asymmetric cryptographic to conceal the Subscriber Public Identifier through the use of the ECIES protocol. As the latter cannot withstand quantum computing, the direct consequence will be the loss of the user's privacy in a way akin to what occurs with IMSI catcher attacks. The most natural solution to this problem would be to move to a post-quantum variant of ECIES based on, e.g. Kyber key encapsulation mechanism. The SUCI calculation takes place in the device (mandatory support) or the USIM (optional support) based on operator decision and therefore both are impacted by PQC transition.

Regarding symmetric algorithms, we note that all the keys involved in the communications belong to a key structure whose root is the long-term key K. The current requirement is that K shall be 128 bits or 256 bits long. Regarding the other keys, transition to 256 bits should be rather easy as most of them are already generated as 256-bit pseudo-random strings before being truncated to 128 bits.

AKA involves a set of algorithms (f1,..,f5) which relies on TUAK (based on the Keccak hash function) or MILENAGE (based on the AES block cipher). Regarding TUAK, transition to 256-bit security should be straightforward. Regarding MILENAGE, the situation is more complex. Indeed, although AES supports 256 bits key size, the block size is restricted to 128, regardless of the key sizes. MILENAGE is therefore likely to undergo some changes to produce 256-bit pseudo-random outputs. This could be done by replacing AES by Rijndael with 256 bits block sizes (AES is Rijndael with 128 bits block size) or by designing an ad-hoc construction using AES as a subroutine.

Once keys are established, communications are protected between the device and the gNB (UP and RAN signalling) or the AMF (NAS signalling) using cryptographic mechanisms based on one of the following primitives: AES, SNOW and ZUC. AES inherently supports 256 bits key size and so will not require any changes to achieve post-quantum security. The situation differs for SNOW and ZUC as they do not support such key sizes. This has led the designers of such schemes to propose 256-bit variants called SNOW 5G and ZUC 256. Regarding SNOW 5G, ETSI SAGE and academic evaluations suggest a strong design, providing a comfortable security margin. Regarding ZUC 256, a recent analysis has shown that the number of rounds in the initialisation phase only provides a limited security margin. For this reason, ETSI SAGE has recommended to increase this number of rounds, which could lead to another version of this algorithm.

The quantum threat also extends to other areas of the network. TLS Is used to secure the N32 interface but also communication between entities in Service Based Architectures (SBA). In both cases, key exchange is performed using classical algorithms (e.g. ECDHE), meaning that any privacy guarantees will vanish with the advent of quantum computers. Authentication based on digital signatures will also be broken.

In the specific case of SBA, an additional issue may arise because of the use of the OAuth 2.0 framework. Indeed, in the case where authorisation tokens are generated using digital signatures, a quantum attacker could forge such tokens and therefore get access to unauthorised resources.

Unlike Public Networks where EAP AKA and 5G AKA are used, the authentication process UE – Network in Non-Public Networks may also be concerned if a given actor choses to rely on EAP methods making use of asymmetric cryptography (e.g. EAP TLS) for authentication and key agreement.

The detailed assessment of the 5G network is under the responsibility of 3GPP SA3.

8.1.3.1 Device

Post quantum security carries implications for user equipment (UE), such as mobile phones, smart devices, mobile IoT and personal computing devices.

Customer owned equipment may exist on a telco network,

The impact on the device concerning the eSIM and 5G Network are captured respectively in sections 8.1.2 and 8.1.3.

8.1.3.2 Operating System Software

Device operating systems generally provide cryptographic software API frameworks. These frameworks are generally proprietary and need to be updated by OS providers before applications (including browsers) can become Quantum-Safe.

