GSMA

Post Quantum Cryptography –
Guidelines for Telecom Use Cases

Executive Summary

February 2024

1.0 Why is this document relevant?

Telecommunication networks are the backbone of digitalisation, underpinning many essential services and sectors through trusted and secure communication systems which impact society as a whole. For this reason, ongoing security and integrity must be at the forefront of telecommunication preparedness. This includes planning for the quantum era and the potential threats that quantum computers pose to telecommunications networks, customer data and devices.

This document provides detailed insights for preparing a cryptographic migration and implementation of post quantum cryptographic capabilities in the context of telecommunication networks; analysing use cases and architecture, highlighting dependencies on standardisation, solution alignment, performance testing and related topics such as Zero Trust Architecture.

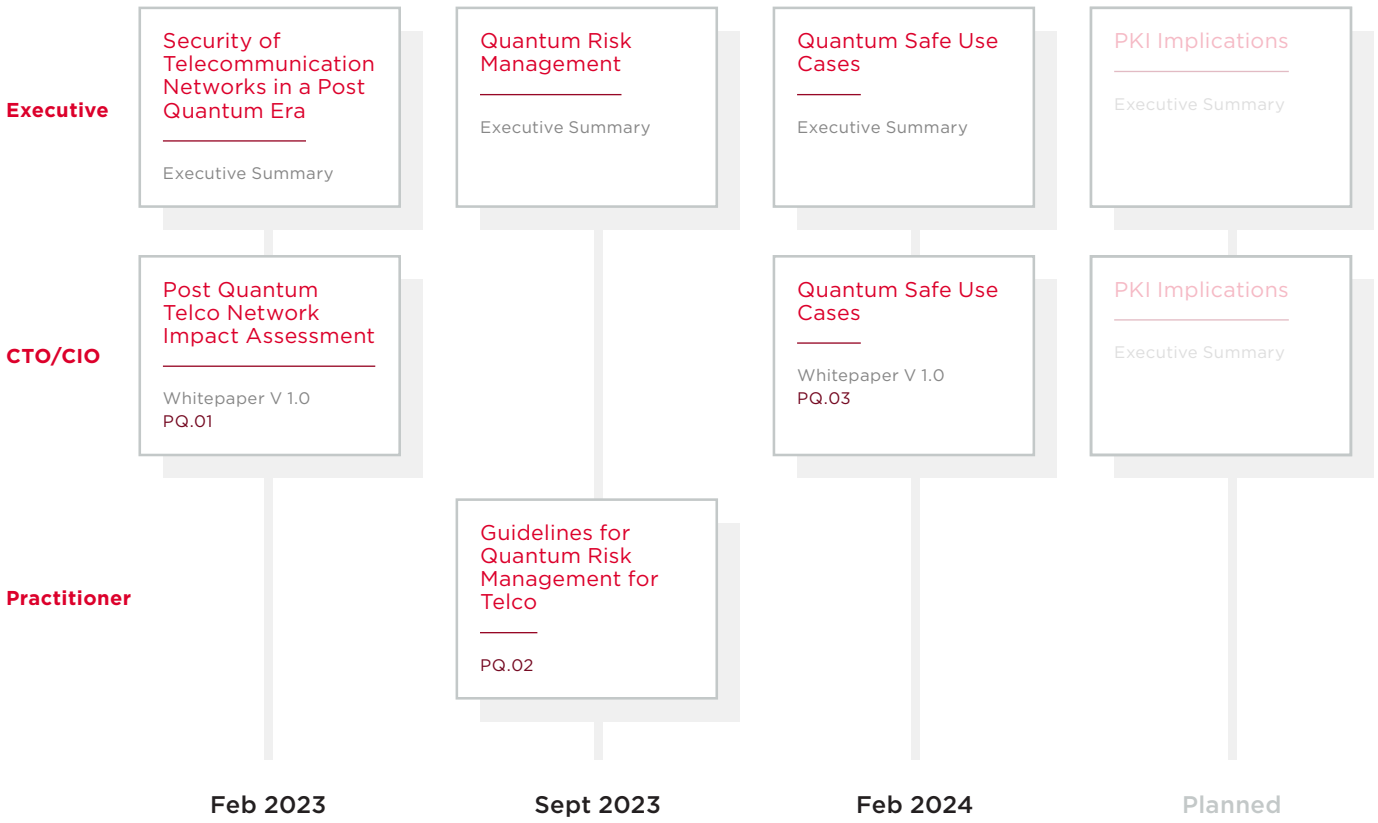
The objective is to build a set of best practice guidelines to support an executable journey to quantum safe for operators and the wider telecommunication ecosystem, leveraging learnings and evolving a collective view of solutions and standards that support interoperability, backward compatibility and performance requirements.

