

# Security of Telecomunication Networks in a Post Quantum Era

**Executive Summary** 



The telecom industry now needs to mobilise to define guidelines and processes for the **Post-Quantum Cryptography (PQC)** transition

# The transition to Post-Quantum Cryptography has started

Quantum Computing has great potential, but also brings business risk with far reaching consequences on telco networks and customers. Governments have begun planning and issuing guidance to mitigate these risks.

#### **Business Risks**

#### Store Now, Decrypt Later

Store sensitive data with the goal to decrypt when quantum computers are available

#### Code-signing and Digital signatures

Compromise service authentication leading to vulnerabilities in software updates

#### **Rewriting history**

Compromise the integrity of digitally signed data e.g. contracts.

#### Key Management Attacks

Long-term data storage can be vulnerable by attacking key management

## How can the industry prepare?

- GSMA Members have defined impact assessment (1) for the transition to Post-Quantum Cryptography in telecom networks
- Refresh of existing security architecture is required as existing algorithms become vulnerable
- Engage with industry groups, government, and vendors on the

roadmaps to implement Post-Quantum Cryptography

- Understand how to treat legacy systems, services and products that may not be updated
- Reduce the creation of cryptographic debt
- Consider impacts to key management systems

#### How can operators prepare?

- Establish a cryptographic inventory: understand where cryptographic algorithms are used in systems or vendor products
- Plan a cryptography risk assessment
- Develop expertise in Post-Quantum Cryptography and security
- Support standardisation & open-source
- Support related research.
- Engage with customers and vendors for requirements
- Develop a Post-Quantum Cryptography transition plan

## **Potential New Services**

- Quantum-Safe VPN
- Quantum-Safe SD-WAN
- Quantum-Safe connection between
  enterprise customers and hybrid cloud
- Quantum-Safe IoT connectivity
- Quantum-Safe satellite communications links
- Quantum-Safe data archive

[1] https://www.gsma.com/newsroom/resources/post-quantum-telconetwork-impact-assessment-whitepaper



# **Government Response**

Governments are aware of the risks and recommend industry to begin planning.

| Country   | PQC<br>Standards | Published Guidance          |
|-----------|------------------|-----------------------------|
| Australia | NIST             | CTPCO (2021) – early        |
|           |                  | implementation from 2025    |
| Canada    | NIST             | Cyber Centre (2021) –       |
|           |                  | implementation from 2025    |
| China     | China            | CACR (2020) - start         |
|           | Specific         | planning                    |
| EC        | NIST             | ENISA (2022) - start        |
|           |                  | planning                    |
| France    | NIST (non-       | ANSSI (2022) - transition   |
|           | exclusive)       | from 2025                   |
| Germany   | NIST (non-       | BSI (2022) - start planning |
|           | exclusive)       |                             |
| Japan     | Monitoring       | CRYPTREC - start            |
|           | NIST             | planning                    |
| New       | NIST             | NZISM (2022) - start        |
| Zealand   |                  | planning                    |
| Singapore | Monitoring       | MCI (2022)                  |
| 0 1       | NIST             | , ,                         |
| South     | KpqC             | MSIT (2022) - competition   |
| Korea     |                  | started 2022                |
| UK        | NIST             | NCSC (2020) – start         |
|           |                  | planning                    |
| USA       | NIST             | NSA (2022) –                |
|           |                  | implementation from 2023    |

# In summary, Operators and Industry Partners are advised to

- Plan for future implementation to the transition to Post-Quantum Cryptography.
- Begin deploying Post-Quantum Cryptographic algorithms as they are standardised.
- Take advantage of cross- industry and Government moment.