8.1.4 Systems (OSS)

Operational support systems typically include connections at L4 and below into the management network, as well as high level APIs. Securing all of these interfaces against advanced quantum computational threat should be a goal, however the security goal of confidentiality of management traffic is usually lower priority than the security goals of data-origin authenticity, integrity and availability. In addition, the shelf time for confidentiality of management traffic is usually not as long-term as for other types of data, such as Personally Identifiable Information (PII). Therefore, it is usually sufficient that the roadmap for upgrading these systems is aligned with the roadmap for the development of quantum computers, since retrospective attacks are usually less significant. The highest priority for early intervention to provide Quantum-Safe confidential communication is for data in transit where large amounts of network addresses related to critical national infrastructure, such as the core network nodes, could be exposed to an adversary who might perform a retrospective attack.

8.1.5 Systems (BSS)

Data at rest: The data residing on BSS platforms being Quantum-Safe.

Data in transit: Data in transit on BSS platforms can be connected to third party software platforms which needs to be Quantum-Safe.

This is important to facilitate Quantum-Safe telco communication cases such as inter-carrier settlements and financial industry transactions.

8.1.6 Systems (ERP)

Data security is dependent on the ERP implementation and the underlying database. The sensitive nature of data in ERP includes financial information that may only have a data cover time until the next financial results are announced, however other information such as the human resources database, which has a long data cover time (and contains data that should always remain confidential). To provide best security, symmetric key methods are recommended (e.g. pre-shared keys).

8.1.7 Infrastructure (Cloud)

The underlying infrastructure (servers, storage, ToR/BoR switches) must support PQC for: low-level management interfaces (e.g. ILO), firmware updates, Identity and Access Management, Privilege Access Management (e.g. jumphosts) and the automation processes (CI/CD).

8.2 Interfaces where Cryptography is used in Telecoms

Cryptography goes beyond the mobile network. It is an end-to-end problem, and not one that can be solved in isolation. Figure 6 presents the high-level architectural actors which use cryptography, and is followed by identifying the relevant interfaces by architectural area.

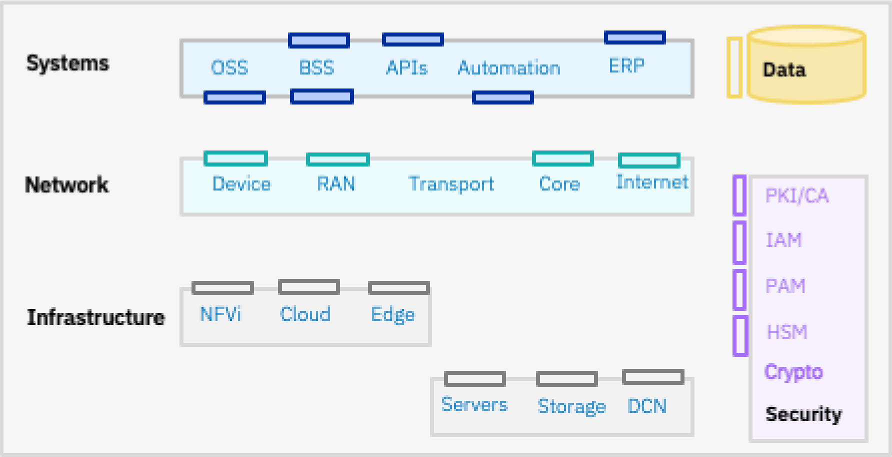

Figure 6: Cryptography Interfaces in Telecoms

This section provides an overview of the systems that are affected by PQC and how they rely on cryptography to secure interfaces or data.

8.2.1 BSS Systems

OSS/BSS system need secure interfaces which generally rely on asymmetric cryptography, e.g. TLS, SSH, etc.”. Operators will need to review the risk exposure and plan to upgrade the systems using Quantum-Safe Alternatives.

8.2.2 Data

Data bases, and federated data stores like data lakes, may need to be secure data at rest by encrypting stored data. They also need to secure remote access interfaces (e.g. ODBC, JDBC, SQL) to ensure confidentiality and integrity of database access.

8.2.3 Infrastructure

All infrastructure whether cloud/NFVI or the underlying servers and storage need secure interfaces to deploy workloads, verify the integrity of software updates and authenticate administrative requests.