2.0
How do we see It evolving?

This is a first version of a working document that covers an initial set of telco use cases impacted by post quantum cryptography. Over time we plan to update and add to these use cases as required, and explore the relevant technology, standards or policies to inform telco ecosystem decision makers. This will provide a telco-focused, practical and actionable perspective, based on learnings, experience and best practice.

The relationship between this document and previous PQTN task force publications is illustrated in Figure 1. Feedback from the wider ecosystem is essential for the continued relevance of the document. Recognising that many aspects regarding standards, policy and solutions are evolving in parallel and have multiple dependencies, the GSMA PQTN Task Force welcomes the opportunity to engage and foster cooperation between all relevant stakeholders. Alignment around technology decisions is likely to become critical in the context of interoperability, backward compatibility, and performance. Developing proofs of concept and testing are essential for timely deployability of commercial solutions.

Figure 1
Taxonomy of PQTN task force publications

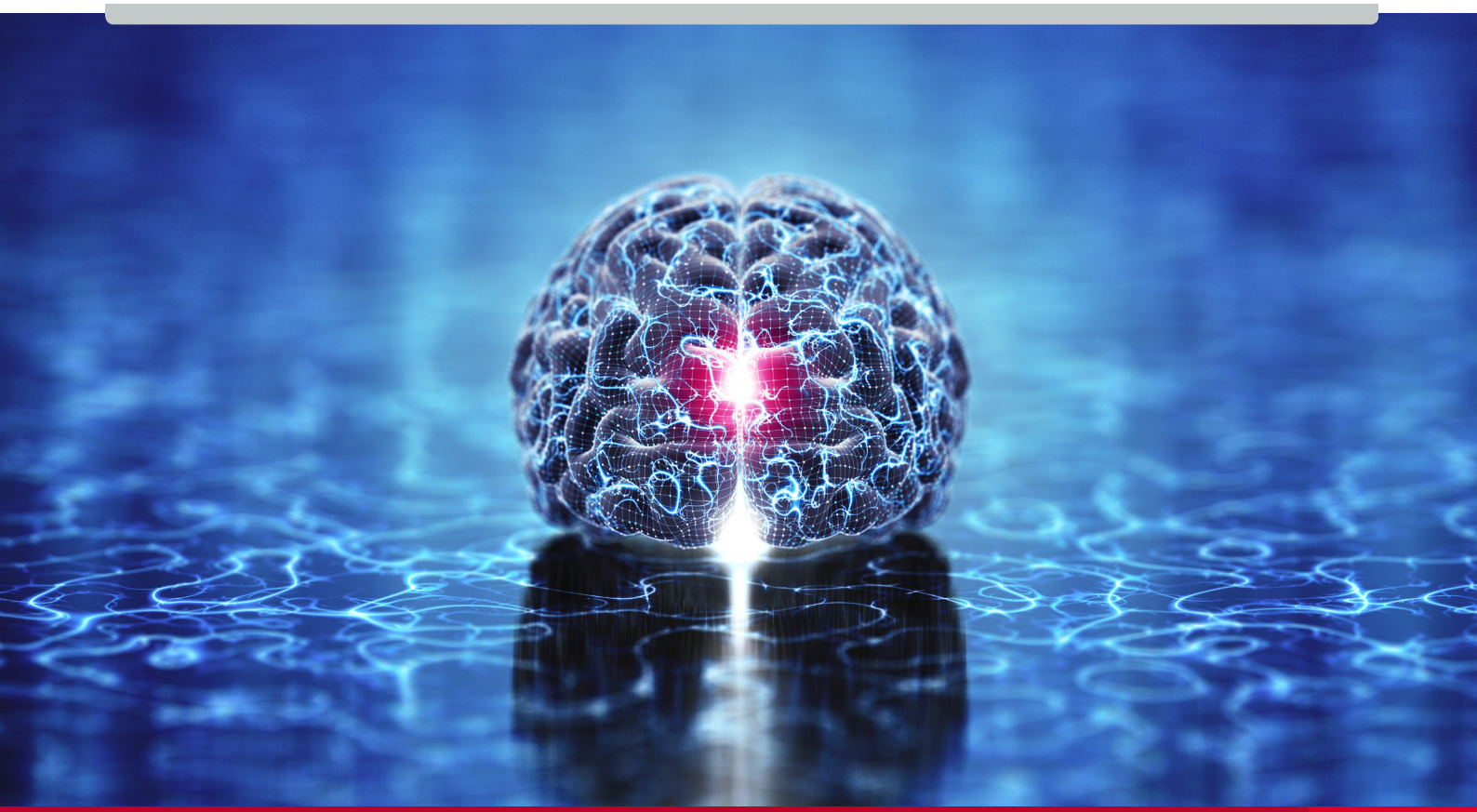


3.0 What is the Quantum Threat?