Updates to server firmware through the ILO port must be cryptographically verified.

Configuration changes through an administrative CLI must be secured (e.g. using SSH and authenticating the requestor).

8.2.4 Security

Operations, Administration and Maintenance of network elements, systems and infrastructure requires authenticating and potentially logging all administrative access.

An Identity and Access Management (IAM) system and a Privilege Access Management (PAM) system underpin the implementation of cryptographic authentication protocols (e.g. TLS, Kerberos, OAuth).

Management of the public keys is usually centralised in a Public Key Infrastructure and operators often implement a Certificate Authority.

Master keys are usually stored in a Hardware Security Module (HSM) which usually supports the PKCS #11 interface for secure access to keys.

Cryptographic libraries are embedded in many components and finding and updating these libraries to be Quantum-safe will be a key task.

Annex A Definitions, Abbreviations and References

A.1 Definitions

Term	Description
Cryptographic Agility	A product is said to be Cryptographically Agile (or *Crypto Agile)* if it includes the possibility to update its cryptographic algorithms without recalling it or substituting it with a new one.
Cryptographically Relevant Quantum Computer	Describes quantum computers that can attack real world cryptographic systems that would be infeasible to attack with a normal computer. If realisable, a CRQC would be capable of undermining the widely deployed public key algorithms used for asymmetric key exchanges and digital signatures.
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.
Post-Quantum/Traditional (PQ/T) Hybrid Scheme	A cryptographic scheme made up of two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.
PQ/T Hybrid Key Encapsulation Mechanism	A Key Encapsulation Mechanism (KEM) made up of two or more component KEM algorithms where at least one is asymmetric post-quantum algorithm and at least one is a traditional algorithm (IETF [90]).
PQ/T Hybrid Public Key Encryption	A Public Key Encryption (PKE) scheme made up of two or more component PKE algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.
PQ/T Hybrid Digital Signature	A digital signature scheme made up of two or more component digital signature algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm. PQ/T hybrid KEMs, PQ/T hybrid PKE, and PQ/T hybrid digital signatures are all examples of PQ/T hybrid schemes.
Quantum-Safe	Generally accepted to be invulnerable or resistant to cryptanalysis by quantum computers.
Quantum Technology	Technology that makes use of quantum physics (such as Quantum Computers, Quantum Key Distribution, QRNG, Quantum Clocks and Quantum Sensors).
Shelf time	The length of time for which plaintext data needs to be kept confidential.

A.2 Abbreviations

Term	Description
AES	Advanced Encryption Standard
ANSSI	Agence nationale de la sécurité des systèmes d’information
BSI	Bundesamt für Sicherheit in der Informationstechnik

Term	Description
BSS	Business Support System
CA	Certificate Authority
CNCF	Cloud Native Computing Foundation
CNSA	Commercial National Security Algorithm Suite
CRM	Customer Relationship Management
CRQC	Cryptographically Relevant Quantum Computer
CSAC	Chip scale atomic clock
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IPsec	Internet Protocol Security
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
KpqC	Korean Post-Quantum Cryptography Competition
NASA	National Aeronautical and Space Administration
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ONAP	Open Network Automation Platform
OSM	Open Source MANO
OSS	Operational Support System
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
PQ/T	Post-Quantum/Traditional
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QRNG	Quantum Random Number Generator
RSA	Rivest, Shamir and Adleman – the most widely-used public-key cryptographic algorithm – named after its inventors
SSH	Secure Shell Protocol
TLS	Transport Layer Security (a major Internet secure communication protocol)