The evolution of quantum computing capabilities poses a threat as they have the potential to render obsolete the most commonly used cryptographic algorithms, such as public key cryptography, which underpin the cyber security solutions we rely on today to keep information and communications safe.

The timing of the threat is uncertain, however significant progress is being made in the evolution of quantum computing performance, quantum algorithms, and error correction.

The telco industry should start now to plan for the post quantum migration. An immediate threat to consider is “Store now decrypt later”, where encrypted data is harvested in anticipation of being decrypted in the future. This is particularly relevant for data that has a long shelf life when considering the possible availability of cryptographically relevant quantum computers in the coming years.



4.0
Use cases, risk analysis and business Impact

For the use cases listed in the table below, an analysis has been provided to inform both business risk and subsequent technology choices.

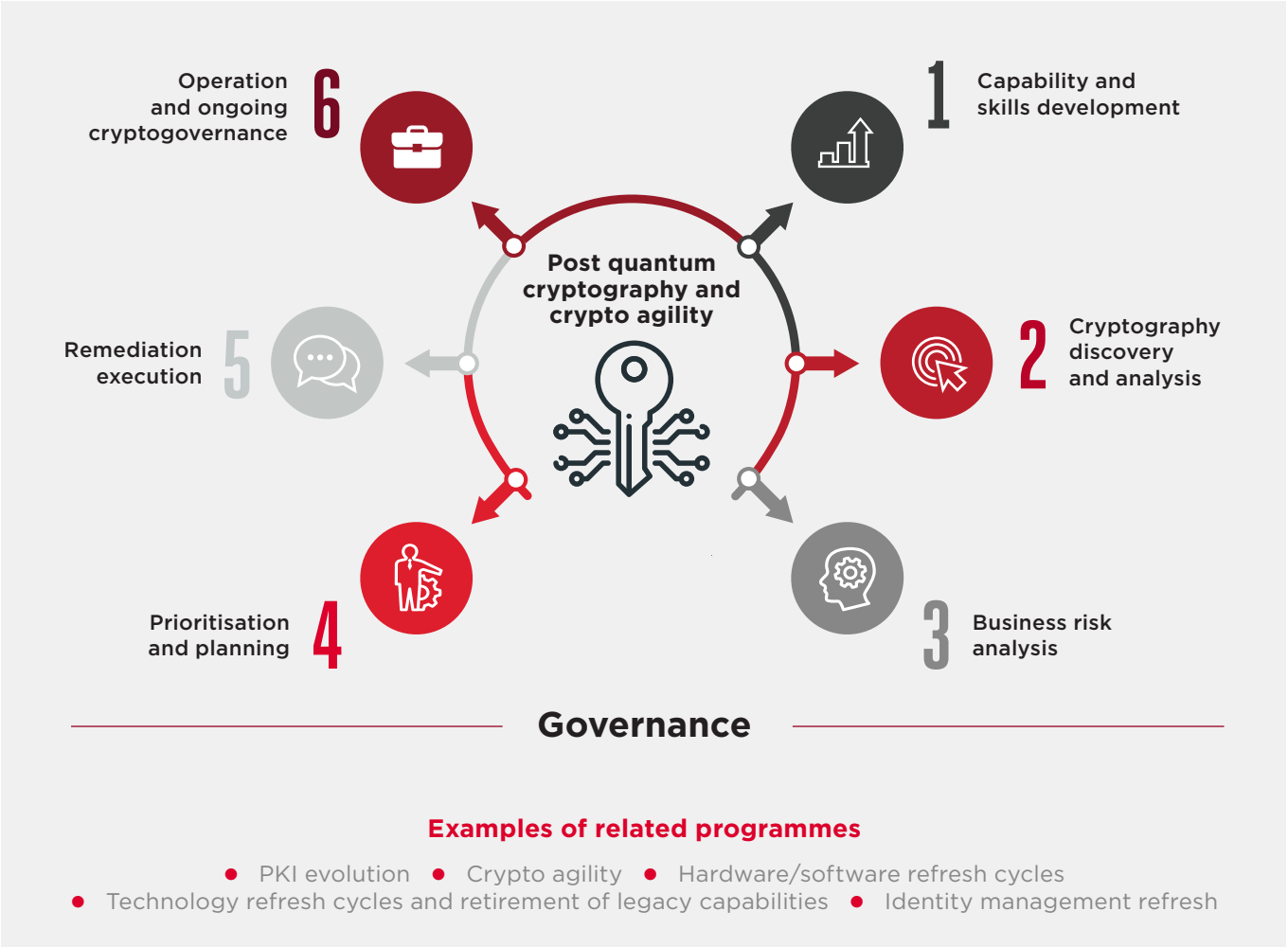
NETWORK OPERATOR USE CASES	CUSTOMER IMPACTING USE CASES
Protection of interface between base stations & security gateway	Virtual Private Network services
Virtualized network functions	SD-WAN services
Cloud Infrastructure	IoT Smart Meters
SIM (physical)	IoT Automotive
eSIM Provisioning (remote)	Lawful Intercept
Devices and firmware upgrade	Privacy of customer data
Concealment of the Subscriber Public Identifier	
Authentication and transport security in 4G and 5G	