Term	Description
SNDL	Store Now, Decrypt Later

A.3 References

Ref	Doc Number	Title
1		ANSSI Views On The Post-Quantum Cryptography Transition https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/
2	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
3	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
4	NIST IR 8413 upd1	Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardisation Process (updated 26 Sept 2022). https://doi.org/10.6028/NIST.IR.8413-upd1
5		Transitioning to a Quantum-Secure Economy, World Economic Forum, September 2022 https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
6		ANSSI Views on the Post-Quantum Cryptography Transition, March 25, 2022 https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf
7		Post-Quantum Cryptography, Critical Technologies Policy Coordination Office, Australian Government, October 2021 https://www.pmc.gov.au/sites/default/files/publications/ctpco-tech-cards-post-quantum-cryptography-aust.pdf
7.1		The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography, CSIRO – Australia's National Science Agency, April 2021 https://data61.csiro.au/~/media/D61/Quantum-cyber-report/21-00107_DATA61_REPORT_QuantumCryptography_WEB_2104221.pdf
8		Post-Quantum Cryptography, Australian Cyber Security Center, Australian Government, July 2022 https://www.cyber.gov.au/sites/default/files/2022-07/PROTECT%20Post-Quantum%20Cryptography%20%28July%202022%29.pdf
8.1		Information Security Manual, Part 22 Guidelines for Cryptography, 01 December 2022, Australian Cyber Security Centre (Australian Government) https://www.cyber.gov.au/acsc/view-all-content/ism
9	ITSAP.00.017	Preparing your organisation for the quantum threat to cryptography – ITSAP.00.017), Canadian Center for Cybersecurity, February 2021

Ref	Doc Number	Title
		https://cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017
9.1	ITSE 00.017	Addressing the quantum computing threat to cryptography (ITSE.00.017) May 2020 https://cyber.gc.ca/en/guidance/addressing-quantum-computing-threat-cryptography-itse00017
10	ITSAP 40.018	Guidance on becoming cryptographically agile, Canadian Centre for 10Cyber Security, ITSAP.40.018, May 2022. https://cyber.gc.ca/sites/default/files/2022-05/ITSAP40018-Guidance-on-becoming-cryptographically-agile-e.pdf
10.1		Canadian National Quantum-Readiness: Best Practices and Guidelines, Version 01 – July 7, 2021 Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf
10.2		Preparing Critical Infrastructure for Post-Quantum Cryptography, Cybersecurity & Infrastructure Security Agency (CISA) (USA) Original release date: August 24, 2022 https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
10.3		Preparing for Quantum-Safe Cryptography, National Cyber Security Centre (NCSC)(UK Government), Version 2, 11 November 2020 https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
11	BSI-0Bro21/01	Quantum-safe cryptography – fundamentals, current developments and recommendations, Federal Office for Information Security (Germany), October 2021, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4
12	TR 103 616	ETSI TR 103 616 V1.1.1 (2021-09) “Quantum-Safe Signatures“
13	TR 103 823	ETSI TR 103 823 V1.1.1 (2021-09) “Quantum-Safe Public Key Encryption and Key Encapsulation”
14	TR 103 619	ETSI TR 103 619 “Migration Strategies and Recommendations for Quantum Safe Schemes”
15		Quantum Computing, Networking and Security, GSMA, Version 1.0 March 2021 https://www.gsma.com/newsroom/wp-content/uploads/IG-11-Quantum-Computing-Networking-and-Security.pdf
16		Quantum Networking and Service, GSMA, Version 1.0 December 2021

Ref	Doc Number	Title
		https://www.gsma.com/newsroom/wp-content/uploads//IG-12-Quantum-Networking-and-Service.pdf
17		Quantum Communications: new potential for the future of communications Ofcom, (UK Government) 28 July 2021
18	RFC 8017	RSA Cryptography Specifications Version 2.2, IETF
19	RFC 6979	Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), IETF
20	RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3, IETF
21		Post-Quantum Security Considerations for the Financial Industry, 22 Sept 2022, DTCC https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/Quantum-Computing-WhitePaper-2022
22	PKCS #11	PKCS #11 Cryptographic Token Interface Base Specification Version 3.0 OASIS Standard, 15 June 2020 https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/os/pkcs11-base-v3.0-os.pdf
23	RFC 8784	Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2, (IKEv2) for Post-quantum Security RFC 8784 – Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security (ietf.org)
24	NCSC	Preparing for Quantum-safe Cryptography, NCSC, 11 Nov 2020 https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
25		Miklos Ajtai. 1996. Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM, 99–108.
26		Miklos Ajtai. 1998. The shortest vector problem in L2 is NP-hard for randomised reductions (extended abstract). In *30th Annual ACM Symposium on Theory of* *Computing*, pages 10–19. ACM Press.
27		Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardisation Process, NISTIR 8413. https://csrc.nist.gov/publications/detail/nistir/8413/final
28		M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner (2015). Ciphers for MPC and FHE. Advances in Cryptology – EUROCRYPT 2015, eds E. Oswald, M. Fischlin (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 430-454.
29		C. Baum, C. D. de Saint Guilhem, D. Kales, E. Orsini, P. Scholl, and G. Zaverucha (2021). Banquet: Short and fast signatures from AES.