5.0 Importance of planning and preparation

The document provides practical guidelines on how organisations can start to plan, engage with internal and external stakeholders, quantify risk and take action.

Forward planning will provide significant benefits to organisations in managing risks and optimising costs of the post quantum migration. A definition of high-level phases to support the journey to Post Quantum Cryptography and subsequent management is outlined in Figure 2, illustrating the iterative nature of the phases.

Figure 2
A phased journey towards Quantum safe



6.0 Government guidance

A multi-country overview of published government guidance (updated from the impact assessment whitepaper), highlighting the increased momentum and activities in progress globally is shown in Table 2. Given this is a rapidly evolving area for governments globally, ongoing monitoring will be required to ensure consistency with strategic plans and roadmaps for telco.

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

Supporting Companies:

3 United Kingdom
AKAYLA
Arqit
AT&T Mobility
Cellular South Inc. d.b.a. C Spire
China Telecom
China Unicom
CK Hutchison
Deutsche Telekom AG
EE Limited
Ericsson
F5, Inc.
Fortinet
Giesecke+Devrient Mobile Security
Hewlett Packard Enterprise
Huawei
IBM
IDEMIA
IMDA
Infineon Technologies AG
Infobip Ltd
Juniper Networks
Kigen
KT Corporation
Maxis Broadband Sdn. Bhd.
National Cyber Security Centre
Nokia
NXP
OFCOM
Orange
Orange France
Palo Alto Networks Inc.
PQ Shield
Proximus Belgium
Qualcomm
Samsung Electronics Co Ltd
SandboxAQ
SK Telecom Co., Ltd.
stc Group
STMicroelectronics
Telcel
Telefónica Germany GmbH & Co. OHG
Telefónica S.A.
TELUS Communications Inc.
Thales DIS France SAS
The MITRE Corporation
TIM S.p.A
Utimaco TS GmbH
Verizon
Vodacom (Pty) Ltd.
Vodafone Germany
Vodafone Portugal
Vodafone Group

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601