Ref	Doc Number	Title
		Public-Key Cryptography – PKC 2021, ed Garay JA (Springer International Publishing, Cham), pp 266–297.
30		Abhishek Banerjee, Chris Peikert, and Alon Rosen. 2012. Pseudorandom functions and lattices. Advances in Cryptology–EUROCRYPT 2012 (2012), 719–737.
31		Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal (2017). NTRU Prime: reducing attack surface at low cost. In International Conference on Selected Areas in Cryptography. Springer, 235-260.
32		Daniel J. Bernstein, Andreas Hulsing, Stefan Kolbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe (2019). The SPHINCS+ signature framework. In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019: 26th Conference on Computer and Communications Security*, pages 2129–2146. ACM Press.
33		Ward Beullens (2022). Breaking Rainbow Takes a Weekend on a Laptop. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology – CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13508. Springer, Cham. https://doi.org/10.1007/978-3-031-15979-4_16
34		Wouter Castryck and Thomas Decru (2022). An efficient key recovery attack on SIDH. https://eprint.iacr.org/2022/975
35		Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar (2016). Another look at tightness II: Practical issues in cryptography. In International Conference on Cryptology in Malaysia. Springer, 21-55.
36		David Cooper, Daniel Apon, Quynh Dang, Michael Davidson, Morris Dworkin, and Carl Miller (2020). NIST Special Publication 800-208: Recommendation for Stateful Hash-Based Signature Schemes. Technical report, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-208.
37		Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman (1998). NTRU: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory – ANTS-III*, volume 1423 of *LNCS*, pages 267–288. Springer. http://dx.doi.org/10.1007/BFb0054868.
38		Andreas Hulsing, Denise Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen (2018). XMSS: Extended Hash-Based Signatures. Internet Requests for Comments.
39		Tanja Lange (2020). Sd8 (post-quantum cryptography) – part 6: Isogeny-based cryptography. Technical Report N 2274, ISO/IEC JTC 1/SC27/WG 2, 2020. https://www.din.de/resource/blob/721042/4f1941ac1de9685115cf53bc1a14ac61/sc27wg2-sd8-data.zip.
40		F. Liu, T. Isobe, and W. Meier (2021). Cryptanalysis of full LowMC and LowMC-M with algebraic techniques. Advances in Cryptology – CRYPTO 2021, eds T. Malkin, C. Peikert (Springer International Publishing, Cham), pp 368-401.
41		F. Liu, G. Wang, W. Meier, S. Sarkar, and T. Isobe (2022). Algebraic meet-in-the-middle attack on LowMC, Cryptology ePrint Archive, Report 2022/019. https://ia.cr/2022 /019.

Ref	Doc Number	Title
42		Robert J. McEliece (1978). A public-key cryptosystem based on algebraic coding theory, theory. JPL DSN Progress Report http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF
43		David A. McGrew, Michael Curcio, and Scott R. Fluhrer (2019). Hash-Based Signatures. RFC 8554, RFC Editor.
44		Petzoldt, and J. Ding (2021). Efficient key recovery for all HFE signature variants. Advances in Cryptology – CRYPTO 2021, eds Malkin T, Peikert C (Springer International Publishing, Cham), pp 70-93.
45	PP-21-1120	Quantum Computing and Post-Quantum Cryptography, Frequently Asked Questions, PP-21-1120, Aug 2021, National Security Agency https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
46		Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin (2022). Lattice-based Key-Sharing Schemes: A survey. ACM Computing Surveys, Volume 54(1), pp 1-39. https://doi.org/10.1145/3422178
47		Oded Regev (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) 56, 6 (2009), 34.
48		C. D. de Saint Guilhem, L. De Meyer, E. Orsini, and N. P Smart (2020). BBQ: Using AES in Picnic signatures. Selected Areas in Cryptography – SAC 2019, eds K. G. Paterson, D. Stebila (Springer International Publishing, Cham), pp 669-692.
49	CARAF	Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, Vaibhav Garg, CARAF: Crypto Agility Risk Assessment Framework, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab013, https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827
49	PP-22-1338	Announcing the Commercial National Security Algorithm Suite 2.0, National Security Agency, Version 1.0, September 2022 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
50		Transitioning National Security Systems to a Post-Quantum Future, 30 November 2022, Morgan Stern from NIST Fourth PQC Standardisation Conference, 29 November – 01 December 2022 https://csrc.nist.gov/csrc/media/Presentations/2022/transitioning-national-security-systems-to-a-post/images-media/session3-stern-transitioning-national-security-systems-pqc2022.pdf
50	IG.11	GSMA IG.11 Quantum Computing, Networking and Security 1.0, December 2021
51	IG.12	GSMA IG.12 Quantum Networking and Service 1.0, July 2021
52		2021 Quantum Threat Timeline Report: Global Risk Institute – Global Risk Institute

Ref	Doc Number	Title
53		Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardisation Process https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf
54		NIST Announces First Four Quantum-Resistant Cryptographic Algorithms https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
55		BIS Innovation Hub announces new projects and expands cyber security and green finance experiments https://www.bis.org/press/p220617.htm
56		Post-Quantum Security Considerations For The Financial Industry https://www.dtcc.com/dtcc-connection/articles/2022/september/21/post-quantum-security-considerations-for-the-financial-industry
57		The Banque de France has successfully experimented with Cryptonext Security post-quantum security technologies https://www.banque-france.fr/en/communique-de-presse/banque-de-france-has-successfully-experimented-cryptonext-security-post-quantum-security
58	Open Quantum Safe	Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project https://link.springer.com/chapter/10.1007/978-3-319-69453-5_2
59		Post-Quantum Cryptography, Australian Cyber Security Center, 06 July 2022 https://www.cyber.gov.au/acsc/view-all-content/publications/post-quantum-cryptography
59.1		Action Plan for Critical Technologies: Post-Quantum Cryptography, Oct 2021 https://www.industry.gov.au/publications/action-plan-critical-technologies/tech-cards/post-quantum-cryptography
60		Post-Quantum Cryptography, Integration Study, October 2022, TP-03-22-080-EN-N , ENISA https://cyber.gc.ca/en/news-events/nist-announces-post-quantum-cryptography-selections

Ref	Doc Number	Title
61		Post-Quantum Cryptography https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study/@@download/fullReport
62		ANSSI Views On The Post-Quantum Cryptography Transition https://www.ssi.gouv.fr/en/publication/53nssi-views-on-the-post-quantum-cryptography-transition/
63		Quantum Technologies and Quantum-Safe Cryptography https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html
64		Japan Quantum Technologies and Quantum-Safe Cryptography https://www.cryptrec.go.jp/en/
65		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 https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/11/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
66		The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography https://data61.csiro.au/~/media/D61/Quantum-cyber-report/21-00107_DATA61_REPORT_QuantumCryptography_WEB_2104221.pdf
67		ACSC “Post-Quantum Cryptography” (July 2022) https://www.cyber.gov.au/sites/default/files/2022-07/PROTECT%20Post-Quantum%20Cryptography%20%28July%202022%29.pdf
68		ACSC Information Security Manual (ISM) https://www.cyber.gov.au/acsc/view-all-content/ism
69	NSM-10	National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems 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/
70		Memorandum For The Heads Of Executive Departments And Agencies https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
71	ITU-T X.1714	ITU-T Recommendation X.1714 (2020), *Key combination and confidential key supply for quantum key distribution networks*.

Ref	Doc Number	Title
72	ETSI TS 103 744	Technical Specification TS 103 744 (2020), *CYBER; Quantum-safe Hybrid Key Exchanges (2020)*
73	NIST SP800-133r2	NIST Special Publication 800-133 Revision 2 (2020), *Recommendation for Cryptographic Key Generation*.
74	NIST SP800-56Cr2	NIST Special Publication 800-56C Revision 2 (2020), *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.
75	IETF RFC 8773	IETF Standard RFC8773 (2020), *TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key*
76	IETF draft-ietf-ipsecme-ikev2-multiple-ke-08	IETF draft standard draft-ietf-ipsecme-ikev2-multiple-ke-08 (2022), *Multiple Key Exchanges in IKEv2 draft-ietf-ipsecme-ikev2-multiple-ke-08*.
77	IETF draft-campagna-tls-bike-sike-hybrid-07	IETF draft experimental draft-campagna-tls-bike-sike-hybrid-07, *Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)*.
78	Mosca, 2018	Mosca, M. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” IEEE Security & Privacy 16, no. 5 (September 2018): 38-41, https://doi.org/10.1109/MSP.2018.3761723
79	PL 117-260	H.R.7535 – Quantum Computing Cybersecurity Preparedness Act https://www.congress.gov/bill/117th-congress/house-bill/7535/text
80	CACR 2022	https://www.cacrnet.org.cn/site/content/854.html
81		Research of Post-Quantum Cryptography in China” Jiwu Jing, Data Assurance and Communications Security Research Center Chinese Academy of Sciences https://docbox.etsi.org/Workshop/2018/201811_ETSI_IQC_QUANTUMSAFE/EXECUTIVETRACK/JING_CHINESEACCADEMYOFSCIENCE.pdf
82		Advisory Board for Cryptographic Technology FY 2020 Annual Report” CRYPTREC, RP-1000-2020 (In Japanese
83		CRYPTREC LS-0001-2012R7 (Japan e-Government Recommended Cipher List, last update: 2022/3/30) has
84		Recent Trends on Research and Development of Quantum Computers and Standardisation of Post-Quantum Cryptography, Discussion Paper No. 2021-E-5
85	ITU-T-X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems, April 2021. https://www.itu.int/rec/T-REC-X.1811-202104-I
86	draft-ietf-ipsecme-	Multiple Key Exchanges in IKEv2”, October 2022

Ref	Doc Number	Title
	ikev2-multiple-ke	https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-multiple-ke
87	NICT_NEWS_2022-491_E	White Paper on Quantum Network. Building an International Hub for Quantum Security https://www.nict.go.jp/en/data/nict-news/NICT_NEWS_2022-491_E.pdf
88		National Quantum Safe Network that provides robust-cybersecurity https://news.nus.edu.sg/national-quantum-safe-network-that-provides-robust-cybersecurity/
89	AIS 20/31	Notes on Application and Interpretation (AIS) in Line with ITSEC and Common Criteria (CC) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Anwendungshinweise-und-Interpretationen/AIS/aiscc_node.html
90		Terminology for Post-Quantum Traditional Hybrid Schemes https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology/
91		Generating Hard Instances of Lattice Problems, M. Ajtai Published 1996, Mathematics, Computer Science. Electron. Colloquium Comput. Complex.
92		NTRU: A ring-based public key cryptosystem. Jeffrey Hoffstein, Jill Pipher & Joseph H. Silverman. 1998
93		On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, Oded Regev May 2, 2009
94		Pseudorandom Functions and Lattices. Abhishek Banerjee, Chris Peikert, and Alon Rosen 2012
95		NTRU Prime: reducing attack surface at low cost. Daniel J. Bernstein , Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal, 2017.
96		Will You Cross the Threshold for Me? Generic Side-Channel Assisted Chosen-Ciphertext Attacks on NTRU-based KEMs. Prasanna Ravi, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, Sujoy Sinha Roy. 2021
97		NIST Special Publication 800-90A Revision 1 (June 2015), Recommendation for Random Number Generation Using Deterministic Random Bit Generators” http://dx.doi.org/10.6028/NIST.SP.800-90Ar1
98	TR 103 618	TR 103 618 “Quantum-Safe Identity-Based Encryption”
99	KpqC	KpqC Comptetion Round 1 Algorithms https ://kpqc.or.kr/
100	ePrint	Cryptology ePrint Archive https://eprint.iacr.org/

Ref	Doc Number	Title
101		Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardisation Process. Cooper et al, 2020
102		Rapidly Verifiable XMSS Signatures. Hulsing et al, 2018
103		Hash-Based Signatures. McGrew et al, 2019
104		The SPHINCS+ Signature Framework. Bernstein et al, 2019
105		Breaking Rainbow Takes a Weekend on a Laptop. Beullens, 2022
106		Efficient Key Recovery for all HFE Signature Variants. Chengdong Tao , Albrecht Petzoldt, Jintai Ding. 2021
106.1		Concrete quantum cryptanalysis of binary elliptic curves. Lange et al, 2020
107		An efficient key recovery attack on SIDH. Wouter Castryck and Thomas Decru. 2022
108	RFC9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)
109		IETF draft- Hybrid key exchange in TLS 1.3
110		IETF draft – Internet X.509 Public Key Infrastructure – Algorithm Identifiers for Kyber
111		IETF draft– Internet X.509 Public Key Infrastructure – Algorithm Identifiers for Kyber
112		IETF draft- Use of the SPHINCS+ Signature Algorithm in the Cryptographic Message Syntax (CMS)
113		Ciphers for MPC and FHE. Albrecht et al, 2015
114		Low-Memory Algebraic Attacks on Round-Reduced LowMC. Liu et al, 2021
115		Algebraic Meet-in-the-Middle Attack on LowMC. Liu et al, 2022
116		BBQ: Using AES in Picnic Signatures. De Saint Guilhem et al, 2019
117		Assurance of Quantum Random Number Generators - Quantum Communications Hub (quantumcommshub.net)
118		BT and Toshiba launch first commercial trial of quantum secured communication services | EY UK
119	SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 4.2, 07 July 2020, GSMA https://www.gsma.com/esim/resources/sgp-02-v4-2/
120	SGP.22	RSP Technical Specification, Version 3.0, 19 Oct 2022, GSMA https://www.gsma.com/esim/resources/sgp-22-v3-0/

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority
V1.0	17/02/2023	Final version sent to PQTN group approval	Technogloy Group

B.2 Other Information

Type	Description
Document Owner	Post Quantum Telco Network Task Force
Editor Name, Company Name	- Ayan Ghosh, Arqit - Daryl Burns Arqit - Daniel Shui, Arqit - Sophie Stevens, Arqit - Catherine White, EE - Jonathan Legh-Smith, EE - Jerome Dumoulin, IDEMIA - Lory Thorpe, IBM - Zygmunt Lozinski, IBM - Saïd Gharout, Kigen - Hyungsoo Kim, KT corp. - Loïc Ferreira, Orange - Olivier Sanders, Orange - Todor Gamishev, Orange - Dong-HI Sim, SK Telecom - Monique Morrow, Syniverse Technologies - Diego Lopez, Telefonica - Luke Ibbetson, Vodafone - Guenter Klas, Vodafone - Jens Ruedinger, Vodafone - Chloe Ai, Vodafone - Kristian McDonald, Vodafone - Michael Salmon, Verizon

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.